ASEAN COUNTRY REPORTS

Prepared for the Economic Research Institute for ASEAN and East Asia (ERIA)

An analysis of the cybersecurity posture for 10 ASEAN countries

Prepared by the CyberGreen Institute

March 2020

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As more countries rely on digital economies, there needs to be an increased focus on the safety, reliability and trust of critical infrastructure. Over time, attacks have increased in size, sophistication, and impact. Perpetrators of these attacks have ranged from individuals to nation states. The dynamic and evolving nature of attacks continues to pose a risk of economic damage as a looming threat.

High-impact attacks include botnets for hire that can, for example, be used to conduct a large-scale amplification Distributed Denial of Service (DDoS) attack which makes use of unmanaged Internet services. Many financial institutions around the world have seen an increase in DDoS activities disrupt trading and other financial services. Not only should a country be concerned about being a recipient of such destructive DDoS attacks, they should also be concerned about whether their countries' computers are being utilized to help launch these destructive attacks.

Email and phishing scams are also growing in numbers and sophistication. Many fake emails use lookalike domains for an organization (e.g. er1a instead of eria), and can seem very realistic. These fake emails could then be used to gain access to critical documents from coworkers, or falsify a seemingly benign attachment which, in reality, is a link to a fraudulent site or malware that may lead to a ransomware attack.

There are also sophisticated attacks which are increasingly using a technique called "route hijacking" to instigate fraud and cause economic harm. One such widely publicized attack in April 2018 succeeded against Ethereum, where a route hijack against the Amazon Web Services DNS network resulted in a $17 million cryptocurrency heist.

Targets of large-scale Internet attacks face the risk of reputational and economic damage. Dubendorfer et al.[a] summarize five types of economic damage that organizations can encounter:

1. **Productivity Loss**: Employees cannot work as efficiently as usual;
2. **Revenue Loss**: Company is not able to fulfill customer requests;
3. **Disaster Recovery**: Human and material resources required to recover after an incident;
4. **Liability**: If a Service Level Agreement (SLA) is in place, a company may be liable to its customer for any deviation from that agreement;
5. **Customer Loss**: Degradation of service or deviation from SLAs may result in loss of existing customer base and reputational damage that affects future customer acquisition.

[a] Dübendorfer, Thomas & Wagner, Arno & Plattner, Bernhard. (2004). An Economic Damage Model for Large-Scale Internet Attacks. Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE. 10.1109/ENABL.2004.11.

To limit the exposure of such reputational or economic harm, the risks and potential attack vectors need to be understood so that proactive measures can be put in place.

Having a comprehensive understanding of what the current state of resiliency against attacks and proactive mitigation measures are makes it easier to determine where added national policies and capacity building measures may be needed. A data-driven, proactive approach to ascertain where increasing incentives for added resiliency measures may be useful, and creating reliable measurable metrics for continued risk assessment, is necessary.

This report is an initial step at showing the value of data measurements and analytics. A more comprehensive framework for measurable metrics and in-depth data analytics would be a useful next step to better compare the ASEAN countries' cyber resiliency and determine trends over time.

RISKS MEASURED IN THIS REPORT

The risk indicators chosen for analysis in this report represent the most comprehensive view of critical infrastructure risks. The open services measured for potential risks are widely used and are a major source of large-scale DDoS attacks. Email is heavily utilized for criminal activities that conduct phishing and spam campaigns. Routing infrastructure is also starting to become a target for more sophisticated attacks where Internet traffic is being rerouted to start attacks whereby criminal behavior can remain undetected for a longer period of time.

The policy recommendation section of this report emphasizes the importance of having a definitive workflow for the mitigation activities that should be undertaken. These mitigations often require participation from a variety of actors, including internet service providers (ISPs), network operators and vendor organizations. Incentives to promote a collective effort of adherence to security best practices is needed.

SUMMARY OF OBSERVED TRENDS

In this initial report, we see the following trends:

OPEN SERVICES

The open services consist of five fundamental Internet services that were chosen due to their susceptibility for abuse and due to each being an important service that is widely utilized. They often run open unmanaged services which are the starting point for many of the successful DDoS attacks.

The initial measurements show that in all ASEAN countries, there are significant numbers of such fundamental Internet services that are open, meaning they are accessible to the Internet

and could potentially be abused to initiate large DDoS attacks. Sometimes in multiples of terabits per second.

This initial data indicates that more in-depth study, measurements, and analytics are required to determine how susceptible the individual countries are to having these services utilized for large scale attacks. In some cases, these open services may be closely monitored and managed by the ISPs running them, whereby any abuse can be quickly identified and mitigated. However, the large number of open services measured does indicate that all ASEAN countries can benefit from training and education to limit exposure to nationwide attacks that can limit access to critical services through proactive mitigation and risk reduction.

EMAIL INFRASTRUCTURE

Email is a critical component of digital communications and it is imperative that this communication can be trusted and relied upon. Technical solutions exist which can minimize email fraud that comes from a fraudulent or impersonated organization. The measurements and data analysis in this report look to see how widespread these technical implementations are and whether the implementations enforce restrictive actions on any detected unauthorized messages.

Overall, the trend in the ASEAN countries is that while many organizations are starting to implement the email security mitigation techniques, there is little to no enforcement applied to any messages. This could use further study to determine whether the implementations are still in testing phases or whether there is a reluctance to enforce mitigation due to a fear of blocking legitimate messages by accident.

ROUTING INFRASTRUCTURE

The routing infrastructure measurements were specifically focused on Resource Public Key Infrastructure (RPKI) deployments which help determine how many authenticated routing origin announcements (“is this autonomous system authorized to originate this prefix?”) and for authenticated intermediary announcements (“is this autonomous system authorized to relay this announcement?”).

A synopsis of the RPKI measurements for all ASEAN countries is as follows:

Country	ASNs	ASNs with RPKI enabled	ASNs with invalid RPKI announcements
Brunei	15	1	0
Cambodia	123	27	14
Indonesia	209	9	4
Laos	29	8	4

Malaysia	272	42	6
Myanmar	93	32	3
Philippines	430	78	28
Singapore	537	72	23
Thailand	509	156	26
Vietnam	34	2	2

An autonomous system number (ASN) denotes networks that are under the same administrative control and all ASEAN countries have ISPs that are in varying phases of deploying cryptographically protected routing security via the RPKI set of services. Some more definitive data is needed to perform a comprehensive comparison between country RPKI deployments. However, the results so far indicate that all ASEAN countries would benefit from RPKI-related education and training since, with the exception of Brunei, all have ASNs that have some indication of invalid routing announcements. More comprehensive measurements and analysis are needed to determine whether these invalid routing announcements are due to configuration errors or due to the lack of acting upon routes that the ASN is not authorized to announce.

This report is meant to serve as a needs analysis. It is important to follow up with future reports to determine whether there are improvements or whether a country is more at risk for Internet ecosystem attacks. Comparing mitigation campaigns that varying ASEAN countries have executed and aligning them with future measurements can help determine which campaigns have been successful in increasing a country's security posture. Any future reports should endeavor to track progress utilizing evidence driven measurements, metrics, and analytics.

METHODOLOGY

OPEN SERVICE ANALYSIS

CyberGreen uses its data, statistics, and analysis to raise awareness about vulnerabilities - in the form of services that are often not managed - which could potentially be used as DDoS infrastructure for launching attacks. The ultimate goal is to provide national stakeholders with the information they need to mitigate the vulnerabilities in their own ecosystems which pose a risk not only to their own country but to others as well.

CyberGreen conducts five scans per week of IPv4 space, each of which focuses on the systematic probing of publicly accessible hosts on five different services:

- **Domain Name System (DNS)**: The Internet's equivalent of a phone book. One important function is that it maps human readable domain names to computer readable IP addresses;

- **Network Time Protocol (NTP)**: Used for clock synchronization between varying computer systems and is widely used to disseminate accurate time to computers and network devices;
- **Simple Network Management Protocol (SNMP)**: Used for exchanging management information between network devices and is widely used to monitor the health and welfare of these devices;
- **Simple Service Discovery Protocol (SSDP)**: Used to determine what services are available on the network;
- **Character Generator Protocol (CHARGEN)**: Used for testing and measurement purposes.

The scans that CyberGreen conducts cover any public-facing device which connects to the Internet, for example, but not limited to: clients, services, virtual instances, embedded systems, and the Internet of Things. CyberGreen does not scan unscannable space (e.g., RFC 1918 addresses, multicast or future use addresses) or IPv6 space, nor does CyberGreen attempt to go behind firewalls or Network Address Translations (NATs), or scan addresses which have opted out of scanning.

The five services that are scanned were chosen due to their susceptibility for abuse and due to each being an important service that is widely utilized, with the exception of CHARGEN. CHARGEN is an outdated service that should no longer be utilized, yet measuring its existence is another useful metric to determine where a country needs added capacity building measures for mitigating security risks through the use of outdated systems and services. All of the open services measured often run open, unmanaged services which are the starting point for many successful DDoS attacks. Obtaining measurement data on the number of open services gives valuable information to ascertain where varying threats are more realizable and where more effective mitigation techniques may need to be deployed

Each of these services often have unauthenticated means of being utilized and can be abused to initiate amplification attacks. Amplification attacks are a type of DDoS where an initial small query turns into a much larger payload, targeted at a specific victim.

DATA

Data is imperfect. Wherever possible, CyberGreen strives to meet or define the gold standard for data collection, and this is an ever-evolving process. Moreover, while CyberGreen's impetus for engaging in its own data collection was to have control over its data, we also rely on third party reference datasets to provide comprehensive statistics and analysis. To the best of our ability, we collect data and map it by country and ISP accordingly, but it should be noted that - for example - inconsistencies in the reference data may lead to imperfect results. Where possible, we have attempted to reconcile these inconsistencies.

We remain confident that the data and analysis, in conjunction with remaining transparent of our limitations, provide a clear sense of where each country and ISP stands and what can be done to make their Internet ecosystems a cleaner space.

METRICS

CyberGreen's weekly scans quantify the open services (DNS, NTP, SNMP, SSDP, and CHARGEN) on the Internet. CyberGreen's metrics report risk to others by factoring in the scale potential for amplification by service and node. CyberGreen's Index ranks countries by the size of the DDoS that could be mounted from the country, the Autonomous System (AS), or the alternate entity if all of their nodes currently available to attackers were used in a single attack. In short, the Index measures "offensive potential" — with the obvious caveat that we do not mean intentional offense but rather the degree to which the country, the AS, or the alternate entity can be made to engage in offense whether it wanted to or not.

An amplification factor is the ratio between the sizes of the responses and requests; the attacker wants to achieve the largest possible. CyberGreen uses the following amplification factors, which are published by US-CERT:

DNS	41
NTP	556.9
SNMP	6.3
SSDP	30.8
CHARGEN	358.8

The data throughout this report related to "**DDoS Potential**" and "**DDoS Rank**" have these amplification values factored in. "**Raw counts"** do not.

Note: Presently, this formula for offensive potential does not consider maximum upstream speeds of the observed unit. Metrics experts at CyberGreen are discussing the development of a new metric to address this.

For the purposes of this report, CyberGreen classified **risk exposure** of a country based on its rank on CyberGreen's index:

- **High** risk exposure: Country's rank falls between 1-81;
- **Moderate** risk exposure: Country's rank falls between 82-162;
- **Low** risk exposure: Country's rank falls between 163-244.

COUNTRY COMPARISON

For each of the 10 ASEAN countries in this report, two other countries were selected with similarly sized IPv4 address spaces.

ISP ANALYSIS

CyberGreen referenced its scan data for the week of October 21, 2019 against GeoIP reference data (by IPv4 blocks registered to each country) from MaxMind.

The top 20 contributing ISPs were then ranked according to raw counts of the respective open service in each country and a pie graph was also included to visualize the distribution among the top 20 ISPs. In some cases, there were less than 20 contributing ISPs. In those cases, all contributing ISPs were included in the tables and graphs. Furthermore, some ISPs with the same count may reflect different ranks. Ranks should be regarded with less importance than the raw count and overall contribution of each listed ISP.

To the best of our ability, multiple ASes owned by the same ISP and, in some cases, subsidiaries, were consolidated under one name with all counts summed.

A column was also included for **Allocated Country** which denotes the country to which an ISP/AS is allocated on its WHOIS record. This information may be helpful for policymakers to address foreign countries that operate networks within their borders. In certain cases, there may be more than one allocated country if multiple ASNs with different country allocations were listed for the same ISP.

For this report, CyberGreen classified ISPs into 4 main **Types**:

- **Telecom**: If an ISP offers telecommunication services/infrastructure;
- **Cloud**: If an ISP's main offerings are cloud-based (e.g. domain hosting). This category includes data centers/colocation;
- **University**: If an ISP is affiliated with a university;
- **Gov**: If an ISP is affiliated with a government entity.

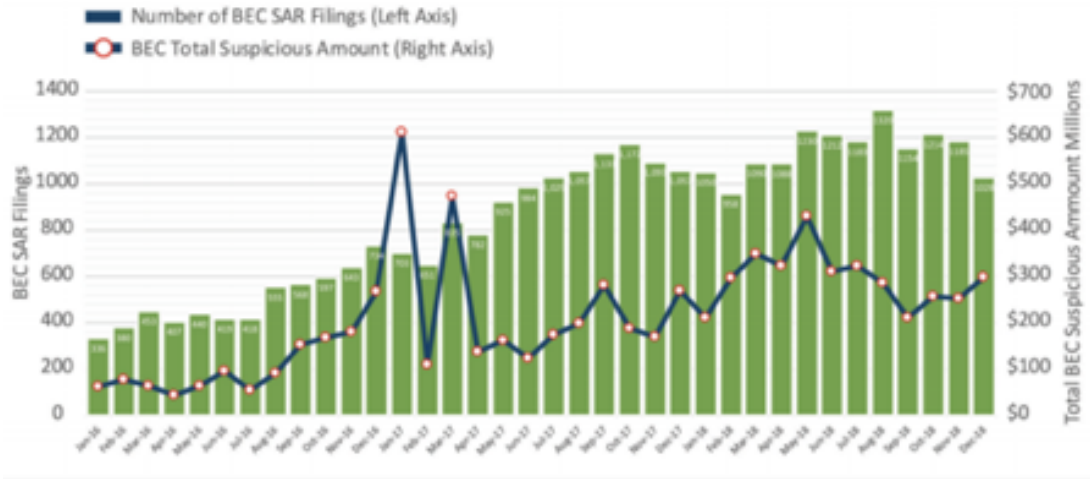
The process of classifying ISPs is a manual one and subject to the information that is publicly available to our researchers. There are instances where ISPs may be classified as "Unknown" due to insufficient publicly available information or where they may be classified uniquely if they do not fit into the 4 traditional, high-level categories listed above.

The ISP Analysis section for each country has a table which summarizes the top five ISPs that host the greatest number of open services in that country. The full results of the analysis described above can be found in the Appendices at the end of this report.

EMAIL INFRASTRUCTURE ANALYSIS

Phishing is a social engineering attack in which a fraudulent email message is sent and appears to be coming from a legitimate organization or user. The goal of this attack is to either steal personal identifiable information (i.e. usernames, passwords, bank or credit card information), to orchestrate fraud (false wire transfer requests) or to infect systems with malware, such as ransomware or a keylogger.

One difficulty for users when it comes to phishing is to determine whether or not the message came from a legitimate organization. Spammers are able to spoof the "From" address on mail messages, resulting in the recipient(s) trusting the mail message. This can lead to Business Email Compromise (BEC), where organizations can lose thousands or millions of dollars because of one fraudulent email that appears to have come from their bank or an executive within the organization.



Domain-based Message Authentication Reporting and Conformance (DMARC) is a solution which can reduce this and help to minimize email fraud using an organization's domain name.

DMARC is valuable to any entity that has an Internet presence, especially with email. DMARC prevents unauthorized usage of an organization's email domain, providing protection against domain spoofing using the "From" address on email messages. It acts as an identity check to ensure that the messages being delivered are passing the authentication and conformance defined in the policy. Ultimately, this protects not only the domain but also the integrity of the organization. It can also increase the deliverability of messages, given that over 80% of the consumer mailboxes worldwide support DMARC. DMARC also provides reports that will inform the organization as to what systems (authorized and unauthorized) are sending using the organization's email domain. It is important that DMARC be set up properly and with reporting enabled. The goal is for DMARC to be applied to all public facing domains regardless of whether the domain is being used for email or not.

DMARC utilizes two authentication mechanisms: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). SPF is a mechanism used to define which systems are

authorized to send messages using an organization's domain name. DKIM is used to add a digital signature for an additional layer to authenticate the sender. Both mechanisms are widely used, but they do have some flaws which DMARC can help make up for.

The Global Cyber Alliance (GCA) conducts automated monthly scans to analyze the implementation rates of DMARC and SPF across multiple domains around the world. GCA does not do automated scans for DKIM. This is due to the uniqueness of the DKIM DNS records (organizations can use any naming convention for the DKIM record). The scan looks for public DNS TXT records. For DMARC, the scanner looks for records with the naming convention of _dmarc.domain.com. For SPF, the scanner checks the value of the record starting with v=spf1.

The scan data is displayed visually on GCA's DMARC leaderboard, which currently consists of 6.5 million domains associated by country and in many cases by sector. The domains were provided by GCA's partners aligned with GCA's mission after having been obtained by those partners for their own business purposes. GCA uses this data as a base for its DMARC leaderboard, makes it available there, and thus has been subject to external review for some time. GCA is able to run scans and reports based on this data on a per-request basis.

GCA uses four classifications for DMARC implementation levels:

- **None**: the lowest level, where no enforcement is applied to messages and is meant for making adjustments to SPF and DKIM before moving to an enforcement level;
- **Quarantine**: the second level, where enforcement is applied, but unauthorized messages are delivered to the recipient's spam/junk folder;
- **Reject**: the highest level of enforcement, where unauthorized messages are dropped;
- **No Policy:** a DMARC policy is not applied.
- **Error**: DMARC implementation was attempted, but there may be a misconfiguration or syntax error.

GCA uses three classifications for SPF implementation levels:

- **Yes:** Some form of SPF has been implemented;
- **No:** SPF has not been implemented;
- **Error:** SPF implementation was attempted, but there may be a misconfiguration or syntax error. Commonly observed errors are too many domain lookups, incomplete policy, or misuse of the 'all' tag.
    - The **'all'** tag is used to define how failed messages are to be handled. The four options are:
        - -all – Hard Fail - only the domain's mail services (and those in the 'a' and 'include' sections) are allowed to send mail for the domain. All others are prohibited.
        - ~all – Soft Fail - if email is from a server not on the policy, the message is still accepted but marked as non compliant.
        - ?all - explicitly that nothing can be said about validity.

- +all - any host can send mail for the domain. This should never be used.

Implementation levels are measured and visualized per country and national sector. Below is a list of national sectors that GCA uses:

Animal Services	Event Services	International Affairs	Pharmaceuticals	Telecommunications
Animation	Executive Office	International Trade and Development	Philanthropy	Translation Services
Arts and Crafts	Facilities Services	IT Services	Photography	Transportation
Automotive	Farming	Legal	Print Services	Utilities
Aviation	Finance	Leisure Travel & Tourism	Production	Waste Management
Biotechnology	Food & Beverages	Local Business	Professional Services	Water Services
Business Management	Fund-Raising	Logistics & Supply Chain	Program Development	Wellness
Charity	Gambling	Machinery	Public Relations and Communications	Wholesale
Chemicals	Gaming	Management Consulting	Publishing	
Civic & Social Organization	Government	Manufacturing	Real Estate	
Communications	Graphic Design	Maritime	Recreational Facilities and Services	
Community Service	Healthcare	Marketing and Advertising	Religion	
Construction	Home Services	Media	Renewables & Environment	
Cosmetics	Hospitality	Medical Devices	Research & Development	
Defense & Space	Human Resources	Mining & Metals	Retail	
Design	Import and Export	Nonprofit Organization Management	Security & Investigations	
Education	Individual & Family Services	Oil & Energy	Semiconductors	
Employment	Industrial Automation	Outsourcing/Offshoring	Software	
Engineering	Information Services	Packaging	Sports	
Environmental Services	Insurance	Personal	Staffing & Recruiting	

ROUTING INFRASTRUCTURE ANALYSIS

Devices on the Internet must be able to determine the path to take from a sender of information to the recipient. A ‘routing protocol’ is utilized to determine this, and the Border Gateway Protocol (BGP) is the Internet routing protocol that enables finding the best path from a device

connected to one network to another device on a different network. On a more technical level, each network is identified via a unique autonomous system (AS) number. Each AS asserts reachability for the destination to which it provides connectivity. BGP is the mechanism by which varying autonomous systems announce which routing prefixes they originate and for which routing prefixes they are an intermediary path.

In its original form, BGP allows for either deliberate or accidental “route hijacks”: situations in which an autonomous system may claim to originate IP address prefixes that do not belong to it, or claim to carry routes which it cannot. These are serious issues, which – whether by malice or mistake – can cause legitimate traffic to be redirected to unauthorized intermediaries.

To enable network operators to make more informed routing decisions and to increase the security of BGP, the Internet Engineering Task Force (IETF) developed the RPKI family of standards to provide security for BGP. Using technologies built on these standards, autonomous systems can cryptographically sign BGP announcements that they make, and verify BGP announcements that they receive. RPKI can be used for authenticating routing origin announcements (“is this autonomous system authorized to originate this prefix?”) and for authenticating path information (“is this autonomous system authorized to relay this announcement?”).

The current implementation of RPKI relies on trust anchors maintained by the five Regional Internet Registries (RIRs), and by subordinate registries that register their trust anchors with their local RIR. This system of trust anchors is used to verify that an autonomous system is authorized to originate a prefix using Route Origin Authorizations (ROAs). This report provides an analysis of ROA deployments for autonomous systems registered in each country.

Autonomous system numbers (ASNs) - which identify autonomous systems registered in each country - are pulled from public data provided at the File Transfer Protocol (FTP) site of the RIR for the Asia-Pacific region, APNIC. Prefixes originated by each ASN are then collected and each prefix is checked to see whether it is covered by a ROA or not. If a prefix is covered by a ROA, the Validated ROA Payload (VRP) is checked for whether it is valid or invalid, and specific error conditions are logged for invalid VRPs. Checking of prefix coverage by ROAs and validation of VRPs is performed against trust anchors maintained by the RIRs, using open source RPKI validator tools.

POLICY RECOMMENDATIONS

Most effective security measures rely on proactive mitigation. The following defenses and policies do not just make the Internet safer for the owner implementing them, they make the Internet safer for everyone else as well. Like vaccines, the more people that adopt best practice security measures, the greater the protection for the community at large. There is no single solution – different organizations face different risks and have different tools they can use to try and assess and mitigate them.

This report focuses on providing the situational awareness needed for regulatory bodies to make the case for implementing the right defenses in the right places at the right time.

Capacity building is required to make sure organizations obtain, improve and retain the knowledge, skills, tools, equipment and resources needed to competently do their jobs. Adoption of best practices by network operators is a multi-step process:

1. **Provide measurement and data:** Reports like this one enable key stakeholders, like ERIA, to deliver evidence to governments, regulatory agencies, and network operators on the state of their Internet ecosystem.
2. **Assess and build capacity where needed:** Network operators may not have the resources or expertise to mitigate. Communicating with network operators to assess their capacity is critical and, where necessary, building their capacity to handle mitigation and adoption of best practices should be considered.
3. **Reward adoption of best practices:** Governments and regulatory agencies should incentivize network operators to reduce risk through rewards. If there is no incentive to mitigate risk, network operators may not go through the effort of mitigation.
4. **Enact regulations:** Where possible, governments and agencies should enact regulations that mandate cyber hygiene and/or adoption of best practices.
5. **Track progress using subsequent data and repeat steps #1-3:** This report acts as a baseline and a needs analysis. Subsequent data collection and reports can help track progress and show the success or failure of mitigation campaigns, who should be rewarded, and whether additional regulations are needed.

OPEN SERVICES

One of the most significant risks with open services is that they get utilized for amplification DDoS attacks. The most effective way to limit DDoS attacks is to reduce the exploitable resources which could be used as attack infrastructure. ISPs and service providers need to incorporate effective mitigation strategies since they typically are the owners and users of many of the open services. There are basic device and service hygiene principles and practices that are recommended:

- **Authentication and Authorized Access:** System Administrators should enforce good credential lifecycle management practices for access to all systems that provide the DNS, NTP, SNMP, SSDP and CHARGEN services. This includes making sure there are policies and processes in place for creating, distributing, storing, recovering, renewing, evoking and destroying credentials. Multi-factor authentication should be enabled on all systems, especially for administrator access.

- **BCP 38 Compliance**: DDoS attacks rely heavily on spoofing – generating traffic using forged source addresses to hide an attack or direct traffic at a target. Internet traffic is like the mail, and the source address is like the sender address on an envelope – a person can write anything they like in the box, and the only party that can verify the address is the first one to pick it up. BCP 38 (http://www.bcp38.info/) is an Internet standard for catching this spoofing at the source, limiting the ability of DDoSers to leverage reflection and botnets.

- **Asset Identification:** Many of the services used for DDoS attacks are purely internal services; that is, they have no reason to be used by anyone outside of the local network. By identifying these services and blocking them at the source, attackers are denied tools for reflection.

- **Cryptographic Protocol Protection:** A cryptographic protocol (also known as encryption protocol) performs security-related functions and applies cryptographic methods. The most common functions are data integrity and data confidentiality. Cryptographic data integrity is about protecting data against improper modification or alteration, and typically also includes authenticity. Cryptographic data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access. Many of the open services have updated cryptographically-protected communication capabilities to ensure the data integrity and confidentiality of the service and to mitigate the risk of these services being used for DDoS attacks.

- **Auditing/Monitoring:** Auditing and monitoring the network services for any incorrect and/or abnormal behavior is a critical component of any resilient infrastructure. There need to be policies and processes in place for reviewing logs for unauthorized access to systems. Moreover, the traffic to and from the services should be monitored for any abnormal behavior.

- **Patch Management:** The systems and protocol implementations for all services can have security-related fixes and upgrades. For any hardware and/or software deployments, it is recommended to create policies and procedures for keeping up with vulnerabilities and to ensure all system security patches have been reviewed and applied as necessary

DDoS is a serious issue which can disrupt critical Internet enabled services that citizens are dependent upon for their daily life and well-being. At the same time, the costs imposed by DDoS often fall on entities other than those managing the assets (open systems) that enable DDoS attacks. Active steps by government are useful to overcome this market failure. These steps can take various forms as preferred by the responsible government:

- Governments and regional groups can undertake dedicated efforts to encourage Internet infrastructure providers regarding best practices. For example, a government could undertake an inquiry with ISPs to ensure they understood the importance of BCP=38 compliance.

- A powerful way to reduce DDoS risks is to identify a set of best practices to implement. These best practices, such as those described above, can be incentivized by:
    - **Measurement**: Scanning to determine compliance with best practices and making the results available to influence public opinion and the market;
    - **Economic encouragement**: Compliance with best practices can be made a requirement for government procurement, use of services by critical infrastructure, etc. For example, government could require an ISP to implement BCP-38 before selling services to government.

- Regulation: where necessary, government can require entities to comply with best practices.

To preserve the public safety and trust in online services, education, incentives, and regulatory efforts are needed to encourage adoption of effective policies and operational best practices.

EMAIL INFRASTRUCTURE

Anti-spam and anti-phishing tools will protect against most fraudulent messages coming from external sources. DMARC is the mechanism that will prevent an organization's domain name from being used in this type of fraudulent activity. In order for DMARC to be successful, organizations must implement a DMARC policy (prevent domain from being used in fraudulent activity) and DMARC verification (check all incoming messages for DMARC policy).

DMARC should be adopted without reservation, even considering the cost to implement and possible costs in analysis of DMARC reports. The Return on Investment (ROI) is much higher than those costs. ROI of DMARC based on Business Email Compromise (BEC) as of August 2018 indicated that there is an annual savings of $19M - $66M USD based on the 1,046 domains that have deployed DMARC at a policy level of "reject" or "quarantine," after using GCA's Setup Guide. Implementation of DMARC, therefore, is strongly recommended, especially for domains set at the lowest policy level of "none".

In order to encourage broad adoption of DMARC, we recommend that the government lead the way and deploy DMARC across all public domains. This allows the government to claim the private sector should do the same, because the government has already proven it is possible and effective. A number of nations, including the United Kingdom, the United States, the Netherlands, Australia, and New Zealand already mandate public use of DMARC. For example, in the United States, Department of Homeland Security (DHS) Binding Operational Directive 18-01 requires the use of DMARC by most civilian government agencies, and a subsequent order extended this requirement to the U.S. Department of Defense.

The best course of action would be to start the implementation of a DMARC policy at level "reject" for all public domains that are not being used for email. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. Then, DMARC should be implemented at policy level "none" on the domains that are used for email. DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of "quarantine" and ultimately "reject" should be implemented.

We recommend that nations either develop the means to receive and understand DMARC reports – there is open source code for doing this – or partner with appropriate private sector entities to accept DMARC reports and provide analysis.

Having implemented DMARC for the government, we would recommend that ASEAN nations consider encouraging private sector entities to do the same. Means to doing so include:

- Identifying or creating tools to help the private sector deploy DMARC;
- Requiring or paying a supplemental amount for government suppliers/contractors to deploy DMARC;
- Purchasing cloud services for email that include DMARC by default, and making those same contractual arrangement more broadly available;
- Providing funds to implement DMARC or requiring its use, such as in regulated industries.

ROUTING INFRASTRUCTURE

A global initiative called the Mutually Agreed Norms for Routing Security (MANRS) outlines concrete actions that ISPs should take. These are best practices and technical solutions that can address and mitigate the most common threats associated with routing security.

In order for network operators to be considered a MANRS participant, the initiative provides a list of compulsory actions that define the steps which should be taken, at minimum:

1. **Filtering** - Preventing propagation of incorrect routing information: Network operators must implement a system whereby they only announce to adjacent networks the AS numbers and IP prefixes they or their customers are legitimately authorized to originate. Network operators must check whether the announcements of their customers are correct; specifically, that each customer legitimately holds the AS numbers and IP address space they announce.
2. **Coordination** - Facilitating global operational communication and coordination: Network operators must ensure that up-to-date contact information is entered and maintained in the appropriate RIR (or NIR) database and/or in PeeringDB. It is strongly recommended that contact information is made publicly available, but at a minimum must be available to other network operators registered with PeeringDB.
3. **Global Validation** - Facilitate routing information on a global scale – IRR**:** Network operators must publicly document their intended routing announcements in the appropriate RIR routing registry, RADB or an RADB-mirrored IRR. This includes ASNs and IP prefixes originating on their own networks, as well as the networks for which they provide transit services.
4. **Anti-Spoofing** - Preventing traffic with spoofed source IP addresses: Network operators must implement a system that enables source address validation to prevent packets with incorrect source IP addresses from entering and leaving the network.

To increase the security and stability of BGP infrastructure, it is recommended that ISPs become compliant with MANRS. This would require training and incentives to facilitate the deployment of capabilities to prevent traffic with spoofed source IP addresses and the capabilities to prevent the propagation of incorrect routing information.

For RPKI to be effective, ISPs first have to issue Route Origin Authorizations (ROAs) to authorize their AS to legitimately originate their IP prefixes. The information in the ROAs can then be used by BGP speakers to perform Route Origin Validation (ROV) on incoming BGP advertisements. The most critical piece is that invalid advertisements need to be acted upon, meaning the routes that are marked as invalid should either be dropped and not propagated further, or should be given a lower preference.

The results in this report show that there needs to be much more training and awareness-raising on the importance and proper deployment of RPKI.

Autonomous systems which do not currently advertise any ROAs should begin advertising ROAs. Getting them to the point of being able to do so will likely take an educational effort consisting of a series of workshops. In some countries, like Brunei, it is unknown how many ASNs implement RPKI validation, but outreach should be performed to come to a determination, and training should be done to bring all ASNs into a state of routing security best-practices conformance, including not only RPKI ROA advertisement and validation, but also implementation of BCP-38 and uRPF where appropriate. APNIC is the entity best situated to conduct RPKI ROA and validation training workshops.

Governments and agencies should make a concerted effort to communicate these best practices to network operators and to track which network operators are MANRS participants. Ideally, governments would enact regulations to mandate MANRS adoption.

GCA is undertaking a study to determine why MANRS has not been more widely adopted, focusing on barriers to adoption, and the results can be shared in the future and included in any upcoming work.

BRUNEI

COUNTRY OVERVIEW

Population: 428,962[b]

GDP: $13.57 billion[b]

Autonomous Systems: 15[c]

IPv4: ~130,560[d]

Percentage of Internet Users: 95%[e]

OPEN SERVICE ANALYSIS

Brunei's overall risk exposure can be classified as moderate - among the highest 66% of countries in the world - and, as depicted in Figure 1, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

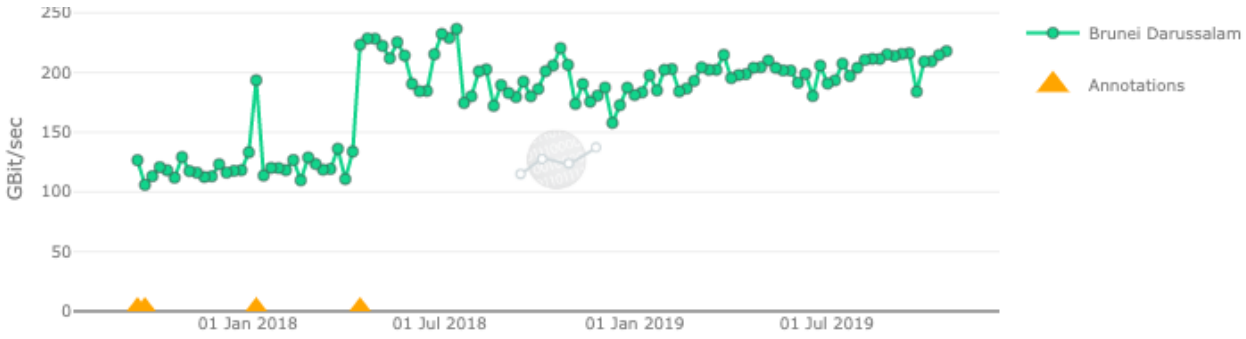


Figure 1: Two-year trend of potential DDoS infrastructure risk in Brunei

[b] *Country Profile - Brunei Darussalam*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=BRN.
[c] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[d] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[e] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

Brunei ranks #162 out of 244 on CyberGreen's index of riskiest DDoS environments (1 = riskiest, 244 = least risky). This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in Brunei and their respective amplification factors. As seen in Table 1, the most prevalent open service in Brunei's network is DNS (656).

Table 1: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
656	343	7	10	3	0.2	162

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for Brunei with priority sorted by highest to lowest amplified counts.

Table 2: Raw Count vs. Amplified Count

Priority	Service	Raw Count	Amplified Count
1	NTP	343	191,017
2	DNS	656	26,896
3	CHARGEN	3	1,076
4	SSDP	10	308
5	SNMP	7	44

Although the raw count for open DNS is highest, NTP has a much higher amplification factor which results in a higher amplified count. Ultimately, those open NTP services pose a higher risk if they were to be used in an attack. Bruneian authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: BRUNEI, U.S. VIRGIN ISLANDS, MYANMAR

With respect to its global standing, the state of Brunei's Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between Brunei, the U.S. Virgin Islands, and Myanmar.

Table 3: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Brunei	656	343	7	10	3	0.2	162
U.S.V.I.	75	774	197	215	0	0.4	147
Myanmar	588	1,884	937	0	0	1	117

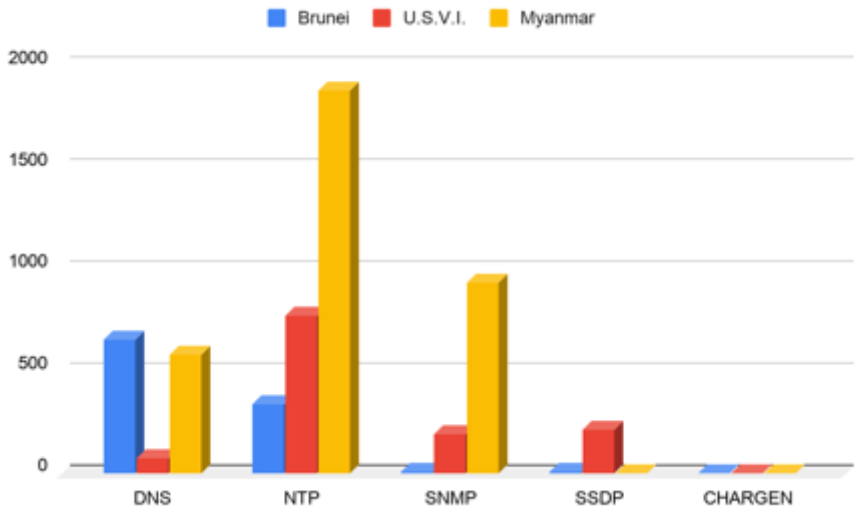


Figure 2: Comparison of raw count of open services

As the figure and table above show, Brunei ranks more favorably in its DDoS exposure relative to the U.S. Virgin Islands and Myanmar. This result is largely driven by the lower number of open NTP services that Brunei operates. NTP is a common networking service used for clock synchronization, and has a high amplification factor, making it an attractive reflector. Although Brunei has a higher open DNS count, the amplification potential is not nearly as high for that service as NTP. Brunei also has a low open SNMP count compared to the other two countries.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 4 shows the top five ISPs that host the greatest number of open services in Brunei. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs.

Table 4: Top five ISP contributors per service

ISP	DNS	NTP	SNMP	SSDP	CHARGEN
Bruhaas (B) Sdn Bhd		5			
EAGLE SKY CO LT	1				
EGNC (E-Government National Centre)	4	4			
Progresif Cellular Sdn Bhd	5	2			
Simpur ISP	3	3			
Telekom Brunei Berhad	2	1	1	1	1

Legend:

1	2	3	4	5

Biggest contributor — Least contributor

Telekom Brunei Berhad ranks high across all services. If Bruneian authorities collaborated with this ISP to launch a mitigation campaign, there could be substantial improvement of these numbers.

A detailed breakdown of ISP contribution for each of the five open services in Brunei is provided in Appendix A.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for the domains located in Brunei. It should be noted that the list of domains is not complete. The information provided is based on 99 domains (mainly government domains).

DMARC

Figure 3 shows DMARC policy implementation for the domains in Brunei.

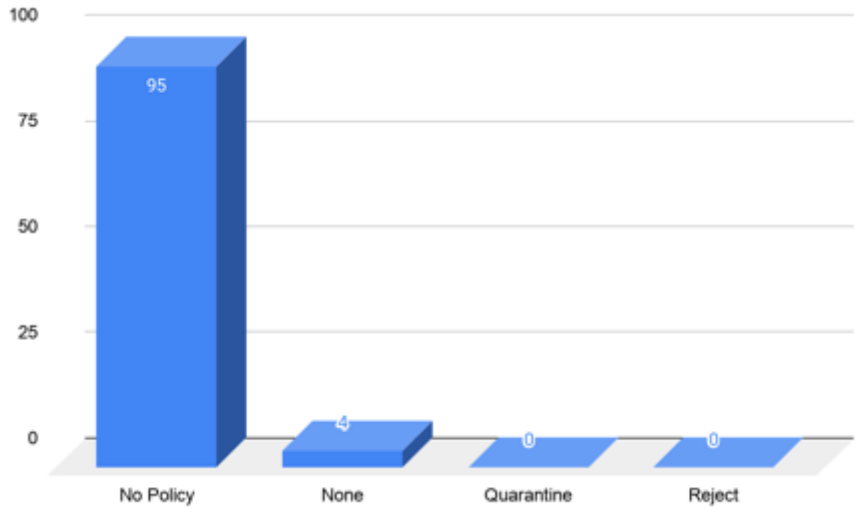


Figure 3: DMARC policy implementation in Brunei

Overall, only four out of 99 domains have DMARC implemented at the policy level of none. Of the four domains, two domains do not have reporting enabled, one of which is a government domain. The purpose of level “none” is simply to enable reporting and review the reports that are being generated; it does not do any filtering or actually enforce DMARC. It is the DMARC reports that provide the information necessary to determine when to change a policy to “quarantine” or “reject.” Only having a policy of “none” with no reporting enabled does not protect a domain or brand, and does not prevent the use of a domain in phishing campaigns. DMARC reporting must be enabled to determine if the authentication and authorization mechanisms for the domain are set up properly. If set up correctly, then the DMARC policy for the domain can be adjusted to a level that allows for enforcement and protection of the domain: "quarantine" and "reject". “Reject” is the policy level that DMARC must be set to when ready. By setting this level, fraudulent messages will not be delivered to the recipient. Whereas, if the policy level remains at "quarantine", legitimate messages could still end up in the recipient's

spam/junk folder, making it difficult for the recipient to determine which messages are legitimate and which are fraudulent.

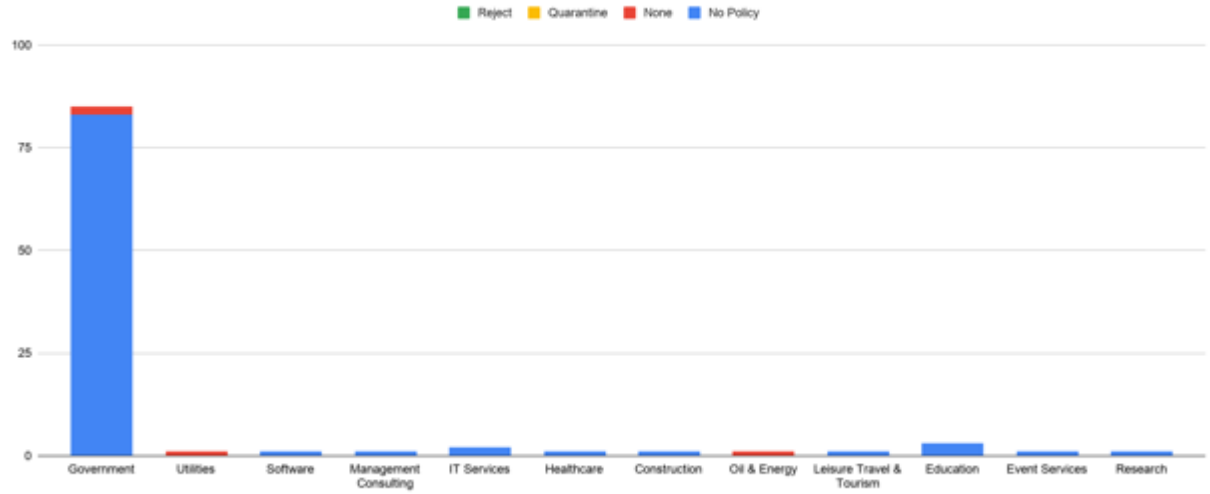


Figure 4: DMARC Implementation by sector

Figure 4 shows the breakdown of the sectors that have implemented DMARC based on the 99 observed domains. The adoption rate is very low based on the data available. The only sectors that are considering DMARC are two government agencies (one of which does not have DMARC reporting enabled and is set to policy of "none"), an organization in utilities, and in oil & energy.

SENDER POLICY FRAMEWORK (SPF)

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in Brunei are using SPF, which is good. However, the use of SPF alone does not provide full security since most receiving systems do not enable SPF Verification. While the sending organization's SPF defines which systems are authorized, the receiving side needs to determine how to handle any unauthorized messages. Most receiving systems do not want to make that decision which is why SPF should be implemented alongside DMARC and DKIM.

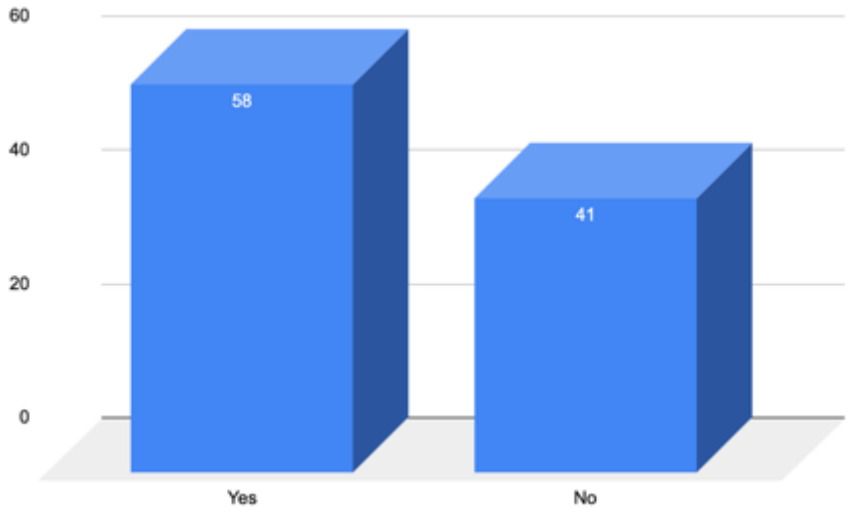


Figure 5: SPF Implementation in Brunei

DMARC AND SPF

Table 5 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 5: DMARC and SPF implementation in Brunei

Policy Level	DMARC	SPF
No Policy	95	54
None	4	4
Quarantine	0	0
Reject	0	0

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be able to be done for the 41 domains that do not have an SPF record. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (58 records that have an SPF record). DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

ROUTING INFRASTRUCTURE ANALYSIS

There are 15 observed ASNs headquartered in Brunei. Together, they advertise 184 IPv4 and 4 IPv6 prefixes.

One of Brunei's ASNs advertises ROAs, while the remaining 14 advertise none.

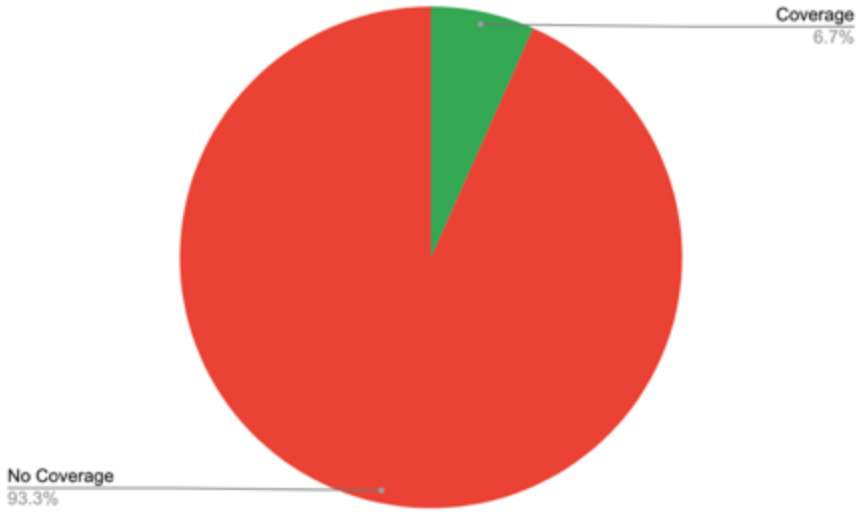


Figure 6: ROA Coverage in Brunei (by ASN)

Of the advertised prefixes, 3 IPv4 and 1 IPv6 prefix are covered by valid ROAs, together constituting 2.13% of Brunei's prefixes.

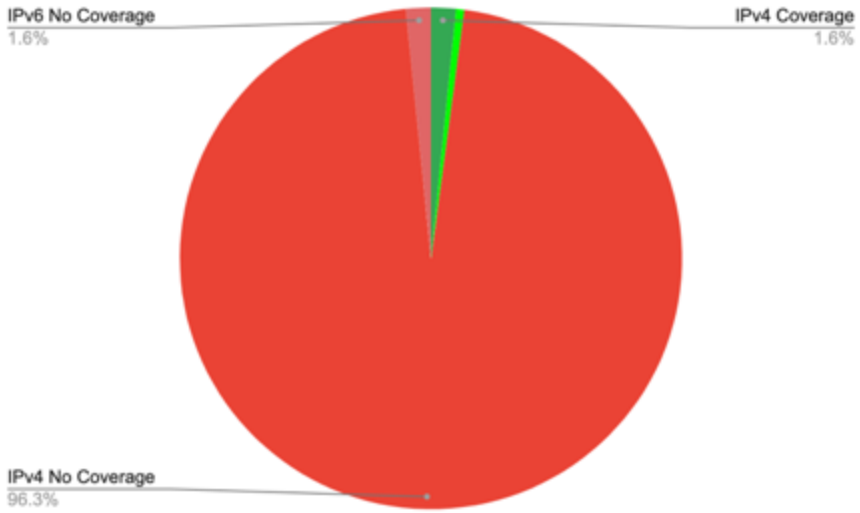


Figure 7: ROA Coverage in Brunei (by advertised prefix)

None of the advertised ROAs were invalid.

At this point, the adoption of RPKI is limited and it is unknown how many ASNs have implemented RPKI validation. There should be outreach to come to a determination as to why so few ASes use ROAs, and training should be done to bring all ASNs into a state of routing security best-practices conformance.

CAMBODIA

COUNTRY OVERVIEW

Population: 16,250,000[f]

GDP: $24.57 billion[f]

Autonomous Systems: 123[g]

IPv4: ~384,512[h]

Percentage of Internet Users: 40%[i]

OPEN SERVICE ANALYSIS

Cambodia's overall risk exposure can be classified as high - among the highest 30% of countries in the world - and, as depicted in Figure 8, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

Figure 8: Two-year trend of potential DDoS infrastructure risk in Cambodia

[f] *Country Profile - Cambodia*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=KHM.
[g] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[h] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[i] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

Cambodia ranks #72 out of 244 on CyberGreen's index of riskiest DDoS environments. This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in Cambodia and their respective amplification factors. As seen in Table 6, the most prevalent open service in Cambodia's network is NTP (8,871).

Table 6: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
2,748	8,871	1,436	32	12	5	72

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for Cambodia with priority sorted by highest to lowest amplified counts.

Table 7: Raw Count vs. Amplified Count

Priority	Service	Raw Count	Amplified Count
1	NTP	8,871	4,940,260
2	DNS	2,748	112,668
3	SNMP	1,436	9,047
4	CHARGEN	12	4,306
5	SSDP	32	986

The raw count of open NTP services in Cambodia is highest, and NTP has the highest amplification factor of the five services analyzed. Ultimately, those open NTP services pose the

highest risk if they were to be used in an attack. Cambodian authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: CAMBODIA, SENEGAL, LIBYA

With respect to its global standing, the state of Cambodia's Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between Cambodia, Senegal, and Libya.

Table 8: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Cambodia	2,748	8,871	1,436	32	12	5	72
Senegal	1,615	800	149	76	0	0.5	139
Libya	1,004	1,280	418	735	2	0.7	129

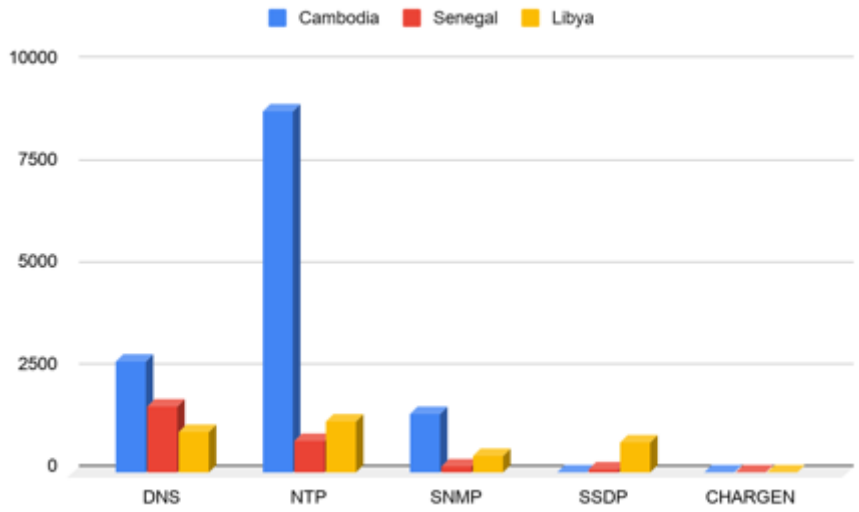


Figure 9: Comparison of raw count of open services

As the figure and table above show, Cambodia ranks less favorably in its DDoS exposure relative to Senegal and Libya. This result is largely driven by the significantly higher number of open NTP services that Cambodia operates as well as the higher number of DNS and SNMP services. NTP is a common networking service used for clock synchronization, and has a high amplification factor, making it an attractive reflector. Although Cambodia also has a higher open DNS, SNMP, and CHARGEN count, the amplification potential is not nearly as high for those services as NTP.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 9 shows the top five ISPs that host the greatest number of open services in Cambodia. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs.

Table 9: Top five ISP contributors per service

ISP	DNS	NTP	SNMP	SSDP	CHARGEN
ANGKOR DATA COMMUNICATION			3		
BGPNET Global ASN	2				
CAMBODIAN SINGMENG TELEMEDIA CO., LTD (Digi/SingMeng)		4			

CAMINTEL, National Telecommunication Provider, Phnom Penh, Cambodia					1
Cogetel Online, Cambodia, ISP	3	2	1	1	2
Metfone	4	1	5	2	
OpenNet ISP Cambodia	1	3		3	
SINET, Cambodia's specialist Internet and Telecom Service Provider.	5		4	4	
WiCAM Corporation Ltd.		5	2	5	

Legend:

Biggest contributor Least contributor

There are three ISPs that have notably high contribution counts across the five services analyzed: OpenNet, Cogetel, and Metfone. If Cambodian authorities collaborated with these ISPs to launch a mitigation campaign, there could be substantial improvement of Cambodia's risk exposure.

A detailed breakdown of ISP contribution for each of the five open services in Cambodia is provided in Appendix B.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for the domains located in Cambodia. It should be noted that the list of domains is not complete. The information provided is based on 217 domains.

DMARC

Figure 10 shows DMARC policy implementation for the domains in Cambodia.

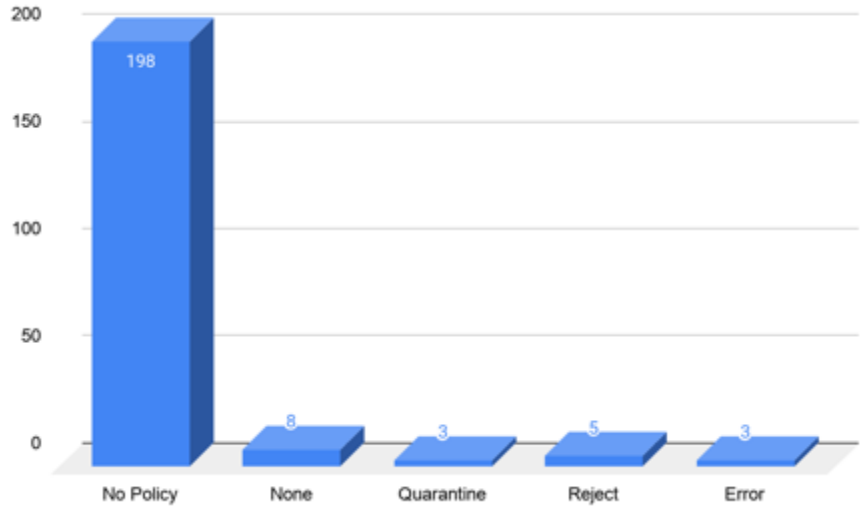


Figure 10: DMARC policy implementation in Cambodia

Overall, sixteen out of 217 domains have DMARC implemented at some level, with the majority being set to policy level of none (8). Of the eight domains, five domains do not have reporting enabled. However, this is not too much of a concern as these domains are set to a DMARC enforcement level (four are set to "reject" and one is set to "quarantine").

The remaining domains are set to either "quarantine" (3) or "reject" (5). It is still recommended that DMARC reporting be enabled even at DMARC enforcement levels. The reports that are generated can provide information if there were a case of a spam/phishing campaign using an organization's domain name. "Reject" is the policy level that DMARC must be set to when ready. By setting this level, fraudulent messages will not be delivered to the recipient. Whereas, if the policy level remains at "quarantine", legitimate messages could still end up in the recipient's spam/junk folder, making it difficult for the recipient to determine which messages are legitimate and which are fraudulent.

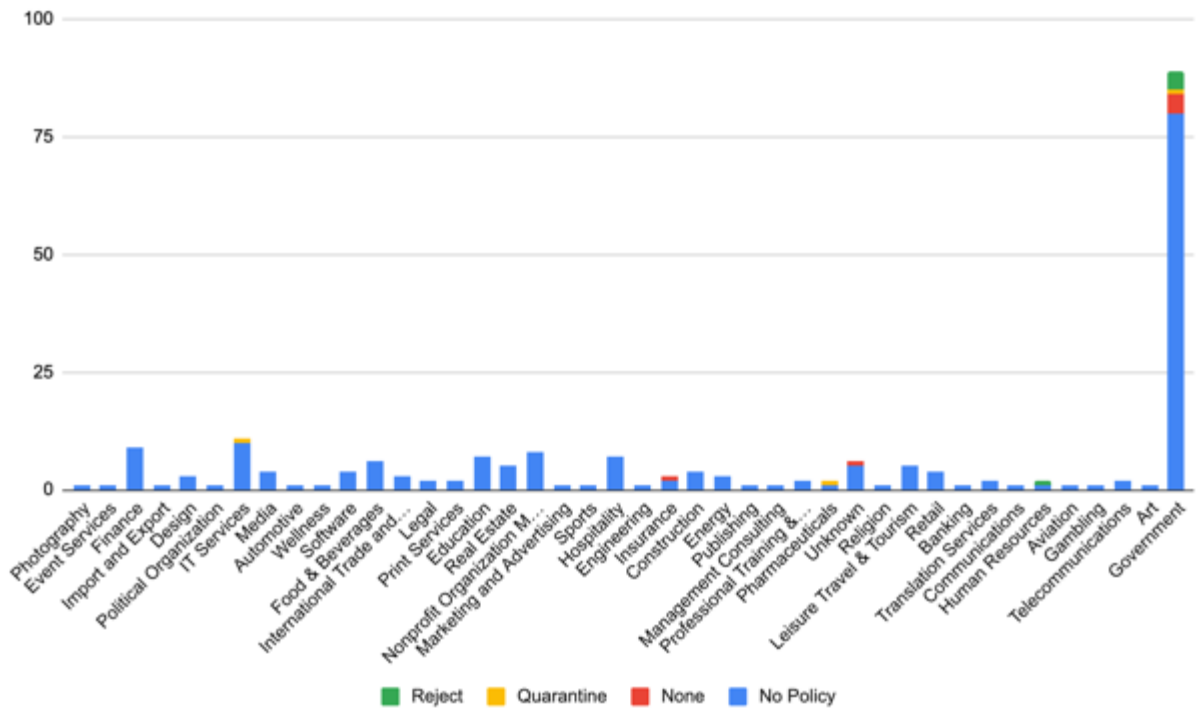


Figure 11: DMARC Implementation by sector

Figure 11 shows the breakdown of the sectors that have implemented DMARC based on the 217 observed domains. The adoption rate is very low based on the data available. The only sectors that are considering DMARC are Pharmaceuticals, IT Services and Human Resources.

The Cambodian government does appear to be focusing on DMARC. Based on 89 government domains, four are set to policy level “none”, one is set to policy level “quarantine” and four are set to policy level of “reject”.

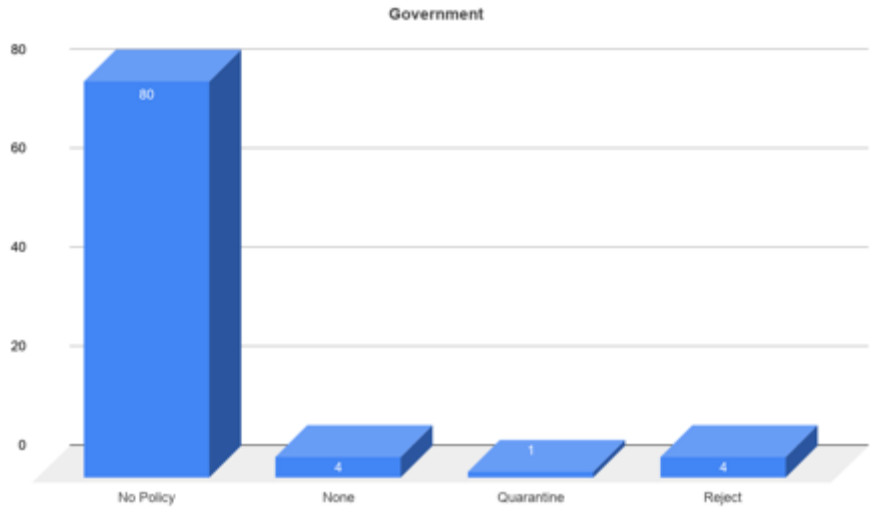


Figure 12: DMARC Implementation in Cambodia’s government sector

SENDER POLICY FRAMEWORK (SPF)

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in Cambodia are using SPF, which is good. However, SPF on its own is not fully secure. The main reason being that most receiving systems do not enable SPF Verification. While the sending organization's SPF defines which systems are authorized, the receiving side needs to determine how to handle any unauthorized messages. Most receiving systems do not want to make that decision. This is why SPF should be implemented alongside DMARC and DKIM.

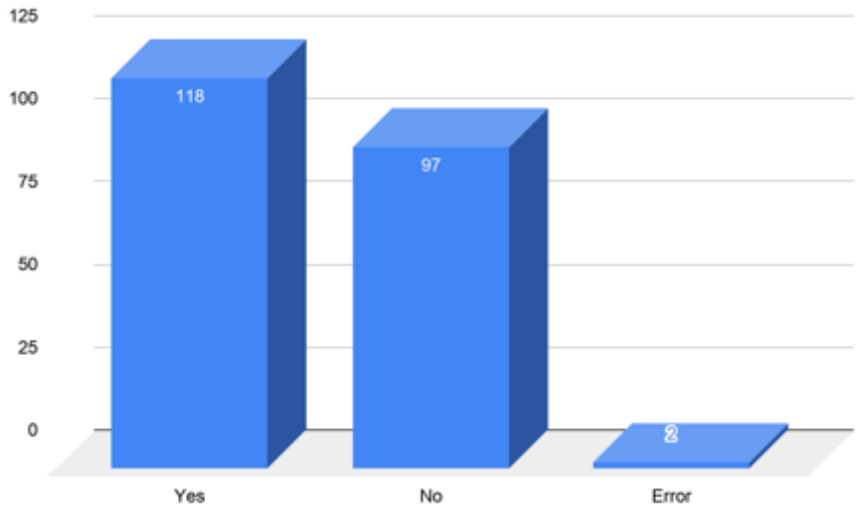


Figure 13: SPF Implementation in Cambodia

A few SPF records are set up incorrectly. There is more than one SPF record present or the SPF value has been merged with another type of record. A domain can only contain one SPF record. These organizations need to combine records into a single DNS record or remove the extra records.

Fourteen domains are using the value of "?all" in their SPF record, which is not recommended. The "?all" stands for neutral, meaning that messages do not pass or fail the SPF authentication check. The recommended value is either "-all" (hard fail) or "~all" (soft fail).

DMARC AND SPF

Table 10 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 10: DMARC and SPF implementation in Cambodia

Policy Level	DMARC	SPF
No Policy	198	100
None	8	7
Quarantine	3	3
Reject	5	5
Error	3	3

For the domains that have DMARC, it is not always expected to have an SPF record when starting with a DMARC policy of “none”. In this case, one domain with a DMARC policy of “none”, does not have an SPF record. This is allowed because the DMARC policy of “none” does not block any messages (fraudulent or legitimate). Most organizations will add the SPF record after reviewing the information presented in the DMARC reports. The DMARC reports can help to build and adjust SPF records.

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be able to be done for the 97 domains that do not have an SPF record. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (116 records that have an SPF record). DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

There are also two domains that have SPF setup incorrectly and should be fixed. The information is as follows:

Domain	SPF Value
angkorenterprise.gov.kh	"google-site-verification=A_p6seT13tc5qhWWb1btXNun-2HemATfu9QuqWS3Q1Q;v=spf1 a mx:angkorenterprise.gov.kh ip4:128.199.147.218 include:_spf.google.com ~all"
mpwt.gov.kh	"v=spf1 include:mailgun.org ~all" and "v=spf1 include:_spf.google.com ~all"

The domain angkorenterprise.gov.kh can be fixed by separating the values in DNS. The SPF record must be on its own and not combined with an existing record. Two TXT records would need to be created. One with the value of “google-site-verification=A_p6seT13tc5qhWWb1btXNun-2HemATfu9QuqWS3Q1Q” and the second with a value of “v=spf1 a mx:angkorenterprise.gov.kh ip4:128.199.147.218 include:_spf.google.com ~all". It is important to note that this domain does have a DMARC policy of “none”. By fixing the SPF record, this should help resolve some issues found in the DMARC reports.

For the domain mpwt.gov.kh, the SPF records must be combined because only one SPF record is allowed per domain. This domain will need to set the value of the SPF record to “v=spf1 include:mailgun.org include:_spf.google.com ~all”

ROUTING INFRASTRUCTURE ANALYSIS

There are 123 observed ASNs headquartered in Cambodia. Together, they advertise 1,779 IPv4 and 63 IPv6 prefixes.

27 of Cambodia’s ASNs advertise ROAs, while the remaining 96 ASNs advertise none.

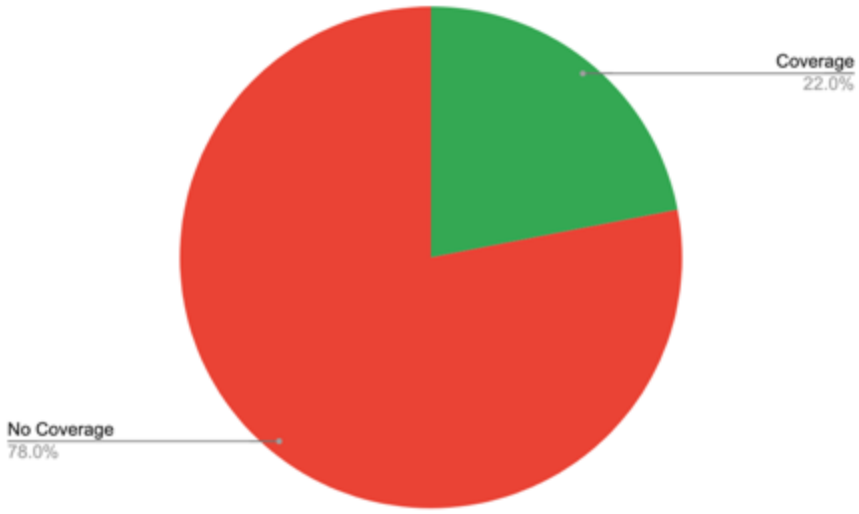


Figure 14: ROA Coverage in Cambodia (by ASN)

Of the advertised prefixes, 709 IPv4 and 31 IPv6 prefixes are covered by valid ROAs, together constituting 40.17% of Cambodia’s prefixes. A further 207 IPv4 prefixes are covered by invalid ROAs, constituting 11.24% of the total.

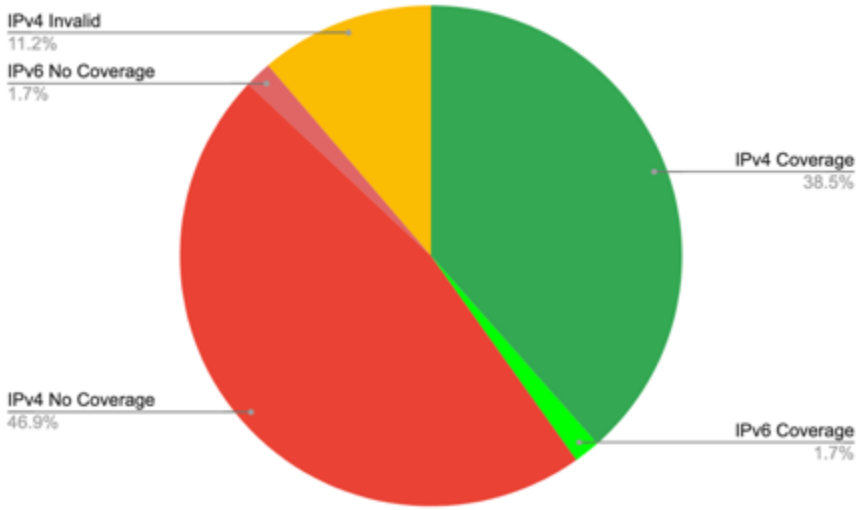


Figure 15: ROA Coverage in Cambodia (by advertised prefix)

The invalid ROAs are being advertised by 14 ASNs. Two different validation errors were observed:

1. The ASN is authorized to originate a prefix, but is announcing a sub-prefix of the authorized prefix instead of the authorized prefix. There were 49 IPv4 prefixes with errors of this kind. This is a relatively less serious error, as the ASN is authorized to originate the covering prefix.
2. The ASN is not authorized to originate a prefix. There were 158 IPv4 prefixes with errors of this kind. This is a serious error, as the ASN is announcing a prefix that it is not authorized for.

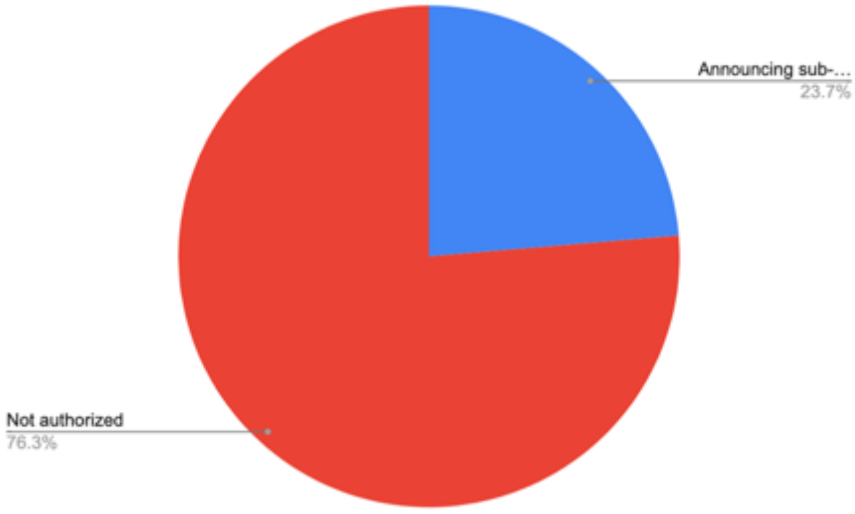


Figure 16: Invalid ROAs in Cambodia

The adoption of RPKI is progressing well in Cambodia, with close to half of the announced IPv4 and IPv6 prefixes announced utilizing ROAs. However, there are some very serious issues with invalid ROAs being advertised. There should be outreach to come to a determination as to why these invalid announcements have occurred and to determine whether these invalid routing announcements are due to configuration errors, or due to the lack of acting upon routes that the ASN is not authorized to announce. Also, outreach and training should be done to increase the adoption of RPKI across additional ASNs and to get them all into a state of routing security best-practices conformance

INDONESIA

COUNTRY OVERVIEW

Population: 267,660,000[j]

GDP: $1042.17 billion[j]

Autonomous Systems: 1614[k]

IPv4: ~21,451,728[l]

Percentage of Internet Users: 40%[m]

OPEN SERVICE ANALYSIS

Indonesia's overall risk exposure can be classified as high - among the highest 13% of countries in the world - and, as depicted in Figure 17, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

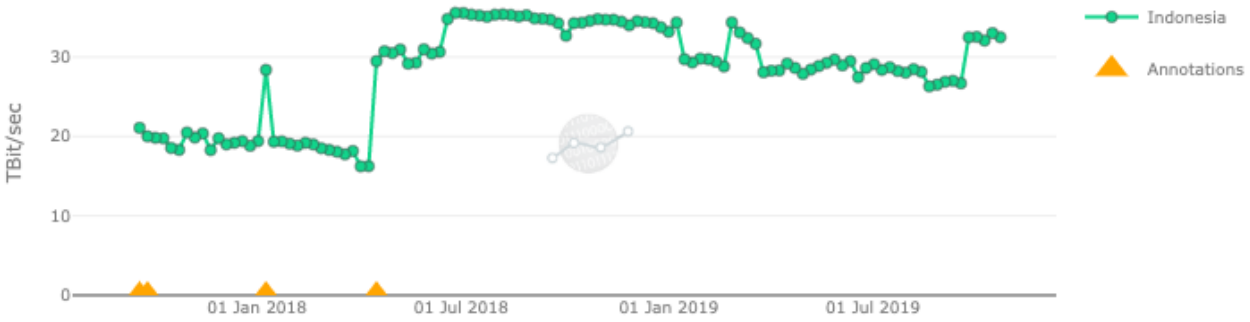


Figure 17: Two-year trend of potential DDoS infrastructure risk in Indonesia

[j] *Country Profile - Indonesia*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=IDN.
[k] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[l] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[m] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

Indonesia ranks #30 out of 244 on CyberGreen's index of riskiest DDoS environments. This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in Indonesia and their respective amplification factors. As seen in Table 11, the most prevalent open service in Indonesia's network is DNS (124,750).

Table 11: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
124,750	48,529	52,527	231	84	33	30

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for Indonesia with priority sorted by highest to lowest amplified counts.

Table 12: Raw Count vs. Amplified Count

Priority	Service	Raw Count	Amplified Count
1	NTP	48,529	27,025,800
2	DNS	124,750	5,114,750
3	SNMP	52,527	330,920
4	CHARGEN	84	30,139
5	SSDP	231	7,115

Although the raw counts for open DNS and open SNMP are higher, NTP has a much higher amplification factor which results in a higher amplified count. Ultimately, those open NTP

services pose a higher risk if they were to be used in an attack. Indonesian authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: INDONESIA, AUSTRIA, EGYPT

With respect to its global standing, the state of Indonesia's Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between Indonesia, Austria, and Egypt.

Table 13: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Indonesia	124,750	48,529	52,527	231	84	33	30
Austria	10,224	29,172	4,184	521	29	17	42
Egypt	151,465	6,244	4,015	81	41	10	53

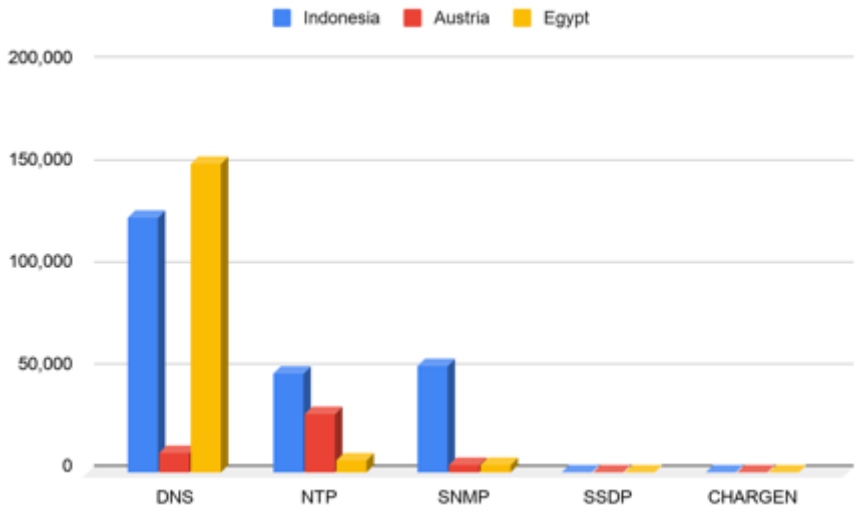


Figure 18: Comparison of raw count of open services

As the figure and table above show, Indonesia ranks less favorably in its DDoS exposure relative to Austria and Egypt. This result is largely driven by the significantly higher number of open NTP and SNMP services that Indonesia operates. NTP is a common networking service used for clock synchronization, and has a high amplification factor, making it an attractive reflector. Although Indonesia also has a higher open SNMP count, the amplification potential is not nearly as high for that service as NTP.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 14 shows the top five ISPs that host the greatest number of open services in Indonesia. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs.

Table 14: Top five ISP contributors per service

ISP	DNS	NTP	SNMP	SSDP	CHARGEN
Alibaba (US) Technology Co., Ltd.					3
Aplikanusa Lintasarta		1	3		
BIZNET NETWORKS	3	3			

INDOSAT	2				5
Jogja Medianet					2
Linknet		5		3	
Media Antar Nusa PT.			5	4	
PT Cyberindo Aditama				2	
PT iForte Global Internet	5		2		
PT INDONESIA COMNETS PLUS (ICON +)	4	4			
PT Telekomunikasi Indonesia	1	2	1	1	1
PT. HIPERNET INDODATA			4		
PT.Mora Telematika Indonesia					4
Universitas Negeri Semarang				5	

Legend:

There are several ISPs that have high contribution counts across the five services analyzed. Among them are: Telekomunikasi Indonesia, Biznet, Aplikanusa Lintasarta, and Indonesia Comnets Plus (ICON +). If Indonesian authorities collaborated with these ISPs to launch a mitigation campaign, there could be substantial improvement of Indonesia's risk exposure.

A detailed breakdown of ISP contribution for each of the five open services in Indonesia is provided in Appendix C.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for domains located in Indonesia. It should be noted that the list of domains is not complete. The information provided is based on 1,693 domains.

DMARC

Figure 19 shows DMARC policy implementation for the domains in Indonesia.

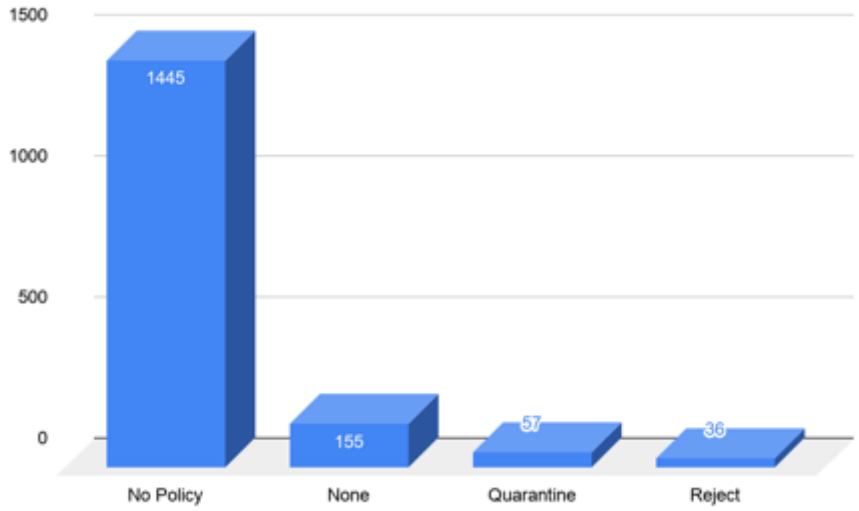


Figure 19: DMARC policy implementation in Indonesia

Overall, 248 out of 1,693 domains have DMARC implemented at some level, with the majority being set to policy level of none (155). Of the 248 domains, 71 domains do not have reporting enabled. What is of concern here is that 45 of these domains are set to the DMARC policy level of none, which does not provide any level of protection. The purpose of level “none” is simply to enable reporting and review the reports that are being generated; it does not do any filtering or actually enforce DMARC. DMARC reporting must be enabled to determine if the authentication and authorization mechanisms for the domain are set up properly. If set up correctly, then the DMARC policy for the domain can be adjusted to a level that allows for enforcement and protection of the domain: "quarantine" and "reject". Only having a policy of “none” with no reporting enabled does not protect a domain or brand, and does not prevent the use of a domain in phishing campaigns. Two of the 45 domains do have forensic reports enabled, but many service providers do not send these reports due to privacy issues. Forensic reports are actually the full message that is being delivered. It can contain the sender email, recipient email, email headers, full message body and in - some cases - may include any attachments. These reports are not enough to help with moving an enforcement level. The remaining domains are set to either "quarantine" (9) or "reject" (17).

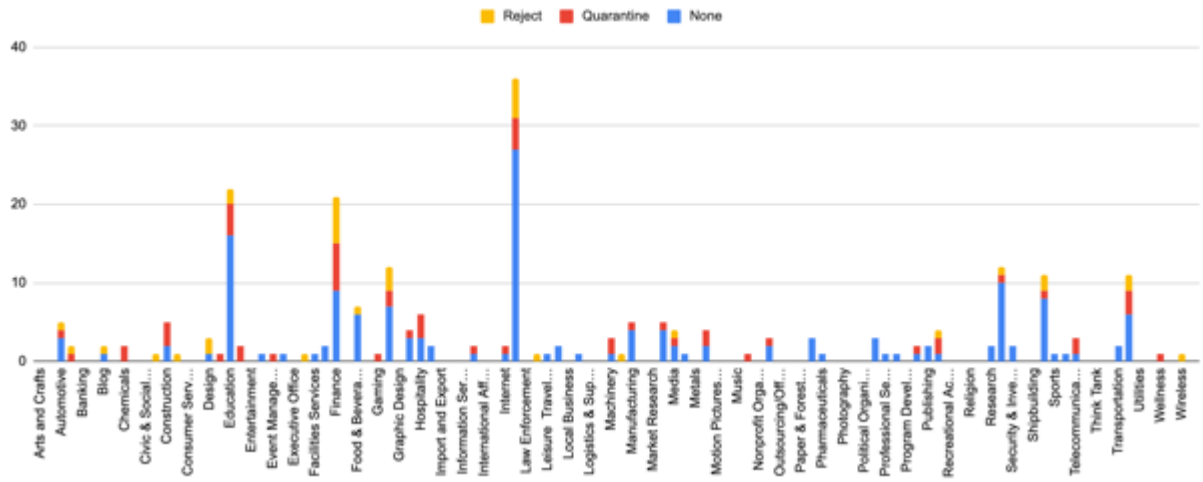


Figure 20: DMARC Implementation by sector

Figure 20 shows the breakdown of the sectors that have implemented DMARC based on the 1,693 observed domains. The domains that have no DMARC policy were excluded to allow for easier viewing. The adoption rate is good based on the data available. IT Services and Education are the two sectors showing the highest level of DMARC adoption.

SENDER POLICY FRAMEWORK (SPF)

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in Indonesia are using SPF. SPF on its own is not fully secure. The main reason being that most receiving systems do not enable SPF Verification. While the sending organization's SPF defines which systems are authorized, the receiving side needs to determine how to handle any unauthorized messages. Most receiving systems do not want to make that decision. This is why SPF should be implemented alongside DMARC and DKIM. There are a few domains that have implemented SPF incorrectly by leaving out a critical tag (all) which defines whether or not an email message is considered failed or not failed.

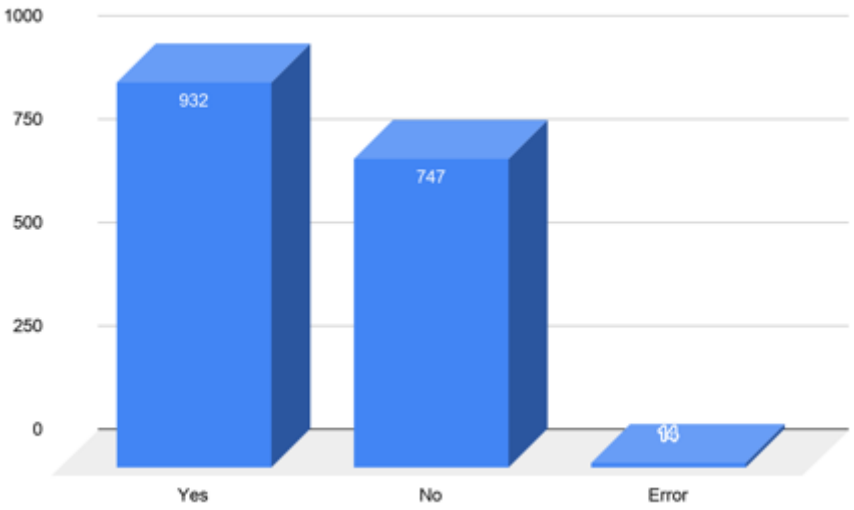


Figure 21: SPF Implementation in Indonesia

There are 26 domains that have implemented SPF as follows: “v=spf1 -all”, which indicates that there are no systems allowed to send messages using their domain. This is good, but would be better if DMARC was implemented alongside the policy level of “reject”. The reason being that more than 80% of consumer mailboxes (based on Valimail reports) are using DMARC verification. If a DMARC policy were to be implemented along with the current SPF record, then the domain would be better secured and decrease the chances of the delivery of fraudulent messages.

There are 14 domains that have implemented SPF incorrectly. Ten domains have left out a critical tag (all) which defines whether or not an email message is considered failed or not failed. One domain has too many domains listed in their SPF record. SPF has a 10 domain lookup limit which is meant to prevent DNS DoS types of activity. These eight domains have between 11 and 23 domains. To fix this, they will need to remove domains (some of which are non-existent), flatten the record (using IP address instead of domain names, which is not recommended especially if the domains belong to third parties), or use dynamic SPF (use regex option of SPF). Two domains have an “all” tag, just missing the -/~/?/+ before it. One of these must be present to complete the tag and allow for the record to function. Two domains have a period at the end of the record value, which must be removed.

There are also 66 domains that use the value of “?all” in their SPF record, which is not recommended. The "?all" stands for neutral, meaning that messages do not pass or fail the SPF authentication check. The recommended value is either "-all" (hard fail) or "~all" (soft fail).

DMARC AND SPF

Table 15 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 15: DMARC and SPF implementation in Indonesia

Policy Level	DMARC	SPF
No Policy	1445	703
None	155	140
Quarantine	57	55
Reject	36	34

It is not always expected to have an SPF record when starting with a DMARC policy of “none”. In this case, 15 domains with a DMARC policy of “none”, do not have SPF records. This is allowed because the DMARC policy of “none” does not block any messages (fraudulent or legitimate). Most organizations will add the SPF record after reviewing the information presented in the DMARC reports. The DMARC reports can help to build and adjust SPF records.

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be done for the 751 domains that do not have an SPF record. This should be done on the 26 domains that have implemented SPF as follows: “v=spf1 -all”. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (1145 records that have an SPF record). DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

A focus should be made on the 14 domains that have implemented SPF incorrectly.

The following ten domains have left out a critical tag (all) which defines whether or not an email message is considered failed or not failed. These can be fixed by adding either "-all" (hard fail) or "~all" (soft fail) at the end of the record value.

Domain	SPF Value
ski-hr.com	v=spf1 a=spf.qwords.net include=_spf.google.com include=spf.protect
empatix.com	v=spf1 include=isphuset.no
kimiafarma.co.id	v=spf1 mx a ip4=180.250.19.103/32 ip4=180.250.19.104/32

tilyanpristka.co.id	v=spf1 ip4=103.31.32.228 a=mail mx=mail.tilyanpristka.co.id
valagoo.com	v=spf1 all
saffanahjokka.com	v=spf1 mx a ip4=103.195.90.233/32 a=ns1.saffanahjokka.com include=ns2.saffanahjokka.com
nawaitunibaro.com	v=spf1 a=spf.qwords.net include=_spf.google.com include=spf.prote
muslimgaleri.co.id	v=spf1 a mx
voltras.co.id	v=spf1 mx a ip4=203.196.90.0/24
megawisata.co.id	v=spf1 a=spf.qwords.net include=_spf.google.com include=spf.protect

One domain (kirim.email) has too many domains listed in their SPF record. SPF has a 10 domain lookup limit which is meant to prevent DNS DoS type of activity. This domain has 25 domains that can be looked up. To fix this, either domains need to be removed (best option as some of the domains listed are non-existent), flatten the record (converting domains into IP addresses, which is not recommended especially if the domains belong to third parties), or use dynamic SPF (using regex capabilities in the SPF value). This domain is set to a DMARC policy of “quarantine” and if the SPF records are not fixed could cause issues with deliverability of legitimate email.

One domain has an “all” tag, just missing the -/~/?/+ before it. One of these must be present to complete the tag and allow for the record to function.

Domain	SPF Value
newspkn.com	v=spf1 ip4=103.10.170.0/23 include=outlook.com include=_spf.google.com all

Two domains have a period at the end of the record value, which must be removed. It is important that this gets fixed as both these domains are set to a DMARC policy of “reject”.

Domain	SPF Value
nihdia.com	v=spf1 ip4:101.50.1.27 ip4:101.50.1.20 +a +mx +ip4:101.50.1.70 +a:antispam.beon.co.id +a:antispam-us.beon.co.id -all.

tentucreative.com	v=spf1 +a +mx +ip4:103.27.206.196 +a:antispam.beon.co.id +a:antispam-us.beon.co.id -all.

There are a few domains that do not have SPF implemented but have a DMARC policy of “quarantine” or “reject”. This could cause issues as SPF is one of the items necessary for DMARC authentication. The domains nihidia.com, tentucreative.com and kirim.email have already been mentioned above. The domain with a policy of “quarantine” and no SPF is goindonesia.com. This domain must have an SPF record in place in order to prevent DMARC from blocking legitimate messages. If this domain is not used for email, then an SPF record with the value of “v=spf1 -all” should be used, adding an additional level of security for an organization that only checks for SPF.

ROUTING INFRASTRUCTURE ANALYSIS

There are 209 observed ASNs headquartered in Indonesia. Together, they advertise 8,812 IPv4 and 322 IPv6 prefixes.

Nine of Indonesia’s ASNs advertise ROAs, while the remaining 200 ASNs advertise none.

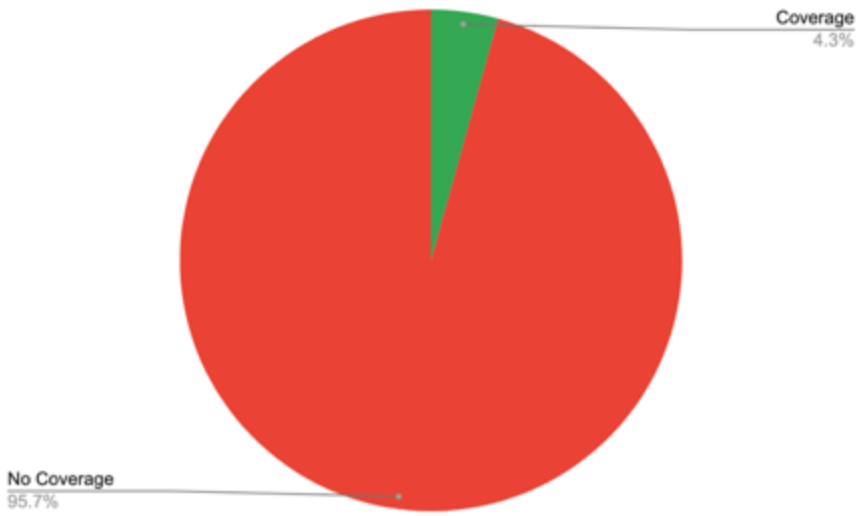


Figure 22: ROA Coverage in Indonesia (by ASN)

Of the advertised prefixes, 381 IPv4 and six IPv6 prefixes are covered by valid ROAs, together constituting 4.24% of Indonesia’s prefixes. A further 510 IPv4 and one IPv6 prefix are covered by invalid ROAs, together constituting 5.59% of the total.

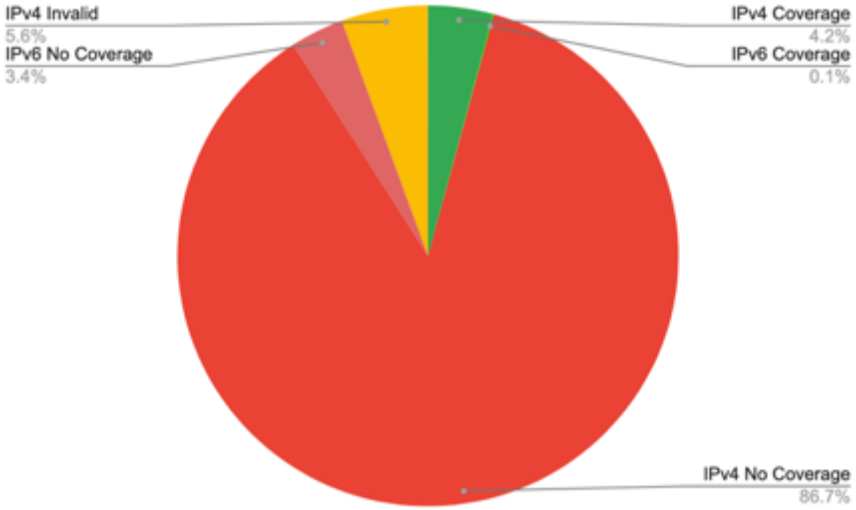


Figure 23: ROA Coverage in Indonesia (by advertised prefix)

The invalid ROAs are being advertised by four ASNs. Two different validation errors were observed:

1. The ASN is authorized to originate a prefix, but is announcing a sub-prefix of the authorized prefix instead of the authorized prefix. There were 500 IPv4 prefixes with errors of this kind. This is a relatively less serious error, as the ASN is authorized to originate the covering prefix.
2. The ASN is not authorized to originate a prefix. There were 10 IPv4 prefixes and one IPv6 prefix with errors of this kind. This is a serious error, as the ASN is announcing a prefix that it is not authorized for.

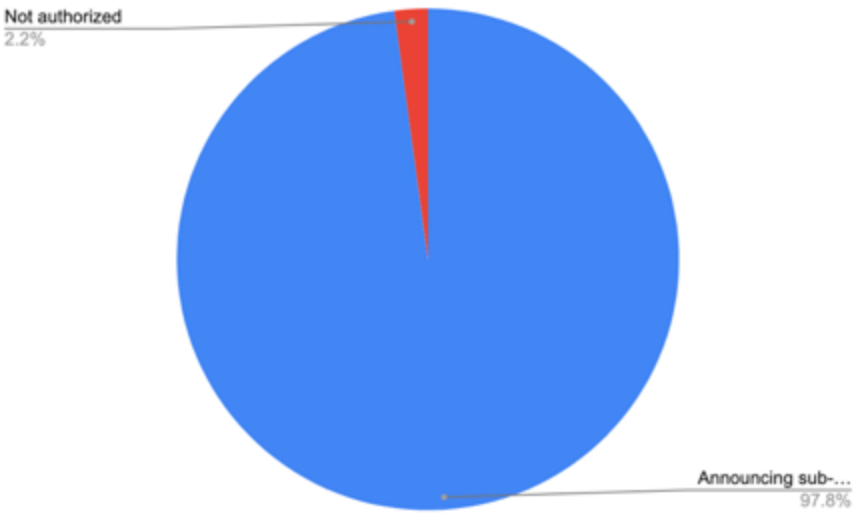
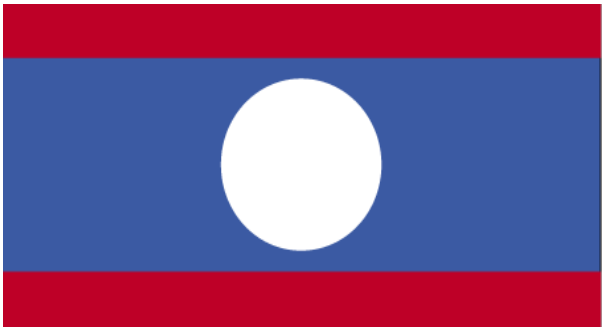


Figure 24: Invalid ROAs in Indonesia

The adoption of RPKI in Indonesia is very low with only a few ASNs announcing routing prefixes with ROAs. Close to half of the ASNs that have deployed RPKI have issues with invalid ROAs although most are not classified as serious. There should be outreach to come to a determination as to why these invalid announcements have occurred and to determine whether these invalid routing announcements are due to configuration errors or due to the lack of acting upon routes that the ASN is not authorized to announce. Also, outreach and training should be done to increase the adoption of RPKI across additional ASNs and to get them all into a state of routing security best-practices conformance.

LAOS

COUNTRY OVERVIEW



Population: 7,060,000[n]

GDP: $18.13 billion[n]

Autonomous Systems: 29[o]

IPv4: ~69,632[p]

Percentage of Internet Users: 26%[q]

OPEN SERVICE ANALYSIS

Laos' overall risk exposure can be classified as moderate - among the highest 57% of countries in the world - and, as depicted in Figure 25, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

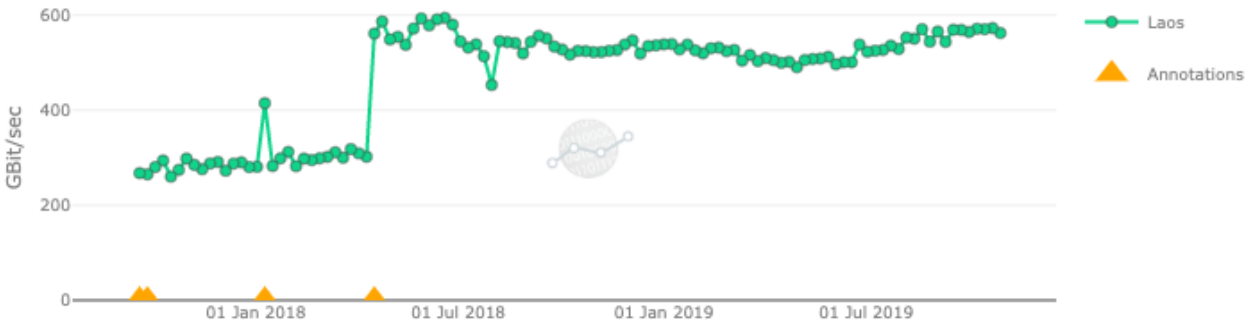


Figure 25: Two-year trend of potential DDoS infrastructure risk in Laos

[n] *Country Profile – Lao PDR*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=LAO.
[o] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[p] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[q] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

Laos ranks #136 out of 244 on CyberGreen's index of riskiest DDoS environments. This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in Laos and their respective amplification factors. As seen Table 16, the most prevalent open service in Laos' network is NTP (1,031).

Table 16: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
537	1,031	184	0	0	0.6	136

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for Laos with priority sorted by highest to lowest amplified counts.

Table 17: Raw Count vs. Amplified Count

Priority	Service	Raw Count	Amplified Count
1	NTP	1,031	574,164
2	DNS	537	22,017
3	SNMP	184	1,159

The raw count of open NTP services in Laos is highest, and NTP has the highest amplification factor of the five services analyzed. Ultimately, those open NTP services pose the highest risk if they were to be used in an attack. Laotian authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: LAOS, GUYANA, ARUBA

With respect to its global standing, the state of Laos' Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between Laos, Guyana, and Aruba.

Table 18: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Laos	537	1,031	184	0	0	0.6	136
Guyana	242	80	214	351	0	0.07	203
Aruba	29	122	64	22	0	0.07	200

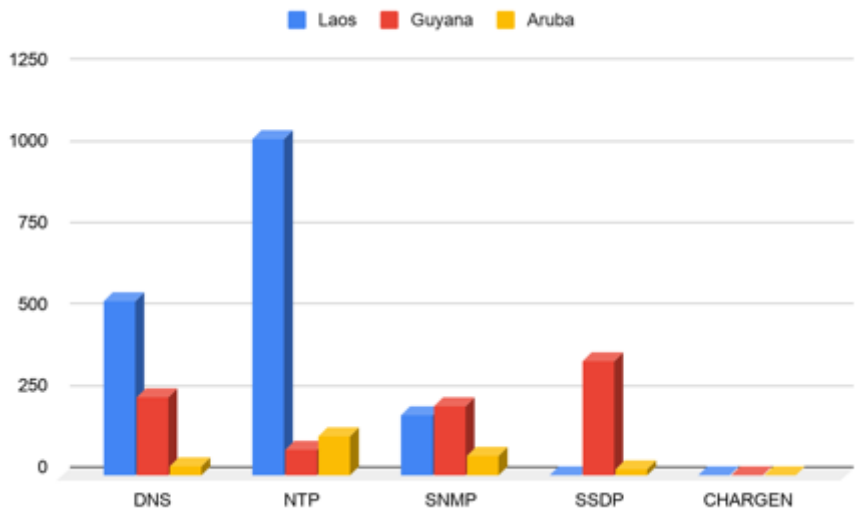


Figure 26: Comparison of raw count of open services

As the figure and table above show, Laos ranks less favorably in its DDoS exposure relative to Guyana and Aruba. This result is largely driven by the significantly higher number of open NTP services that Laos operates. NTP is a common networking service used for clock

synchronization, and has a high amplification factor, making it an attractive reflector. Although Laos also has a higher open DNS count, the amplification potential is not nearly as high for DNS as NTP.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 19 shows the top five ISPs that host the greatest number of open services in Laos. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs.

Table 19: Top five ISP contributors per service

ISP	DNS	NTP	SNMP
Enterprise of Telecommunications Lao		1	5
Lao Telecom Communication, LTC	2	2	1
Planet Online Laos, Internet Service Provider in LAO PDR		4	
Siamdata	1		
SkytelecomTransit provider and ISP in Vientiene.	5		2
Unitel (Star Telecom)	3	3	3
Vimpelcom Lao Co Ltd (VEON)	4	5	4

Legend:

There are several ISPs that have high contribution counts across multiple services that were analyzed. Among them are: Lao Telecom Communication, Unitel (Star Telecom), and Vimpelcom. If Laotian authorities collaborated with these ISPs to launch a mitigation campaign, there could be substantial improvement of Laos' risk exposure.

A detailed breakdown of ISP contribution for each of the five open services in Laos is provided in Appendix D.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for the domains located in Laos. It should be noted that the list of domains is not complete. The information provided is based on 66 domains.

DMARC

Figure 27 shows DMARC policy implementation for the domains in Laos.

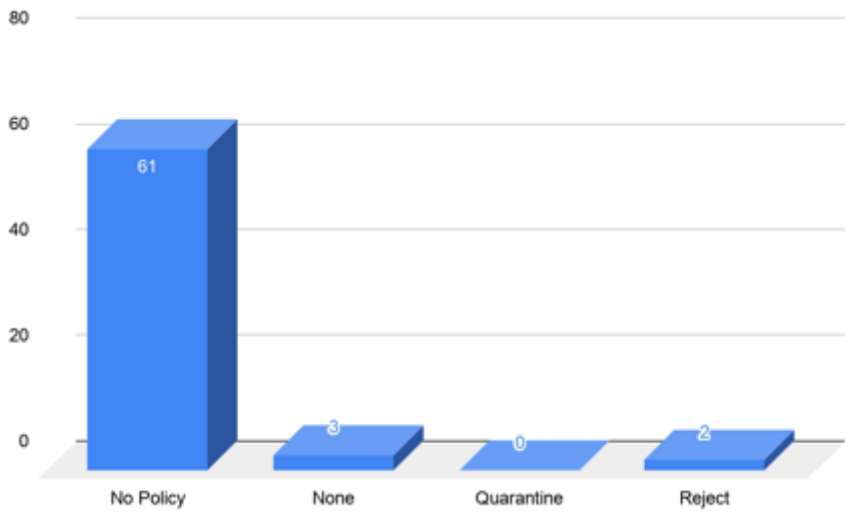


Figure 27: DMARC policy implementation in Laos

Overall, five out of 66 domains have DMARC implemented at some level, with the majority being set to policy level of “none” (3). Of the five domains, two domains do not have reporting enabled. One of these domains is set to the DMARC policy level of “none”, which does not provide any level of protection. The purpose of level “none” is simply to enable reporting and review the reports that are being generated; it does not do any filtering or actually enforce DMARC. It is the DMARC reports that provide the information necessary to determine when to change a policy to “quarantine” or “reject.” Only having a policy of “none” with no reporting enabled does not protect a domain or brand, and does not prevent the use of a domain in phishing campaigns. DMARC reporting must be enabled to determine if the authentication and authorization mechanisms for the domain are set up properly. The remaining domains are set to "reject" (2). It is still recommended that DMARC reporting be enabled even at DMARC enforcement levels since these reports can provide information if there were a case of a spam/phishing campaign using an organization’s domain name.

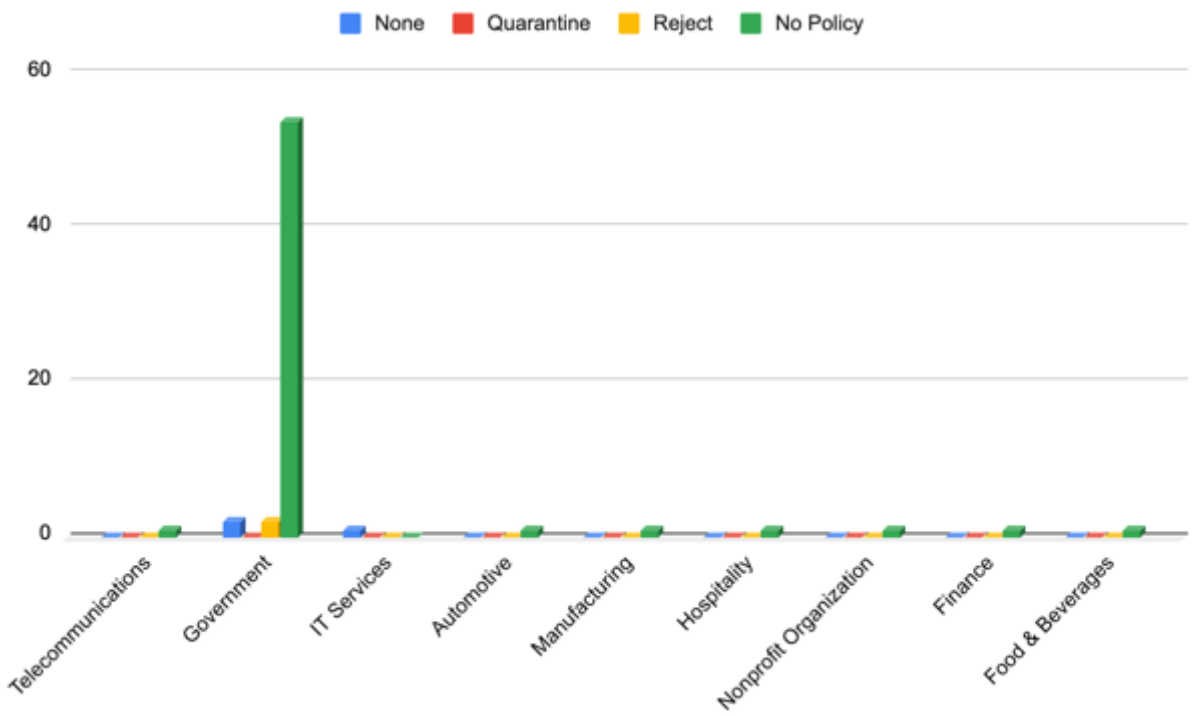


Figure 28: DMARC Implementation by sector

Figure 28 shows the breakdown of the sectors that have implemented DMARC based on the 66 observed domains. The adoption rate is very low based on the data available. The only sectors that are considering DMARC are Government and IT Services.

SENDER POLICY FRAMEWORK (SPF)

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in Laos are not using SPF. The use of SPF alone does not provide full security since most receiving systems do not enable SPF Verification. While the sending organization's SPF defines which systems are authorized, the receiving side needs to determine how to handle any unauthorized messages. Most receiving systems do not want to make that decision. This is why SPF should be implemented alongside DMARC and DKIM.

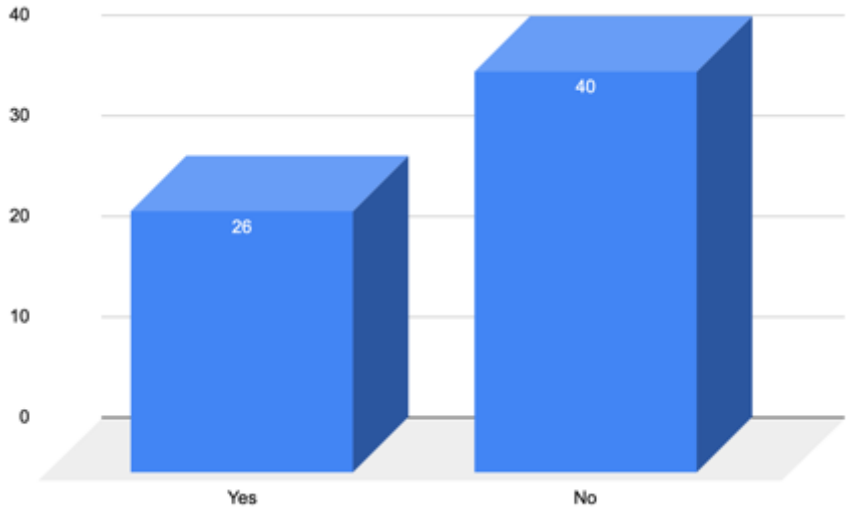


Figure 29: SPF Implementation in Laos

DMARC AND SPF

Table 20 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 20: DMARC and SPF implementation in Laos

Policy Level	DMARC	SPF
No Policy	61	21
None	3	3
Quarantine	0	0
Reject	2	2

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be able to be done for the 40 domains that do not have an SPF record. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (61 records that do not have DMARC). DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

ROUTING INFRASTRUCTURE ANALYSIS

There are 29 observed ASNs headquartered in Laos. Together, they advertise 274 IPv4 and 52 IPv6 prefixes.

Eight of Laos' ASNs advertise ROAs, while the remaining 21 ASNs advertise none.

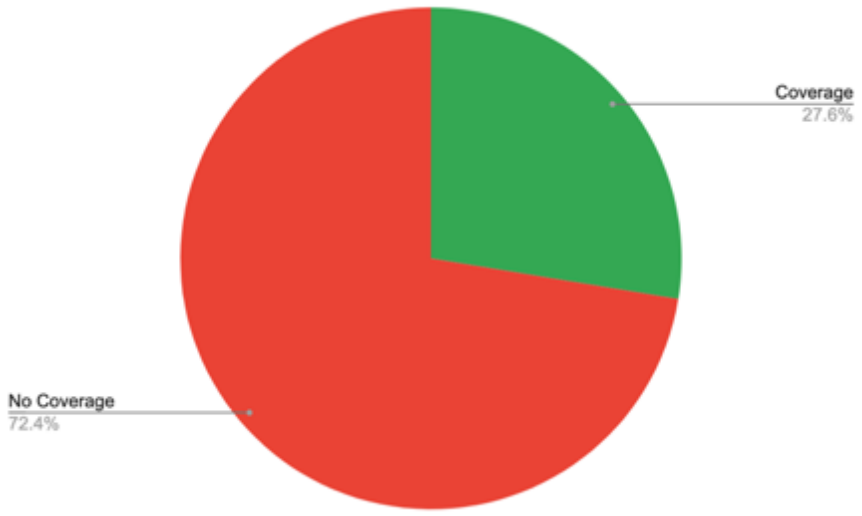


Figure 30: ROA Coverage in Laos (by ASN)

Of the advertised prefixes, 88 IPv4 and 18 IPv6 prefixes are covered by valid ROAs, together constituting 32.52% of Laos' prefixes. A further 108 IPv4 prefixes and 32 IPv6 prefixes are covered by invalid ROAs, together constituting 42.94% of the total.

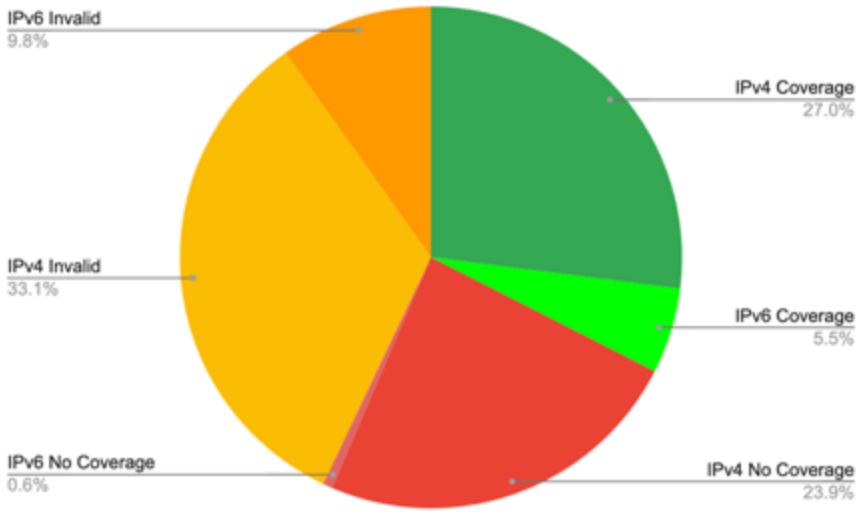


Figure 31: ROA Coverage in Laos (by advertised prefix)

The invalid ROAs are being advertised by four ASNs. Two different validation errors were observed:

1. The ASN is authorized to originate a prefix, but is announcing a sub-prefix of the authorized prefix instead of the authorized prefix. There were 106 IPv4 prefixes and 32 IPv6 prefixes with errors of this kind. This is a relatively less serious error, as the ASN is authorized to originate the covering prefix.
2. The ASN is not authorized to originate a prefix. There were two IPv4 prefixes with errors of this kind. This is a serious error, as the ASN is announcing a prefix that it is not authorized for.

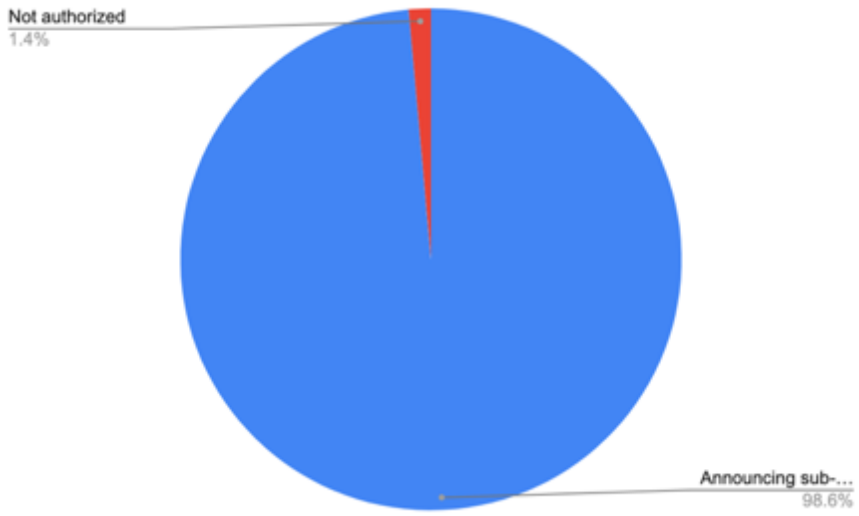
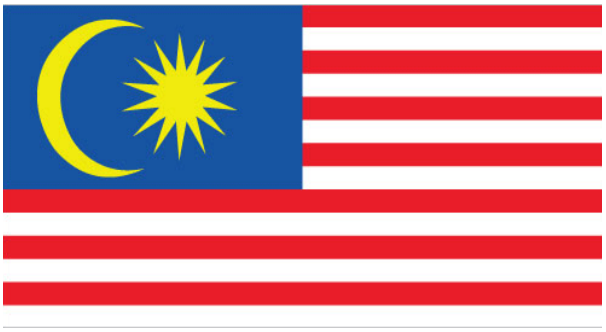


Figure 32: Invalid ROAs in Laos

The adoption of RPKI is progressing well in Laos, with many of the larger ISPs announcing prefixes with ROAs. However, over half of the ROAs announced are invalid and more data is needed to understand why this is occurring. Only a very small percentage of these invalid ROAs are categorized as serious issues. There should be outreach to come to a determination as to why these invalid announcements have occurred and to determine whether these invalid routing announcements are due to configuration errors, or due to the lack of acting upon routes that the ASN is not authorized to announce. Also, outreach and training should be done to increase the adoption of RPKI across additional ASNs and to get them all into a state of routing security best-practices conformance.

MALAYSIA

COUNTRY OVERVIEW



Population: 31,530,000[r]

GDP: $354.35 billion[r]

Autonomous Systems: 272[s]

IPv4: ~6,334,711[t]

Percentage of Internet Users: 81%[u]

OPEN SERVICE ANALYSIS

Malaysia's overall risk exposure can be classified as high - among the highest 19% of countries in the world - and, as depicted in Figure 33, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

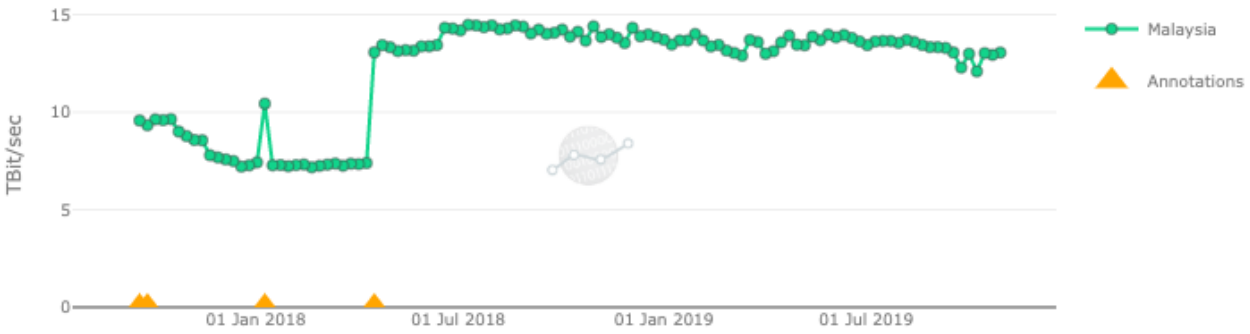


Figure 33: Two-year trend of potential DDoS infrastructure risk in Malaysia

[r] *Country Profile - Malaysia*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=MYS.
[s] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[t] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[u] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

Malaysia ranks #46 out of 244 on CyberGreen's index of riskiest DDoS environments. This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in Malaysia and their respective amplification factors. As seen in Table 21, the most prevalent open service in Malaysia's network is DNS (28,142).

Table 21: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
28,142	20,454	9,838	9,300	138	13	46

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for Malaysia with priority sorted by highest to lowest amplified counts.

Table 22: Raw Count vs. Amplified Count

Priority	Service	Raw Count	Amplified Count
1	NTP	20,454	11,390,833
2	DNS	28,142	1,153,822
3	SSDP	9,300	286,440
4	SNMP	9,838	61,979
5	CHARGEN	138	49,514

Although the raw count for open DNS is higher, NTP has a much higher amplification factor which results in a higher amplified count. Ultimately, those open NTP services pose a higher

risk if they were to be used in an attack. Malaysian authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: MALAYSIA, NEW ZEALAND, PORTUGAL

With respect to its global standing, the state of Malaysia's Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between Malaysia, New Zealand, and Portugal.

Table 23: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Malaysia	28,142	20,454	9,838	9,300	138	13	46
New Zealand	7,432	8,750	3,037	442	68	5	70
Portugal	19,776	46,387	8,741	1,962	22	27	34

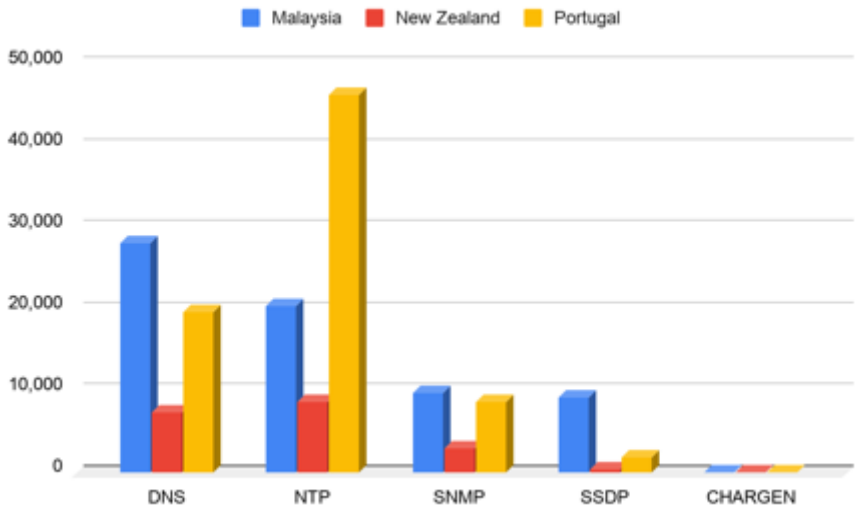


Figure 34: Comparison of raw count of open services

As the figure and table above show, Malaysia ranks less favorably than New Zealand and more favorably than Portugal with respect to its DDoS exposure. This result is largely driven by the countries' respective open NTP counts. NTP is a common networking service used for clock synchronization, and has a high amplification factor, making it an attractive reflector. Although Malaysia has higher counts than both New Zealand and Portugal for the other four services, the amplification potential is not as high for those services as NTP, which is the main reason why Portugal is ranked the worst among the three countries.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 24 shows the top five ISPs that host the greatest number of open services in Malaysia. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs.

Table 24: Top five ISP contributors per service

ISP	DNS	NTP	SNMP	SSDP	CHARGEN
Alibaba (US) Technology Co., Ltd.					3
Binariang Berhad (Maxis)		3	4	2	2
Exa Bytes	2		5		

Gigabit Hosting Sdn Bhd	4	2			
IP ServerOne Solutions Sdn Bhd					5
REDtone		5	3	4	
Shinjiru Technology Sdn Bhd	3				
TIME dotCom Berhad	5	4	1	3	4
TM Net, Internet Service Provider	1	1	2	1	1
YTL COMMUNICATIONS SDN BHD				5	

Legend:

Biggest contributor Least contributor

There are several ISPs that have high contribution counts across the five services analyzed. Among them are: TM Net, Exa Bytes, Gigabit Hosting, Binariang Berhad (Maxis), and Time dotCom. If Malaysian authorities collaborated with these ISPs to launch a mitigation campaign, there could be substantial improvement of Malaysia's risk exposure.

A detailed breakdown of ISP contribution for each of the five open services in Malaysia is provided in Appendix E.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for the domains located in Malaysia. It should be noted that the list of domains is not complete. The information provided is based on 2,485 domains.

DMARC

Figure 35 shows DMARC policy implementation for the domains in Malaysia.

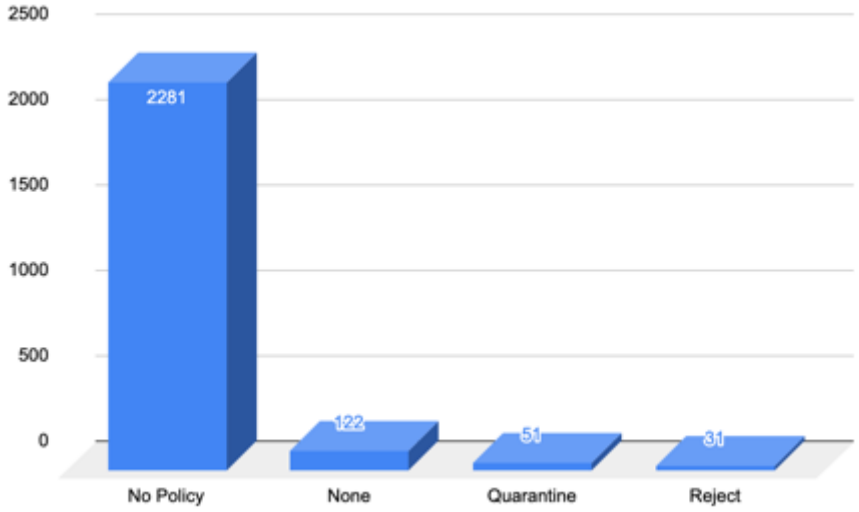


Figure 35: DMARC policy implementation in Malaysia

Overall, 204 out of 2,485 domains have DMARC implemented at some level, with the majority being set to policy level of “none” (122). The remaining domains are set to either “quarantine” (51) or “reject” (31). Of the 204 domains, 69 domains do not have reporting enabled. Fifty of these domains are set to the DMARC policy level of none, which does not provide any level of protection. The purpose of level “none” is simply to enable reporting and review the reports that are being generated; it does not do any filtering or actually enforce DMARC. DMARC reporting must be enabled to determine if the authentication and authorization mechanisms for the domain are set up properly. If setup correctly, then the DMARC policy for the domain can be adjusted to a level that allows for enforcement and protection of the domain: “quarantine” and “reject”. Only having a policy of “none” with no reporting enabled does not protect a domain or brand, and does not prevent the use of a domain in phishing campaigns.

The remaining domains without DMARC reporting are set to either "quarantine" (14) or "reject" (5).

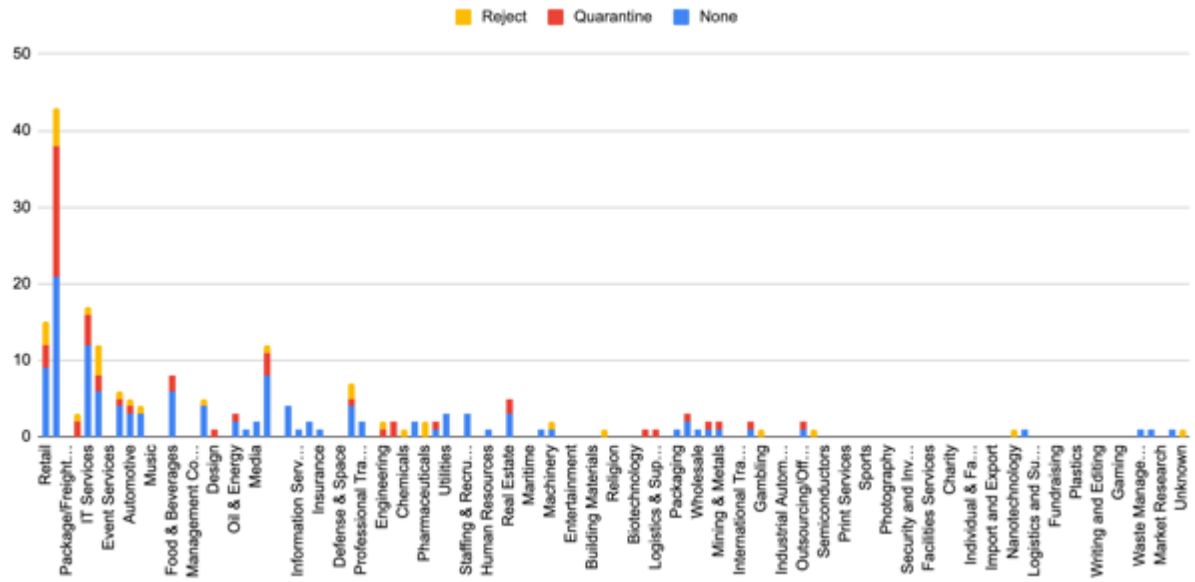


Figure 36: DMARC Implementation by sector

Figure 36 shows the breakdown of the sectors that have implemented DMARC based on the 2,458 observed domains. The domains that have no DMARC policy were excluded to allow for easier viewing. The adoption rate is good based on the data available, as quite a few sectors are adopting DMARC.

SENDER POLICY FRAMEWORK (SPF)

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in Malaysia are using SPF. The use of SPF alone does not provide full security since most receiving systems do not enable SPF Verification. While the sending organization's SPF defines which systems are authorized, the receiving side needs to determine how to handle any unauthorized messages. Most receiving systems do not want to make that decision. This is why SPF should be implemented alongside DMARC and DKIM.

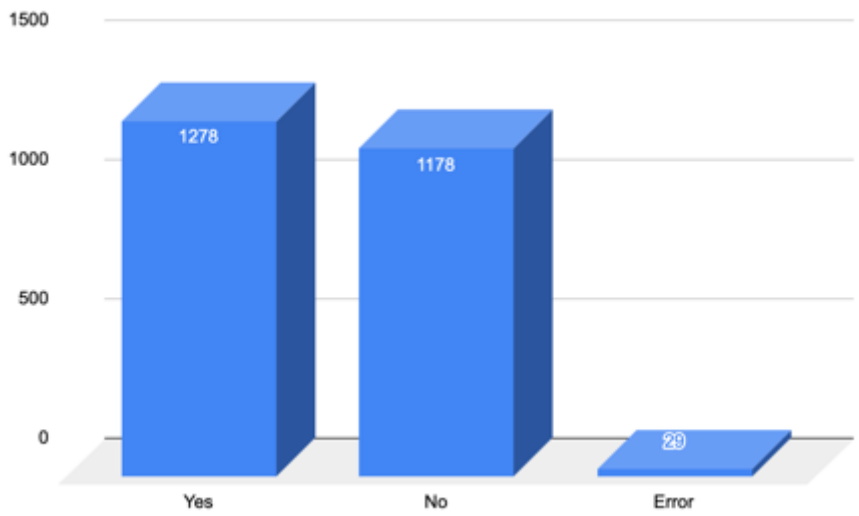


Figure 37: SPF Implementation in Malaysia

There are 15 domains that have implemented SPF as follows: “v=spf1 -all”, which means there are no systems allowed to send messages using their domain. This is good, but would be better if DMARC was implemented with the policy level of “reject”. The reason being that more than 80% of consumer mailboxes (based on Valimail reports) are using DMARC verification. If a DMARC policy were to be implemented along with the current SPF record, then the domain would be better secured and decrease the chances of the delivery of fraudulent messages.

There are 22 domains that have implemented SPF incorrectly by leaving out a critical tag ("all") which defines whether or not an email message is considered failed or not failed.

There are also 85 domains that use the value of "?all" in their SPF record, which is typically not recommended to use. The "?all" stands for neutral, meaning that messages do not pass or fail the SPF authentication check. The recommended value is either "-all" (hard fail) or "~all" (soft fail).

There are ten domains that have an “all” tag, just missing the -/~/?/+ before it. One of these must be present to complete the tag and allow for the record to function.

DMARC AND SPF

Table 25 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 25: DMARC and SPF implementation in Malaysia

Policy Level	DMARC	SPF
No Policy	2281	1084
None	122	116
Quarantine	51	50
Reject	31	28

For the domains that have DMARC, it is not always expected to have an SPF record when starting with a DMARC policy of “none”. In this case, six domains with a DMARC policy of “none” do not have SPF records. This is allowed because the DMARC policy of “none” does not block any messages (fraudulent or legitimate). Most organizations will add the SPF record after reviewing the information presented in the DMARC reports. The DMARC reports can help to build and adjust SPF records.

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be done for the 1,179 domains that do not have an SPF record, as well as the 16 domains with an SPF record of “v=spf1 -all”. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (2281 records that do not have DMARC). DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

There are 22 domains that have implemented SPF incorrectly by leaving out a critical tag ("all") which defines whether or not an email message is considered failed or not failed. The recommended tag to add is either "-all" (hard fail) or "~all" (soft fail). The domains are:

Domain	SPF Value
mbas.gov.my	v=spf1 mx a
dominant-semi.com	v=spf1 mx a=mail1.dominant-semi.com
edusibu.gov.my	v=spf1 a mx
acentury.net	v=spf1 a mx
honghwaigroup.com	v=spf1 a mx

moha.gov.my	v=spf1 ip4=202.75.5.167 ip4=203.217.177.249
kesedar.gov.my	v=spf1 ip4=103.245.89.4 ip4=103.245.89.5
kkmm.gov.my	v=spf1 ip4=49.236.205.110 ip4=49.236.205.108 ip4=49.236.205.109 ip4=49.236.205.105 ip4=103.245.89.4 ip4=103.245.89.5
my3dvision.com	v=spf1 include=spf.efwd.registrar-services.com a mx
klikegroup.com	v=spf1 include=spf.efwd.registrar-services.com a mx
lpktn.gov.my	v=spf1 ip4=103.245.89.4 ip4=103.245.89.5
pkns.gov.my	v=spf1 include=aspmx.googlemail.com
ppanpk.gov.my	v=spf1 a mx
sabahrmp.gov.my	v=spf1 a mx
rurallink.gov.my	v=spf1 ip4=49.236.205.110 ip4=49.236.205.108 ip4=49.236.205.109 ip4=49.236.205.105 ip4=103.245.89.4 ip4=103.245.89.5
showahdm.com	v=spf1 a mx
sprm.gov.my	v=spf1 ip4=203.217.178.5
yayasanmelaka.gov.my	v=spf1 a mx
rcj.com.my	v=spf1 ip4=174.36.116.62 ip4=67.228.93.4 a mx
moh.gov.my	v=spf1 ip4=49.236.205.110 ip4=49.236.205.108 ip4=49.236.205.109 ip4=49.236.205.105 ip4=103.245.89.4 ip4=103.245.89.5
kemas.gov.my	v=spf1 ip4=49.236.205.110 ip4=49.236.205.108 ip4=49.236.205.109 ip4=49.236.205.105 ip4=103.245.89.4 ip4=103.245.89.5

pknns.gov.my	v=spf1 a mx

The domain kesedar.gov.my should fix this first as they have a DMARC policy of “quarantine”, and this could cause legitimate messages from being delivered.

There are also a few domains that do not have SPF implemented but have a DMARC policy of "quarantine" or "reject". This could potentially cause issues as SPF is one of the items required for DMARC authentication. The domain kesedar.gov.my has already been mentioned above. The two domains with a policy of “reject” and no SPF are:

cibavision.com.my
msd-malaysia.com

Both of these domains must have an SPF record in place in order to prevent DMARC from blocking legitimate messages. If these domains are not used for email then an SPF record with the value of “v=spf1 -all” should be used, as this will add an additional level of security for organizations that only check for SPF.

ROUTING INFRASTRUCTURE ANALYSIS

There are 272 observed ASNs headquartered in Malaysia. Together, they advertise 3,048 IPv4 and 333 IPv6 prefixes.

42 of Malaysia’s ASNs advertise ROAs, while the remaining 230 ASNs advertise none.

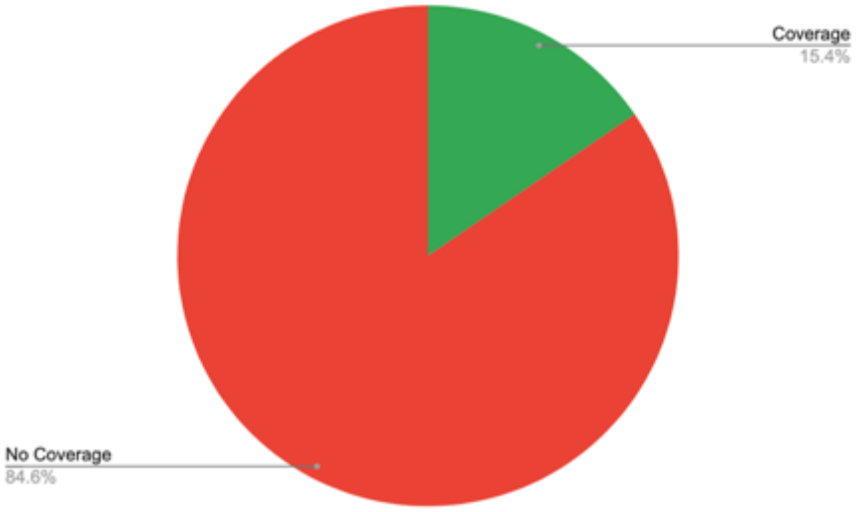


Figure 38: ROA Coverage in Malaysia (by ASN)

Of the advertised prefixes, 618 IPv4 and 57 IPv6 prefixes are covered by valid ROAs, together constituting 19.96% of Malaysia's prefixes. A further ten IPv4 and one IPv6 prefixes are covered by invalid ROAs, together constituting 0.33% of the total.

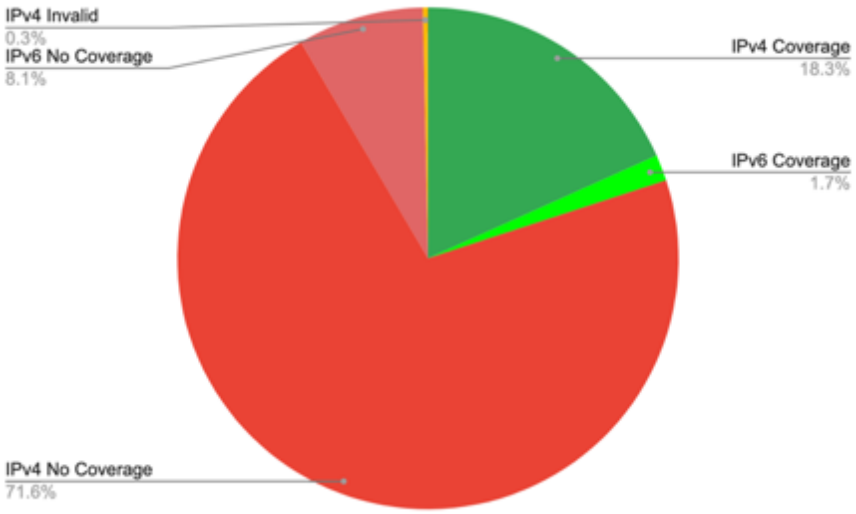


Figure 39: ROA Coverage in Malaysia (by advertised prefix)

The invalid ROAs are being advertised by 6 ASNs. Two different validation errors were observed:

1. The ASN is authorized to originate a prefix, but is announcing a sub-prefix of the authorized prefix instead of the authorized prefix. There were 6 IPv4 prefixes and one IPv6 prefix with errors of this kind. This is a relatively less serious error, as the ASN is authorized to originate the covering prefix.

2. The ASN is not authorized to originate a prefix. There were four IPv4 prefixes with errors of this kind. This is a serious error, as the ASN is announcing a prefix that it is not authorized for.

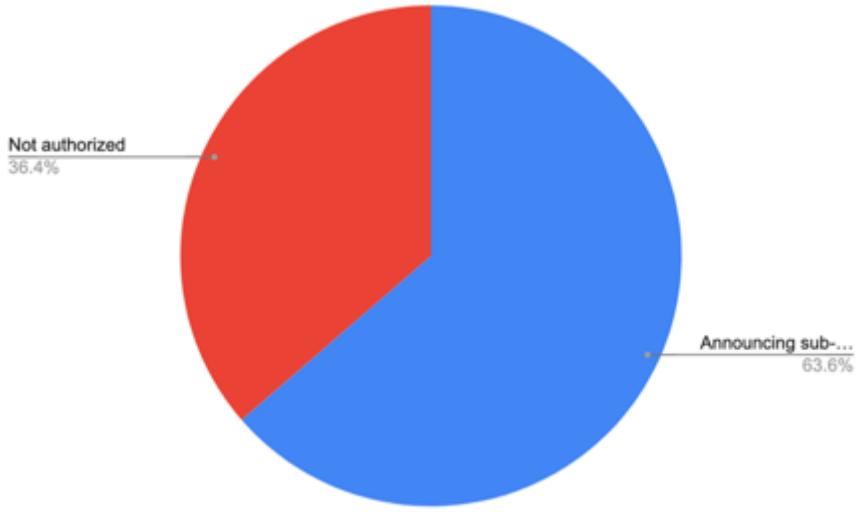


Figure 40: Invalid ROAs in Malaysia

The adoption of RPKI in Malaysia is not very high both in the number of ASNs and the number of actual prefixes that are announced via ROAs. However, of the RPKI deployments, there are a very low number of invalid ROAs. Even so, there should be outreach to come to a determination as to why these invalid announcements have occurred and to determine whether these invalid routing announcements are due to configuration errors, or due to the lack of acting upon routes that the ASN is not authorized to announce. Also, outreach and training should be done to increase the adoption of RPKI across additional ASNs and to get them all into a state of routing security best-practices conformance.

MYANMAR

COUNTRY OVERVIEW

Population: 53,710,000[v]

GDP: $71.21 billion[v]

Autonomous Systems: 92[w]

IPv4: ~116,224[x]

Percentage of Internet Users: 31%[y]

OPEN SERVICE ANALYSIS

Myanmar's overall risk exposure can be classified as moderate - among the highest 48% of countries in the world - and, as depicted in Figure 41, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

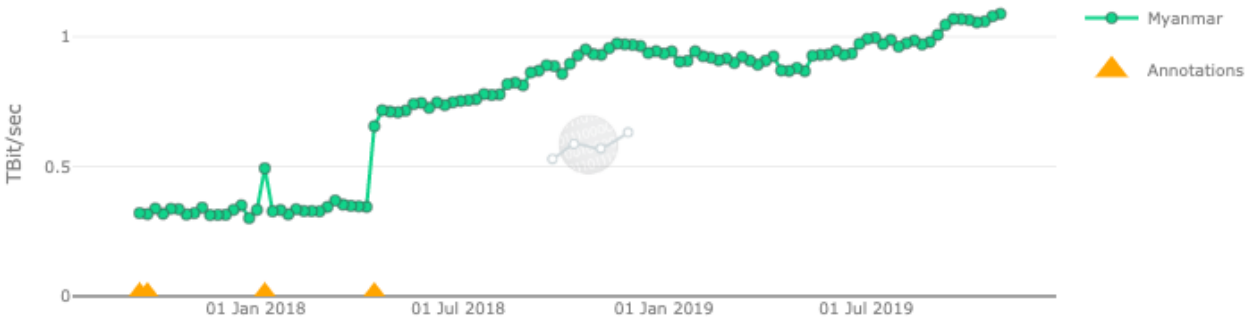


Figure 41: Two-year trend of potential DDoS infrastructure risk in Myanmar

[v] *Country Profile - Myanmar*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=MMR.
[w] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[x] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[y] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

Myanmar ranks #117 out of 244 on CyberGreen's index of riskiest DDoS environments. This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in Myanmar. As seen in Table 26, the most prevalent open service in Myanmar is NTP (1,884).

Table 26: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
588	1,884	937	0	0	1.1	117

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for Myanmar with priority sorted by highest to lowest amplified counts.

Table 27: Raw Count vs. Amplified count

Priority	Service	Raw Count	Amplified Count
1	NTP	1,884	1,049,200
2	DNS	588	24,108
3	SNMP	937	5,903

The raw count of open NTP services in Myanmar is highest, and NTP has the highest amplification factor of the five services analyzed. Ultimately, those open NTP services pose the highest risk if they were to be used in an attack. Myanmarese authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: MYANMAR, REPUBLIC OF THE CONGO, BERMUDA

With respect to its global standing, the state of Myanmar's Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between Myanmar, the Republic of the Congo, and Bermuda.

Table 28: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Myanmar	588	1,884	937	0	0	1.1	117
Republic of the Congo	157	189	115	0	0	0.1	187
Bermuda	139	1,288	2,378	72	0	0.7	132

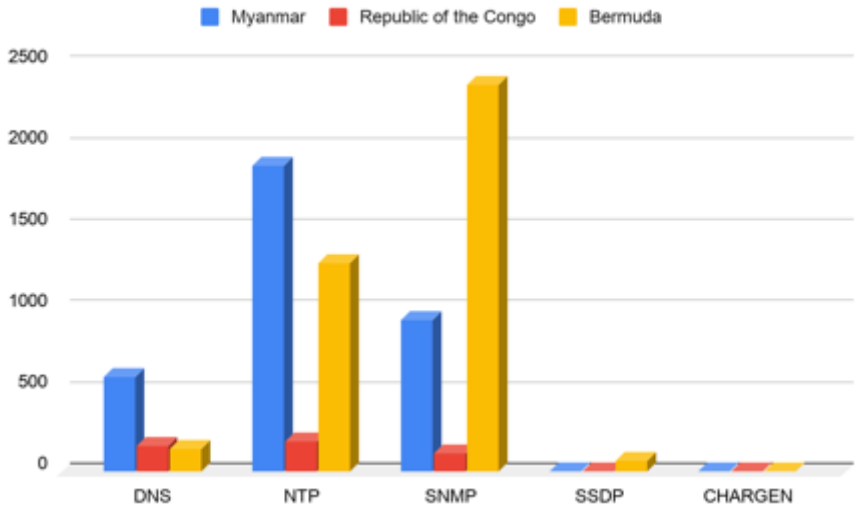


Figure 42: Comparison of raw count of open services

As the figure and table above show, Myanmar ranks less favorably than the Republic of Congo and Bermuda with respect to its DDoS exposure. This result is largely driven by the countries' respective open NTP counts. NTP is a common networking service used for clock synchronization, and has a high amplification factor, making it an attractive reflector. Although Bermuda has higher counts than both Myanmar and the Republic of the Congo for open SNMP, the amplification potential is not as high for that service as NTP, which is the main reason why Myanmar is ranked the worst among the three countries.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 29 shows the top five ISPs that host the greatest number of open services in Myanmar. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs

Table 29: Top five ISP contributors per service

ISP	DNS	NTP	SNMP
Frontiir Co. Ltd		3	
Golden TMH Telecom Co. Ltd		4	
IT Spectrum Company Limited (mm-link)	3		1
Myanma Posts and Telecommunications	1	1	2
OOREDOO MYANMAR	5	2	4
Spectrum Life Company Limited (Netcore)	2		3
Telenor Myanmar		5	
Terabit Wave Company Limited	4		5

Legend:

There are several ISPs that have high contribution counts across multiple services that were analyzed. Among them are: Myanmar Posts and Telecommunications, Spectrum Life Company Limited (Netcore), IT Spectrum Company Limited (mm-link), and Ooredoo. If Myanmarese authorities collaborated with these ISPs to launch a mitigation campaign, there could be substantial improvement of Myanmar's risk exposure.

A detailed breakdown of ISP contribution for each of the five open services in Myanmar is provided in Appendix F.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for the domains located in Myanmar. It should be noted that the list of domains is not complete. The information provided is based on 189 domains.

DMARC

Figure 43 shows DMARC policy implementation for the domains in Myanmar.

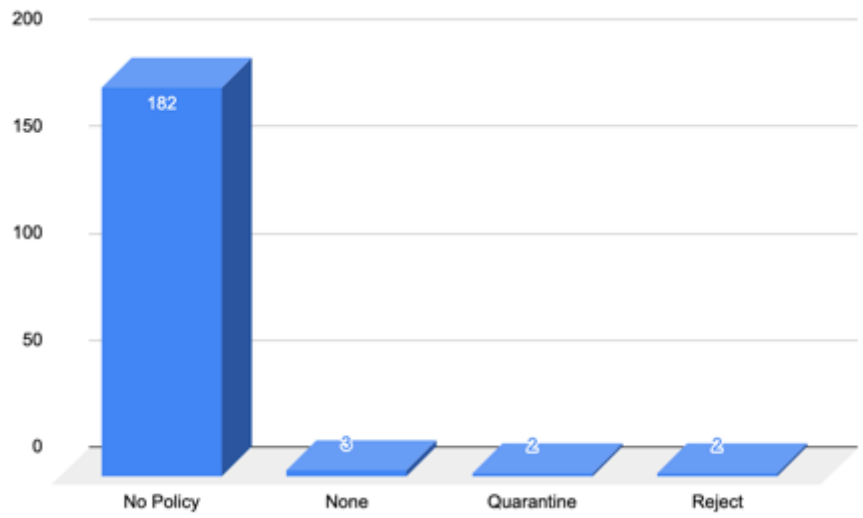


Figure 43: DMARC policy implementation in Myanmar

Overall, seven out of 189 domains have DMARC implemented at some level, with the majority being set to policy level of "none" (3). The remaining domains are set to either "quarantine" (2) or "reject" (2). All of the domains have DMARC reporting enabled. DMARC reporting must be enabled to determine if the authentication and authorization mechanisms for the domain are set up properly. If set up correctly, then the DMARC policy for the domain can be adjusted to a level that allows for enforcement and protection of the domain: "quarantine" and "reject".

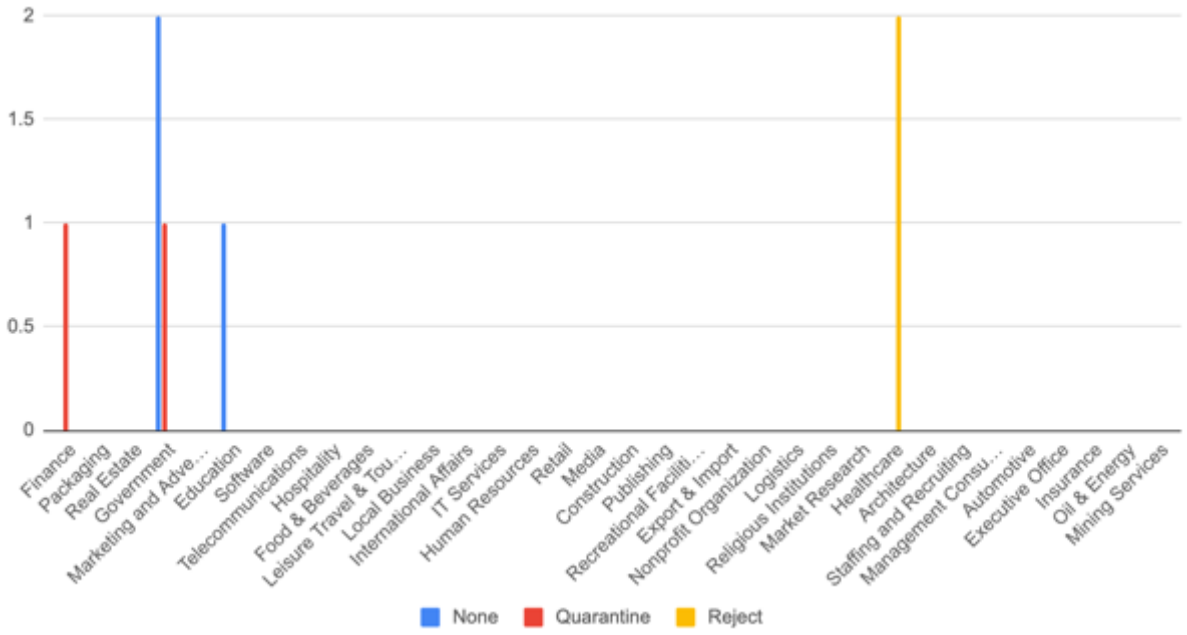


Figure 44: DMARC Implementation by sector

Figure 44 shows the breakdown of the sectors that have implemented DMARC based on the 189 observed domains. The domains that have no DMARC policy were excluded to allow for easier viewing. The adoption rate is very low based on the data available. Government, Finance, Education and Healthcare are the sectors showing any level of DMARC adoption.

SENDER POLICY FRAMEWORK (SPF)

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in Myanmar are not using SPF. The use of SPF alone does not provide full security since most receiving systems do not enable SPF Verification. While the sending organization's SPF defines which systems are authorized, the receiving side needs to determine how to handle any unauthorized messages. Most receiving systems do not want to make that decision. This is why SPF should be implemented alongside DMARC and DKIM.

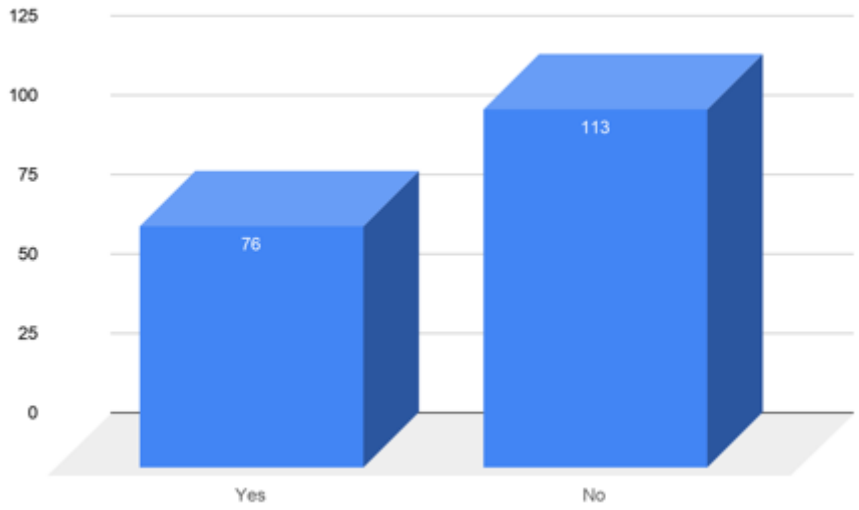


Figure 45: SPF Implementation in Myanmar

There are a few domains that have implemented SPF as follows: “v=spf1 -all”, which indicates that there are no systems allowed to send messages using their domain. This is good, but would be better if DMARC was implemented alongside the policy level of “reject”. The reason being that more than 80% of consumer mailboxes (based on Valimail reports) are using DMARC verification. If a DMARC policy were to be implemented along with the current SPF record, then the domain would be better secured and decrease the chances of the delivery of fraudulent messages.

DMARC AND SPF

Table 30 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 30: DMARC and SPF implementation in Myanmar

Policy Level	DMARC	SPF
No Policy	182	69
None	3	3
Quarantine	2	2
Reject	2	2

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be able to be done for the 113 domains that do not have an SPF record, as well as the three domains with an SPF record of “v=spf1 -all”. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (182 records that do not have DMARC). DMARC reports should be reviewed, appropriate adjustments should be made to SPF

and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

ROUTING INFRASTRUCTURE ANALYSIS

There are 93 observed ASNs headquartered in Myanmar. Together, they advertise 495 IPv4 and 90 IPv6 prefixes.

32 of Myanmar’s ASNs advertise ROAs, while the remaining 61 ASNs advertise none.

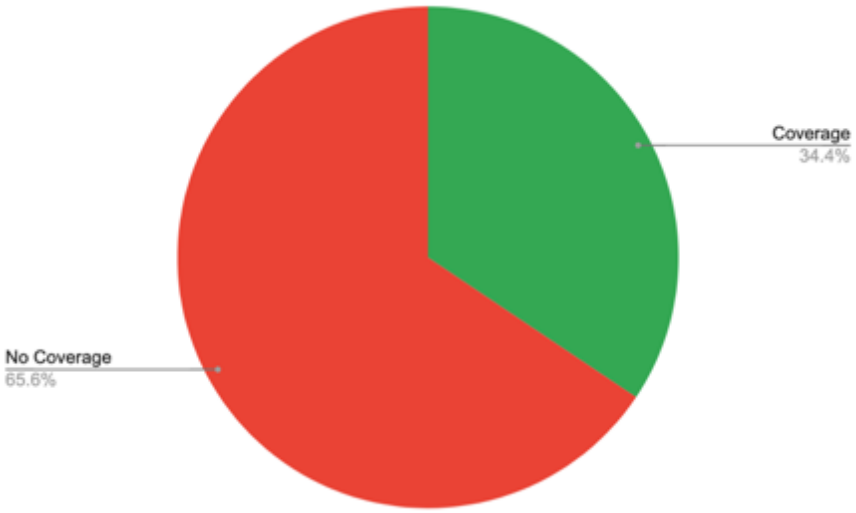


Figure 46: ROA Coverage in Myanmar (by ASN)

Of the advertised prefixes, 238 IPv4 and 9 IPv6 prefixes are covered by valid ROAs, together constituting 42.22% of Myanmar’s prefixes. A further 17 IPv4 and 75 IPv6 prefixes are covered by invalid ROAs, together constituting 15.73% of the total.

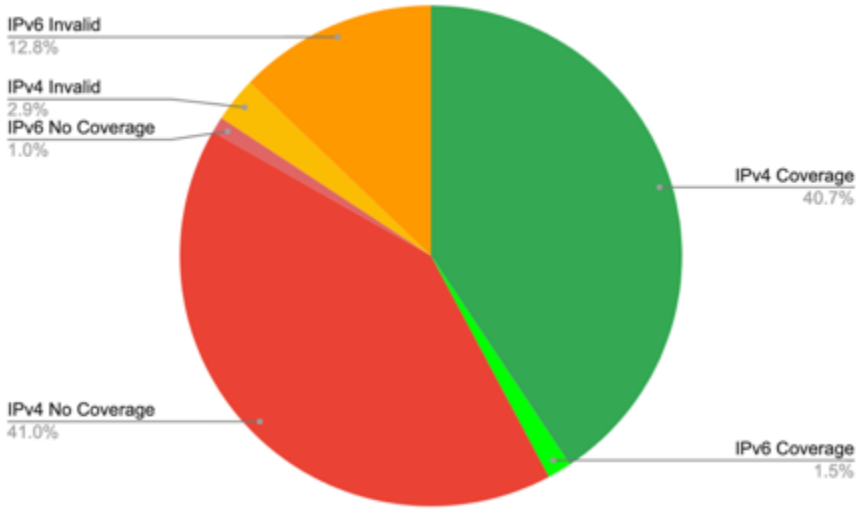


Figure 47: ROA Coverage in Myanmar (by advertised prefix)

The invalid ROAs are being advertised by three ASNs. Two different validation errors were observed:

1. The ASN is authorized to originate a prefix, but is announcing a sub-prefix of the authorized prefix instead of the authorized prefix. There were 16 IPv4 prefixes and 74 IPv6 prefixes with errors of this kind. This is a relatively less serious error, as the ASN is authorized to originate the covering prefix.
2. The ASN is not authorized to originate a prefix. There was one IPv4 prefix and one IPv6 prefix with errors of this kind. This is a serious error, as the ASN is announcing a prefix that it is not authorized for.

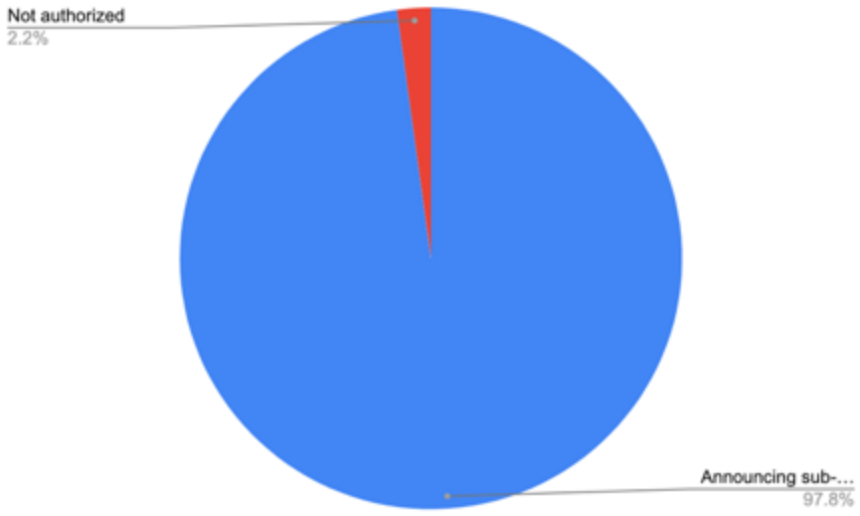


Figure 48: Invalid ROAs in Myanmar

The adoption of RPKI in Myanmar is progressing, but there are some issues with invalid ROAs that need attention. There should be outreach to come to a determination as to why these invalid announcements have occurred and to determine whether these invalid routing announcements are due to configuration errors, or due to the lack of acting upon routes that the ASN is not authorized to announce. Also, outreach and training should be done to increase the adoption of RPKI across additional ASNs and to get them all into a state of routing security best-practices conformance.

PHILIPPINES

COUNTRY OVERVIEW

Population: 106,650,000[z]

GDP: $330.91 billion [z]

Autonomous Systems: 450[aa]

IPv4: ~5,374,176[bb]

Percentage of Internet Users: 60%[cc]

OPEN SERVICE ANALYSIS

The Philippines' overall risk exposure can be classified as high - among the highest 17% of countries in the world - and, as depicted in Figure 49, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

Figure 49: Two-year trend of potential DDoS infrastructure risk in the Philippines

[z] *Country Profile - Philippines*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=PHL.
[aa] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[bb] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[cc] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

The Philippines ranks #41 out of 244 on CyberGreen's index of riskiest DDoS environments. This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in the Philippines and their respective amplification factors. As seen in Table 31, the most prevalent open service in the Philippines is NTP (29,769).

Table 31: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
15,577	29,769	17,029	742	241	17	41

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for the Philippines with priority sorted by highest to lowest amplified counts.

Table 32: Raw Count vs. Amplified Count

Priority	Service	Raw Count	Amplified Count
1	NTP	29,769	16,578,356
2	DNS	15,577	638,657
3	SNMP	17,029	107,283
4	CHARGEN	241	86,471
5	SSDP	742	22,854

The raw count of open NTP services in the Philippines is highest, and NTP has the highest amplification factor of the five services analyzed. Ultimately, those open NTP services pose the

highest risk if they were to be used in an attack. Philippino authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: PHILIPPINES, VENEZUELA, KENYA

With respect to its global standing, the state of the Philippines' Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between the Philippines, Venezuela, and Kenya.

Table 33: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Philippines	15,577	29,769	17,029	742	241	17	41
Venezuela	68,948	9,305	10,705	5,962	92	8	59
Kenya	2,597	11,743	1,908	78	9	7	64

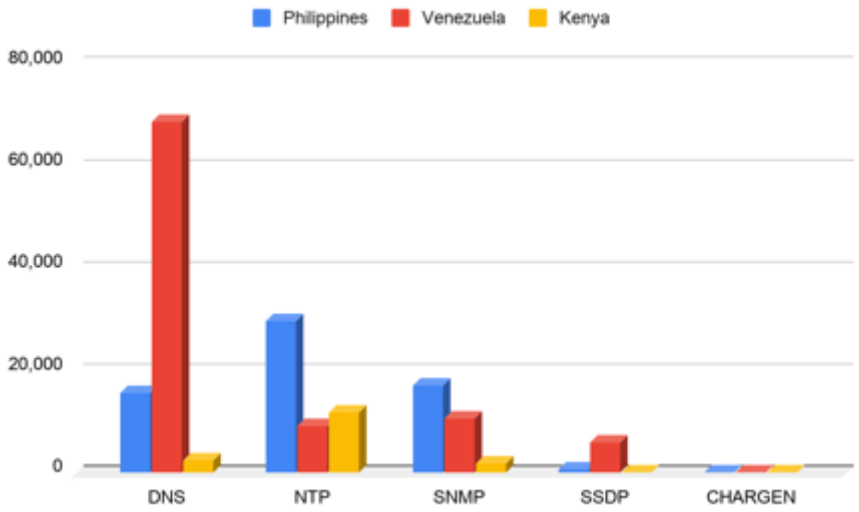


Figure 50: Comparison of raw count of open services

As the figure and table above show, the Philippines ranks less favorably than Venezuela and Kenya with respect to its DDoS exposure. This result is largely driven by the countries' respective open NTP counts. NTP is a common networking service used for clock synchronization, and has a high amplification factor, making it an attractive reflector. Although Venezuela has a substantially higher count than both the Philippines and Kenya for open DNS, the amplification potential is not as high for that service as NTP, which is the main reason why the Philippines is ranked the worst among the three countries.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 34 shows the top five ISPs that host the greatest number of open services in the Philippines. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs.

Table 34: Top five ISP contributors per service

ISP	DNS	NTP	SNMP	SSDP	CHARGEN
BSITC PHILS., INC.				5	
Converge ICT Solutions Inc.	4	4		3	5
Eastern Telecoms Phils., Inc.	3	1	2	4	4
ePLDT Inc.					1

Globe Telecoms	2	2	5	2	3
NewMountainView Satellite Corporation	5				
Philippine Long Distance Telephone Company	1	3	3	1	2
Philippine Telegraph and Telephone Corporation			4		
SKYBroadband SKYCable Corporation			1		
WifiCity Inc. (Fibercom)		5			

Legend:

There are several ISPs that have high contribution counts across the five services analyzed. Among them are: Philippine Long Distance Telephone Company, Globe Telecom, Eastern Telecoms, and Converge ICT Solutions. If Philippino authorities collaborated with these ISPs to launch a mitigation campaign, there could be substantial improvement of the Philippines' risk exposure.

A detailed breakdown of ISP contribution for each of the five open services in the Philippines is provided in Appendix G.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for the domains located in the Philippines. It should be noted that the list of domains is not complete. The information provided is based on 1,274 domains.

DMARC

Figure 51 shows DMARC policy implementation for the domains in the Philippines.

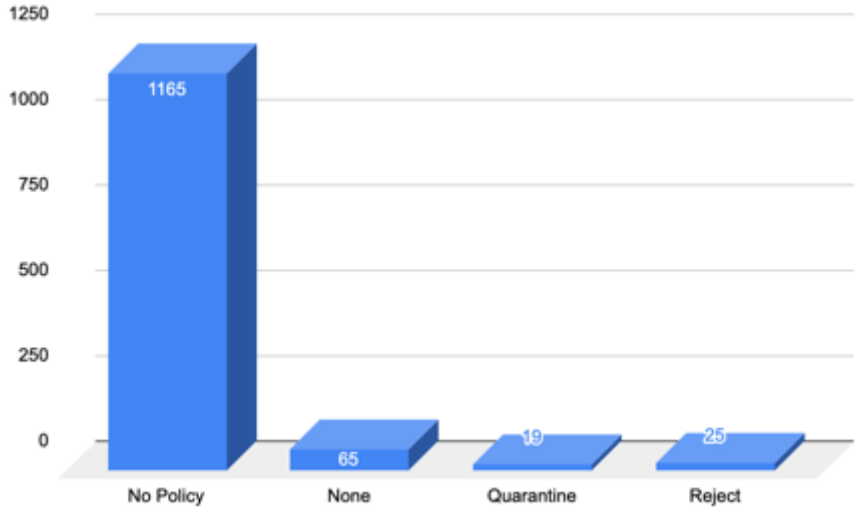


Figure 51: DMARC policy implementation in the Philippines

Overall, 109 out of 1,274 domains have DMARC implemented at some level, with the majority being set to policy level of “none” (65). The remaining domains are set to either “quarantine” (19) or “reject” (25). Of the 109 domains, 30 domains do not have reporting enabled. What is of concern here is that 22 of these domains are set to the DMARC policy level of “none”, which does not provide any level of protection. The purpose of level “none” is simply to enable reporting and review the reports that are being generated; it does not do any filtering or actually enforce DMARC. DMARC reporting must be enabled to determine if the authentication and authorization mechanisms for the domain are set up properly. If set up correctly, then the DMARC policy for the domain can be adjusted to a level that allows for enforcement and protection of the domain: "quarantine" and "reject". Only having a policy of “none” with no reporting enabled does not protect a domain or brand, and does not prevent the use of a domain in phishing campaigns. The remaining domains without DMARC reporting are set to either "quarantine" (4) or "reject" (5).

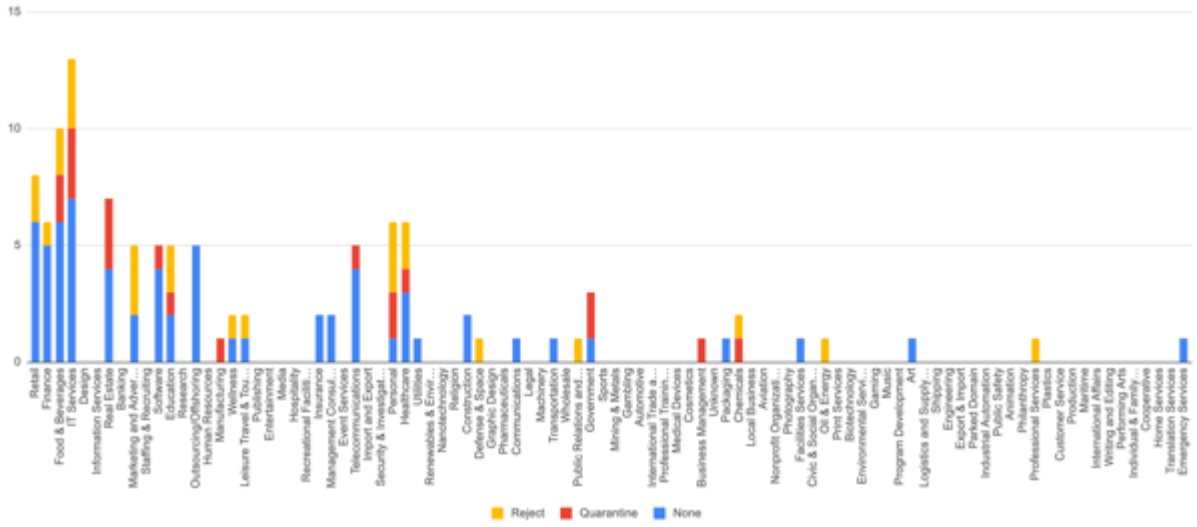


Figure 52: DMARC Implementation by sector

Figure 52 shows the breakdown of the sectors that have implemented DMARC based on the 1,268 observed domains. The domains that have no DMARC policy were excluded. The adoption rate is good based on the data available, as quite a few sectors are adopting DMARC.

SENDER POLICY FRAMEWORK (SPF)

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in the Philippines are not using SPF. The use of SPF alone does not provide full security since most receiving systems do not enable SPF Verification. While the sending organization's SPF defines which systems are authorized, the receiving side needs to determine how to handle any unauthorized messages. Most receiving systems do not want to make that decision. This is why SPF should be implemented alongside DMARC and DKIM.

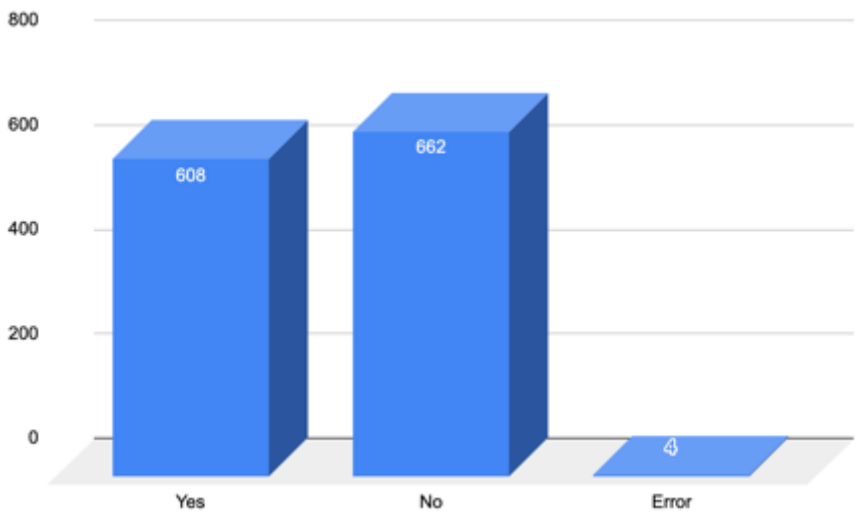


Figure 53: SPF Implementation in the Philippines

There are 24 domains that have implemented SPF as follows: “v=spf1 -all”, which indicates that there are no systems allowed to send messages using their domain. This is good, but would be better if DMARC was implemented alongside the policy level of “reject”. The reason being that more than 80% of consumer mailboxes (based on Valimail reports) are using DMARC verification. If a DMARC policy were to be implemented along with the current SPF record, then the domain would be better secured and decrease the chances of the delivery of fraudulent messages.

There are a few domains that have implemented SPF incorrectly by leaving out a critical tag ("all") which defines whether or not an email message is considered failed or not failed.

There are also 97 domains that use the value of "?all" in their SPF record, which is typically not recommended to use. The "?all" stands for neutral, meaning that messages do not pass or fail the SPF authentication check. The recommended value is either "-all" (hard fail) or "~all" (soft fail).

DMARC AND SPF

Table 35 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 35: DMARC and SPF implementation in the Philippines

Policy Level	DMARC	SPF
No Policy	1165	508
None	65	59
Quarantine	19	18
Reject	25	23

It is not always expected to have an SPF record when starting with a DMARC policy of “none”. In this case, six domains with a DMARC policy of “none”, do not have SPF records. This is allowed because the DMARC policy of “none” does not block any messages (fraudulent or legitimate). Most organizations will add the SPF record after reviewing the information presented in the DMARC reports. The DMARC reports can help to build and adjust SPF records.

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be done for the 662 domains that do not have an SPF record, as well as the 24 domains with an SPF record of “v=spf1 -all”. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (1165 records that do not have DMARC). DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

There are a few domains that have implemented SPF incorrectly by leaving out a critical tag ("all") which defines whether or not an email message is considered failed or not failed. Those domains are:

Domain	SPF Value
americaneye.com.ph	v=spf1 ip4=45.55.198.220
e-telligent.net	v=spf1 a mx
federalland.ph	v=spf1 a mx ip4=23.91.115.204
myflowertowne.ph	v=spf1 include=spf.efwd.registrar-services.com a mx

All of these domains are missing the “all” tag. The “all “ tag is required in order for SPF to work correctly. The appropriate entry would be to include “-all” (hard fail) or “~all” (soft fail) to the end of each SPF record.

There are also a few domains without an SPF record and DMARC policies of “quarantine” or “reject”. Those domains are:

Domain	DMARC Policy
bioseedph.com	Quarantine
novartis.com.ph	Reject
gsk.com.ph	Reject

These domains must have an SPF record in place in order to prevent DMARC from blocking legitimate messages. If these domains are not used for email then an SPF record with the value of “v=spf1 -all” should be used. This will add an additional level of security for organizations that only check for SPF.

ROUTING INFRASTRUCTURE ANALYSIS

There are 430 observed ASNs headquartered in the Philippines. Together, they advertise 4,371 IPv4 and 360 IPv6 prefixes.

78 of the Philippines’ ASNs advertise ROAs, while the remaining 352 ASNs advertise none.

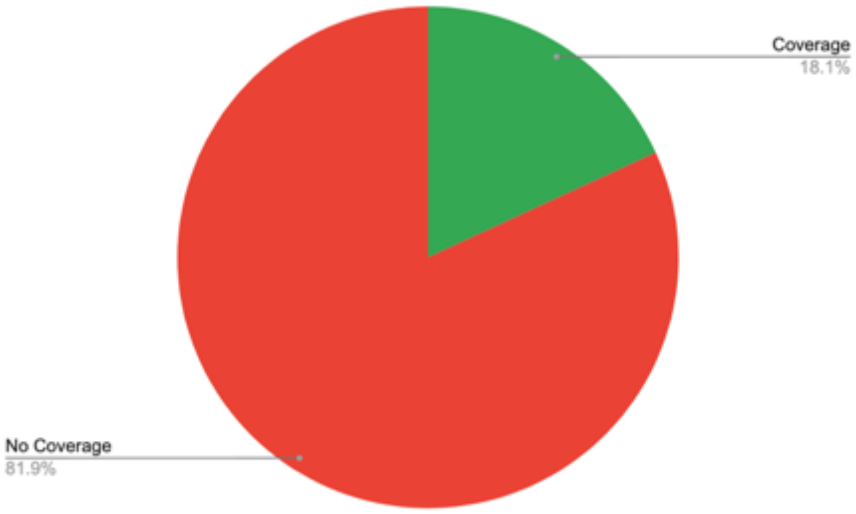


Figure 54: ROA Coverage in the Philippines (by ASN)

Of the advertised prefixes, 1,858 IPv4 and 26 IPv6 prefixes are covered by valid ROAs, 39.82% of the Philippines' prefixes. A further 256 IPv4 and five IPv6 prefixes are covered by invalid ROAs, together constituting 5.52% of the total.

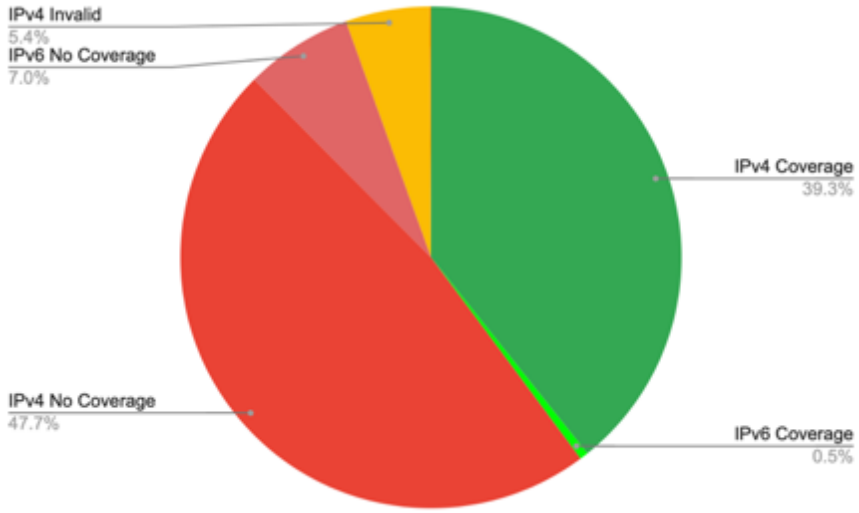


Figure 55: ROA Coverage in the Philippines (by advertised prefix)

The invalid ROAs are being advertised by 28 ASNs. Two different validation errors were observed:

1. The ASN is authorized to originate a prefix, but is announcing a sub-prefix of the authorized prefix instead of the authorized prefix. There were 219 IPv4 prefixes and five IPv6 prefixes with errors of this kind. This is a relatively less serious error, as the ASN is authorized to originate the covering prefix.
2. The ASN is not authorized to originate a prefix. There were 37 IPv4 prefixes with errors of this kind. This is a serious error, as the ASN is announcing a prefix that it is not authorized for.

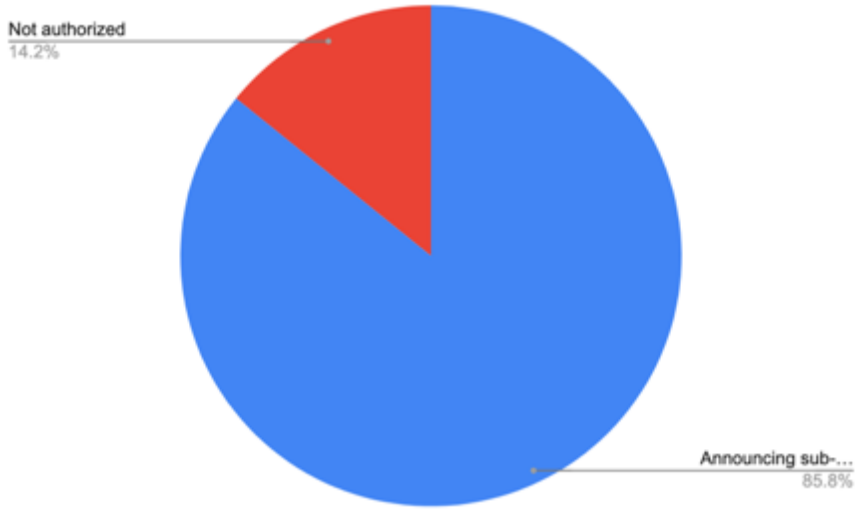


Figure 56: Invalid ROAs in the Philippines

The adoption of RPKI is limited in the Philippines and there are some issues with invalid ROAs. There should be outreach to come to a determination as to why these invalid announcements have occurred and to determine whether these invalid routing announcements are due to configuration errors, or due to the lack of acting upon routes that the ASN is not authorized to announce. Also, outreach and training should be done to increase the adoption of RPKI across additional ASNs and to get them all into a state of routing security best-practices conformance.

SINGAPORE

COUNTRY OVERVIEW

Population: 5,640,000[dd]

GDP: $364.16 billion[dd]

Autonomous Systems: 546[ee]

IPv4: ~5,802,829[ff]

Percentage of Internet Users: 88%[gg]

OPEN SERVICE ANALYSIS

Singapore's overall risk exposure can be classified as high - among the highest 11% of countries in the world - and, as depicted in Figure 57, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

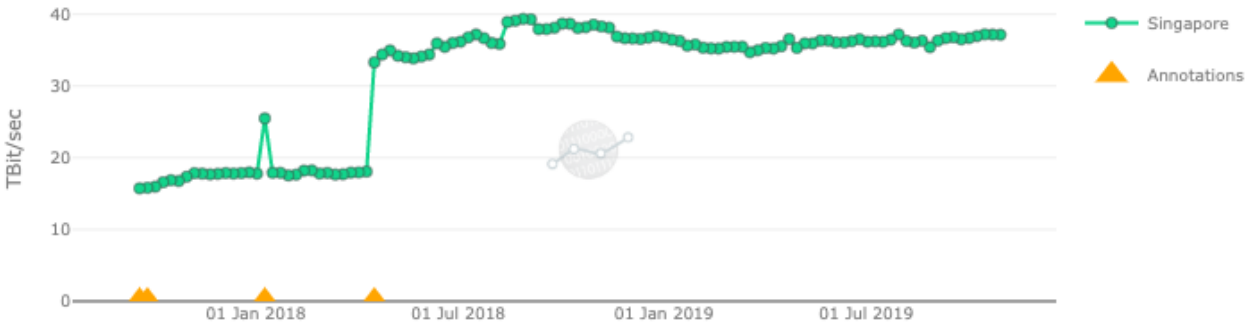


Figure 57: Two-year trend of potential DDoS infrastructure risk in Singapore

[dd] *Country Profile - Singapore*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=SGP.
[ee] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[ff] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[gg] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

Singapore ranks #26 out of 244 on CyberGreen's index of riskiest DDoS environments. This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in Singapore and their respective amplification factors. As seen in Table 36, the most prevalent open service in Singapore is NTP (63,064).

Table 36: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
47,977	63,064	3,503	753	109	37	26

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for Singapore with priority sorted by highest to lowest amplified counts.

Table 37: Raw Count vs. Amplified Count

Priority	Service	Raw Count	Amplified Count
1	NTP	63,064	35,120,342
2	DNS	47,977	1,967,057
3	CHARGEN	109	39,109
4	SSDP	753	23,192
5	SNMP	3,503	22,069

The raw count of open NTP services in Singapore is highest, and NTP has the highest amplification factor of the five services analyzed. Ultimately, those open NTP services pose the

highest risk if they were to be used in an attack. Singaporean authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: SINGAPORE, PAKISTAN, NEW ZEALAND

With respect to its global standing, the state of Singapore's Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between Singapore, Pakistan, and New Zealand.

Table 38: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Singapore	47,977	63,064	3,503	753	109	37	26
Pakistan	11,608	22,233	4,248	727	10	13	47
New Zealand	7,432	8,750	3,037	442	68	5	70

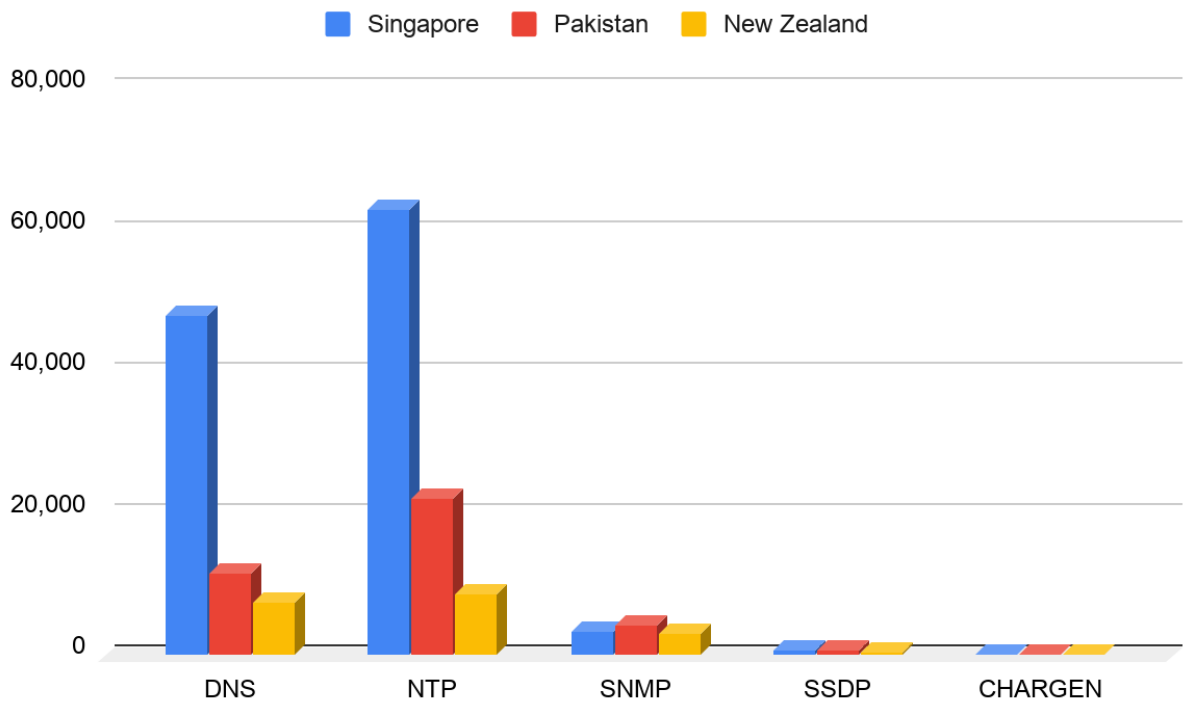


Figure 58: Comparison of raw count of open services

As the figure and table above show, Singapore ranks less favorably than Pakistan and New Zealand with respect to its DDoS exposure. Although Singapore's counts are higher across almost all the services, this result is largely driven by the countries' respective open NTP counts. NTP is a common networking service used for clock synchronization, and has a high amplification factor, making it an attractive reflector. Although Singapore also has a substantially higher count than both the Pakistan and New Zealand for open DNS, the total amplification value is not as high for that service as NTP, which is why the most focused effort for Singapore should be to reduce its open NTP contribution.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 39 shows the top five ISPs that host the greatest number of open services in Singapore. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs.

Table 39: Top five ISP contributors per service

ISP	DNS	NTP	SNMP	SSDP	CHARGEN
Alibaba (US) Technology Co., Ltd.		4			1
Amazon.com, Inc.				5	
BGPNET Global ASN	4				
DigitalOcean, LLC	1	1			4
GMO-Z com NetDesign Holdings Co., Ltd.	5				
MobileOne		3	5	2	
MyRepublic Ltd.				4	
OVH SAS	2				
SingNet	3	5	3		2
Singtel			4	3	
StarHub Ltd			2	1	5
Tencent		2			3
Viewqwest Pte Ltd			1		

Legend:

Biggest contributor Least contributor

There are several ISPs that have high contribution counts across the five services analyzed. Among them are: DigitalOcean, OVH SAS, SingNet, Singtel, MobileOne, and StarHub. If Singaporean authorities collaborated with these ISPs to launch a mitigation campaign, there could be substantial improvement of Singapore's risk exposure.

It is also worth noting that Singapore hosts many open services at entities that are allocated to foreign countries. Singaporean authorities should consider how they might tighten regulations or communicate with those foreign entities.

A detailed breakdown of ISP contribution for each of the five open services in Singapore is provided in Appendix H.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for the domains located in Singapore. It should be noted that the list of domains is not complete. The information provided is based on 3,079 domains.

DMARC

Figure 59 shows DMARC policy implementation for the domains in Singapore.

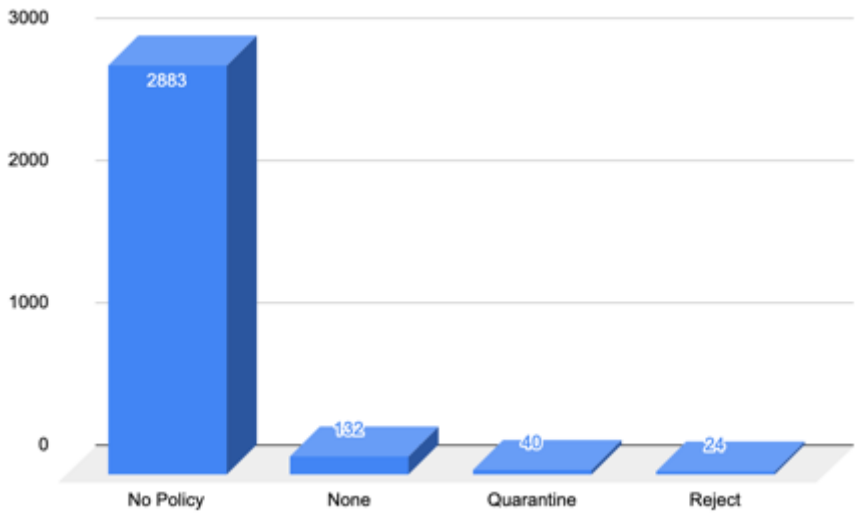


Figure 59: DMARC policy implementation in Singapore

Overall, 196 out of 3,079 domains have DMARC implemented at some level, with the majority being set to policy level of “none” (132). The remaining domains are set to either “quarantine” (40) or “reject” (24). Compared to February 2019, the number of domains with DMARC implementation increased by 38 domains. Twenty more domains set to policy level of “none”, 12 more set to policy level of “quarantine”, and four more set to policy level of “reject”.

Of the 196 domains, 45 domains do not have reporting enabled. Thirty of these domains are set to the DMARC policy level of “none”, which does not provide any level of protection. The purpose of level “none” is simply to enable reporting and review the reports that are being generated; it does not do any filtering or actually enforce DMARC. DMARC reporting must be enabled to determine if the authentication and authorization mechanisms for the domain are set up properly. If set up correctly, then the DMARC policy for the domain can be adjusted to a level that allows for enforcement and protection of the domain: “quarantine” and “reject”. Only having

a policy of “none” with no reporting enabled does not protect a domain or brand, and does not prevent the use of a domain in phishing campaigns. The remaining domains without DMARC reporting are set to either "quarantine" (10) or "reject" (5).

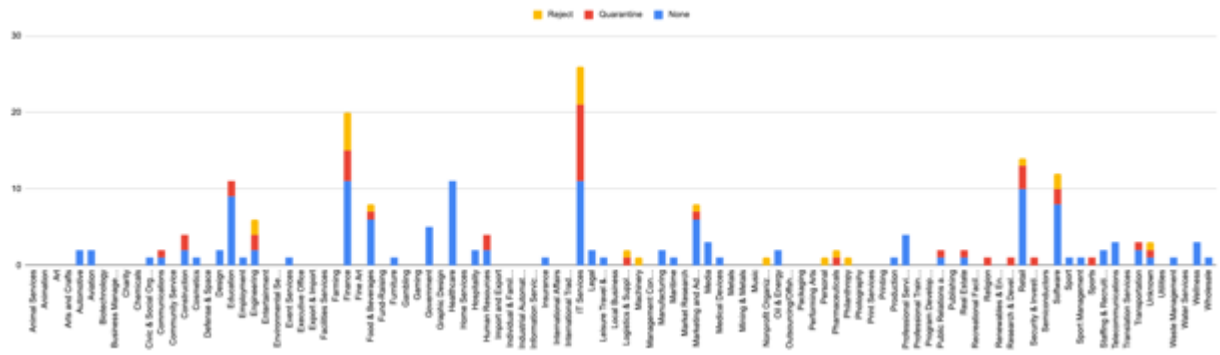


Figure 60: DMARC Implementation by sector

Figure 60 shows the breakdown of the sectors that have implemented DMARC based on the 3,078 observed domains. The domains that have no DMARC policy were excluded to allow for easier viewing. The adoption rate is good based on the data available, as many sectors are adopting DMARC. The IT Service sector is showing the strongest adoption of DMARC, followed by the Finance sector, Retail, Software and Education. Both of these sectors are also using the highest DMARC policy of "reject". These sectors are most likely showing the largest adoption rate due to the understanding of the requirements of implementation (IT Sector) and the benefits of protecting customers and reducing the amount of fraudulent activity (Finance) using the organization's domain name. For these same reasons, other sectors, such as Healthcare & Insurance and Government, need to adopt and implement DMARC at the highest policy level.

SENDER POLICY FRAMEWORK (SPF)

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in Singapore are using SPF. The use of SPF alone does not provide full security since most receiving systems do not enable SPF Verification. While the sending organization’s SPF defines which systems are authorized, the receiving side needs to determine how to handle any unauthorized messages. Most receiving systems do not want to make that decision. This is why SPF should be implemented alongside DMARC and DKIM.

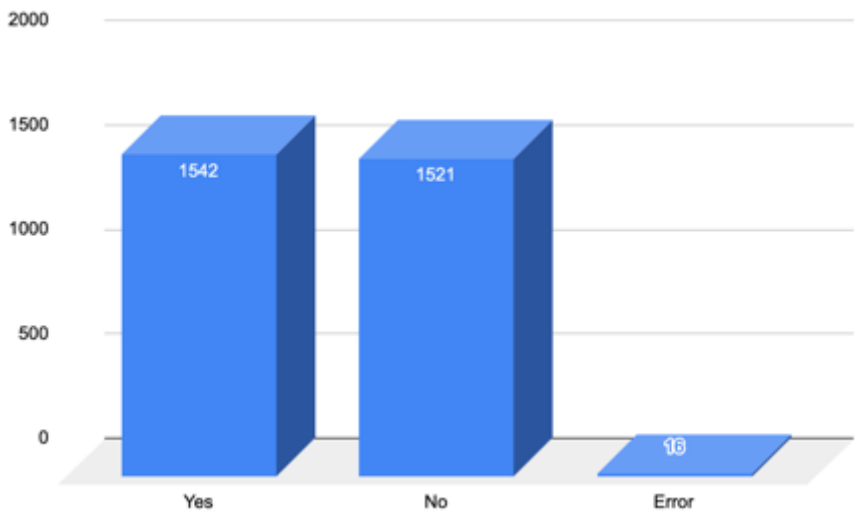


Figure 61: SPF Implementation in Singapore

There are 39 domains that have implemented SPF as follows: “v=spf1 -all”, which indicates that there are no systems allowed to send messages using their domain. 38 domains are not using a DMARC policy, and one has a DMARC policy of “quarantine”. This is good, but would be better if DMARC was implemented alongside the policy level of “reject”. The reason being that more than 80% of consumer mailboxes (based on Valimail reports) are using DMARC verification. If a DMARC policy were to be implemented along with the current SPF record, then the domain would be better secured and decrease the chances of the delivery of fraudulent messages.

There are 16 domains that have implemented SPF incorrectly. Nine domains have left out a critical tag ("all") which defines whether or not an email message is considered failed or not failed. One domain was set up incorrectly with an extra “all” tag. Two domains are missing spaces between tags. Three domains have an “all” tag, just missing the -/~/?/+ before it. One of these must be present to complete the tag and allow for the record to function.

There are also 147 domains that use the value of “?all” in their SPF record, which is typically not recommended to use. The "?all" stands for neutral, meaning that messages do not pass or fail the SPF authentication check. The recommended value is either "-all" (hard fail) or "~all" (soft fail).

DMARC AND SPF

Table 40 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 40: DMARC and SPF implementation in Singapore

Policy Level	DMARC	SPF
No Policy	2883	1355

None	132	125
Quarantine	40	40
Reject	24	22

The chart above shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present. For the domains that have DMARC, it is not always expected to have an SPF record when starting with a DMARC policy of “none”. In this case, seven domains with a DMARC policy of “none”, do not have SPF records. This is allowed because the DMARC policy of “none” does not block any messages (fraudulent or legitimate). Most organizations will add the SPF record after reviewing the information presented in the DMARC reports. The DMARC reports can help to build and adjust SPF records.

Anti-spam and anti-phishing tools will protect against most fraudulent messages coming from external sources. DMARC is the mechanism that will prevent an organization’s domain name from being used in this type of fraudulent activity. In order for DMARC to be successful, organizations must implement a DMARC policy (prevent domain from being used in fraudulent activity) and DMARC verification (check all incoming messages for DMARC policy). Historically, there has been success with DMARC adoption when the government mandates implementation of DMARC to all government agencies. So far, the United Kingdom, United States, the Netherlands, Australia, New Zealand and Saudi Arabia have done so with great success.

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be able to be done for the 1,524 domains that do not have an SPF record, as well as the 39 domains with an SPF record of “v=spf1 -all”. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. It is important to confirm whether or not the 1,524 domains are being used for email or not before implementing a DMARC policy of “reject” as legitimate message could be blocked. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (2883 records that do not have DMARC). DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

There are 16 domains that have implemented SPF incorrectly that need to be fixed. Nine domains have left out a critical tag ("all") which defines whether or not an email message is considered failed or not failed.

Domain	SPF Value
moneysense.gov.sg	v=spf1 include=support.gov.sg a=mailrelay1.g-cloud.gov.sg a=mailrelay2.g-cloud.gov.sg a=smtp.mas.gov.sg a=smtp2.mas.gov.sg ip4=118.189.126.12 ip4=119.73.244.12 ip4=118.189.126.25 ip4=119.73.244.25

brainteclabs.com	v=spf1 ip4=159.203.152.145 mx a=tejassm.dnsracks.com mx=mailer.brainteclabs.com include=tejassm.dnsracks.com
kata.ai	v=spf1 include=_spf.google.com
ivoice.sg	v=spf1 mx a ip4=208.64.181.188 include=spf.google.com
lifeiq.net	v=spf1 mx a ip4=64.98.40.0/22 ip4=66.79.253.160/28 include
scigenltd.com	v=spf1 a mx
tri-niche.com	v=spf1 a mx include=spf.se.web-hosting.com
wholesaleservice.net	v=spf1 include=spf.efwd.registrar-services.com a mx
gitigroup.com	v=spf1 ?include=custspf.register.com

The “all “ tag is required in order for SPF to work correctly. The appropriate entry would be to include “-all” (hard fail) or “~all” (soft fail) to the end of each SPF record.

The following domain has an extra “all” tag.

Domain	SPF Value
businesscatalyst.com.sg	v=spf1 a mx ip4=119.31.235.60 ip4=101.100.208.11 ip4=101.100.208.40 include=_spf.google.com~all ~all

The extra “~all” must be removed.

The following two domains are missing spaces between tags.

Domain	SPF Value
eitan.sg	v=spf1 a mx ip4=173.254.24.26 ip4=118.200.6.166?all

pigeon.com.sg	v=spf1 a mx ip4=113.29.237.108?all

The following three domains have an “all” tag, just missing the -/~/?/+ before it. One of these must be present to complete the tag and allow for the record to function.

Domain	SPF Value
dpdental.com.sg	v=spf1 a mx mx=mail.dpdental.com.sg a=mail.dpdental.com.sg include=_spf.google.com all
passions.com.sg	v=spf1 a mx ip4=103.11.151.81 all
zuji.com	v=spf1 include=hnair.com include=mediacorp.com.sg include=spf.protection.outlook.com all

The last domain has too many domains and surpasses the 10 domain lookup limitations of SPF:

Domain	SPF Value
multiwall.com.sg	v=spf1 mx a a=smtp.clients.netdns.net a=roton.hostcentral.net a=quark.hostcentral.net a=webmail.multiwall.com.sg ip4=103.26.43.156 include=spf.mschosting.com a=spfilter-1.mschosting.com a=spfilter-2.mschosting.com a=spfilter-3.mschosting.com a=spfilter-4.mschosting.com a=spfilter1-out1.sew01.mschosting.com a=spfilter1-out2.sew01.mschosting.com a=spfilter1-out3.sew01.mschosting.com a=spfilter1-out4.sew01.mschosting.com a=spfilter2-out1.sew01.mschosting.com a=spfilter2-out2.sew01.mschosting.com a=spfilter2-out3.sew01.mschosting.com a=spfilter2-out4.sew01.mschosting.com a=spfilter3-out1.sew01.mschosting.com a=spfilter3-out2.sew01.mschosting.com a=spfilter3-out3.sew01.mschosting.com a=spfilter3-out4.sew01.mschosting.com a=spfilter1-out4.sew01.mschosting.com -all

The total domain lookup is 26. This must be brought under 10, as it will cause issues and prevent the delivery of legitimate messages.

There is one domain which has a DMARC policy of "reject" but no SPF record. That domain is visa.com.sg. This is not an issue as visa.com.sg is not used for email purposes. However, it is recommended that an SPF record with the value of “v=spf1 -all” be used. This will add an additional level of security for organizations that only check for SPF.

ROUTING INFRASTRUCTURE ANALYSIS

There are 537 observed ASNs headquartered in Singapore. Together, they advertise 6,107 IPv4 and 972 IPv6 prefixes.

72 of Singapore's ASNs advertise ROAs, while the remaining 465 ASNs advertise none.

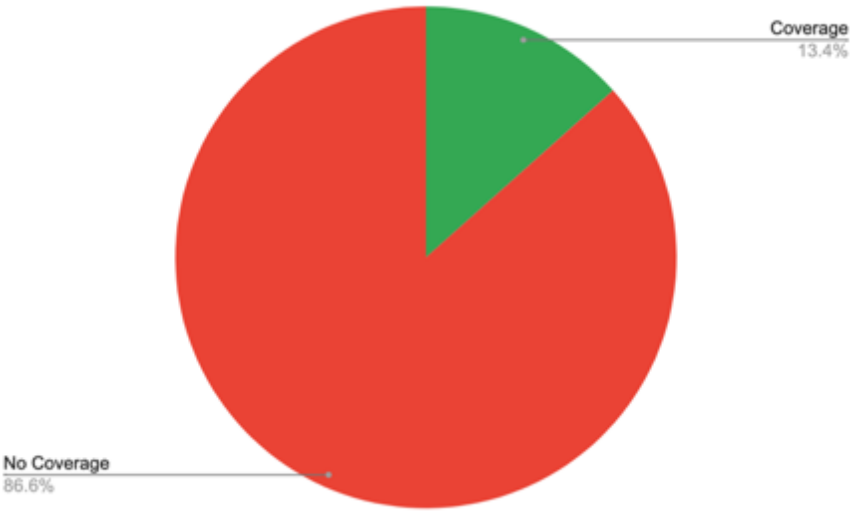


Figure 62: ROA Coverage in Singapore (by ASN)

Of the advertised prefixes, 2,475 IPv4 and 503 IPv6 prefixes are covered by valid ROAs, together constituting 42.07% of Singapore's prefixes. A further 99 IPv4 and 67 IPv6 prefixes are covered by invalid ROAs, together constituting 2.34% of the total.

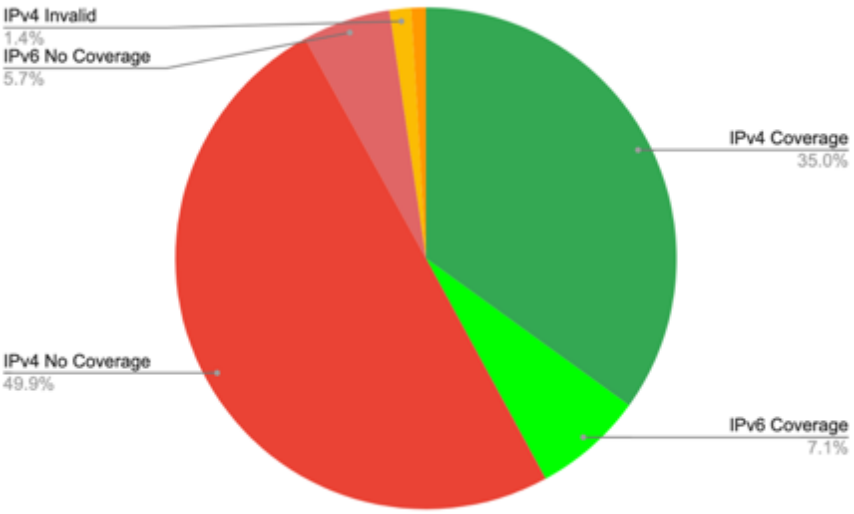


Figure 63: ROA Coverage in Singapore (by advertised prefix)

The invalid ROAs are being advertised by 23 ASNs. Two different validation errors were observed:

1. The ASN is authorized to originate a prefix, but is announcing a sub-prefix of the authorized prefix instead of the authorized prefix. There were 81 IPv4 prefixes and 64 IPv6 prefixes with errors of this kind. This is a relatively less serious error, as the ASN is authorized to originate the covering prefix.
2. The ASN is not authorized to originate a prefix. There were 18 IPv4 prefixes and three IPv6 prefixes with errors of this kind. This is a serious error, as the ASN is announcing a prefix that it is not authorized for.

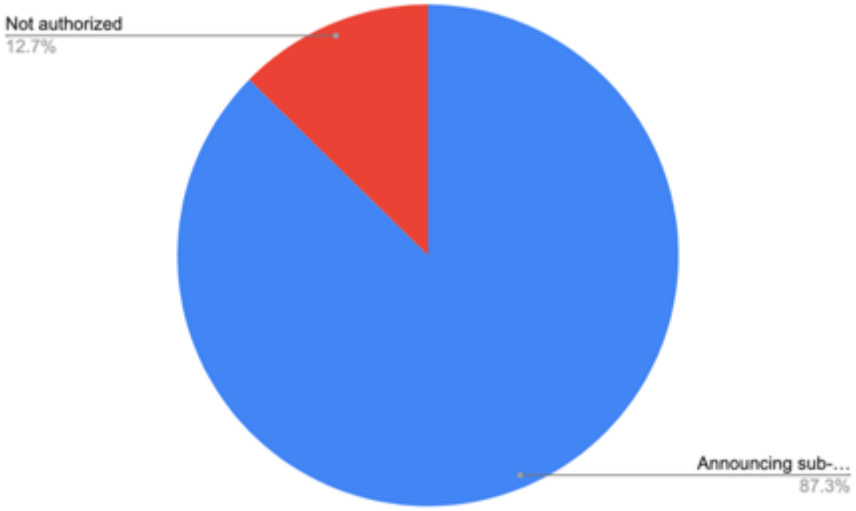


Figure 64: Invalid ROAs in Singapore

The adoption of RPKI in Singapore is limited and there are some issues with invalid ROAs. There should be outreach to come to a determination as to why these invalid announcements have occurred and to determine whether these invalid routing announcements are due to configuration errors, or due to the lack of acting upon routes that the ASN is not authorized to announce. Also, outreach and training should be done to increase the adoption of RPKI across additional ASNs and to get them all into a state of routing security best-practices conformance.

THAILAND

COUNTRY OVERVIEW

Population: 69,430,000[hh]

GDP: $504.99 billion[hh]

Autonomous Systems: 520[ii]

IPv4: ~8,414,976[jj]

Percentage of Internet Users: 57%[kk]

OPEN SERVICE ANALYSIS

Thailand's overall risk exposure can be classified as high - among the highest 9% of countries in the world - and, as depicted in Figure 65, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

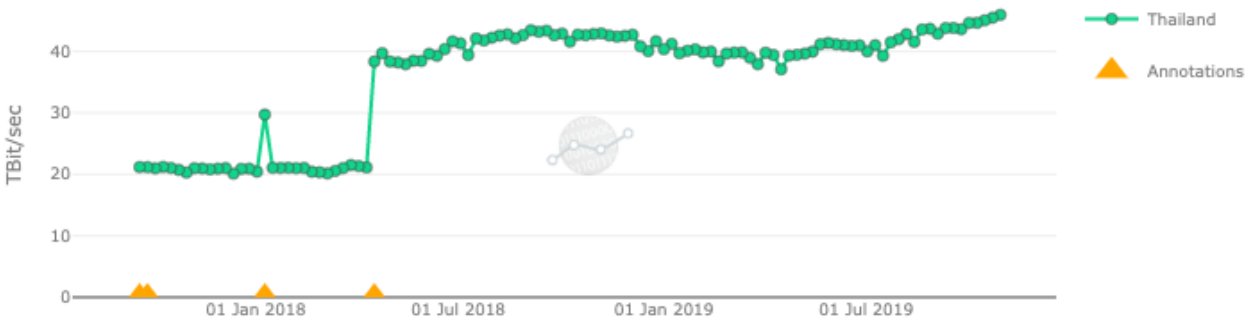


Figure 65: Two-year trend of potential DDoS infrastructure risk in Thailand

[hh] *Country Profile - Thailand*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=THA.
[ii] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[jj] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[kk] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

Thailand ranks #20 out of 244 on CyberGreen's index of riskiest DDoS environments. This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in Thailand. As seen in Table 41, the most prevalent open service in Thailand is NTP (77,973).

Table 41: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
38,863	77,973	22,947	5,966	391	45	20

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for Thailand with priority sorted by highest to lowest amplified counts.

Table 42: Raw Count vs. Amplified Count

Priority	Service	Raw Count	Amplified Count
1	NTP	77,973	43,423,164
2	DNS	38,863	1,593,383
3	SSDP	5,966	183,753
4	SNMP	22,947	144,566
5	CHARGEN	391	140,291

The raw count of open NTP services in Thailand is highest, and NTP has the highest amplification factor of the five services analyzed. Ultimately, those open NTP services pose the

highest risk if they were to be used in an attack. Thai authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: THAILAND, SAUDI ARABIA, CZECH REPUBLIC

With respect to its global standing, the state of Thailand's Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between Thailand, Saudi Arabia, and the Czech Republic.

Table 43: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Thailand	38,863	77,973	22,947	5,966	391	45	20
Saudi Arabia	14,264	21,439	1,140	273	76	13	48
Czech Republic	30,233	57,128	11,605	1,409	17	33	29

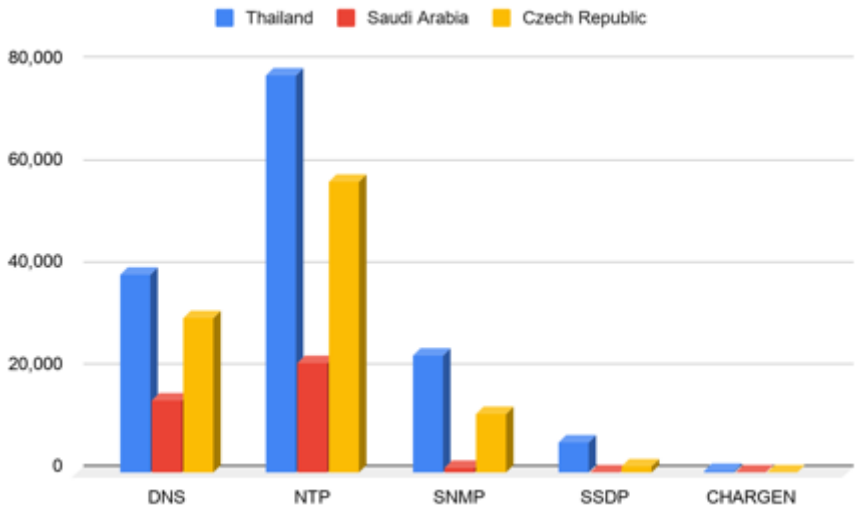


Figure 66: Comparison of raw count of open services

As the figure and table above show, Thailand ranks less favorably than Saudi Arabia and the Czech Republic with respect to its DDoS exposure. Although Thailand's counts are higher across all the services, this result is largely driven by the countries' respective open NTP counts. NTP is a common networking service used for clock synchronization, and has a high amplification factor, making it an attractive reflector. Policymakers in Thailand should focus on reducing its open NTP contribution.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 44 shows the top five ISPs that host the greatest number of open services in Thailand. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs.

Table 44: Top five ISP contributors per service

ISP	DNS	NTP	SNMP	SSDP	CHARGEN
AIS Fibre		5	4	3	
CAT TELECOM Public Company Ltd,CAT	2		3		
Chulalongkorn University				4	

CS LOXINFO PUBLIC COMPANY LIMITED	4	2			2
Jasmine Internet Co, Ltd.					1
KSC Commercial Internet Co. Ltd.			5		3
The Communication Authority of Thailand, CAT		4			
TOT Public Company Limited	1	3	1	1	
Triple T Internet/Triple T Broadband	5			2	5
TRUE INTERNET Co.,Ltd.	3	1	2	5	4

Legend:

1	2	3	4	5

Biggest contributor Least contributor

There are several ISPs that have high contribution counts across the five services analyzed. Among them are: TOT, CAT Telecom, True Internet, AIS Fibre, and CS LOXINFO. If Thai authorities collaborated with these ISPs to launch a mitigation campaign, there could be substantial improvement of Thailand's risk exposure.

A detailed breakdown of ISP contribution for each of the five open services in Thailand is provided in Appendix I.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for the domains located in Thailand. It should be noted that the list of domains is not complete. The information provided is based on 878 domains.

DMARC

Figure 67 shows DMARC policy implementation for the domains in Thailand.

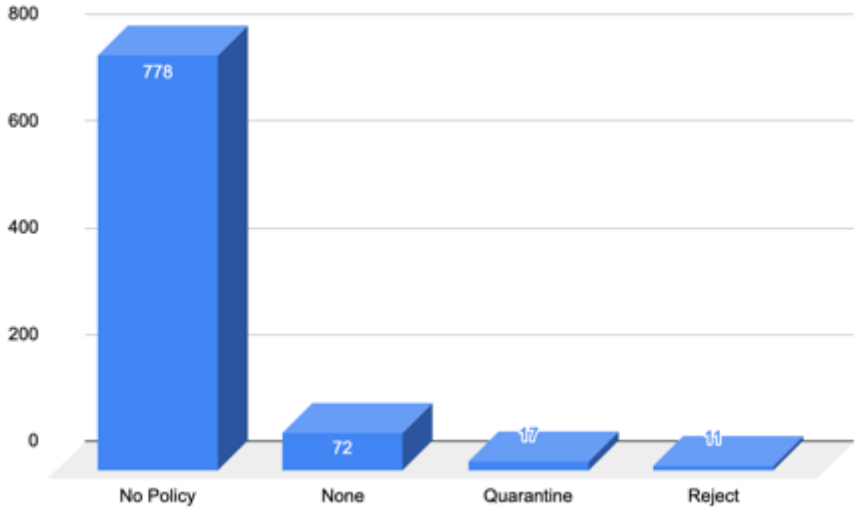


Figure 67: DMARC policy implementation in Thailand

Overall, 101 out of 878 domains have DMARC implemented at some level, with the majority being set to policy level of “none” (72). Of the 101 domains, 21 domains do not have reporting enabled. What is of concern here is that 17 of these domains are set to the DMARC policy level of “none”, which does not provide any level of protection. The purpose of level “none” is simply to enable reporting and review the reports that are being generated; it does not do any filtering or actually enforce DMARC. DMARC reporting must be enabled to determine if the authentication and authorization mechanisms for the domain are set up properly. If setup correctly, then the DMARC policy for the domain can be adjusted to a level that allows for enforcement and protection of the domain: “quarantine” and “reject”. Only having a policy of “none” with no reporting enabled does not protect a domain or brand, and does not prevent the use of a domain in phishing campaigns. The remaining domains are set to either "quarantine" (17) or "reject" (11).

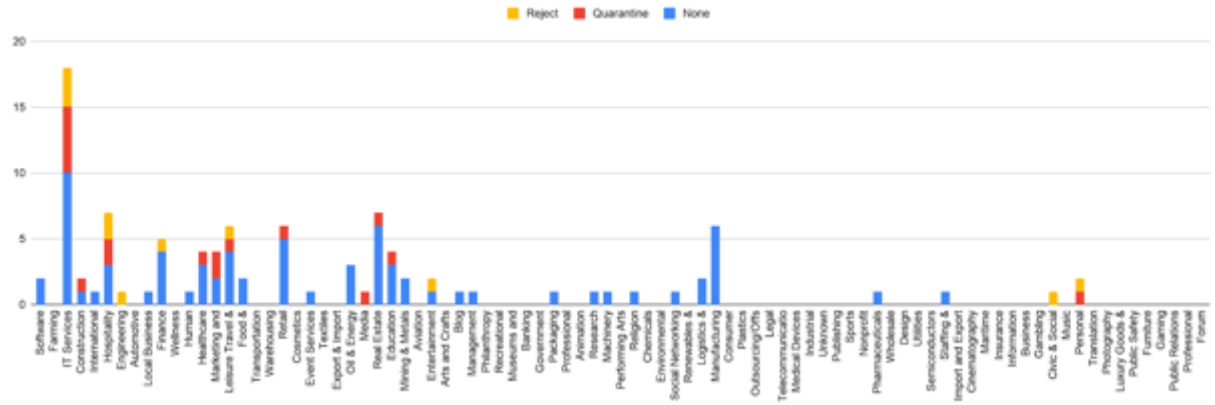


Figure 68: DMARC Implementation by sector

Figure 68 shows the breakdown of the sectors that have implemented DMARC based on the 877 domains. The domains that have no DMARC policy were excluded to allow for easier

viewing. The adoption rate is very low based on the data available. IT Services and Hospitality are the two sectors showing a level of DMARC adoption.

SENDER POLICY FRAMEWORK (SPF)

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in Thailand are using SPF. The use of SPF alone does not provide full security since most receiving systems do not enable SPF Verification. While the sending organization's SPF defines which systems are authorized, the receiving side needs to determine how to handle any unauthorized messages. Most receiving systems do not want to make that decision. This is why SPF should be implemented alongside DMARC and DKIM.

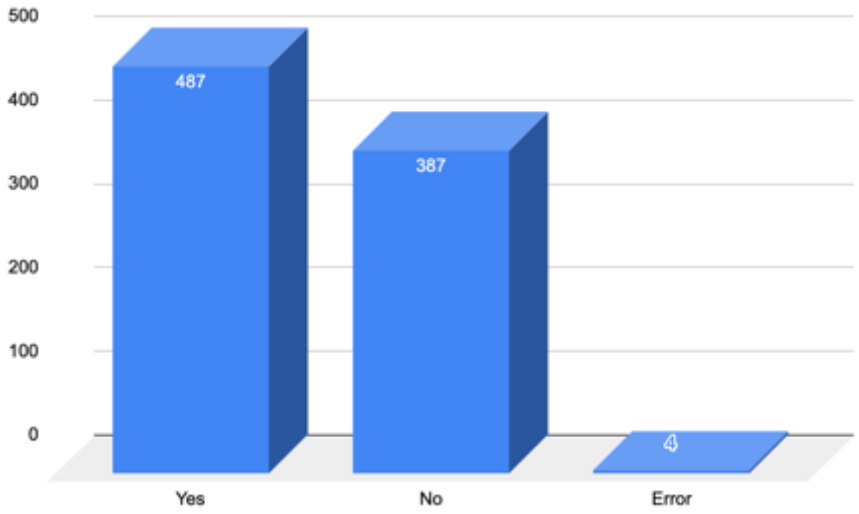


Figure 69: SPF Implementation in Thailand

There are a few domains that have implemented SPF incorrectly by leaving out a critical tag ("all") which defines whether or not an email message is considered failed or not failed.

DMARC AND SPF

Table 45 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 45: DMARC and SPF implementation in Thailand

Policy Level	DMARC	SPF
No Policy	778	391
None	72	68
Quarantine	17	17
Reject	11	11

It is not always expected to have an SPF record when starting with a DMARC policy of “none”. In this case, four domains with a DMARC policy of “none”, do not have SPF records. This is allowed because the DMARC policy of “none” does not block any messages (fraudulent or legitimate). Most organizations will add the SPF record after reviewing the information presented in the DMARC reports. The DMARC reports can help to build and adjust SPF records.

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be able to be done for the 387 domains that do not have an SPF record. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. It is important to confirm whether or not the 387 domains are being used for email or not before implementing a DMARC policy of “reject” as legitimate messages could be blocked. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (778 records that do not have DMARC). DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

There are a few domains that have implemented SPF incorrectly by leaving out a critical tag ("all") which defines whether or not an email message is considered failed or not failed. Those domains are:

Domain	SPF Value
fresenius-kabi.com	v=spf1 mx ip4=216.135.65.51 ip4=85.214.64.99 ip4=209.59.4.246 ip4=209.59.4.252 ip4=52.184.224.255 ip4=52.90.148.16 ip4=54.208.221.68 ip4=205.186.161.217 ip4=208.75.123.0/24 include=et._spf.pardot.com
brilliantmillion.com	v=spf1 include=_spf.google.com a=brillia
xtend-life.co.th	v=spf1 ip4=203.151.233.51 ip4=27.254.34.37 ip4=203.151.233.55 a mx
poar.co	v=spf1 a mx

The “all “ tag is required in order for SPF to work correctly. The appropriate entry would be to include “-all” (hard fail) or “~all” (soft fail) to the end of each SPF record.

ROUTING INFRASTRUCTURE ANALYSIS

There are 509 observed ASNs headquartered in Thailand. Together, they advertise 7686 IPv4 and 1125 IPv6 prefixes.

156 of Thailand’s ASNs advertise ROAs, while the remaining 353 ASNs advertise none.

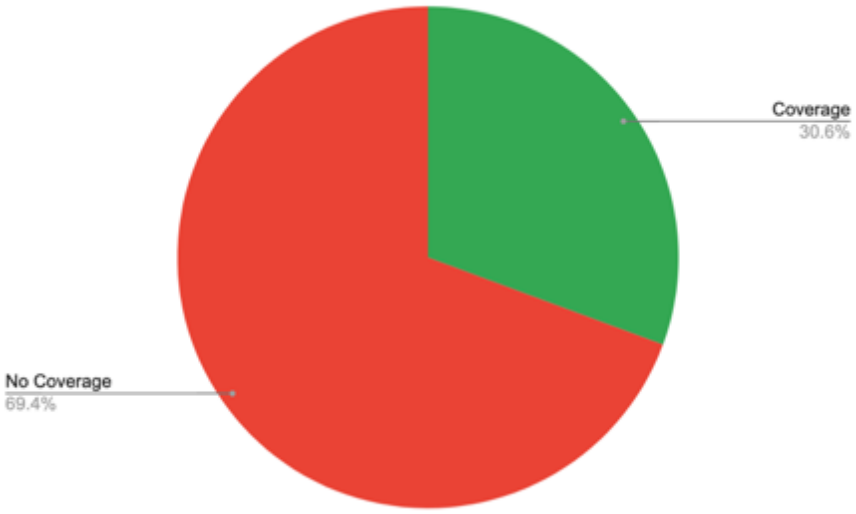


Figure 70: ROA Coverage in Thailand (by ASN)

Of the advertised prefixes, 2,225 IPv4 and 345 IPv6 prefixes are covered by valid ROAs, together constituting 29.17% of Thailand’s prefixes. A further 156 IPv4 and 245 IPv6 prefixes are covered by invalid ROAs, together constituting 4.55% of the total.

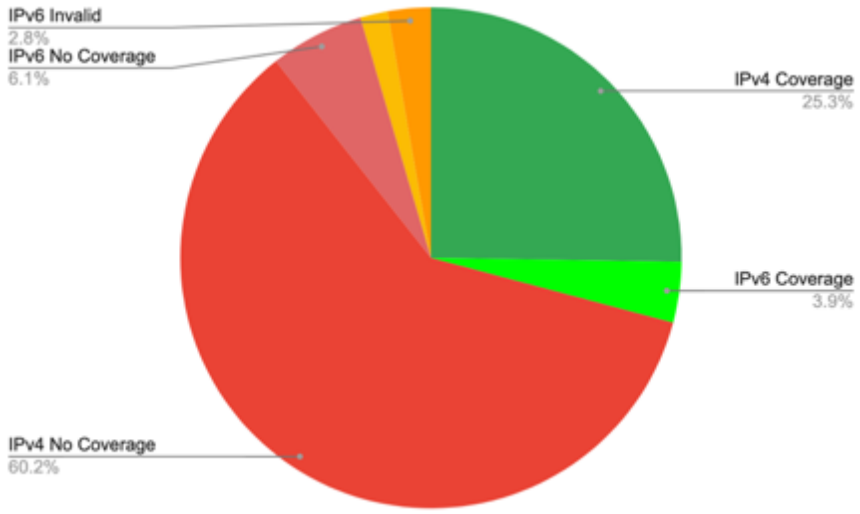


Figure 71: ROA Coverage in Thailand (by advertised prefix)

The invalid ROAs are being advertised by 26 ASNs. Two different validation errors were observed:

1. The ASN is authorized to originate a prefix, but is announcing a sub-prefix of the authorized prefix instead of the authorized prefix. There were 97 IPv4 prefixes and 239 IPv6 prefixes with errors of this kind. This is a relatively less serious error, as the ASN is authorized to originate the covering prefix.
2. The ASN is not authorized to originate a prefix. There were 59 IPv4 prefixes and 6 IPv6 prefixes with errors of this kind. This is a serious error, as the ASN is announcing a prefix that it is not authorized for.

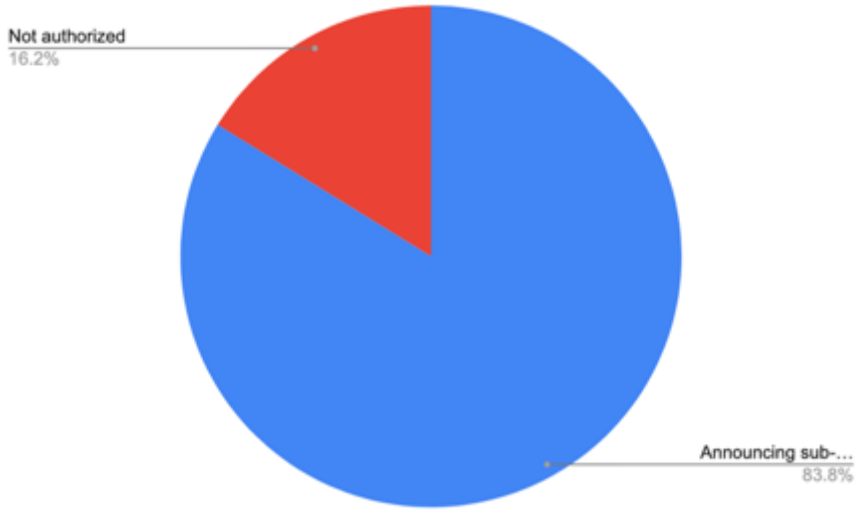


Figure 72: Invalid ROAs in Thailand

The adoption of RPKI in Thailand is progressing well and, in most of the deployments, there are few invalid ROAs. However, some invalid ROAs do exist which calls for outreach to determine why these invalid announcements have occurred and to determine whether these invalid routing announcements are due to configuration errors or due to the lack of acting upon routes that the ASN is not authorized to announce. Also, outreach and training should be done to increase the adoption of RPKI across additional ASNs and to get them all into a state of routing security best-practices conformance.

VIETNAM

COUNTRY OVERVIEW

Population: 95,540,000[ll]

GDP: $244.95 billion[ll]

Autonomous Systems: 352[mm]

IPv4: ~15,064,530[nn]

Percentage of Internet Users: 70%[oo]

OPEN SERVICE ANALYSIS

Vietnam's overall risk exposure can be classified as high - among the highest 15% of countries in the world - and, as depicted in Figure 73, has remained fairly consistent over the past 2 years. That consistency suggests that there has not been a concerted national mitigation effort during this period.

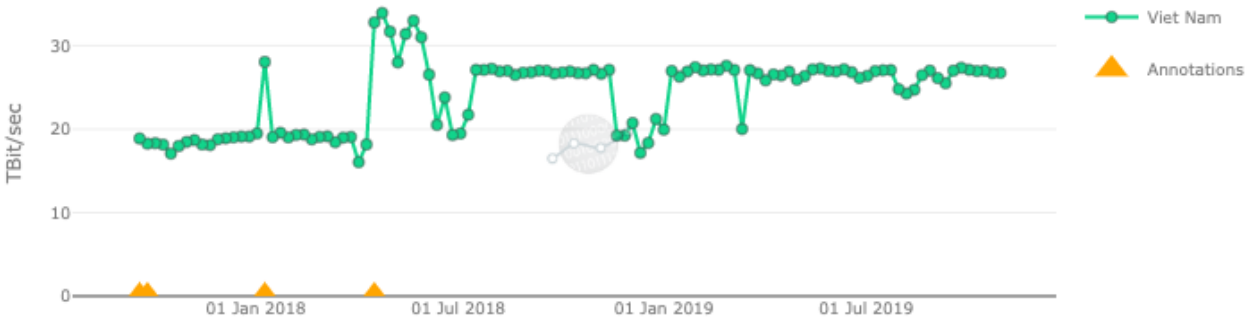


Figure 73: Two-year trend of potential DDoS infrastructure risk in Vietnam

[ll] *Country Profile - Vietnam*, World Bank, https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=VNM.
[mm] *AS Overview*, CyberGreen, Oct. 2019, https://stats.cybergreen.net/asn.
[nn] *Country Report*, ipfinder, Oct. 2019, https://ipfinder.io/countries/.
[oo] *Percentage of Individuals Using the Internet*. ITU, June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Jun2019.xls.

Note: The sharp spike seen in April 2018 is due to a halving of CyberGreen's scan speed, intended to reduce the impact of the scans, which ultimately resulted in an increase in responses to the scans.

Vietnam ranks #35 out of 244 on CyberGreen's index of riskiest DDoS environments. This ranking is based on the presence of five types of open services (NTP, DNS, SSDP, SNMP, CHARGEN) in Vietnam and their respective amplification factors. As seen in Table 46, the most prevalent open service in Vietnam is NTP (44,811).

Table 46: Raw count of open services per service

DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
40,485	44,811	7,098	1,227	68	27	35

While raw count of open services is helpful to quantify the presence of vulnerabilities within the Internet ecosystem, the amplified count can assist with prioritizing mitigation activities. The following table summarizes the raw counts and amplified counts for Vietnam with priority sorted by highest to lowest amplified counts.

Table 47: Raw Count vs. Amplified Count

Priority	Service	Raw Count	Amplified Count
1	NTP	44,811	24,955,246
2	DNS	40,485	1,659,885
3	SNMP	7,098	44,717
4	SSDP	1,227	37,792
5	CHARGEN	68	24,398

The raw count of open NTP services in Vietnam is highest, and NTP has the highest amplification factor of the five services analyzed. Ultimately, those open NTP services pose the

highest risk if they were to be used in an attack. Vietnamese authorities should prioritize mitigation of open NTP services.

Not every country's breakdown of reflectors will look the same. Devices and infrastructure vary from country to country. A comparative analysis between countries can shed some light on this differentiation.

COUNTRY COMPARISON: VIETNAM, TURKEY, NORWAY

With respect to its global standing, the state of Vietnam's Internet health can be further contextualized by conducting a comparative analysis against other countries with similar IPv4 address counts. For this section, a comparative analysis has been conducted between Vietnam, Turkey, and Norway.

Table 48: Comparison of raw count of open services

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (Tbit/Sec)	DDoS Rank (1 = worst 244 = best)
Vietnam	40,485	44,811	7,098	1,227	68	27	35
Turkey	212,146	45,460	15,437	2,174	130	34	28
Norway	20,254	31,136	4,560	4,042	101	18	39

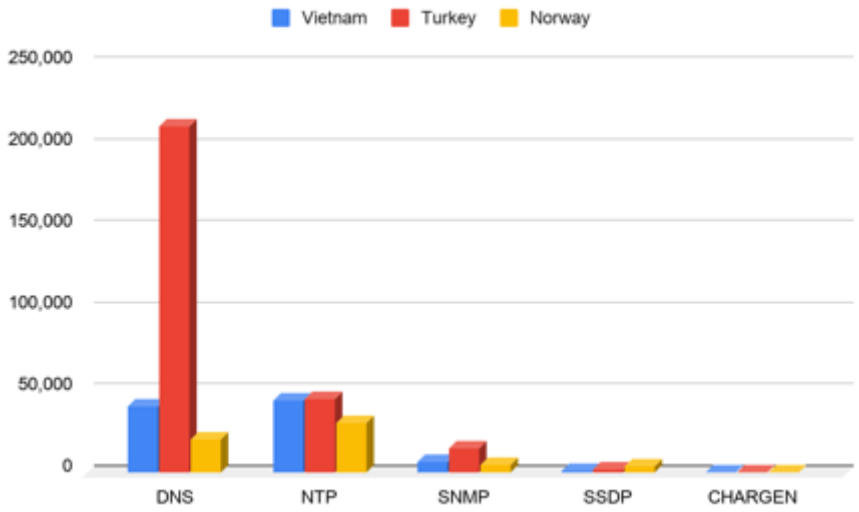


Figure 74: Comparison of raw count of open services

As the figure and table above show, Vietnam ranks less favorably than Norway and more favorably than Turkey with respect to its DDoS exposure. Turkey's standing is largely driven by the country's high open DNS count, which is the ninth highest in the world. Because NTP has a high amplification factor, it can and should be a point of priority for mitigation for many countries.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open services, determining their owners, and encouraging those owners to enact more rigorous defenses.

ISP ANALYSIS

Table 49 shows the top five ISPs that host the greatest number of open services in Vietnam. In some cases, there are ISPs that are listed in the top five across multiple services. This table should ultimately help policymakers focus their outreach efforts on specific ISPs.

Table 49: Top five ISP contributors per service

ISP	DNS	NTP	SNMP	SSDP	CHARGEN
CMC Telecom Infrastructure Company	5	4			2
NhanHoa Software company	4				5
Saigon Postel Corporation		5	5		
SCTV			2	5	
The Corporation for Financing & Promoting Technology (FPT)	3	3	4	3	3

Viettel Group	2	1	3	2	4
VNPT Corp	1	2	1	1	1
VTC				4	

Legend:

There are several ISPs that have high contribution counts across the five services analyzed. Among them are: VNPT, Viettel, The Corporation for Financing & Promoting Technology (FPT), SCTV, and CMC Telecom Infrastructure Company. If Vietnamese authorities collaborated with these ISPs to launch a mitigation campaign, there could be substantial improvement of Vietnam's risk exposure.

A detailed breakdown of ISP contribution for each of the five open services in Vietnam is provided in Appendix J.

EMAIL INFRASTRUCTURE ANALYSIS

The following analysis on email infrastructure is based on the results for the domains located in Vietnam. It should be noted that the list of domains is not complete. The information provided is based on 1,928 domains.

DMARC

Figure 75 shows DMARC policy implementation for the domains in Vietnam.

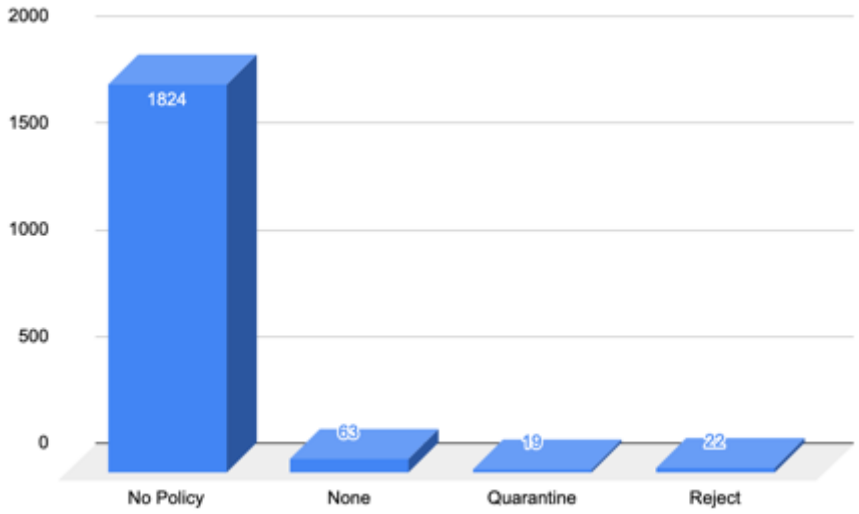


Figure 75: DMARC policy implementation in Vietnam

Overall, a total of 104 out of 1,928 domains have DMARC implemented at some level, with the majority being set to policy level of none (63). Of the 104 domains, twelve domains do not have reporting enabled. What is of concern here is that these domains are set to the DMARC policy level of none, which does not provide any level of protection. The purpose of level “none” is simply to enable reporting and review the reports that are being generated; it does not do any filtering or actually enforce DMARC. DMARC reporting must be enabled to determine if the authentication and authorization mechanisms for the domain are set up properly. If setup correctly, then the DMARC policy for the domain can be adjusted to a level that allows for enforcement and protection of the domain: "quarantine" and "reject" Only having a policy of “none” with no reporting enabled does not protect a domain or brand, and does not prevent the use of a domain in phishing campaigns. The remaining domains are set to either "quarantine" (19) or "reject" (22).

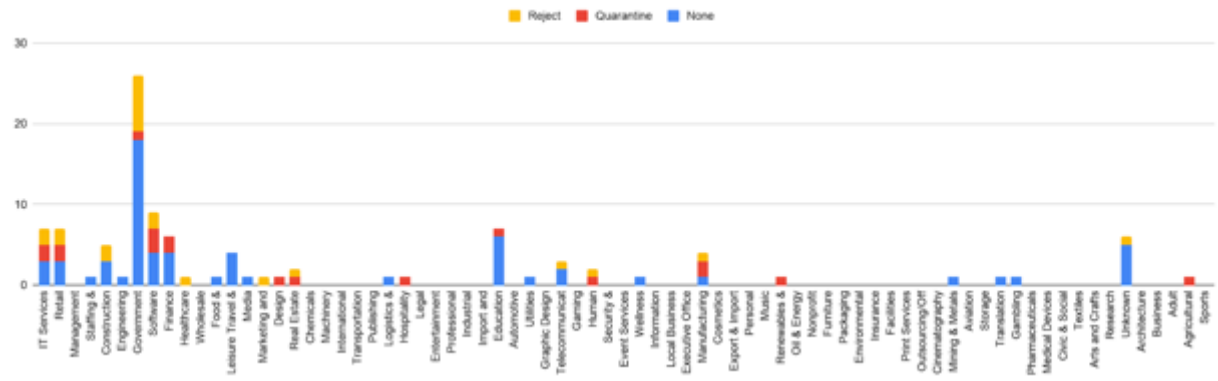


Figure 76: DMARC Implementation by sector

Figure 76 shows the breakdown of the sectors that have implemented DMARC based on the 1,928 observed domains. The domains that have no DMARC policy were excluded to allow for

easier viewing. The adoption rate is good based on the data available, as quite a few sectors are adopting DMARC. The Government sector is showing the strongest adoption of DMARC.

SENDER POLICY FRAMEWORK

SPF is an authorization mechanism used by recipient systems to determine if email messages are coming from an authorized system. A majority of the domains in Vietnam are not using SPF. Even though SPF on its own is not fully secure. It is a mechanism which does help to secure email and should be implemented alongside DMARC and DKIM.

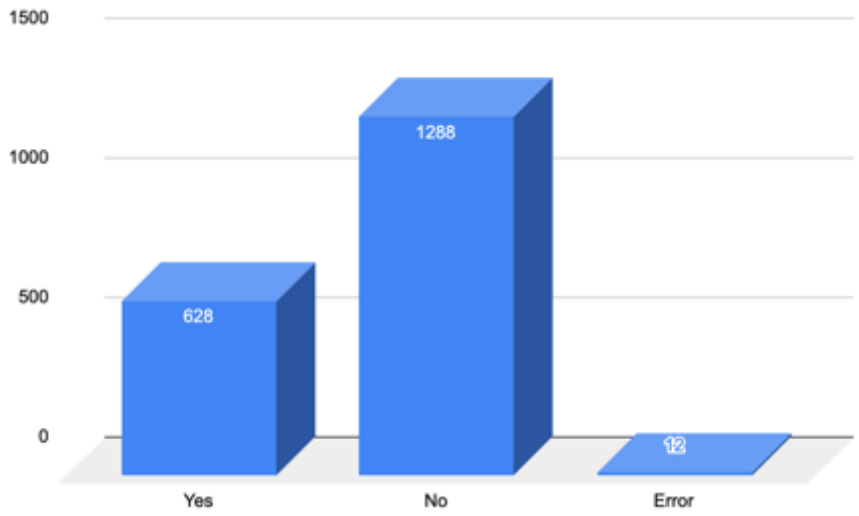


Figure 77: SPF Implementation in Vietnam

There are 14 domains that have implemented SPF as follows: “v=spf1 -all”. This means that there are no systems allowed to send messages using their domain. This is good, but would be better if DMARC was implemented alongside the policy level of “reject”. The reason being that more than 80% of consumer mailboxes (based on Valimail reports) are using DMARC verification. If a DMARC policy were to be implemented along with the current SPF record, then the domain would be better secured and decrease the chances of the delivery of fraudulent messages.

There are 12 domains that have implemented SPF incorrectly by leaving out a critical tag ("all") which defines whether or not an email message is considered failed or not failed.

There are also 58 domains that use the value of "?all" in their SPF record, which is typically not recommended to use. The "?all" stands for neutral, meaning that messages do not pass or fail the SPF authentication check. The recommended value is either "-all" (hard fail) or "~all" (soft fail). There is one domain that has an all tag, just missing the -/~/?/+ before it. One of these must be present to complete the tag and allow for the record to function.

DMARC AND SPF

Table 50 shows the number of domains with a DMARC policy along with how many of those domains have an SPF record present.

Table 50: DMARC and SPF implementation in Vietnam

Policy Level	DMARC	SPF
No Policy	1824	529
None	63	58
Quarantine	19	19
Reject	22	22

It is not always expected to have an SPF record when starting with a DMARC policy of “none”. In this case, five domains with a DMARC policy of “none”, do not have SPF records. This is allowed because the DMARC policy of “none” does not block any messages (fraudulent or legitimate). Most organizations will add the SPF record after reviewing the information presented in the DMARC reports. The DMARC reports can help to build and adjust SPF records.

The best course of action would be to start the implementation of a DMARC policy at level “reject” for all public domains that are not being used for email. This may be able to be done for the 1290 domains that do not have an SPF record, as well as the 14 domains that have implemented SPF as follows: “v=spf1 -all”. This will provide immediate protection and help ensure that these domains cannot be used for fraudulent email activity. It is important to confirm whether or not the 1290 domains are being used for email or not before implementing a DMARC policy of “reject” as legitimate messages could be blocked. Then, DMARC should be implemented at a policy level “none” on the domains that are used for email (1824 records that do not have DMARC). DMARC reports should be reviewed, appropriate adjustments should be made to SPF and/or DKIM and, gradually, DMARC enforcement levels of “quarantine” and ultimately “reject” should be implemented.

There are 12 domains that have implemented SPF incorrectly by leaving out a critical tag (“all”) which defines whether or not an email message is considered failed or not failed. Those domains are:

Domain	SPF Value
dinhdoclap.gov.vn	v=spf1 include=_spf.idcmn.vnptdata.vn
eza-binhphuoc.gov.vn	v=spf1 mx

iic.vn	v=spf1 mx
ita-trans.com.vn	v=spf1 include=_spf.idcmn.vnptdata.vn
mekong-energy.com	v=spf1 a mx a=mail.mekong-energy.com mx=mail.mekong-energy.com include=dnsexit.com ip4=203.162.101.198/32 ip4=203.162.103.26
moc.gov.vn	v=spf1 mx a ip4=203.113.135.30
moit.gov.vn	v=spf1 mx a ip4=103.9.0.52/32
ntsc.gov.vn	v=spf1 mx a ip4=103.19.99.42/32
quangnam.gov.vn	v=spf1 a mx ip4=203.162.31.186 all
thanhnamgroup.com.vn	v=spf1 mx
vietnamobile.com.vn	v=spf1 mx a ip4=202.172.4.15/32
vksbinhduong.gov.vn	v=spf1 a mx ptr ip4=113.161.160.186 a=vksbinhduong.gov.vn mx=mail.vksbinhduong.gov.vnmx:vksbinhduong.gov.vn include=vksbinhduong.gov.vn

The “all“ tag is required in order for SPF to work correctly. The appropriate entry would be to include “-all” (hard fail) or “~all” (soft fail) to the end of each SPF record.

ROUTING INFRASTRUCTURE ANALYSIS

There are 34 observed ASNs headquartered in Vietnam. Together, they advertise 6218 IPv4 and 1114 IPv6 prefixes.

Two of Vietnam’s ASNs advertise ROAs, while the remaining 32 ASNs advertise none.

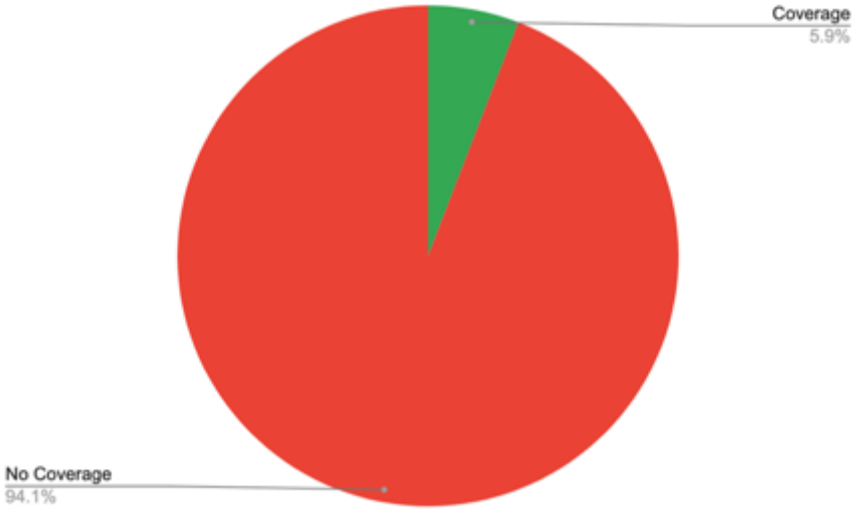


Figure 78: ROA Coverage in Vietnam (by ASN)

Of the advertised prefixes, 2093 IPv4 and 66 IPv6 prefixes are covered by valid ROAs, together constituting 29.45% of Vietnam's prefixes. A further 17 IPv4 prefixes are covered by invalid ROAs, constituting 0.23% of the total.

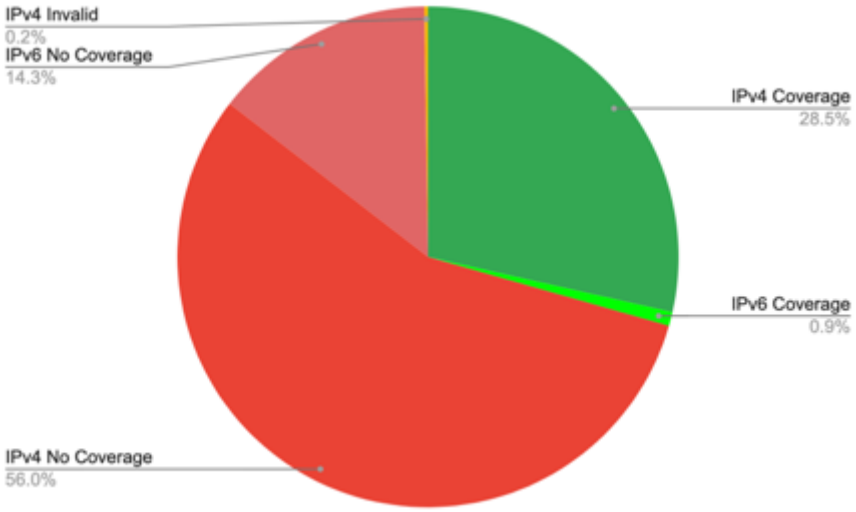


Figure 79: ROA Coverage in Vietnam (by advertised prefix)

The invalid ROAs are being advertised by two ASNs. Two different validation errors were observed:

1. The ASN is authorized to originate a prefix, but is announcing a sub-prefix of the authorized prefix instead of the authorized prefix. There were 17 IPv4 prefixes with

errors of this kind. This is a relatively less serious error, as the ASN is authorized to originate the covering prefix.

2. The ASN is not authorized to originate a prefix. There were 17 IPv4 prefixes with errors of this kind. This is a serious error, as the ASN is announcing a prefix that it is not authorized for.

Figure 80: Invalid ROAs in Vietnam

The adoption of RPKI in Vietnam is very limited and there are some issues with invalid ROAs. There should be outreach to come to a determination as to why these invalid announcements have occurred and to determine whether these invalid routing announcements are due to configuration errors or due to the lack of acting upon routes that the ASN is not authorized to announce. Also, outreach and training should be done to increase the adoption of RPKI across additional ASNs and to get them all into a state of routing security best-practices conformance.

APPENDIX A: DETAILED ISP CONTRIBUTION IN BRUNEI

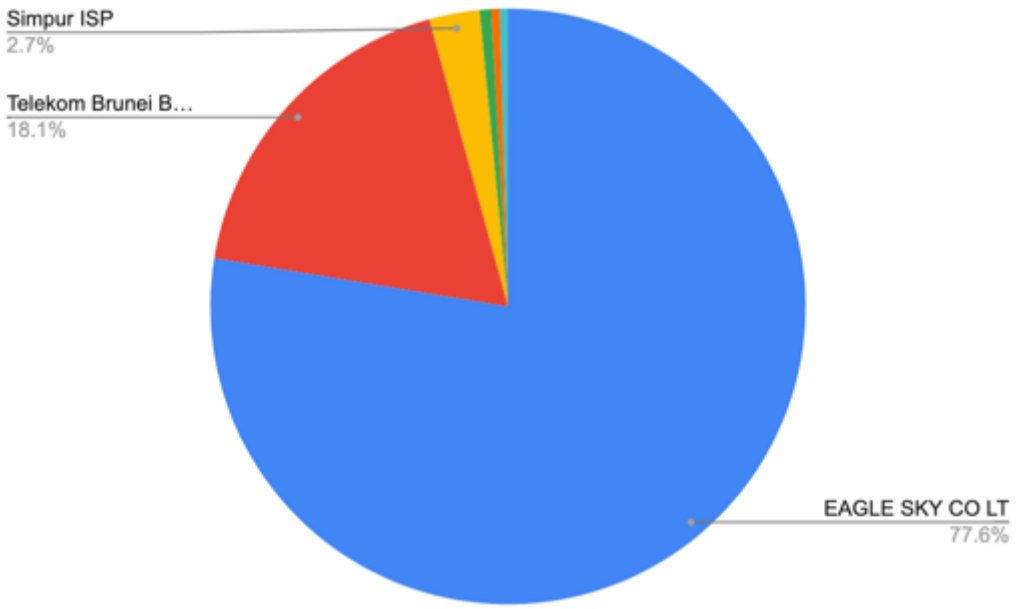
The following rankings and charts provide insight into the ISPs that host the greatest number of open services in Brunei. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the most prevalent of those risks in Brunei. Of the 656 open DNS services nationwide, all of them (100%) are hosted by the ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	EAGLE SKY CO LT	509	Telecom	Philippines
2	Telekom Brunei Berhad	119	Telecom	Brunei
3	Simpur ISP	18	Unknown	Brunei
4	EGNC (E-Government National Centre)	4	Gov	Brunei
5	Progresif Cellular Sdn Bhd	3	Telecom	Brunei
6	M247 Ltd	3	Telecom	United Kingdom

The pie graph below illustrates, among those 656 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with these ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.

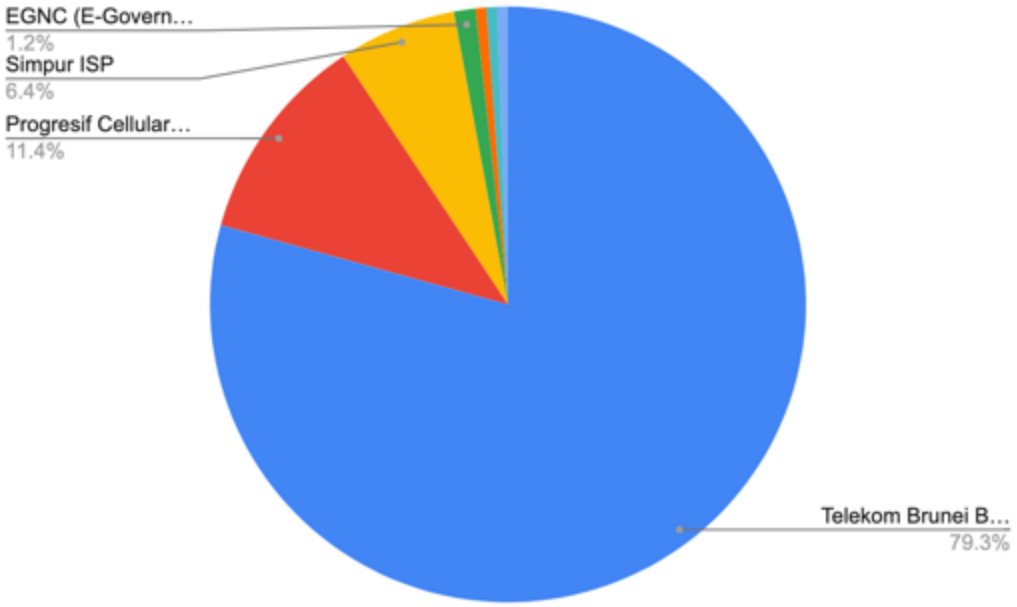


MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the second most prevalent of those risks in Brunei. Of the 343 open NTP services nationwide, all of them (100%) are hosted by the ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Telekom Brunei Berhad	272	Telecom	Brunei
2	Progresif Cellular Sdn Bhd	39	Telecom	Brunei
3	Simpur ISP	22	Unknown	Brunei
4	EGNC (E-Government National Centre)	4	Gov	Brunei
5	Bruhaas (B) Sdn Bhd	2	Telecom	Brunei
6	M247 Ltd	2	Telecom	United Kingdom
7	EAGLE SKY CO LT	2	Telecom	Philippines

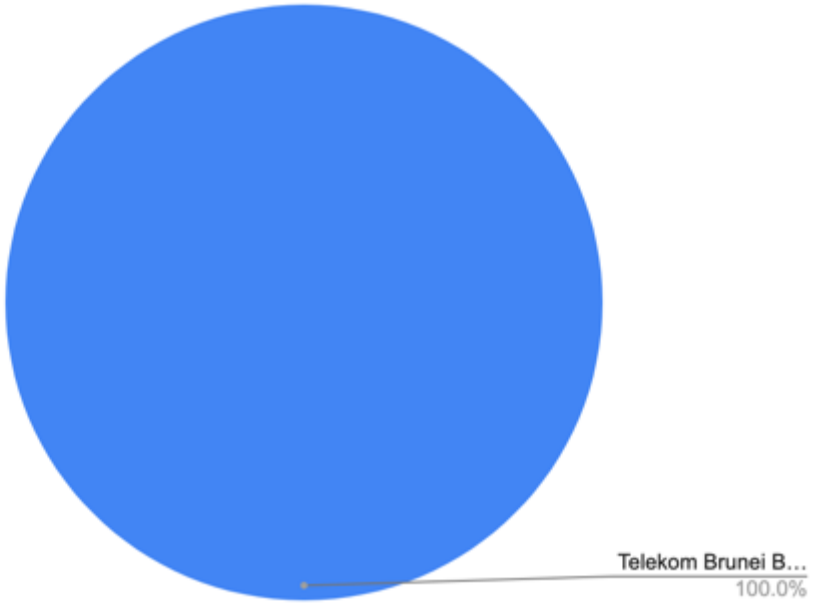
The pie graph below illustrates, among those 343 open DNS services quantified in the table above, the contribution of each ISP. Beginning a mitigation campaign by reaching out and collaborating with these ISPs could result in a substantial reduction of potential DDoS infrastructure.



MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the fourth most prevalent of those risks in Brunei. Of the 7 open SNMP services nationwide, all of them (100%) are hosted by the Bruneian ISP listed in the table below.

Rank	ISP	Count	Allocated Country
1	Telekom Brunei Berhad	7	Brunei

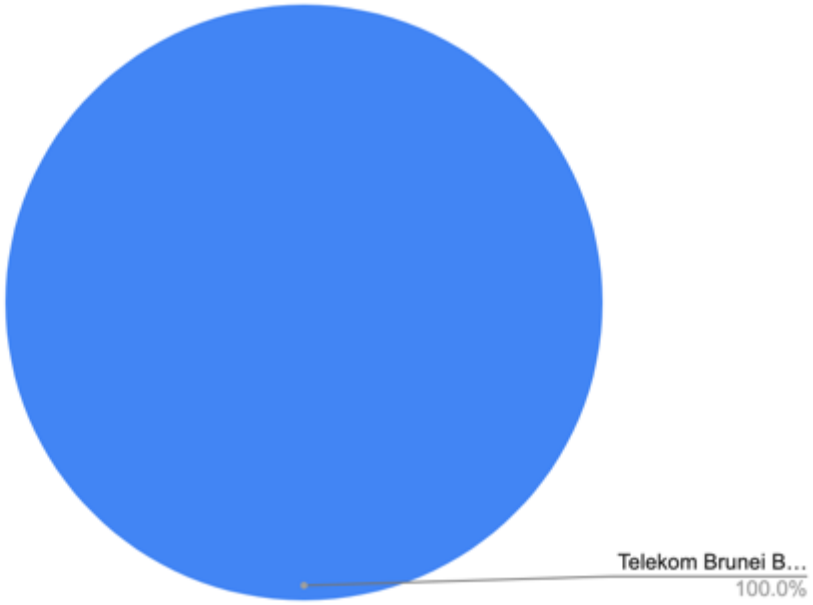


Reaching out and collaborating with this ISP to mitigate could result in a reduction of potential DDoS infrastructure.

MAJOR SSDP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SSDP is the third most prevalent of those risks in Brunei. Of the 10 open SSDP services nationwide, all of them (100%) are hosted by the Bruneian ISP listed in the table below.

Rank	ISP	Count	Allocated Country
1	Telekom Brunei Berhad	10	Brunei

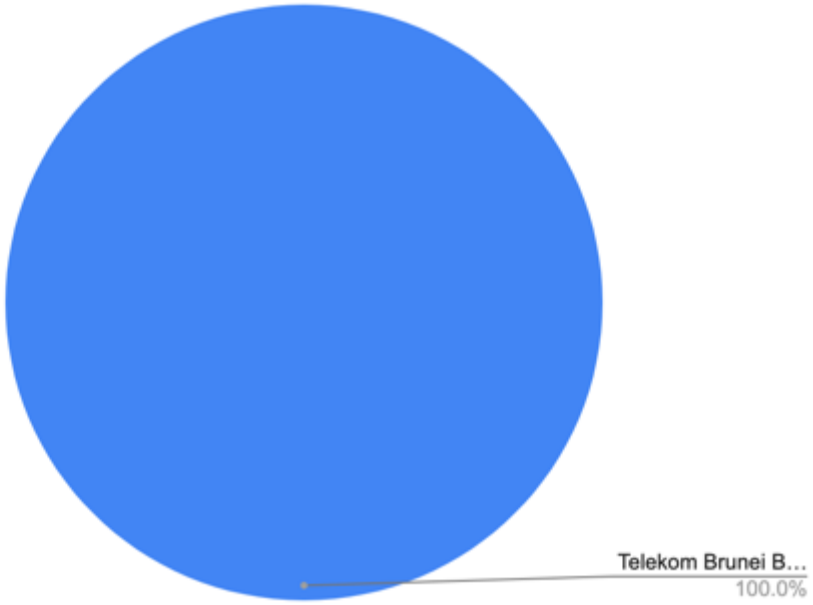


Reaching out and collaborating with this ISP to mitigate could result in a reduction of potential DDoS infrastructure.

MAJOR CHARGEN CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, CHARGEN is the least prevalent of those risks in Brunei. Of the 3 open CHARGEN services nationwide, all of them (100%) are hosted by the Bruneian ISP listed in the table above.

Rank	ISP	Count	Allocated Country
1	Telekom Brunei Berhad	3	Brunei



Reaching out and collaborating with this ISP to mitigate could result in a reduction of potential DDoS infrastructure.

APPENDIX B: DETAILED ISP CONTRIBUTION IN CAMBODIA

The following rankings and charts provide insight into the ISPs that host the greatest number of open services in Cambodia. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

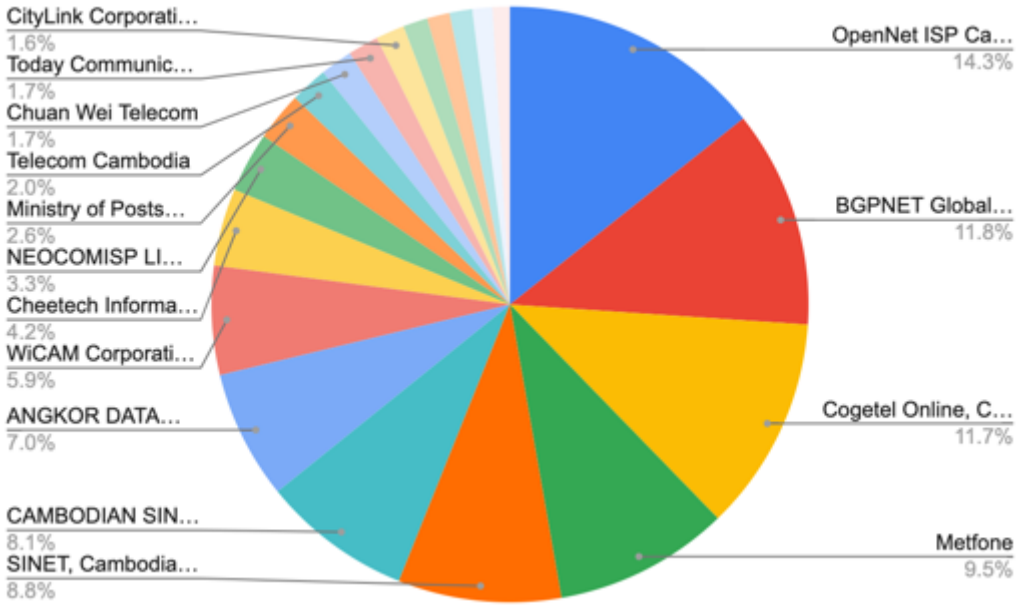
MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the second most prevalent of those risks in Cambodia. Of the 2748 open DNS services nationwide, 2117 of them (77%) are hosted by the top twenty ISPs listed in the table above.

Rank	ISP	Count	Type	Allocated Country
1	OpenNet ISP Cambodia	302	Telecom	Cambodia
2	BGPNET Global ASN	250	Cloud	Singapore
3	Cogetel Online, Cambodia, ISP	247	Telecom	Cambodia

4	Metfone	201	Telecom	Cambodia
5	SINET, Cambodia's specialist Internet and Telecom Service Provider.	187	Telecom	Cambodia
6	CAMBODIAN SINGMENG TELEMEDIA CO., LTD (Digi/SingMeng)	172	Telecom	Cambodia
7	ANGKOR DATA COMMUNICATION (Mekong)	148	Telecom	Cambodia
8	WiCAM Corporation Ltd.	125	Telecom	Cambodia
9	Cheetech Information Technology Co., Ltd.	89	Unknown	Cambodia
10	NEOCOMISP LIMITED, IPTX Transit and Network Service Provider in Cambodia.	69	Cloud	Cambodia
11	Ministry of Posts and Telecommunication	56	Gov	Cambodia
12	Telecom Cambodia	43	Telecom	Cambodia
14	Chuan Wei Telecom	37	Telecom	Cambodia
15	Today Communication Co.,Ltd	35	Telecom	Cambodia
16	CityLink Corporation, LTD	33	Telecom	Cambodia
17	CAMINTEL, National Telecommunication Provider, Phnom Penh, Cambodia	28	Telecom	Cambodia
18	Maximum Business Information Technology (MaxBIT)	26	Telecom	Cambodia
19	SOUTH EAST ASIA TELECOM (Cambodia) Co., LTD (yes)	26	Telecom	Cambodia
20	Fast CDN	23	Cloud	Cambodia
19	Cambo.Host Ltd Phnom Penh	20	Cloud	Cambodia

The pie graph below illustrates, among those 2117 open DNS services quantified in the table above, the contribution of each ISP. Beginning a mitigation campaign by reaching out and collaborating with the top 5 ISPs could result in a substantial reduction of potential DDoS infrastructure.



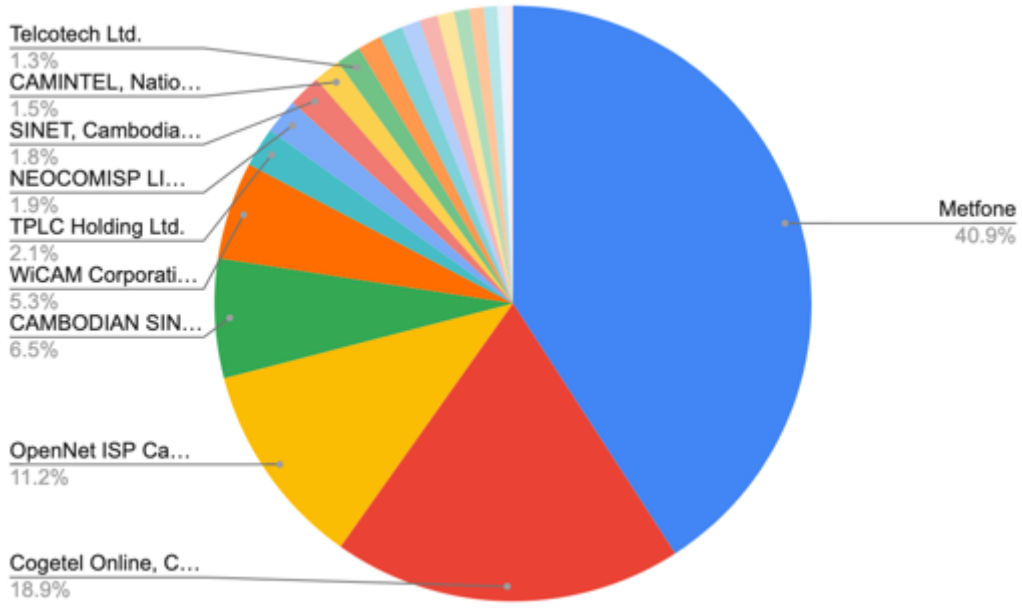
MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the most prevalent of those risks in Cambodia with the highest amplification factor. Of the 8871 open NTP services nationwide, 8665 of them (98%) are hosted by the top twenty Cambodian ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Metfone	3540	Telecom	Cambodia
2	Cogetel Online, Cambodia, ISP	1641	Telecom	Cambodia
3	OpenNet ISP Cambodia	967	Telecom	Cambodia
4	CAMBODIAN SINGMENG TELEMEDIA CO., LTD (Digi/SingMeng)	561	Telecom	Cambodia
5	WiCAM Corporation Ltd.	459	Telecom	Cambodia
6	TPLC Holding Ltd.	186	Telecom	Cambodia
7	NEOCOMISP LIMITED, IPTX Transit and Network Service Provider in Cambodia.	166	Cloud	Cambodia
8	SINET, Cambodia's specialist Internet and Telecom Service Provider.	153	Telecom	Cambodia
9	CAMINTEL, National Telecommunication Provider,	128	Telecom	Cambodia

	Phnom Penh, Cambodia			
10	Telcotech Ltd.	116	Cloud	Cambodia
11	PPCTV broadband service is the first cable and DSL internet in Cambodia	111	Telecom	Cambodia
12	Chuan Wei Telecom	110	Telecom	Cambodia
13	SOUTH EAST ASIA TELECOM (Cambodia) Co., LTD (yes)	88	Telecom	Cambodia
14	Chubu Telecommunications Company, Inc.	84	Telecom	Japan
15	Telecom Cambodia	80	Telecom	Cambodia
16	CAMKOM CABLE TV CO, LTD.	71	Cloud	Cambodia
17	Today Communication Co.,Ltd	67	Telecom	Cambodia
18	CityLink Corporation, LTD	64	Telecom	Cambodia
19	ANGKOR E & C (CAMBODIA) Co.,Ltd.	37	Cloud	Cambodia
20	CAMGSM Company Ltd	36	Telecom	Cambodia

The pie graph below illustrates, among those 8665 open NTP services quantified in the table above, the contribution of each ISP. Beginning a mitigation campaign by reaching out and collaborating with the top 5 ISPs could result in a substantial reduction of potential DDoS infrastructure.

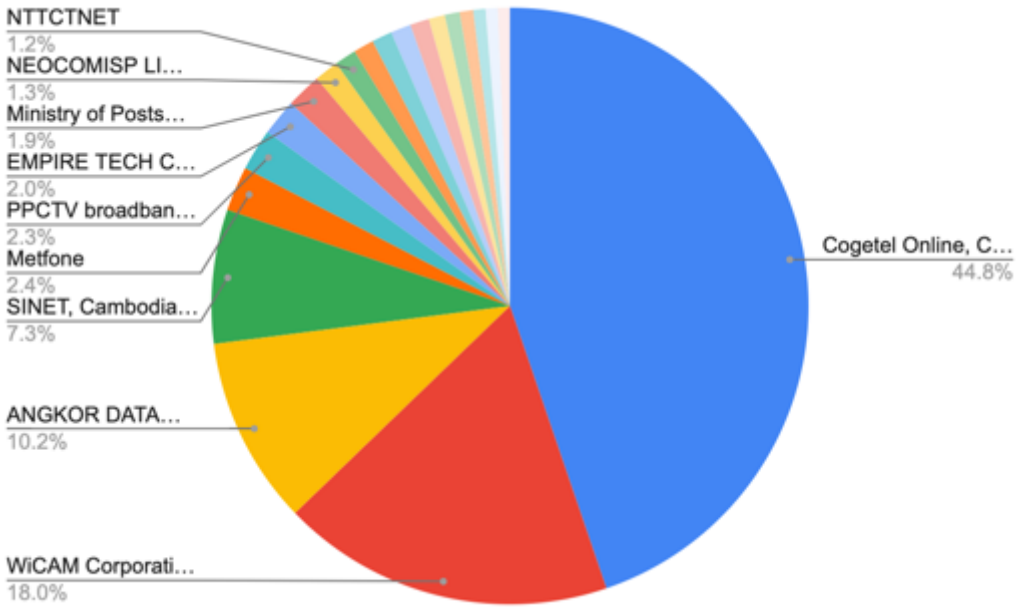


MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the third most prevalent of those risks in Cambodia. Of the 1436 open SNMP services nationwide, 1365 of them (95%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Cogetel Online, Cambodia, ISP	611	Telecom	Cambodia
2	WiCAM Corporation Ltd.	246	Telecom	Cambodia
3	ANGKOR DATA COMMUNICATION	139	Telecom	Cambodia
4	SINET, Cambodia's specialist Internet and Telecom Service Provider.	99	Telecom	Cambodia
5	Metfone	33	Telecom	Cambodia
6	PPCTV broadband service is the first cable and DSL internet in Cambodia	31	Telecom	Cambodia
7	EMPIRE TECH Co., Ltd.	27	Unknown	Cambodia
8	Ministry of Posts and Telecommunication	26	Gov	Cambodia
9	NEOCOMISP LIMITED, IPTX Transit and Network Service Provider in Cambodia.	18	Cloud	Cambodia
10	NTTCTNET	16	Cloud	Thailand
11	BigHub Co.,Ltd	15	Unknown	Cambodia
12	OpenNet ISP Cambodia	15	Telecom	Cambodia
13	CAMINTEL, National Telecommunication Provider, Phnom Penh, Cambodia	15	Telecom	Cambodia
14	iOne Co., Ltd	14	Cloud	Cambodia
15	TELNET CO.,LTD	12	Cloud	Cambodia
16	CAMBODIAN SINGMENG TELEMEDIA CO., LTD (Digi/SingMeng)	11	Telecom	Cambodia
17	KH77-NET CO., LTD	10	Unknown	Cambodia
18	Maximum Business Information Technology (MaxBIT)	9	Telecom	Cambodia
19	Telecom Cambodia	9	Telecom	Cambodia
20	FAST ONE (CAMBODIA) CO., LTD (ultraNET)	9	Telecom	Cambodia

The pie graph below illustrates, among those 1365 open SNMP services quantified in the table above, the contribution of each ISP. Beginning a mitigation campaign by reaching out and collaborating with the top 5 ISPs could result in a substantial reduction of potential DDoS infrastructure.



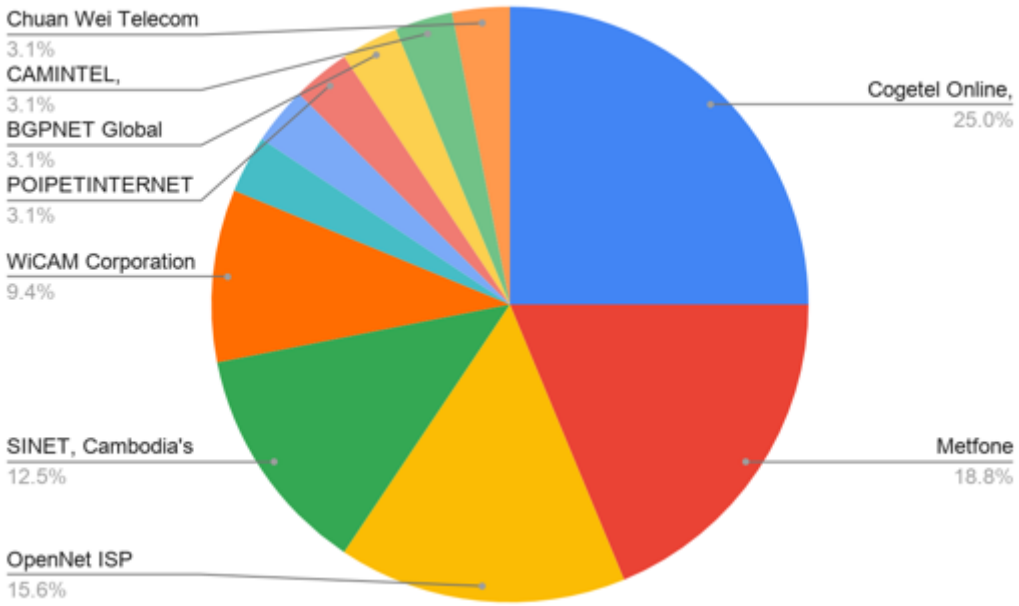
MAJOR SSDP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SSDP is the fourth most prevalent of those risks in Cambodia. Of the 32 open SSDP services nationwide, all of them (100%) are hosted by the 11 ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Cogetel Online, Cambodia, ISP	8	Telecom	Cambodia
2	Metfone	6	Telecom	Cambodia
3	OpenNet ISP Cambodia	5	Telecom	Cambodia
4	SINET, Cambodia's specialist Internet and Telecom Service Provider.	4	Telecom	Cambodia
5	WiCAM Corporation Ltd.	3	Telecom	Cambodia
6	CityLink Corporation, LTD	1	Telecom	Cambodia

7	Telecom Cambodia	1	Telecom	Cambodia
8	POIPETINTERNET DOT COM	1	Telecom	Cambodia
9	BGPNET Global ASN	1	Cloud	Singapore
10	CAMINTEL, National Telecommunication Provider, Phnom Penh, Cambodia	1	Telecom	Cambodia
11	Chuan Wei Telecom	1	Telecom	Cambodia

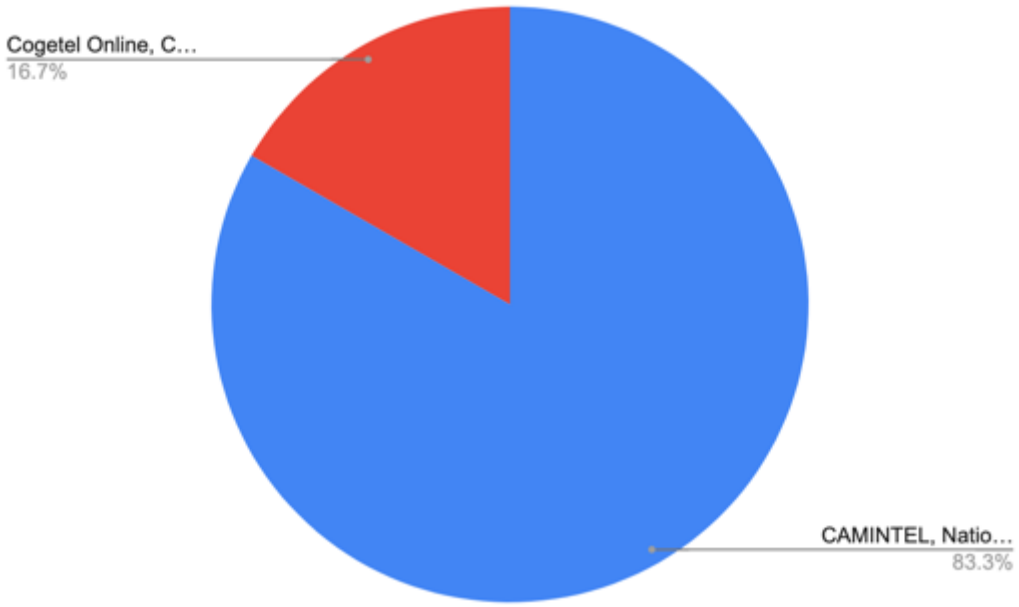
The pie graph below illustrates, among those 32 open SSDP services quantified in the table above, the contribution of each ISP. Beginning a mitigation campaign by reaching out and collaborating with the top 5 ISPs could result in a reduction of potential DDoS infrastructure.



MAJOR CHARGEN CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, CHARGEN is the least prevalent of those risks in Cambodia. Of the 12 open CHARGEN services nationwide, all of them (100%) are hosted by the two Cambodian ISPs listed in the table below.

Rank	ISP	Count	Allocated Country
1	CAMINTEL, National Telecommunication Provider, Phnom Penh, Cambodia	10	Cambodia
2	Cogetel Online, Cambodia, ISP	2	Cambodia



Reaching out and collaborating with these ISPs to mitigate could result in a reduction of potential DDoS infrastructure.

APPENDIX C: DETAILED ISP CONTRIBUTION IN INDONESIA

The following rankings and charts provide insight into the ISPs that host the greatest number of open services in Indonesia. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

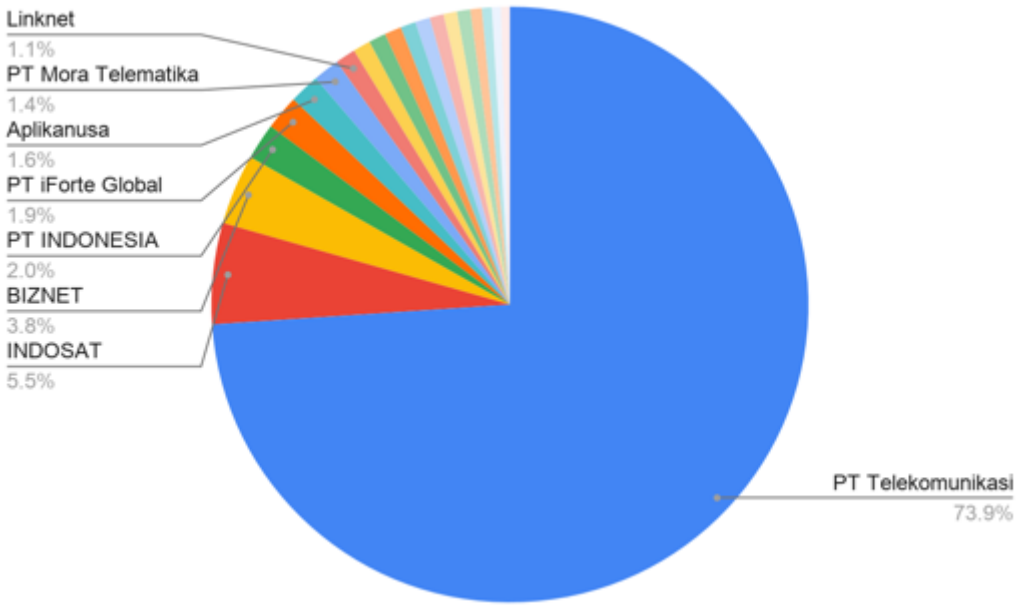
MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the most prevalent of those risks in Indonesia. Of the 124,750 open DNS services nationwide, 101,142 of them (81%) are hosted by the top twenty Indonesian ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	PT Telekomunikasi Indonesia	74780	Telecom	Indonesia
2	INDOSAT	5545	Telecom	Indonesia
3	BIZNET NETWORKS	3861	Telecom	Indonesia
4	PT INDONESIA COMNETS PLUS (ICON +)	1993	Telecom	Indonesia

5	PT iForte Global Internet	1900	Telecom	Indonesia
6	Aplikanusa Lintasarta	1657	Telecom	Indonesia
7	PT Mora Telematika Indonesia	1443	Telecom	Indonesia
8	Linknet	1112	Telecom	Indonesia
9	PT. Pasifik Satelit Nusantara	962	Telecom	Indonesia
10	PT Maxindo Mitra Solusi	933	Telecom	Indonesia
11	PT. Arjuna Global Teknologi Indonesia	926	Telecom	Indonesia
12	PT Netciti Persada	834	Telecom	Indonesia
13	Varnion Technology Semesta, PT	809	Telecom	Indonesia
14	PT. DIGITAL NETWORK ANTANUSA (DNA.net)	765	Telecom	Indonesia
15	Media Antar Nusa PT.	739	Telecom	Indonesia
16	PT CITRA INFOMEDIA	727	Unknown	Indonesia
17	PT Cyberindo Aditama	625	Telecom	Indonesia
18	PT. HIPERNET INDODATA	542	Telecom	Indonesia
19	ARDH GLOBAL INDONESIA, PT	496	Cloud	Indonesia
20	PT Infinys System Indonesia	493	Cloud	Indonesia

The pie graph below illustrates, among those 101,142 open DNS services quantified in the table above, the contribution of each ISP. With a substantial number of open DNS services contributed by Telekomunikasi Indonesia, outreach to their team and a mitigation campaign with that one ISP alone would result in a substantial reduction of potential DDoS infrastructure



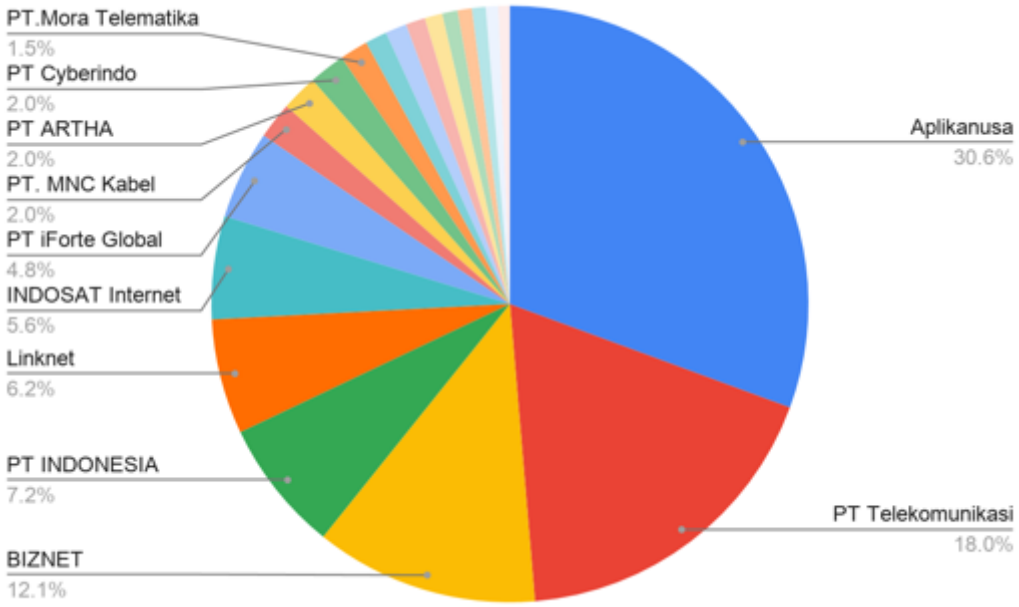
MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the third most prevalent of those risks in Indonesia with the highest amplification factor. Of the 48,529 open NTP services nationwide, 36,744 of them (76%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Aplikanusa Lintasarta	11257	Telecom	Indonesia
2	PT Telekomunikasi Indonesia	6623	Telecom	Indonesia
3	BIZNET NETWORKS	4442	Telecom	Indonesia
4	PT INDONESIA COMNETS PLUS (ICON +)	2638	Telecom	Indonesia
5	Linknet	2294	Telecom	Indonesia
6	INDOSAT	2052	Telecom	Indonesia
7	PT iForte Global Internet	1762	Telecom	Indonesia
8	PT. MNC Kabel Mediacom	727	Telecom	Indonesia
9	PT ARTHA TELEKOMINDO	725	Cloud	Indonesia
10	PT Cyberindo Aditama	720	Cloud	Indonesia
11	PT.Mora Telematika Indonesia	563	Telecom	Indonesia
12	PT. NTT Indonesia	435	Cloud	Indonesia
13	Alibaba (US) Technology Co., Ltd.	425	Cloud	United States

14	PT. Usaha Adisanggoro	387	Cloud	Indonesia
15	DTPNET NAP	352	Cloud	Indonesia
16	Telemedia Dinamika Sarana, PT (gasnet)	305	Telecom	Indonesia
17	Hutchison CP Telecommunications, PT (3)	285	Telecom	Indonesia
18	PT. NAP Info Lintas Nusa	274	Cloud	Indonesia
19	PT Infinys System Indonesia	248	Cloud	Indonesia
20	Sekretariat Daerah Kota Salatiga	230	Gov	Indonesia

The pie graph below illustrates, among those 36,744 open NTP services quantified in the table above, the contribution of each ISP. Beginning a mitigation campaign by reaching out and collaborating with the top 5 ISPs could result in a substantial reduction of potential DDoS infrastructure.



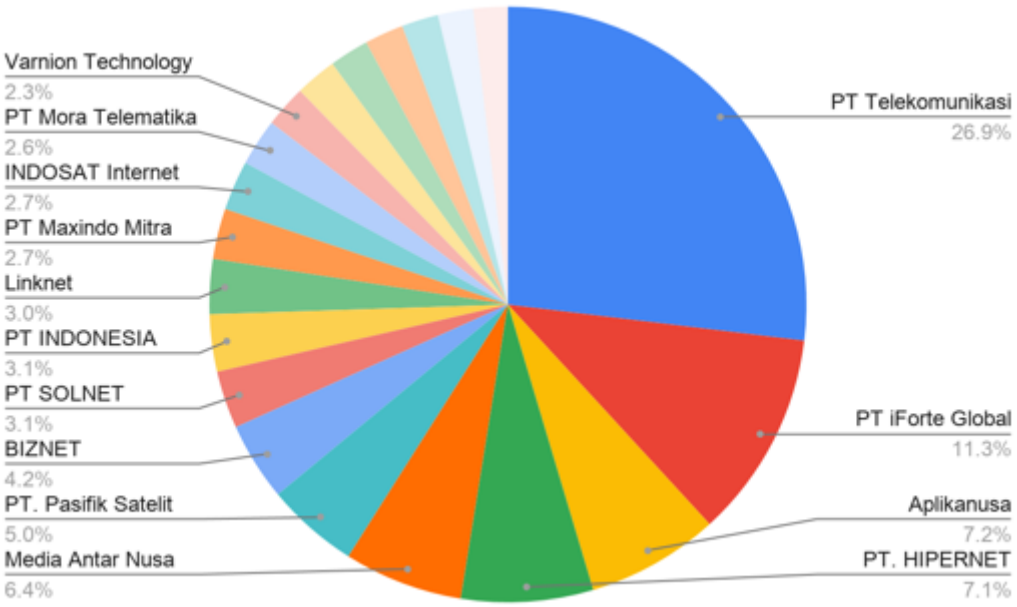
MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the second most prevalent of those risks in Indonesia. Of the 52,527 open SNMP services nationwide, 27,423 of them (52%) are hosted by the top twenty Indonesian ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	PT Telekomunikasi Indonesia	7386	Telecom	Indonesia

2	PT iForte Global Internet	3088	Telecom	Indonesia
3	Aplikanusa Lintasarta	1972	Telecom	Indonesia
4	PT. HIPERNET INDODATA	1958	Telecom	Indonesia
5	Media Antar Nusa PT.	1768	Telecom	Indonesia
6	PT. Pasifik Satelit Nusantara	1379	Telecom	Indonesia
7	BIZNET NETWORKS	1165	Telecom	Indonesia
8	PT SOLNET INDONESIA	856	Telecom	Indonesia
9	PT INDONESIA COMNETS PLUS (ICON +)	853	Telecom	Indonesia
10	Linknet	815	Telecom	Indonesia
11	PT Maxindo Mitra Solusi	753	Telecom	Indonesia
12	INDOSAT	738	Telecom	Indonesia
13	PT Mora Telematika Indonesia	701	Telecom	Indonesia
14	Varnion Technology Semesta, PT	627	Telecom	Indonesia
15	PT DES Teknologi Informasi	619	Telecom	Indonesia
16	Padi Internet	584	Telecom	Indonesia
17	PT Cyberindo Aditama	579	Cloud	Indonesia
18	Tele Globe Global, PT	547	Cloud	Indonesia
19	INDO Internet, PT	521	Cloud	Indonesia
20	PT Solusi Aksesindo Pratama	514	Cloud	Indonesia

The pie graph below illustrates, among those 27,423 open SNMP services quantified in the table above, the contribution of each ISP. Beginning a mitigation campaign by reaching out and collaborating with the top 5 ISPs could result in a substantial reduction of potential DDoS infrastructure.



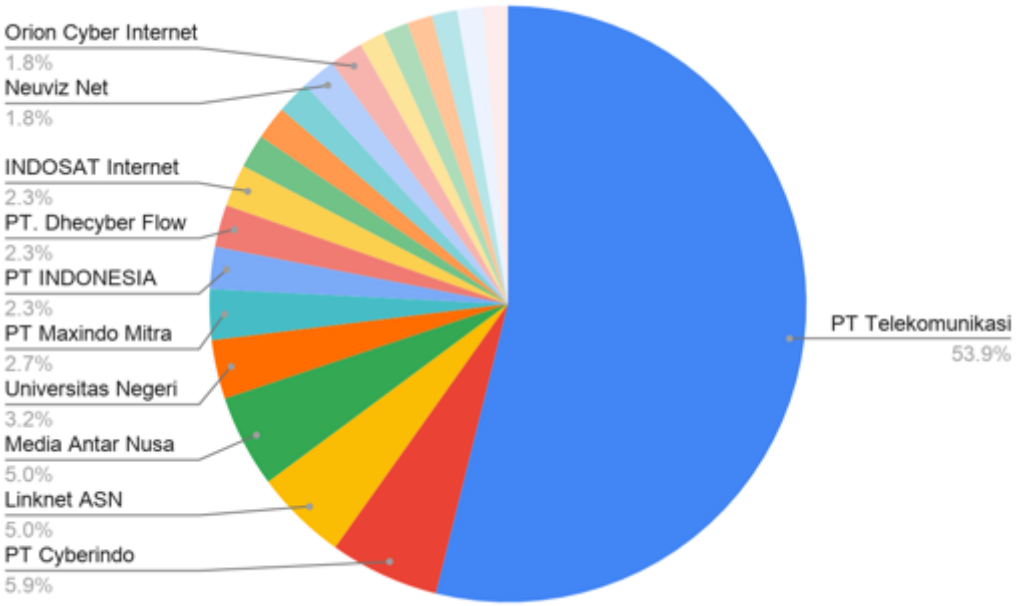
MAJOR SSDP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SSDP is the fourth most prevalent of those risks in Indonesia. Of the 231 open SSDP services nationwide, 219 (95%) are hosted by the top twenty Indonesian ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	PT Telekomunikasi Indonesia	118	Telecom	Indonesia
2	PT Cyberindo Aditama	13	Telecom	Indonesia
3	Linknet	11	Telecom	Indonesia
4	Media Antar Nusa PT.	11	Telecom	Indonesia
5	Universitas Negeri Semarang	7	University	Indonesia
6	PT Maxindo Mitra Solusi	6	Telecom	Indonesia
7	PT INDONESIA COMNETS PLUS (ICON +)	5	Telecom	Indonesia
8	PT. Dhecyber Flow Indonesia	5	Telecom	Indonesia
9	INDOSAT	5	Telecom	Indonesia
10	PT Media Sarana Data (GMedia)	4	Telecom	Indonesia
11	PT Remala Abadi	4	Telecom	Indonesia
12	PT. Eka Mas Republik	4	Telecom	Indonesia

13	Neuviz Net	4	Telecom	Indonesia
14	Orion Cyber Internet	4	Telecom	Indonesia
15	INDO Internet, PT	3	Cloud	Indonesia
16	DTPNET NAP	3	Cloud	Indonesia
17	Transkon Jaya, PT	3	Telecom	Indonesia
18	Melsa-i-net AS	3	Cloud	Indonesia
19	PT. MATRIXNET GLOBAL INDONESIA	3	Telecom	Indonesia
20	PT. Pasifik Satelit Nusantara	3	Telecom	Indonesia

The pie graph below illustrates, among those 219 open SSDP services quantified in the table above, the contribution of each ISP. Beginning a mitigation campaign by reaching out and collaborating with the top 5 ISPs could result in a reduction of potential DDoS infrastructure.



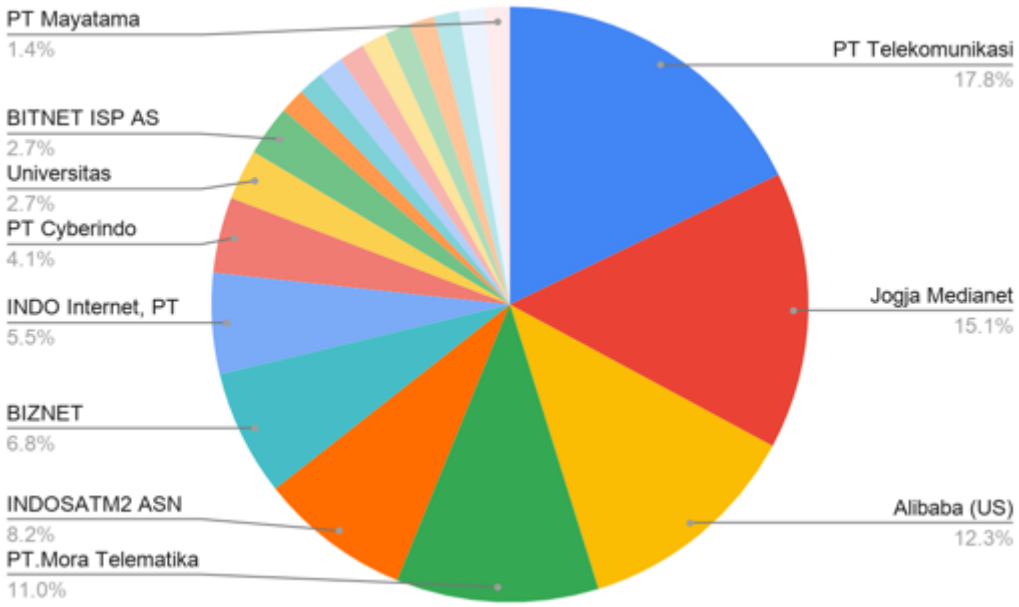
MAJOR CHARGEN CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, CHARGEN is the least prevalent of those risks in Indonesia. Of the 84 open CHARGEN services nationwide, 73 of them (87%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country

1	PT Telekomunikasi Indonesia	13	Telecom	Indonesia
2	Jogja Medianet	11	Telecom	Indonesia
3	Alibaba (US) Technology Co., Ltd.	9	Telecom	United States
4	PT.Mora Telematika Indonesia	8	Telecom	Indonesia
5	INDOSAT	6	Telecom	Indonesia
6	BIZNET NETWORKS	5	Telecom	Indonesia
7	INDO Internet, PT	4	Cloud	Indonesia
8	PT Cyberindo Aditama	3	Telecom	Indonesia
9	Universitas Diponegoro	2	University	Indonesia
10	BITNET ISP AS	2	Telecom	Indonesia
11	PT Citra Jelajah Informatika	1	Telecom	Indonesia
12	PT Bintang Komunikasi Utama	1	Telecom	Indonesia
13	PT. Inet Global Indo	1	Telecom	Indonesia
14	PT Indopratama Teleglobal (ISP)Wisma BSG Floor 6	1	Telecom	Indonesia
15	PT Remala Abadi	1	Telecom	Indonesia
16	PT INDONESIA COMNETS PLUS	1	Telecom	Indonesia
17	ARDH GLOBAL INDONESIA, PT	1	Cloud	Indonesia
18	Badan Meteorologi dan Geofisika	1	Cloud	Indonesia
19	University of Delaware	1	University	United States
20	PT Mayatama Solusindo	1	Telecom	Indonesia

The pie graph below illustrates, among those 73 open CHARGEN services quantified in the table above, the contribution of each ISP. Beginning a mitigation campaign by reaching out and collaborating with the top 5 ISPs could result in a reduction of potential DDoS infrastructure.



APPENDIX D: DETAILED ISP CONTRIBUTION IN LAOS

The following rankings and charts provide insight into the ISPs that host the greatest number of open services in Laos. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

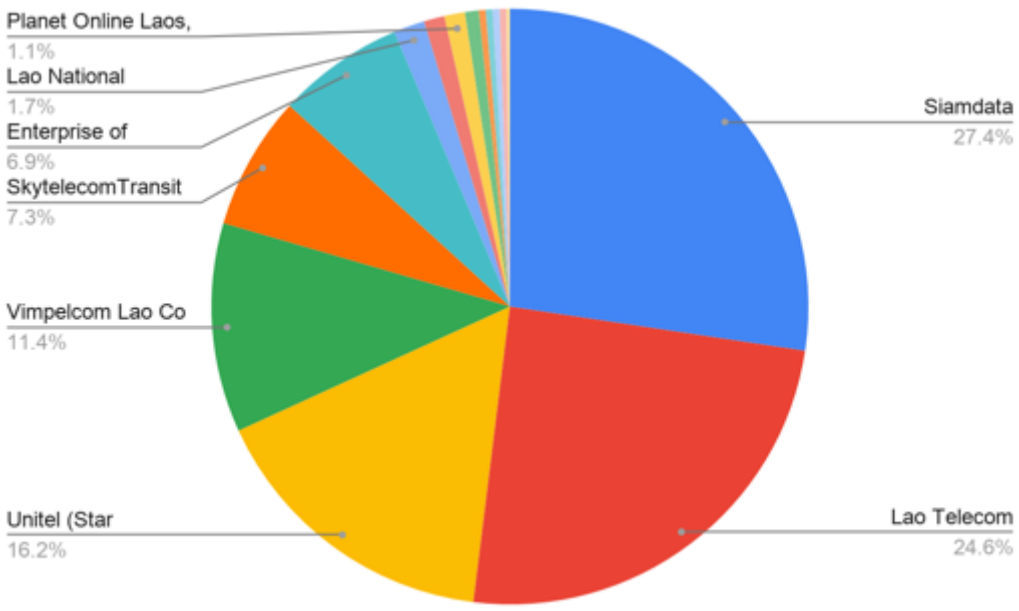
MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the second most prevalent of those risks in Laos. Of the 537 open DNS services nationwide, all of them (100%) are hosted by the ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Siamdata	147	Cloud	Thailand
2	Lao Telecom Communication, LTC	132	Telecom	Laos
3	Unitel (Star Telecom)	87	Telecom	Laos
4	Vimpelcom Lao Co Ltd (VEON)	61	Telecom	Laos
5	SkytelecomTransit provider and ISP in Vientiene.	39	Telecom	Laos
6	Enterprise of Telecommunications Lao	37	Telecom	Laos

7	Lao National Internet Center (LANIC)	9	Cloud	Laos
8	Mangkone Technology Co. Ltd.	6	Cloud	Laos
9	Planet Online Laos, Internet Service Provider in LAO PDR	6	Telecom	Laos
10	LeapSwitch Networks Pvt Ltd	4	Cloud	India
11	S-Tech Development Co., Ltd	2	Cloud	Laos
12	Datacom Sole Co., Ltd	2	Cloud	Laos
13	LERNET at LAOs	2	University	Laos
14	Lao Gateway Co., Ltd	2	Cloud	Laos
15	DE-CORP (Digital Realty data center)	1	Cloud	United States

The pie graph below illustrates, among those 537 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.

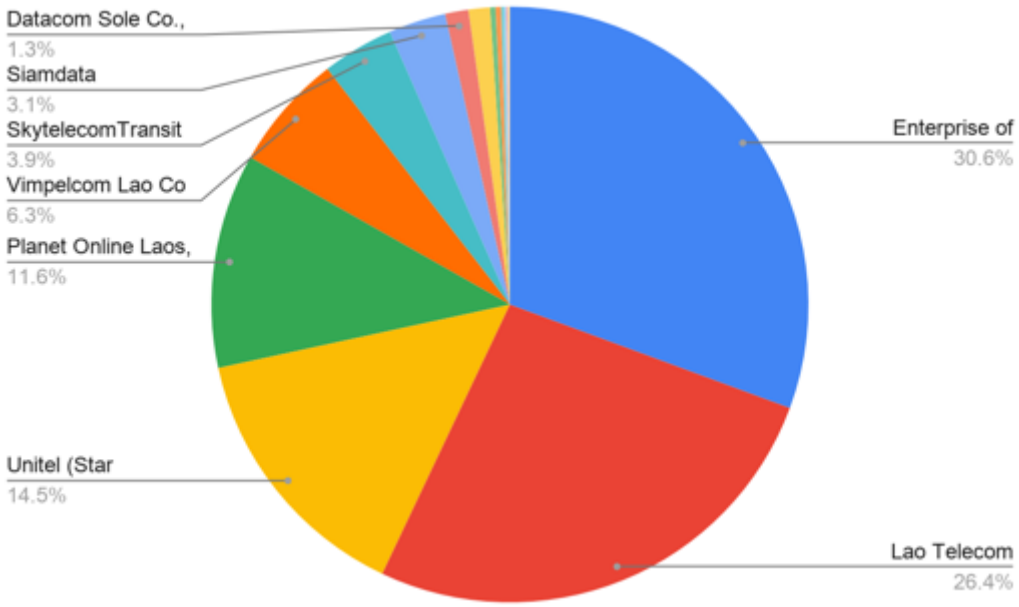


MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the most prevalent of those risks in Laos, and has the highest amplification factor. Of the 1,031 open NTP services nationwide, all of them (100%) are hosted by the ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Enterprise of Telecommunications Lao	316	Telecom	Laos
2	Lao Telecom Communication, LTC	272	Telecom	Laos
3	Unitel (Star Telecom)	150	Telecom	Laos
4	Planet Online Laos, Internet Service Provider in LAO PDR	120	Telecom	Laos
5	Vimpelcom Lao Co Ltd (VEON)	65	Telecom	Laos
6	SkytelecomTransit provider and ISP in Vientiene.	40	Telecom	Laos
7	Siamdata	32	Cloud	Thailand
8	Datacom Sole Co., Ltd	13	Cloud	Laos
9	Lao Data Center	12	Cloud	Laos
10	Lao National Internet Center (LANIC)	3	Cloud	Laos
11	Lao Asia Pacific Satellite Co., Ltd.	3	Telecom	Laos
12	LERNET at LAOs	2	University	Laos
13	Mangkone Technology Co. Ltd.	1	Cloud	Laos
14	Lao International Technology Service Sole Co., Ltd	1	Unknown	Laos
15	Etern Laos Communication Technology Sole Co .,Ltd	1	Manufacturing	Laos

Among the top 10 highest contributors to open NTP services, the top 5 ISPs host nearly 93%. Beginning a mitigation campaign by reaching out and collaborating with these 5 ISPs could result in a substantial reduction of potential DDoS infrastructure.



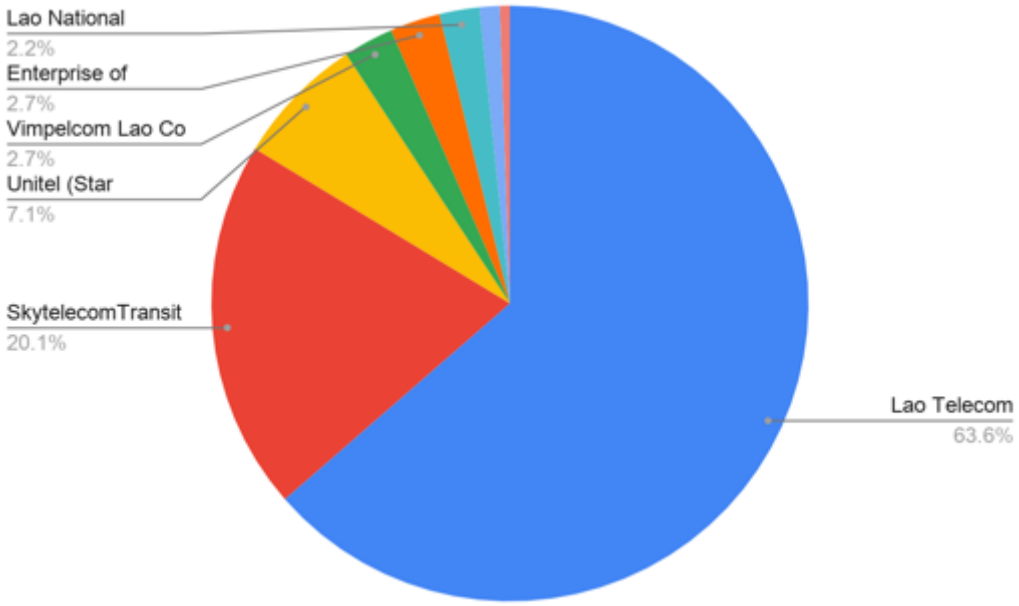
MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the third most prevalent of those risks in Laos. Of the 184 open SNMP services nationwide, all of them (100%) are hosted by the ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Lao Telecom Communication, LTC	117	Telecom	Laos
2	SkytelecomTransit provider and ISP in Vientiene.	37	Telecom	Laos
3	Unitel (Star Telecom)	13	Telecom	Laos
4	Vimpelcom Lao Co Ltd (VEON)	5	Telecom	Laos
5	Enterprise of Telecommunications Lao	5	Telecom	Laos
6	Lao National Internet Center (LANIC)	4	Cloud	Laos
7	Planet Online Laos, Internet Service Provider in LAO PDR	2	Telecom	Laos
8	Siamdata	1	Cloud	Thailand

Since the distribution of all the open SNMP services is only across eight ISPs, it might be

worthwhile to reach out to all of these ISPs with the goal of achieving a 0 count for open SNMP services in Laos. Certainly, reaching out to the top 3 ranked ISPs on the list would be a good start, as they collectively host nearly 91% of the open SNMP services across the nation.



MAJOR SSDP CONTRIBUTORS

For the week analyzed, the count for open SSDP services in Laos was 0.

MAJOR CHARGEN CONTRIBUTORS

For the week analyzed, the count for open CHARGEN services in Laos was 0.

APPENDIX E: DETAILED ISP CONTRIBUTION IN MALAYSIA

The following rankings and charts provide insight into the ISPs that host the greatest number of open services in Malaysia. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

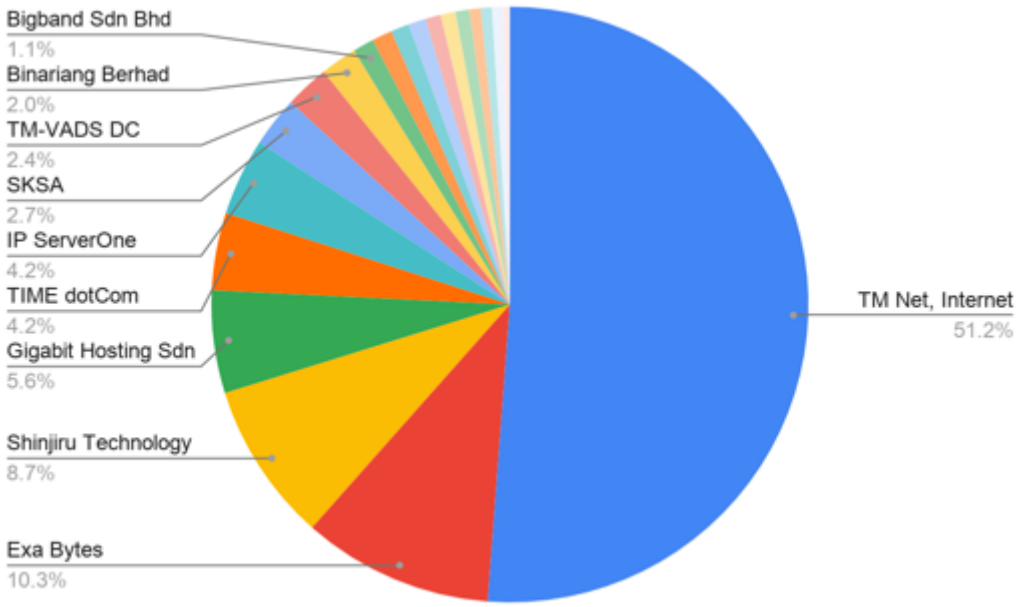
MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the most prevalent of those

risks in Malaysia. Of the 28,142 open DNS services nationwide, 26,465 of them (94%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	TM Net, Internet Service Provider	13546	Telecom	Malaysia
2	Exa Bytes	2737	Cloud	Malaysia & Indonesia
3	Shinjiru Technology Sdn Bhd	2294	Cloud	Malaysia
4	Gigabit Hosting Sdn Bhd	1474	Cloud	Malaysia
5	TIME dotCom Berhad	1113	Telecom	Malaysia
6	IP ServerOne Solutions Sdn Bhd	1108	Cloud	Malaysia
7	SKSA TECHNOLOGY SDN BHD	720	Cloud	Malaysia
8	TM-VADS DC Hosting	635	Cloud	Malaysia
9	Binariang Berhad (Maxis)	522	Telecom	Malaysia
10	Bigband Sdn Bhd	303	Cloud	Malaysia
11	iCore Technology Sdn Bhd	290	Cloud	Malaysia
12	REDtone	262	Telecom	Malaysia
13	Extreme Broadband - Total Broadband Experience	250	Telecom	Malaysia
14	Defense Australia Network (Mytek)	221	Unknown	Australia
15	ModernOne Data Solutions Sdn. Bhd.	214	Cloud	Malaysia
16	NTT MSC	197	Cloud	Malaysia
17	Acme Commerce (webserver.com.my)	165	Cloud	Malaysia
18	Hitachi Sunway Information Systems	156	Cloud	Malaysia
19	DiGi Telecommunications Sdn. Bhd.	150	Telecom	Malaysia
20	Net Onboard Sdn Bhd - Quality & Reliable Cloud Hosting Provider	108	Cloud	Malaysia

The pie graph below illustrates, among those 26,465 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure. Given the sizable percentage of open DNS services contributed by TM Net, outreach to their team and a mitigation campaign with that one ISP alone could have a considerable impact.



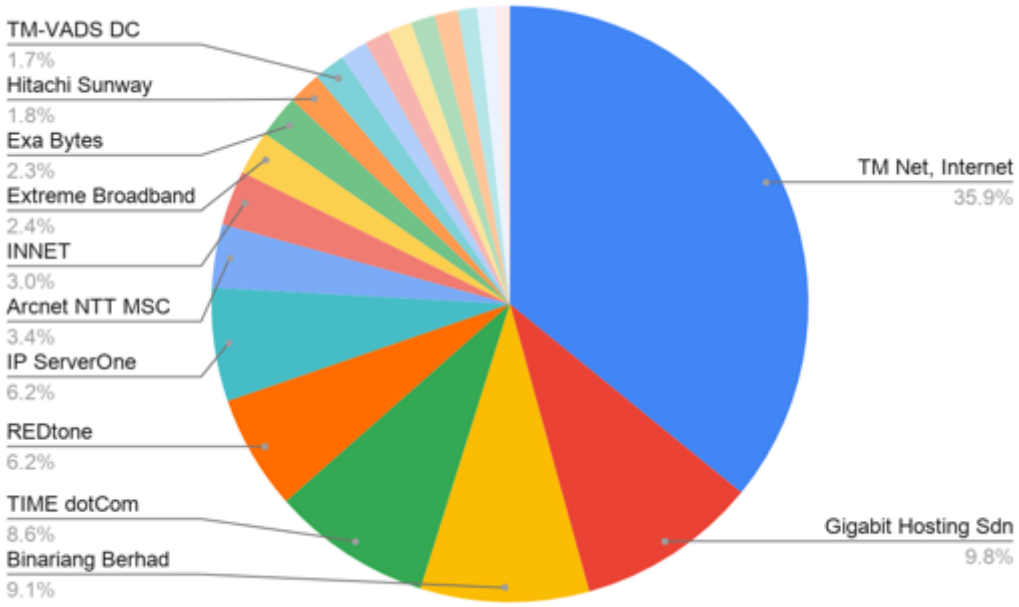
MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the second most prevalent of those risks in Malaysia, with the highest amplification factor. Of the 20,454 open NTP services nationwide, 18,384 of them (90%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	TM Net, Internet Service Provider	6597	Telecom	Malaysia
2	Gigabit Hosting Sdn Bhd	1808	Cloud	Malaysia
3	Binariang Berhad (Maxis)	1678	Telecom	Malaysia
4	TIME dotCom Berhad	1590	Telecom	Malaysia
5	REDtone	1145	Telecom	Malaysia
6	IP ServerOne Solutions Sdn Bhd	1131	Cloud	Malaysia
7	Arcnet NTT MSC ISP	631	Cloud	Malaysia
8	INNET SOLUTIONS SDN BHD	547	Telecom	Malaysia
9	Extreme Broadband - Total Broadband Experience	439	Telecom	Malaysia
10	Exa Bytes	426	Cloud	Malaysia & Indonesia
11	Hitachi Sunway Information Systems	331	Cloud	Malaysia

12	TM-VADS DC Hosting	317	Cloud	Malaysia
13	MyKRIS Asia Sdn Bhd	266	Telecom	Malaysia
14	Alibaba (US) Technology Co., Ltd.	248	Cloud	United States
15	WEBE DIGITAL SDN. BHD. (unifi)	241	Telecom	Malaysia
16	Macro Lynx Sdn Bhd, Internet Service Provider, Malaysia	240	Telecom	Malaysia
17	Malaysian Research & Education Network	231	Gov	Malaysia
18	Bigband Sdn Bhd	192	Cloud	Malaysia
19	Shinjiru Technology Sdn Bhd	182	Cloud	Malaysia
20	ALLO TECHNOLOGY SDN. BHD.	144	Telecom	Malaysia

The pie graph below illustrates, among those 18,384 open NTP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.

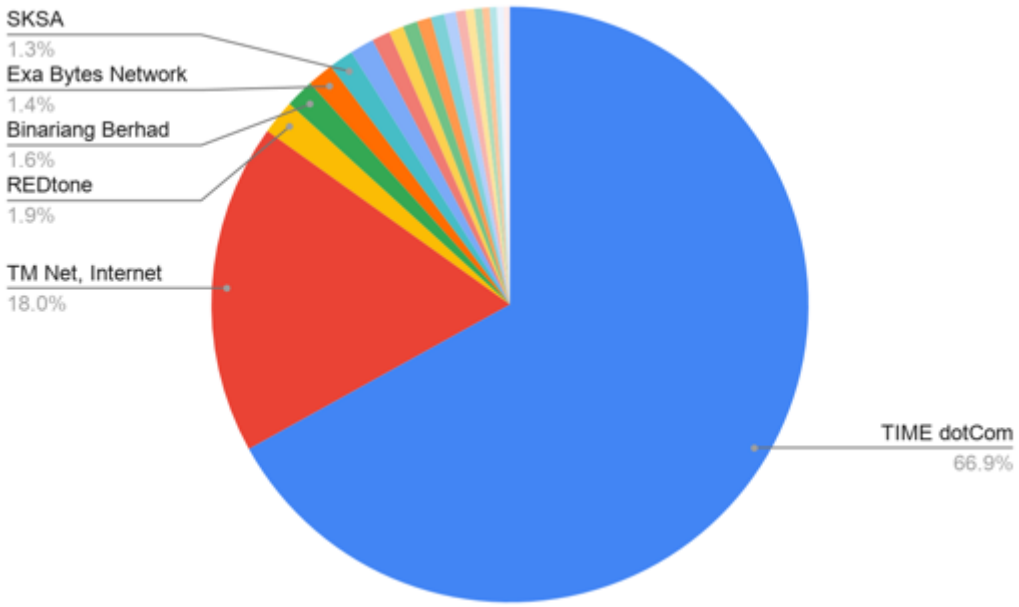


MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the third most prevalent of those risks in Malaysia. Of the 9,838 open SNMP services nationwide, 9,410 of them (96%) are hosted by the top twenty Malaysian ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	TIME dotCom Berhad	6299	Telecom	Malaysia
2	TM Net, Internet Service Provider	1690	Telecom	Malaysia
3	REDtone	176	Telecom	Malaysia
4	Binariang Berhad (Maxis)	146	Telecom	Malaysia
5	Exa Bytes	134	Cloud	Malaysia
6	SKSA TECHNOLOGY SDN BHD	126	Cloud	Malaysia
7	TM-VADS DC Hosting	122	Cloud	Malaysia
8	Macro Lynx Sdn Bhd, Internet Service Provider, Malaysia	93	Telecom	Malaysia
9	YTL COMMUNICATIONS SDN BHD	75	Telecom	Malaysia
10	IP ServerOne Solutions Sdn Bhd	74	Cloud	Malaysia
11	No.31-A, Jalan Tiara, Tiara Square	72	Telecom	Malaysia
12	Extreme Broadband - Total Broadband Experience	69	Telecom	Malaysia
13	Shinjiru Technology Sdn Bhd	59	Cloud	Malaysia
14	Celcom Axiata Berhad	50	Telecom	Malaysia
15	Gigabit Hosting Sdn Bhd	45	Cloud	Malaysia
16	MyKRIS Asia Sdn Bhd	39	Telecom	Malaysia
17	K-7-10, No. 2 Jalan Solaris, Solaris Mon't Kiara	38	Telecom	Malaysia
18	JENEXUS HOLDING SDN BHD	36	Telecom	Malaysia
19	VC Telecoms Sdn. Bhd.	35	Telecom	Malaysia
20	Lynuxtel Malaysia Sdn Bhd	32	Cloud	Malaysia

The pie graph below illustrates, among those 9,410 open SNMP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure. The top two ISPs, TIME and TM Net, host over 80% of the nation’s open SNMP services. Beginning a mitigation campaign by reaching out and collaborating with those two ISPs could result in a substantial reduction of potential DDoS infrastructure.



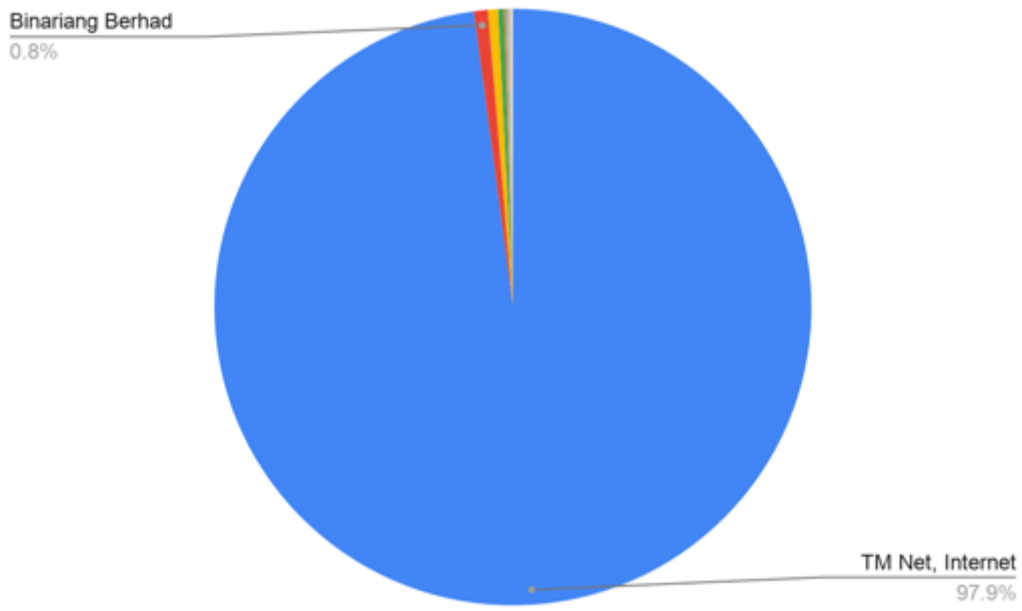
MAJOR SSDP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SSDP is the fourth most prevalent of those risks in Malaysia. Of the 9,300 open SSDP services nationwide, 9,296 are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	TM Net, Internet Service Provider	9101	Telecom	Malaysia
2	Binariang Berhad (Maxis)	70	Telecom	Malaysia
3	TIME dotCom Berhad	51	Telecom	Malaysia
4	REDtone	27	Telecom	Malaysia & Pakistan
5	YTL COMMUNICATIONS SDN BHD	9	Telecom	Malaysia
6	Celcom Axiata Berhad	7	Telecom	Malaysia
7	INNET SOLUTIONS SDN BHD	4	Telecom	Malaysia
8	ALLO TECHNOLOGY SDN. BHD.	4	Telecom	Malaysia
9	DiGi Telecommunications Sdn Bhd	4	Telecom	Malaysia
10	Macro Lynx Sdn Bhd, Internet Service Provider, Malaysia	3	Telecom	Malaysia

11	OCE Sdn Bhd ISP	3	Printing	Malaysia
12	Malaysian Research & Education Network	2	Gov	Malaysia
13	TechAvenue Malaysia	2	Cloud	Malaysia
14	Arcnet NTT MSC ISP	2	Cloud	Malaysia
15	Exa Bytes	2	Cloud	Malaysia
16	LightsUp Network Solution	1	Telecom	Malaysia
17	ACODA Networks Sdn Bhd	1	Telecom	Malaysia
18	Sunway	1	Manufacturing	Malaysia
19	Shinjiru Technology Sdn Bhd	1	Cloud	Malaysia
20	IP ServerOne Solutions Sdn Bhd	1	Cloud	Malaysia

The pie graph below illustrates, among those 9,296 open SSDP services quantified in the table above, the contribution of each ISP. The top contributing ISP (TM Net) hosts nearly 98% of the nation's open SSDP services. The most significant impact, therefore, for reducing the risk posed by open SSDP services in Malaysia would be to reach out to TM Net for mitigation.

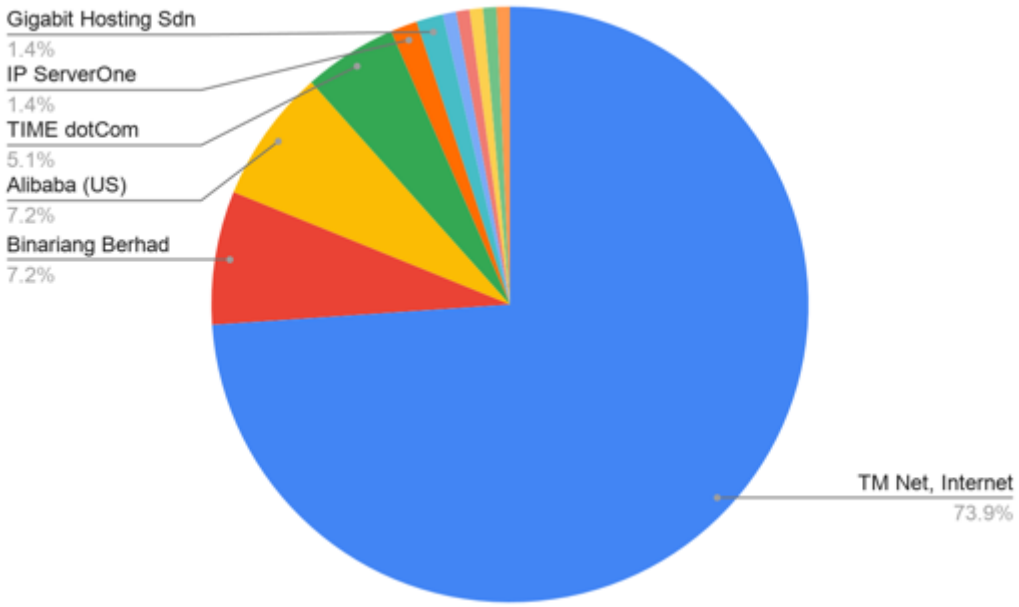


MAJOR CHARGEN CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, CHARGEN is the least prevalent of those risks in Malaysia. Of the 138 open CHARGEN services nationwide, all of them (100%) are hosted by the ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	TM Net, Internet Service Provider	102	Telecom	Malaysia
2	Binariang Berhad (Maxis)	10	Telecom	Malaysia
3	Alibaba (US) Technology Co., Ltd.	10	Cloud	United States
4	TIME dotCom Berhad	7	Telecom	Malaysia
5	IP ServerOne Solutions Sdn Bhd	2	Cloud	Malaysia
6	Gigabit Hosting Sdn Bhd	2	Cloud	Malaysia
7	Celcom Axiata Berhad	1	Telecom	Malaysia
8	WEBE DIGITAL SDN. BHD. (Unify)	1	Telecom	Malaysia
9	Arcnet NTT MSC ISP	1	Cloud	Malaysia
10	Acme Commerce Sdb Bhd, Malayia, Network	1	Cloud	Malaysia
11	TM-VADS DC Hosting	1	Cloud	Malaysia

The pie graph below illustrates, among those 138 open CHARGEN services quantified in the table above, the contribution of each ISP. The top contributing ISP (TM Net) hosts nearly 74% of the nation's open CHARGEN services. The most significant impact, therefore, for reducing the risk posed by open SSDP services in Malaysia would be to reach out to TM Net for mitigation.



APPENDIX F: DETAILED ISP CONTRIBUTION IN MYANMAR

The following rankings and charts provide insight into the ISPs that host the greatest number of open services in Myanmar. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

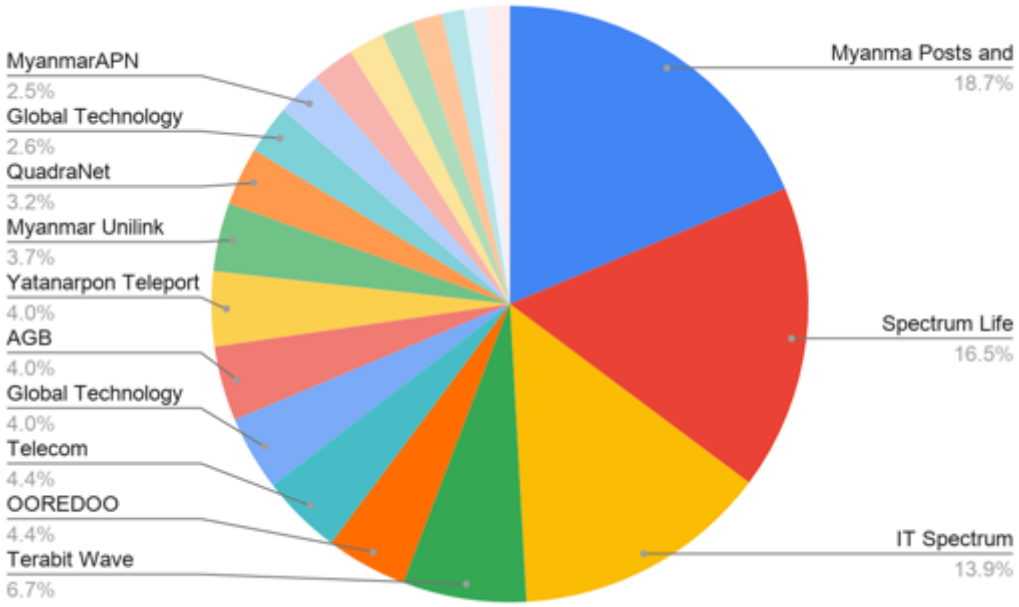
MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the third most prevalent of those risks in Myanmar. Of the 588 open DNS services nationwide, 568 of them (97%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Myanma Posts and Telecommunications	106	Telecom	Myanmar
2	Spectrum Life Company Limited (Netcore)	94	Telecom	Myanmar
3	IT Spectrum Company Limited (mm-link)	79	Telecom	Myanmar
4	Terabit Wave Company Limited	38	Telecom	Myanmar
5	OOREDOO MYANMAR	25	Telecom	Myanmar
6	Telecom International Myanmar Co., Ltd (mytel)	25	Telecom	Myanmar
7	Global Technology Co., Ltd. (GlobalNet)	23	Telecom	Myanmar
8	AGB Communication Co.Ltd	23	Telecom	Myanmar
9	Yatanarpon Teleport Company Limited	23	Telecom	Myanmar
10	Myanmar Unilink Communication Company Limited	21	Telecom	Myanmar
11	QuadraNet Enterprises LLC	18	Cloud	United States
12	Global Technology	15	Telecom	Myanmar
13	MyanmarAPN Company Limited	14	Telecom	Myanmar
14	HO'NGSA' TELECOM COMPANY LIMITED	13	Telecom	Myanmar
15	Golden TMH Telecom Co. Ltd	11	Cloud	Myanmar
16	Myanmar Country Co., Ltd.	10	Telecom	Myanmar
17	Frontiir Co. Ltd	9	Telecom	Myanmar
18	Myanmar Network Company Limited	7	Telecom	Myanmar
19	Telenor Myanmar	7	Telecom	Myanmar

20	MYANMAR INFORMATION HIGHWAY LIMITED	7	Telecom	Myanmar

The pie graph below illustrates, among those 568 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.



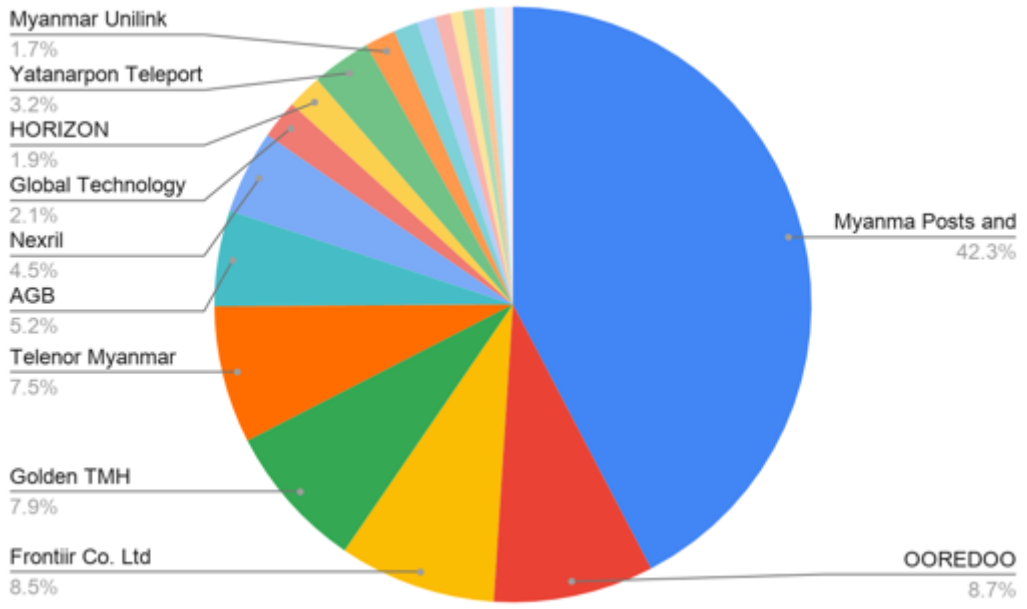
MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the most prevalent of those risks in Myanmar, with the highest amplification factor. Of the 1,884 open NTP services nationwide, 1,809 of them (96%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Myanma Posts and Telecommunications	766	Telecom	Myanmar
2	OOREDOO MYANMAR	157	Telecom	Myanmar
3	Frontiir Co. Ltd	154	Telecom	Myanmar
4	Golden TMH Telecom Co. Ltd	143	Cloud	Myanmar
5	Telenor Myanmar	135	Telecom	Myanmar
6	AGB Communication Co.Ltd	94	Telecom	Myanmar
7	Nexril	82	Cloud	United States

8	Global Technology Co., Ltd. (GlobalNet)	38	Telecom	Myanmar
9	HORIZON TELECOM INTERNATIONAL COMPANY LIMITED	34	Telecom	Myanmar
10	Yatanarpon Teleport Company Limited	58	Telecom	Myanmar
11	Myanmar Unilink Communication Company Limited	30	Telecom	Myanmar
12	Ocean Wave Communication Co., Ltd	24	Telecom	Myanmar
13	Myanmar Net	18	Telecom	Myanmar
14	Yoma Bank Limited	15	Bank	Myanmar
15	Myanmar Speed Net Co.,Ltd	12	Telecom	Myanmar
16	Telecom International Myanmar Co., Ltd (mytel)	11	Telecom	Myanmar
17	WELINK	10	Telecom	Myanmar
18	Campana MYTHIC Co. Ltd.	10	Telecom	Myanmar
19	Myint & Associates Telecommunications Ltd	9	Cloud	Myanmar
20	Internet Maekhong Network Company Limited	9	Unknown	Myanmar

The pie graph below illustrates, among those 1,809 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.

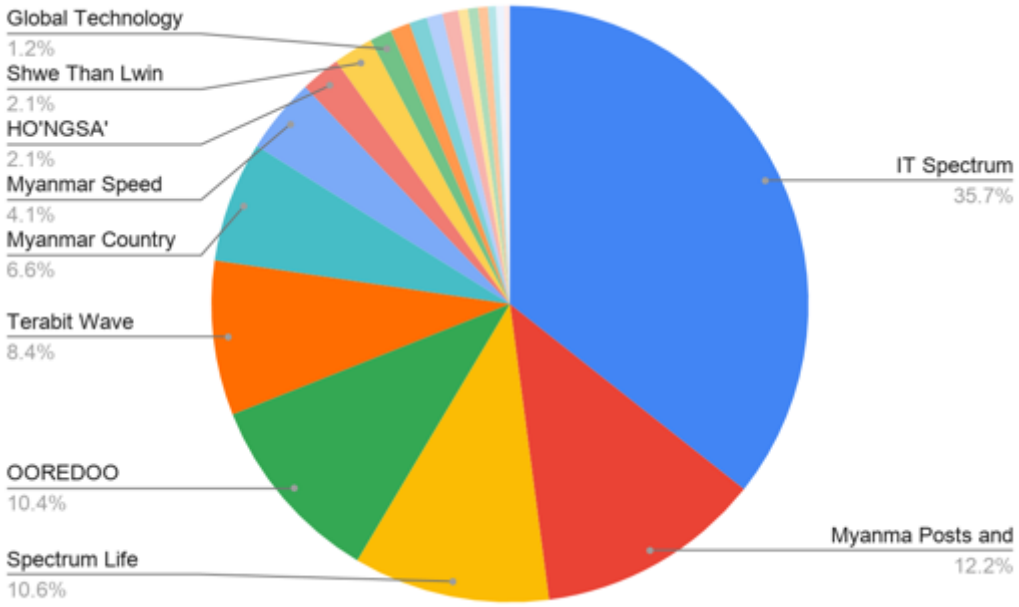


MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the second most prevalent of those risks in Myanmar. Of the 937 open SNMP services nationwide, 931 of them (99%) are hosted by the top twenty Myanmarese ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	IT Spectrum Company Limited (mm-link)	332	Telecom	Myanmar
2	Myanma Posts and Telecommunications	114	Telecom	Myanmar
3	Spectrum Life Company Limited (Netcore)	99	Telecom	Myanmar
4	OOREDOO MYANMAR	97	Telecom	Myanmar
5	Terabit Wave Company Limited	78	Telecom	Myanmar
6	Myanmar Country Co., Ltd.	61	Telecom	Myanmar
7	Myanmar Speed Net Co.,Ltd	38	Telecom	Myanmar
8	HO'NGSA' TELECOM COMPANY LIMITED	20	Telecom	Myanmar
9	Shwe Than Lwin Media Co.,Ltd.	20	Telecom	Myanmar
10	Global Technology Co., Ltd. (GlobalNet)	11	Telecom	Myanmar
11	Yatanarpon Teleport Company Limited	10	Telecom	Myanmar
12	Internet Maekhong Network Company Limited	9	Unknown	Myanmar
13	Frontiir Co. Ltd	8	Telecom	Myanmar
14	AGB Communication Co.Ltd	8	Telecom	Myanmar
15	Golden TMH Telecom Co. Ltd	5	Cloud	Myanmar
16	Asia Mega Link	5	Telecom/Infrastructure	Myanmar
17	AUNG GABAR COMPANY LIMITED	5	Import/Export	Myanmar
18	Global Technology	4	Telecom	Myanmar
19	Thoolei Co., Ltd.	4	Telecom	Myanmar
20	Telecom International Myanmar Co., Ltd	3	Telecom	Myanmar

The pie graph below illustrates, among those 931 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.



MAJOR SSDP CONTRIBUTORS

For the week analyzed, the count for open SSDP services in Myanmar was 0.

MAJOR CHARGEN CONTRIBUTORS

For the week analyzed, the count for open CHARGEN services in Myanmar was 0.

APPENDIX G: DETAILED ISP CONTRIBUTION IN THE PHILIPPINES

The following rankings and charts provide insight into the ISPs that host the greatest number of open services in the Philippines. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

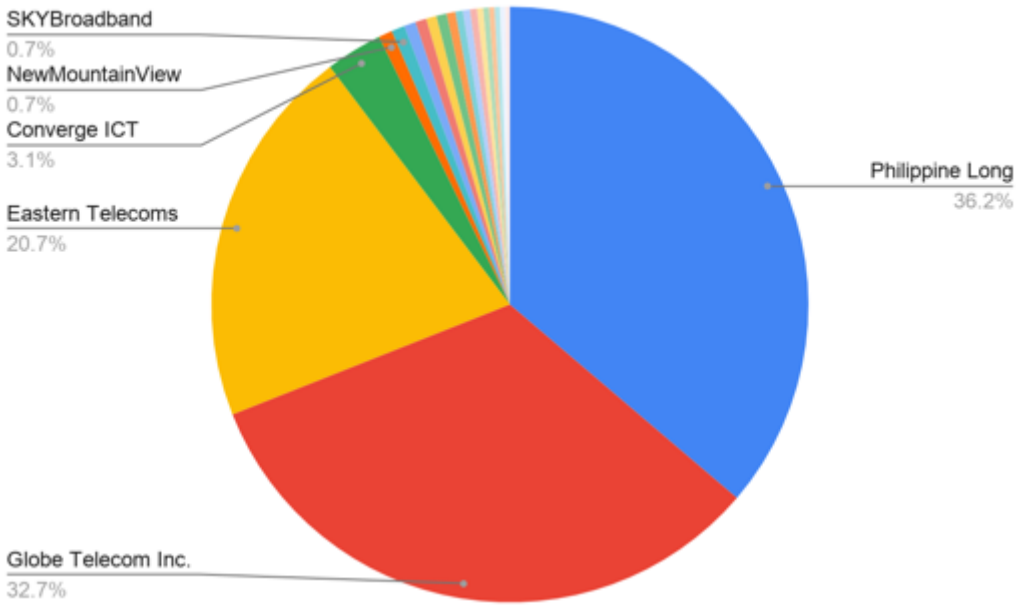
MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the third most prevalent of

those risks in the Philippines. Of the 15,577 open DNS services nationwide, 14,911 of them (96%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Philippine Long Distance Telephone Company	5405	Telecom	Philippines
2	Globe Telecoms	4880	Telecom	Philippines
3	Eastern Telecoms Phils., Inc.	3090	Telecom	Philippines
4	Converge ICT Solutions Inc.	458	Telecom	Philippines
5	NewMountainView Satellite Corporation	111	Telecom	Philippines
6	SKYBroadband SKYCable Corporation	108	Telecom	Philippines
7	IP-Converge Data Center, Inc.	94	Cloud	Philippines
8	Philippine Telegraph and Telephone Corporation	89	Telecom	Philippines
9	SunValley New Oriental	84	Telecom	Philippines
10	Philcom	83	Telecom	Philippines
11	RADIUS TELECOMS, INC.	71	Telecom	Philippines
12	iWeb Technologies Inc.	60	Cloud	Canada
13	Smart Broadband, Inc.	58	Telecom	Philippines
14	WifiCity Inc. (Fibercom)	56	Telecom	Philippines
15	Parasat Cable TV, Inc	50	Telecom	Philippines
16	Infinivan Incorporated	46	Telecom	Philippines
17	DCTech Micro Services	44	Telecom	Philippines
18	TELMARC CORPORATION	43	Telecom	Philippines
19	Department of Science and Technology	42	Research/Gov	Philippines
20	Integranet Network Services	39	Telecom	Philippines

The pie graph below illustrates, among those 14,911 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.



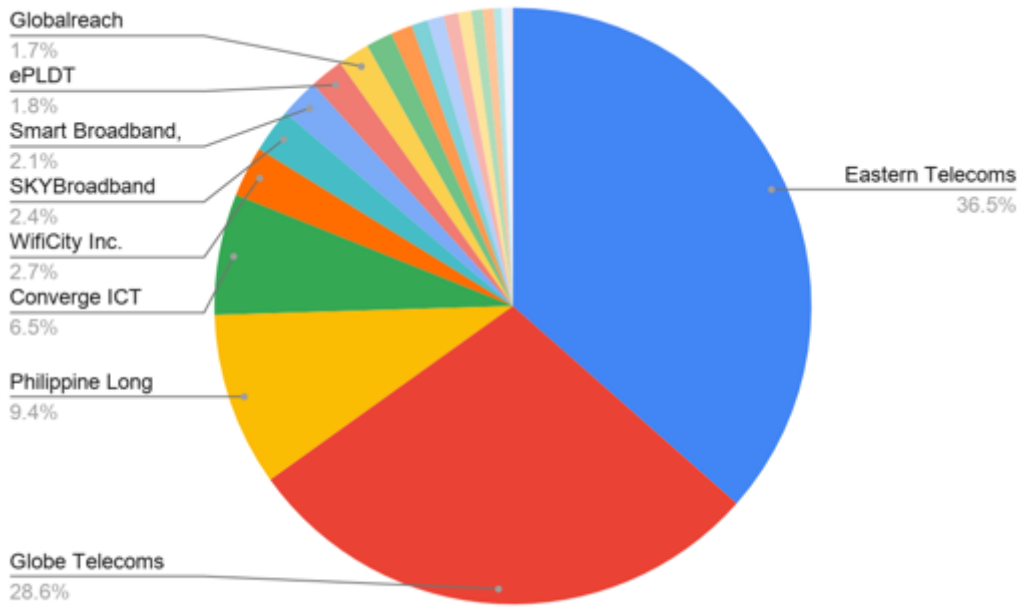
MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the most prevalent of those risks in the Philippines, with the highest amplification factor. Of the 29,769 open NTP services nationwide, 28,156 of them (95%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Eastern Telecoms Phils., Inc.	10281	Telecom	Philippines
2	Globe Telecoms	8049	Telecom	Philippines
3	Philippine Long Distance Telephone Company	2654	Telecom	Philippines
4	Converge ICT Solutions Inc.	1843	Telecom	Philippines
5	WifiCity Inc. (Fibercom)	774	Telecom	Philippines
6	SKYBroadband SKYCable Corporation	674	Telecom	Philippines
7	Smart Broadband, Inc.	596	Telecom	Philippines
8	ePLDT	516	Cloud	Philippines
9	Globalreach eBusiness Networks, Inc.	484	Cloud	Philippines
10	DCTV Cable Network Broadband Services Inc	403	Telecom	Philippines
11	IP-Converge Data Center, Inc.	328	Cloud	Philippines

12	Cablelink & Holdings Corp. Transit AS Internet Service Provider Philippines	250	Telecom	Philippines
13	SunValley New Oriental	250	Telecom	Philippines
14	Department of Science and Technology	221	Research/Gov	Philippines
15	BICOLANDIA CABLE TV INCORPORATED	201	Telecom	Philippines
16	Chubu Telecommunications Company, Inc.	173	Telecom	Japan
17	Total Information Management Corporation	165	Cloud	Philippines
18	PRODATANET INC.	121	Cloud	Philippines
19	Infinivan Incorporated	104	Telecom	Philippines
20	NewMountainView Satellite Corporation	69	Telecom	Philippines

The pie graph below illustrates, among those 28,156 open NTP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs - with particular focus on Eastern Telecoms and Globe Telecoms - to mitigate could result in a substantial reduction of potential DDoS infrastructure.

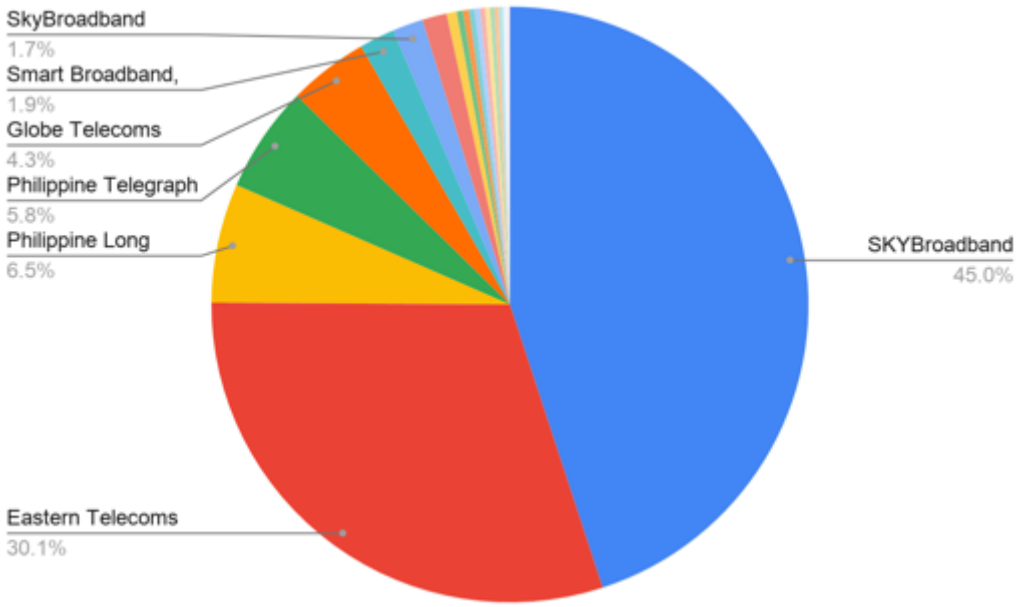


MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the second most prevalent of those risks in the Philippines. Of the 17,029 open SNMP services nationwide, 16,663 of them (98%) are hosted by the top twenty Philippino ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	SKYBroadband SKYCable Corporation	7493	Telecom	Philippines
2	Eastern Telecoms Phils., Inc.	5021	Telecom	Philippines
3	Philippine Long Distance Telephone Company	1078	Telecom	Philippines
4	Philippine Telegraph and Telephone Corporation	964	Telecom	Philippines
5	Globe Telecoms	721	Telecom	Philippines
6	Smart Broadband, Inc.	320	Telecom	Philippines
7	SkyBroadband Provincial Network	276	Telecom	Philippines
8	Converge ICT Solutions Inc.	221	Telecom	Philippines
9	Asian Vision Cable	91	Telecom	Philippines
10	Fil Products Service Television Incorporated	57	Telecom	Philippines
11	NewMountainView Satellite Corporation	55	Telecom	Philippines
12	IP-Converge Data Center, Inc.	49	Cloud	Philippines
13	Philcom	49	Telecom	Philippines
14	Infinivan Incorporated	45	Telecom	Philippines
15	TELMARC CORPORATION	45	Telecom	Philippines
16	DCTech Micro Services	40	Telecom	Philippines
17	WifiCity Inc. (Fibercom)	38	Telecom	Philippines
18	RADIUS TELECOMS, INC.	38	Telecom	Philippines
19	Cablelink & Holdings Corp. Transit AS Internet Service Provider Philippines	36	Telecom	Philippines
20	Planet Cable Inc.	26	Telecom	Philippines

The pie graph below illustrates, among those 16,663 open SNMP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs - with particular focus on SKYBroadband and Eastern Telecoms - to mitigate could result in a substantial reduction of potential DDoS infrastructure.



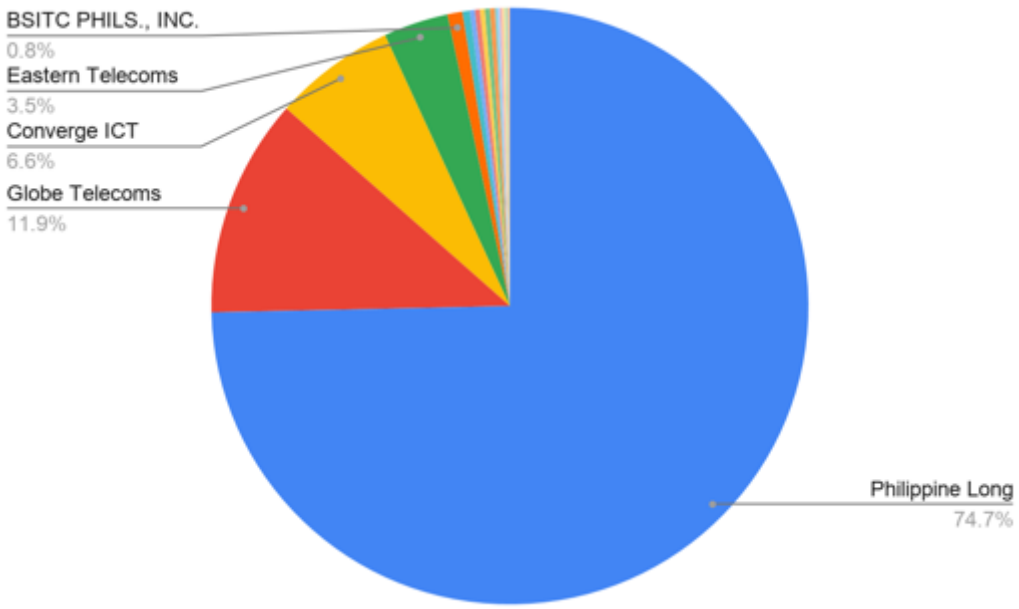
MAJOR SSDP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SSDP is the fourth most prevalent of those risks in the Philippines. Of the 742 open SSDP services nationwide, all of them (100%) are hosted by the 17 Philippino ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Philippine Long Distance Telephone Company	554	Telecom	Philippines
2	Globe Telecoms	88	Telecom	Philippines
3	Converge ICT Solutions Inc.	49	Telecom	Philippines
4	Eastern Telecoms Phils., Inc.	26	Telecom	Philippines
5	BSITC PHILS., INC.	6	Cloud	Philippines
6	DCTV Cable Network Broadband Services Inc	3	Telecom	Philippines
7	Fil Products Service Television Incorporated	2	Telecom	Philippines
8	Smart Broadband, Inc.	2	Telecom	Philippines
9	IP-Converge Data Center, Inc.	2	Cloud	Philippines
10	Philcom	2	Telecom	Philippines
11	NewMountainView Satellite Corporation	2	Telecom	Philippines

12	University of the Philippines Diliman	1	University	Philippines
13	Parasat Cable TV, Inc	1	Telecom	Philippines
14	Black Fiber Solutions Corporation	1	Telecom	Philippines
15	Advanced Science and Technology Institute	1	Gov	Philippines
16	RADIUS TELECOMS, INC.	1	Telecom	Philippines
17	DCTech Micro Services	1	Telecom	Philippines

The pie graph below illustrates, among those 742 open SSDP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs - with particular focus on Philippine Long Distance Telephone Company - to mitigate could result in a substantial reduction of potential DDoS infrastructure.



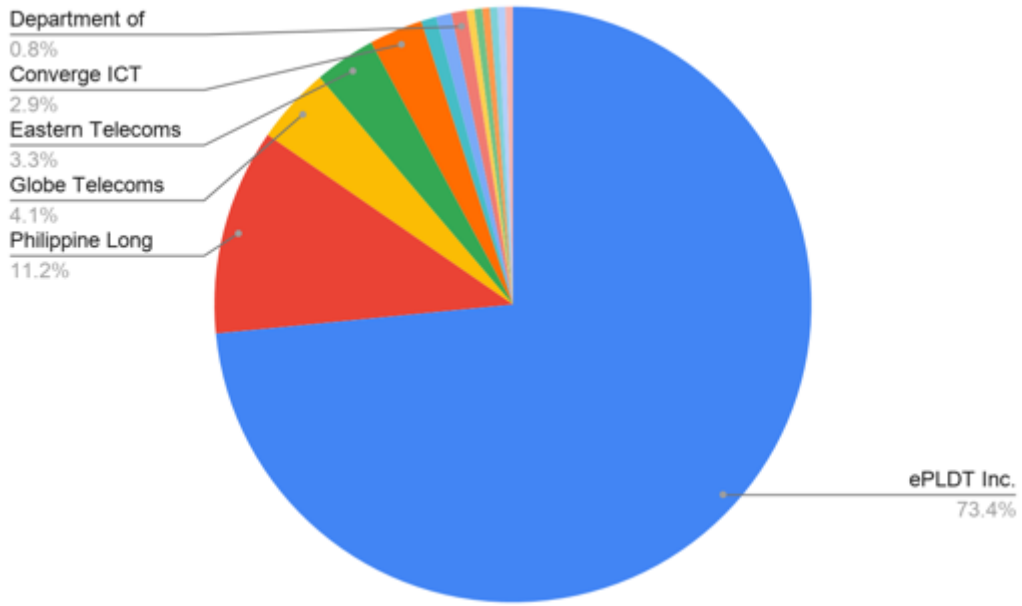
MAJOR CHARGEN CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, CHARGEN is the least prevalent of those risks in the Philippines. Of the 241 open CHARGEN services nationwide, all of them (100%) are hosted by the fourteen Philippino ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	ePLDT Inc.	177	Cloud	Philippines

2	Philippine Long Distance Telephone Company	27	Telecom	Philippines
3	Globe Telecoms	10	Telecom	Philippines
4	Eastern Telecoms Phils., Inc.	8	Telecom	Philippines
5	Converge ICT Solutions Inc.	7	Telecom	Philippines
6	IP-Converge Data Center, Inc.	2	Cloud	Philippines
7	WifiCity Inc. (Fibercom)	2	Telecom	Philippines
8	Department of Science and Technology	2	Research/Gov	Philippines
9	Globalreach eBusiness Networks, Inc.	1	Cloud	Philippines
10	Infinivan Incorporated	1	Telecom	Philippines
11	Black Fiber Solutions Corporation	1	Telecom	Philippines
12	iOne Resources, Inc.	1	Cloud	Philippines
13	SKYBroadband SKYCable Corporation	1	Telecom	Philippines
14	RADIUS TELECOMS, INC.	1	Telecom	Philippines

The pie graph below illustrates, among those 241 open CHARGEN services quantified in the table above, the contribution of each ISP. Because the vast majority of Philippino open CHARGEN services are hosted by ePLDT Inc., it would be most beneficial to reach out to their team directly to collaborate and mitigate.



APPENDIX H: DETAILED ISP CONTRIBUTION IN SINGAPORE

The following rankings and charts provide insight into the ISPs that host the greatest number of open services in Singapore. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

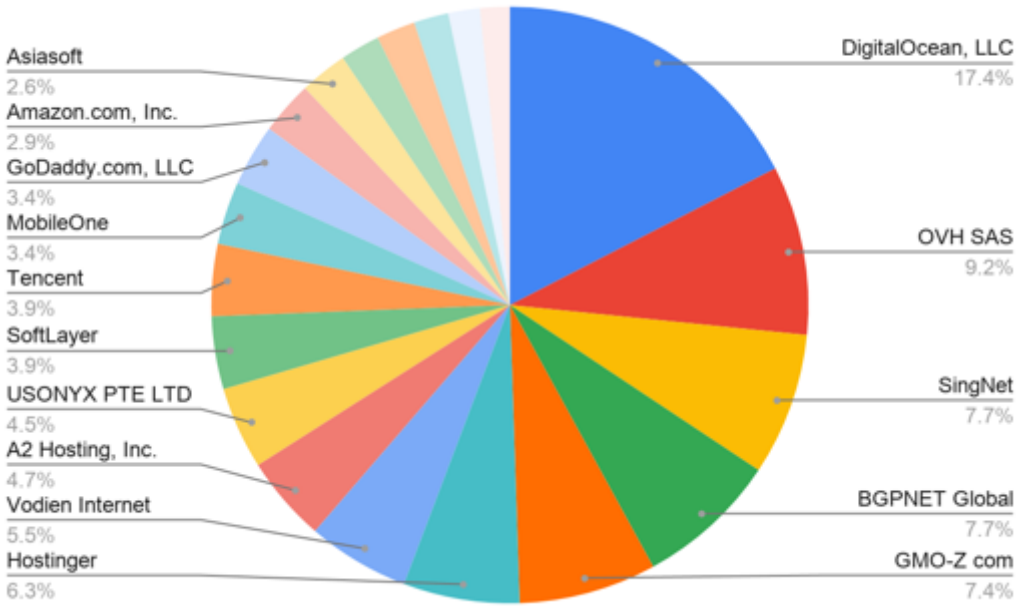
MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the second most prevalent of those risks in Singapore. Of the 47,977 open DNS services nationwide, 33,620 of them (70%) are hosted by the top 20 ISPs listed below.

Rank	ISP	Count	Type	Allocated Country
1	DigitalOcean, LLC	5858	Cloud	United States
2	OVH SAS	3085	Cloud	France
3	SingNet	2600	Cloud	Singapore
4	BGPNET Global ASN	2588	Cloud	Singapore
5	GMO-Z com NetDesign Holdings Co., Ltd.	2504	Cloud	Singapore
6	Hostinger International Limited	2116	Cloud	Lithuania
7	Vodien Internet Solutions Pte Ltd	1864	Cloud	Singapore
8	A2 Hosting, Inc.	1568	Cloud	United States
9	USONYX PTE LTD	1502	Cloud	Singapore
10	SoftLayer Technologies Inc. (IBM Cloud)	1326	Cloud	United States
11	Tencent	1311	Cloud	China
12	MobileOne	1140	Telecom	Singapore
13	GoDaddy.com, LLC	1136	Cloud	United States
14	Amazon.com, Inc.	971	Cloud	United States
15	Asiasoft	871	Cloud	Singapore
16	Sparkstation	722	Cloud	Singapore
17	Singtel	708	Telecom	Singapore

18	Linode, LLC	633	Cloud	United States
19	SG.GS	575	Telecom	Singapore
20	Leaseweb Asia Pacific pte. ltd.	542	Cloud	Singapore

The pie graph below illustrates, among those 33,620 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.



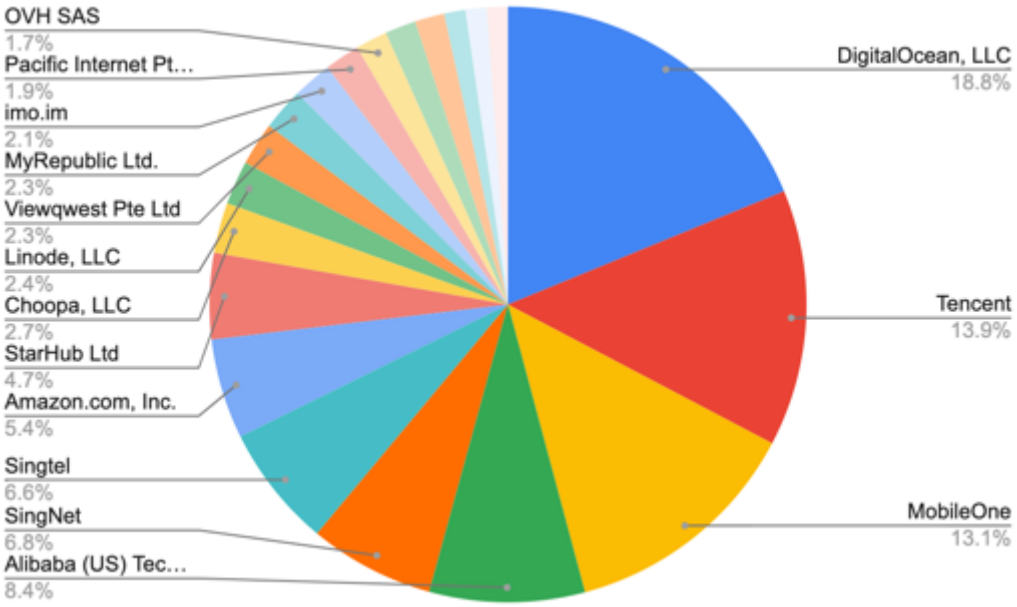
MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the most prevalent of those risks in Singapore, with the highest amplification factor. Of the 63,064 open NTP services nationwide, 43,510 of them (69%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	DigitalOcean, LLC	8175	Cloud	United States
2	Tencent	6059	Cloud	China
3	MobileOne	5712	Telecom	Singapore
4	Alibaba (US) Technology Co., Ltd.	3661	Telecom	United States
5	SingNet	2953	Cloud	Singapore

6	Singtel	2891	Telecom	Singapore
7	Amazon.com, Inc.	2362	Cloud	United States
8	StarHub Ltd	2031	Telecom	Singapore
9	Choopa, LLC	1190	Cloud	United States
10	Linode, LLC	1033	Cloud	United States
11	Viewqwest Pte Ltd	1017	Telecom	Singapore
12	MyRepublic Ltd.	1004	Telecom	Singapore
13	imo.im	921	Telecom	United States
14	Pacific Internet Pte Ltd	831	Cloud	Singapore
15	OVH SAS	748	Cloud	France
16	SoftLayer Technologies Inc.	727	Cloud	United States
17	LGA International	697	Telecom	Singapore
18	Zenlayer Inc	502	Cloud	United States
19	Opera Software AS	500	Cloud	Norway
20	NETPLUZ HOLDINGS PRIVATE LIMITED	496	Telecom	Singapore

The pie graph below illustrates, among those 43,510 open NTP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.



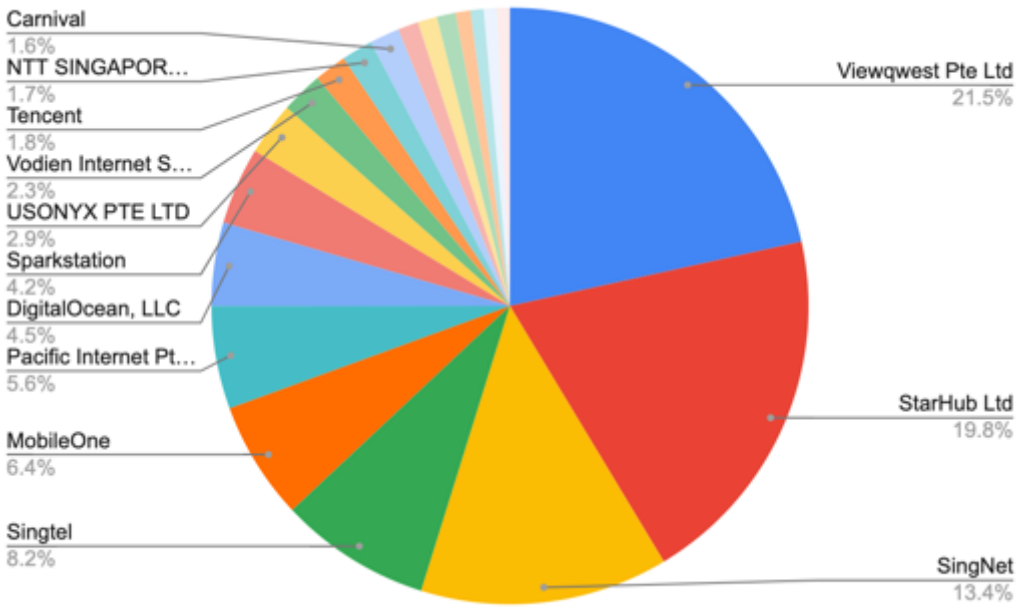
MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the third most prevalent of those risks in Singapore. Of the 3,503 open SNMP services nationwide, 2,963 of them (85%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Viewqwest Pte Ltd	638	Telecom	Singapore
2	StarHub Ltd	588	Telecom	Singapore
3	SingNet	398	Cloud	Singapore
4	Singtel	243	Telecom	Singapore
5	MobileOne	190	Telecom	Singapore
6	Pacific Internet Pte Ltd	165	Cloud	Singapore
7	DigitalOcean, LLC	134	Cloud	United States
8	Sparkstation	124	Cloud	Singapore
9	USONYX PTE LTD	85	Cloud	Singapore
10	Vodien Internet Solutions Pte Ltd	67	Cloud	Singapore
11	Tencent	52	Cloud	China

12	NTT SINGAPORE PTE LTD	50	Telecom	Singapore
13	Carnival	48	Telecom	Bangladesh
14	MyRepublic Ltd.	33	Telecom	Singapore
15	SoftLayer Technologies Inc. (IBM Cloud)	31	Cloud	United States
16	Amazon.com, Inc.	30	Cloud	United States
17	NETPLUZ HOLDINGS PRIVATE LIMITED	24	Telecom	Singapore
18	Alibaba (US) Technology Co., Ltd.	21	Telecom	United States
19	SuperInternet ACCESS Pte Ltd	21	Telecom	Singapore
20	Global Integrated Communications Pte Ltd	21	Cloud	Singapore

The pie graph below illustrates, among those 2,963 open SNMP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.

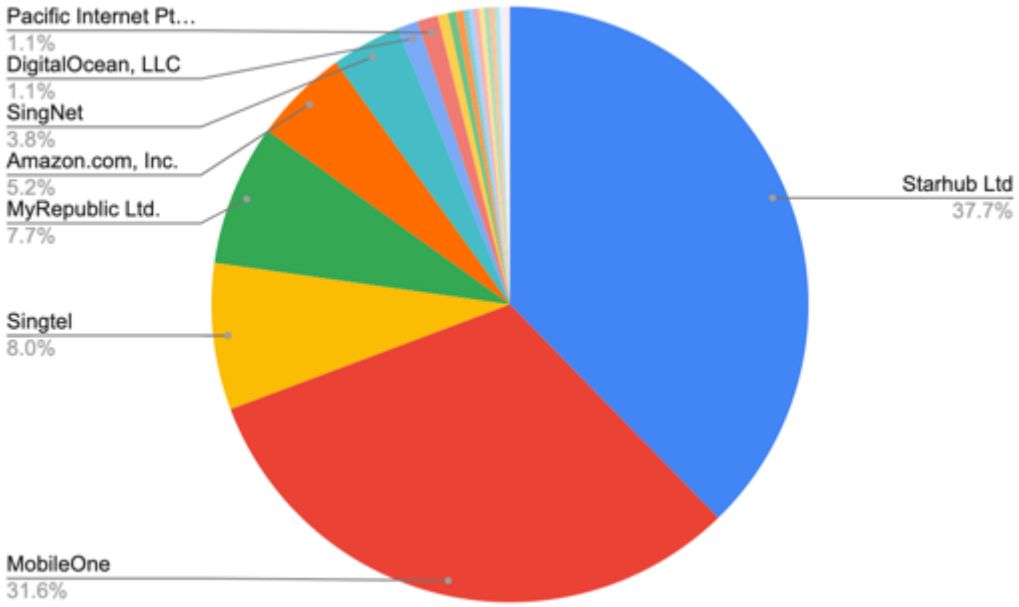


MAJOR SSDP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SSDP is the fourth most prevalent of those risks in Singapore. Of the 753 open SSDP services nationwide, 716 (95%) are hosted by the twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Starhub Ltd	270	Telecom	Singapore
2	MobileOne	226	Telecom	Singapore
3	Singtel	57	Telecom	Singapore
4	MyRepublic Ltd.	55	Telecom	Singapore
5	Amazon.com, Inc.	37	Cloud	United States
6	SingNet	27	Cloud	Singapore
7	DigitalOcean, LLC	8	Cloud	United States
8	Pacific Internet Pte Ltd	8	Cloud	Singapore
9	Telin	4	Telecom	Singapore & Indonesia
10	Digital Realty (data center)	3	Cloud	United States
11	SYSNETPRO SOLUTION PTE LTD	3	Unknown	Singapore
12	Iconz-Webvisions Pte. Ltd.	2	Cloud	Singapore
13	Continent 8 LLC	2	Cloud	United States
14	RigNet, Communication to remote locations in Asia/Pacific.	2	Telecom	Singapore
15	Carnival	2	Telecom	Bangladesh
16	US Dedicated	2	Cloud	United States
17	Vodien Internet Solutions Pte Ltd	2	Cloud	Singapore
18	Linode, LLC	2	Cloud	United States
19	MARINA BAY SANDS PTE LTD	2	Hospitality	Singapore
20	ZONE Telecom Pte Ltd	2	Telecom	Singapore

The pie graph below illustrates, among those 716 open SSDP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs - and particularly Starhub and MobileOne - to mitigate could result in a substantial reduction of potential DDoS infrastructure.



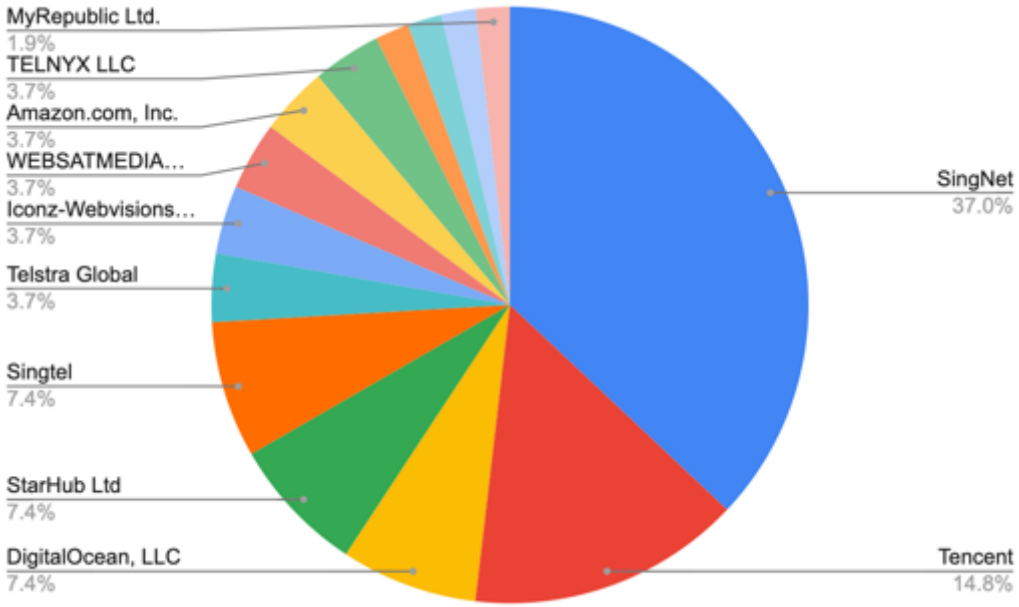
MAJOR CHARGEN CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, CHARGEN is the least prevalent of those risks in Singapore. Of the 109 open CHARGEN services nationwide, all of them (100%) are hosted by the fifteen ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Alibaba (US) Technology Co., Ltd.	55	Telecom	United States
2	SingNet	20	Cloud	Singapore
3	Tencent	8	Cloud	China
4	DigitalOcean, LLC	4	Cloud	United States
5	StarHub Ltd	4	Telecom	Singapore
6	Singtel	4	Telecom	Singapore
7	Telstra Global	2	Telecom	Hong Kong
8	Iconz-Webvisions Pte. Ltd.	2	Cloud	Singapore
9	WEBSATMEDIA PTE LTD, Satellite Over IP, Singapore	2	Telecom	Singapore
10	Amazon.com, Inc.	2	Cloud	United States

11	TELNYX LLC	2	Telecom	United States
12	MobileOne	1	Telecom	Singapore
13	Leaseweb Asia Pacific pte. ltd.	1	Cloud	Singapore
14	NETPLUZ HOLDINGS PRIVATE LIMITED	1	Telecom	Singapore
15	MyRepublic Ltd.	1	Telecom	Singapore

The pie graph below illustrates, among those 109 open CHARGEN services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a reduction of potential DDoS infrastructure.



APPENDIX I: DETAILED ISP CONTRIBUTION IN THAILAND

The following rankings and charts provide insight into the ISPs that host the greatest number of open services in Thailand. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

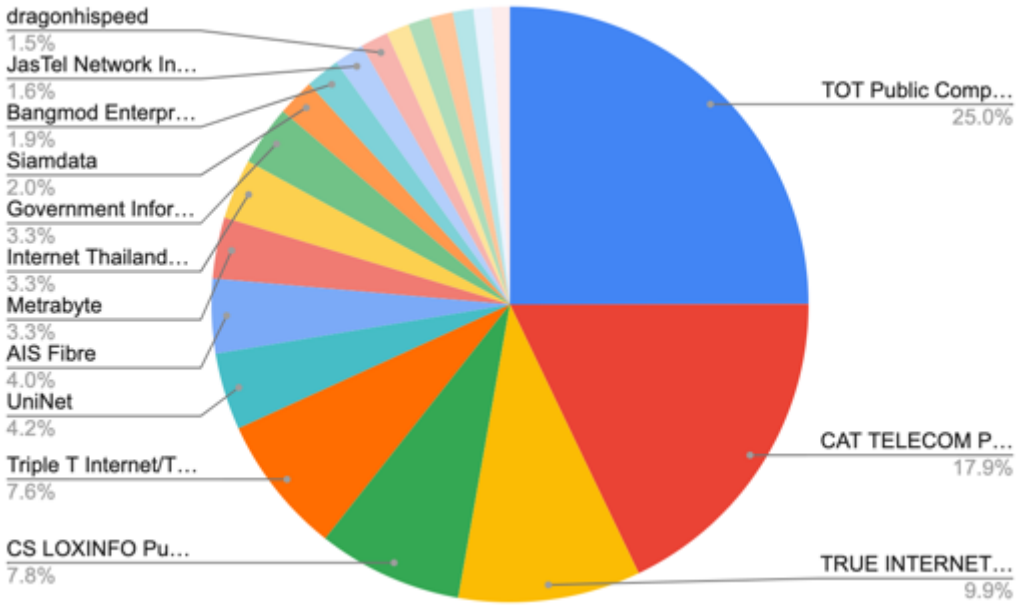
MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the second most prevalent of

those risks in Thailand. Of the 38,863 open DNS services nationwide, 34,183 of them (88%) are hosted by the top twenty ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	TOT Public Company Limited	8537	Telecom	Thailand
2	CAT TELECOM Public Company Ltd,CAT	6128	Telecom	Thailand
3	TRUE INTERNET Co.,Ltd.	3376	Telecom	Thailand
4	CS LOXINFO PUBLIC COMPANY LIMITED	2681	Cloud	Thailand
5	Triple T Internet/Triple T Broadband	2581	Telecom	Thailand
6	UniNet	1429	Research/Uni	Thailand
7	AIS Fibre	1382	Telecom	Thailand
8	Metrabyte	1135	Cloud	Thailand
9	Internet Thailand Company Limited	1115	Telecom	Thailand
10	Government Information Technology Services (NECTEC)	1113	Research	Thailand
11	Siamdata	691	Cloud	Thailand
12	Bangmod Enterprise Co., Ltd.	635	Cloud	Thailand
13	JasTel Network International Gateway	553	Telecom	Thailand
14	dragonhispeed	513	Cloud	Thailand
15	UIH	424	Cloud	Thailand
16	POPIDC powered by CSLoxinfo	418	Unknown	Thailand
17	Proimage Engineering and Communication Co.,Ltd. (PROEN)	415	Cloud	Thailand
18	Digital Realty data center	380	Cloud	United States
19	Internet Solution & Service Provider Co., Ltd.	339	Telecom	Thailand
20	Symphony Communication (Thailand) PCL.	338	Telecom	Thailand

The pie graph below illustrates, among those 34,183 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.



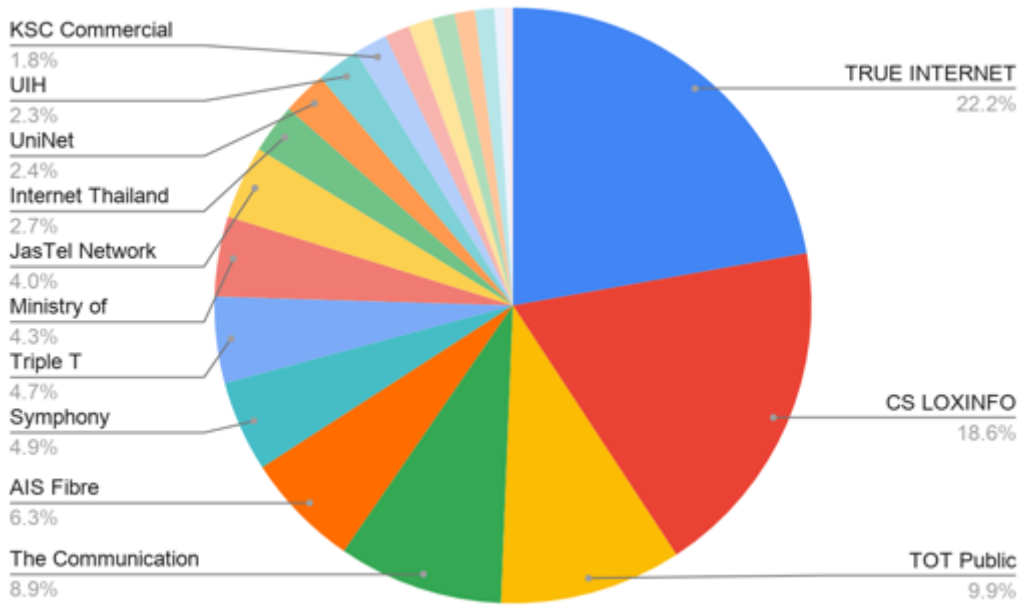
MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the most prevalent of those risks in Thailand, with the highest amplification factor. Of the 77,973 open NTP services nationwide, 72,404 of them (93%) are hosted by the top twenty Thai ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	TRUE INTERNET Co.,Ltd.	16063	Telecom	Thailand
2	CS LOXINFO PUBLIC COMPANY LIMITED	13459	Cloud	Thailand
3	TOT Public Company Limited	7143	Telecom	Thailand
4	The Communication Authority of Thailand, CAT	6469	Telecom	Thailand
5	AIS Fibre	4549	Telecom	Thailand
6	Symphony Communication (Thailand) PCL.	3572	Telecom	Thailand
7	Triple T Internet/Triple T Broadband	3392	Telecom	Thailand
8	Ministry of Information Communication Technology	3147	Gov	Thailand
9	JasTel Network International Gateway	2876	Telecom	Thailand

10	Internet Thailand Company Limited	1942	Telecom	Thailand
11	UniNet	1721	Research/Uni	Thailand
12	UIH	1684	Cloud	Thailand
13	KSC Commercial Internet Co. Ltd.	1304	Telecom	Thailand
14	Proimage Engineering and Communication Co.,Ltd. (PROEN)	968	Cloud	Thailand
15	KIRZ Service Provider	962	Cloud	Thailand
16	Internet Solution & Service Provider Co., Ltd.	874	Telecom	Thailand
17	Jasmine Internet Co, Ltd.	795	Telecom	Thailand
18	NTTCTNET	759	Cloud	Thailand
19	Siamdata	383	Cloud	Thailand
20	T.C.C. Technology Co., Ltd.	342	Cloud	Thailand

The pie graph below illustrates, among those 72,404 open NTP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.



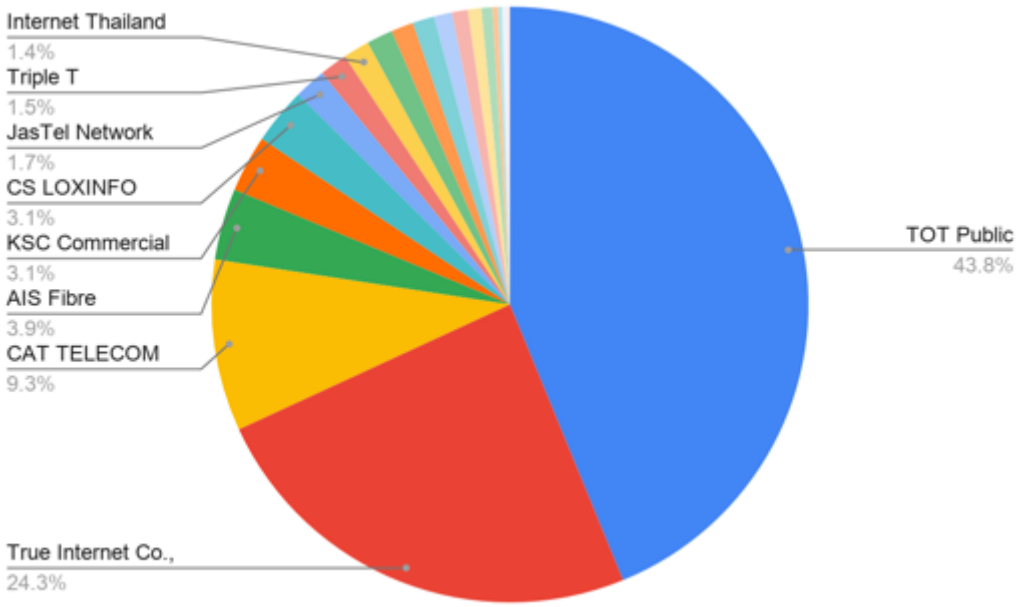
MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the third most prevalent of

those risks in Thailand. Of the 22,947 open SNMP services nationwide, 22,311 of them (97%) are hosted by the top twenty Thai ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	TOT Public Company Limited	9775	Telecom	Thailand
2	True Internet Co.,Ltd.	5421	Telecom	Thailand
3	CAT TELECOM Public Company Ltd,CAT	2078	Telecom	Thailand
4	AIS Fibre	864	Telecom	Thailand
5	KSC Commercial Internet Co. Ltd.	689	Telecom	Thailand
6	CS LOXINFO PUBLIC COMPANY LIMITED	685	Cloud	Thailand
7	JasTel Network International Gateway	381	Telecom	Thailand
8	Triple T Internet/Triple T Broadband	336	Telecom	Thailand
9	Internet Thailand Company Limited	319	Telecom	Thailand
10	UIH	315	Cloud	Thailand
11	UniNet	269	Research/Uni	Thailand
12	Proimage Engineering and Communication Co.,Ltd. (PROEN)	264	Cloud	Thailand
13	KIRZ Service Provider	218	Cloud	Thailand
14	World Internetwork Co.,LtdThailand.	192	Unknown	Thailand
15	T.C.C. Technology Co., Ltd.	163	Cloud	Thailand
16	Symphony Communication (Thailand) PCL.	131	Telecom	Thailand
17	134 Yenchit Road (New Shine Internet)	68	Unknown	Thailand
18	Express Data Co.,Ltd	48	Telecom	Thailand
19	Magik Pivot Company Limited	48	Cloud	Thailand
20	THAICOM Public Company Limited	47	Telecom	Thailand

The pie graph illustrates, among those 22,311 open SNMP services quantified in the table, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.



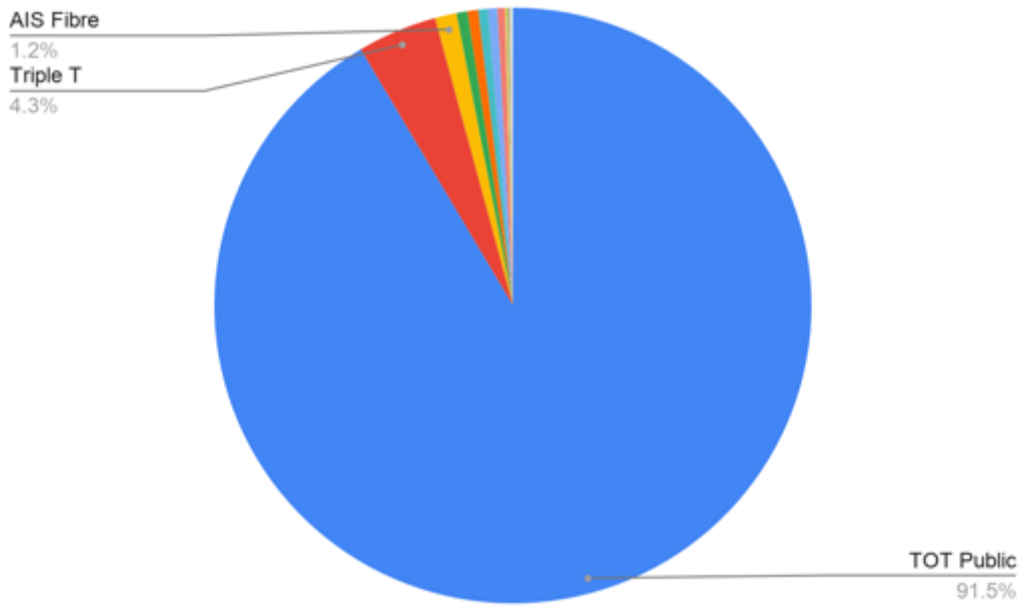
MAJOR SSDP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SSDP is the fourth most prevalent of those risks in Thailand. Of the 5,966 open SSDP services nationwide, 5,964 of them (nearly 100%) are hosted by the twenty Thai ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	TOT Public Company Limited	5456	Telecom	Thailand
2	Triple T Internet/Triple T Broadband	257	Telecom	Thailand
3	AIS Fibre	70	Telecom	Thailand
4	Chulalongkorn University	35	University	Thailand
5	TRUE INTERNET Co.,Ltd.	35	Telecom	Thailand
6	CS LOXINFO PUBLIC COMPANY LIMITED	31	Cloud	Thailand
7	Internet Thailand Company Limited	30	Telecom	Thailand
8	JasTel Network International Gateway	24	Telecom	Thailand
9	KSC Commercial Internet Co. Ltd.	6	Telecom	Thailand

10	Internet Solution & Service Provider Co., Ltd.	5	Telecom	Thailand
11	World Internetwork Co.,LtdThailand.	4	Unknown	Thailand
12	134 Yenchit Road (New Shine Internet)	2	Unknown	Thailand
13	Two S One N Co Ltd, Internet Service Provider and IT Solutions	2	Telecom	Thailand
14	Jasmine Internet Co, Ltd.	1	Telecom	Thailand
15	KIRZ Service Provider	1	Cloud	Thailand
16	Symphony Communication (Thailand) PCL.	1	Telecom	Thailand
17	Internet Datacenter Network	1	Cloud	Thailand
18	Thammasat University in thailand	1	University	Thailand
19	NIPA TECHNOLOGY CO., LTD	1	Cloud	Thailand
20	T.C.C. Technology Co., Ltd.	1	Cloud	Thailand

The pie graph below illustrates, among those 5,964 open SSDP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs - particularly TOT Public Company Limited, which hosts nearly 92% of the open SSDP services in Thailand - to mitigate could result in a substantial reduction of potential DDoS infrastructure.

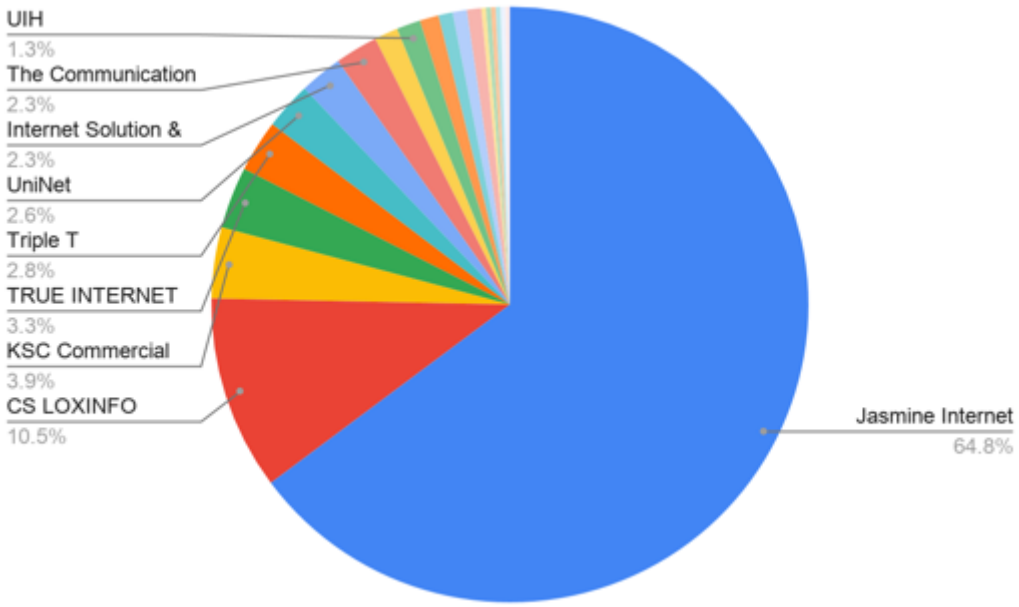


MAJOR CHARGEN CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, CHARGEN is the least prevalent of those risks in Thailand. Of the 391 open CHARGEN services nationwide, 389 of them (nearly 100%) are hosted by the twenty Thai ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Jasmine Internet Co, Ltd.	252	Telecom	Thailand
2	CS LOXINFO PUBLIC COMPANY LIMITED	41	Cloud	Thailand
3	KSC Commercial Internet Co. Ltd.	15	Telecom	Thailand
4	TRUE INTERNET Co.,Ltd.	13	Telecom	Thailand
5	Triple T Internet/Triple T Broadband	11	Telecom	Thailand
6	UniNet	10	Research/Uni	Thailand
7	Internet Solution & Service Provider Co., Ltd.	9	Telecom	Thailand
8	The Communication Authority of Thailand, CAT	9	Telecom	Thailand
9	Internet Thailand Company Limited	5	Telecom	Thailand
10	UIH	5	Cloud	Thailand
11	134 Yenchit Road (New Shine Internet)	4	Unknown	Thailand
12	Bangkok Airways Co., Ltd.	3	Airline	Thailand
13	TOT Public Company Limited	3	Telecom	Thailand
14	JasTel Network	3	Telecom	Thailand
15	Symphony Communication (Thailand) PCL.	1	Telecom	Thailand
16	Mahasarakham University	1	University	Thailand
17	NIPA TECHNOLOGY CO., LTD	1	Cloud	Thailand
18	Metrabyte	1	Cloud	Thailand
19	Ministry of Finance	1	Gov	Thailand
20	Proimage Engineering and Communication Co.,Ltd. (PROEN)	1	Cloud	Thailand

The pie graph below illustrates, among those 389 open CHARGEN services quantified in the table above, the contribution of each ISP. Because the majority of open CHARGEN services are hosted by Jasmine Internet, it would be most beneficial to reach out to their team directly to collaborate and mitigate.



APPENDIX J: DETAILED ISP CONTRIBUTION IN VIETNAM

The following rankings and charts provide insight into the ISPs that host the greatest number of open services in Vietnam. CyberGreen ranks the top 20 ISPs (where applicable) that host these services and visualizes them in a pie chart.

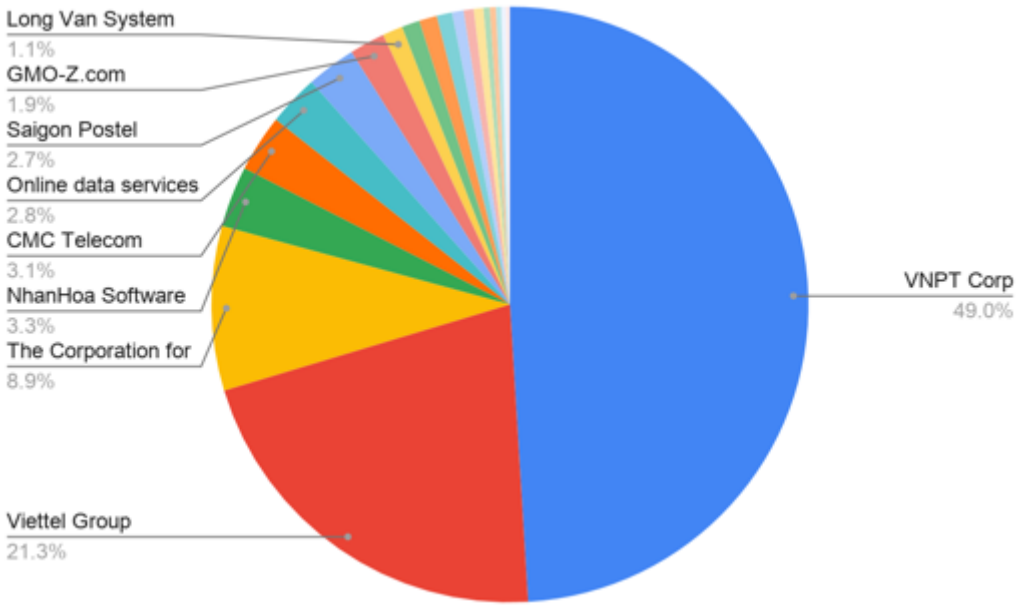
MAJOR DNS CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, DNS is the second most prevalent of those risks in Vietnam. Of the 40,485 open DNS services nationwide, 38,967 of them (96%) are hosted by the top twenty Vietnamese ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	VNPT Corp	19104	Telecom	Vietnam
2	Viettel Group	8301	Telecom	Vietnam
3	The Corporation for Financing & Promoting Technology (FPT)	3478	Telecom	Vietnam
4	NhanHoa Software company	1287	Cloud	Vietnam
5	CMC Telecom Infrastructure Company	1208	Telecom	Vietnam

6	Online data services	1078	Cloud	Vietnam
7	Saigon Postel Corporation	1042	Telecom	Vietnam
8	GMO-Z.com Runsystem Joint Stock Company	746	Cloud	Vietnam
9	Long Van System Solution JSC	428	Cloud	Vietnam
10	Viet Solutions Services Trading Company Limited (vHost)	379	Cloud	Vietnam
11	Rainbow E-Commerce Company Limited (Bizmac)	376	Cloud	Vietnam
12	Quang Trung Software City Development Company (QTSC)	325	Telecom	Vietnam
13	AZDIGI Corporation	244	Cloud	Vietnam
14	TIEN PHAT TECHNOLOGY CORPORATION (TPCOMS)	212	Cloud	Vietnam
15	SUPERDATA	204	Cloud	Vietnam
16	Ehost software company limited	131	Cloud	Vietnam
17	Netnam Company	130	Telecom	Vietnam
18	Maxdata	109	Cloud	Vietnam
19	Ligh technology viet joint stock company	94	Cloud	Vietnam
20	Webico Company Limited	91	Cloud	Vietnam

The pie graph below illustrates, among those 38,967 open DNS services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure. Moreover, nearly half of the open DNS services in Vietnam are hosted by the top-contributing ISP, VNPT Corp. Outreach and mitigation efforts should begin with and focus on that ISP.



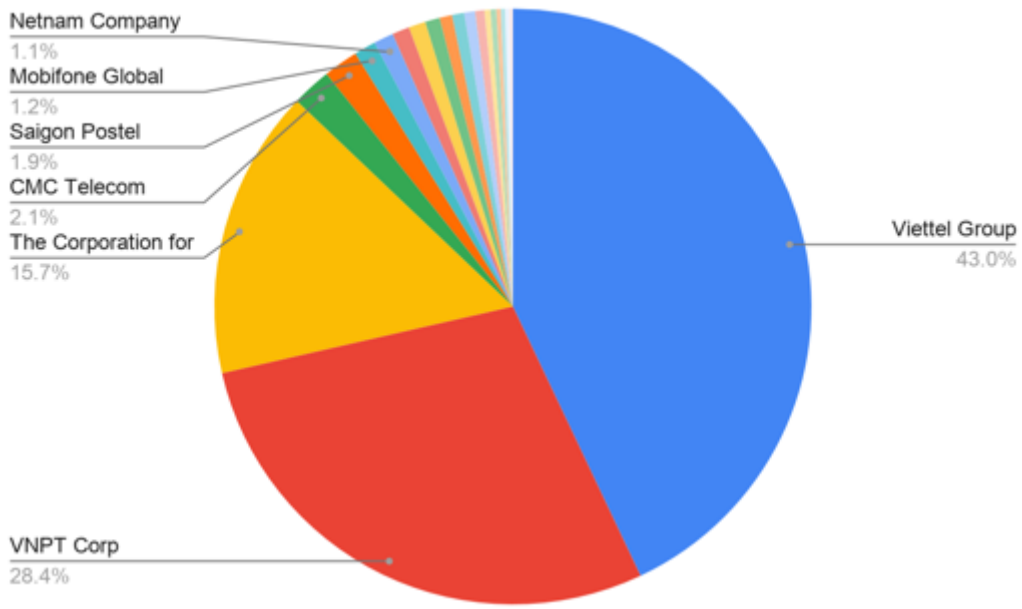
MAJOR NTP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, NTP is the most prevalent of those risks in Vietnam, with the highest amplification factor. Of the 44,811 open NTP services nationwide, 43,165 of them (96%) are hosted by the top twenty Vietnamese ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	Viettel Group	18546	Telecom	Vietnam
2	VNPT Corp	12274	Telecom	Vietnam
3	The Corporation for Financing & Promoting Technology (FPT)	6784	Telecom	Vietnam
4	CMC Telecom Infrastructure Company	925	Telecom	Vietnam
5	Saigon Postel Corporation	813	Telecom	Vietnam
6	Mobifone Global JSC	509	Telecom	Vietnam
7	Netnam Company	463	Telecom	Vietnam
8	GMO-Z.com Runsystem Joint Stock Company	404	Cloud	Vietnam
9	SCTV	396	Telecom	Vietnam
10	TIEN PHAT TECHNOLOGY CORPORATION	343	Cloud	Vietnam

	(TPCOMS)			
11	SUPERDATA	291	Cloud	Vietnam
12	Online data services	285	Cloud	Vietnam
13	VTC	255	Telecom	Vietnam
14	Minh Tu Telecom Limited Company	215	Telecom	Vietnam
15	Vietnamobile Telecommunications Joint Stock Company	141	Telecom	Vietnam
16	Quang Trung Software City Development Company (QTSC)	136	Telecom	Vietnam
17	Viet Solutions Services Trading Company Limited (vHost)	101	Cloud	Vietnam
18	Long Van System Solution JSC	101	Cloud	Vietnam
19	Vietnam Technology and Telecommunication JSC (VNTT)	100	Telecom	Vietnam
20	Global Telecom Corp (GMobile)	83	Telecom	Vietnam

The pie graph below illustrates, among those 43,165 open NTP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs - and, in particular, the top three - to mitigate could result in a substantial reduction of potential DDoS infrastructure.

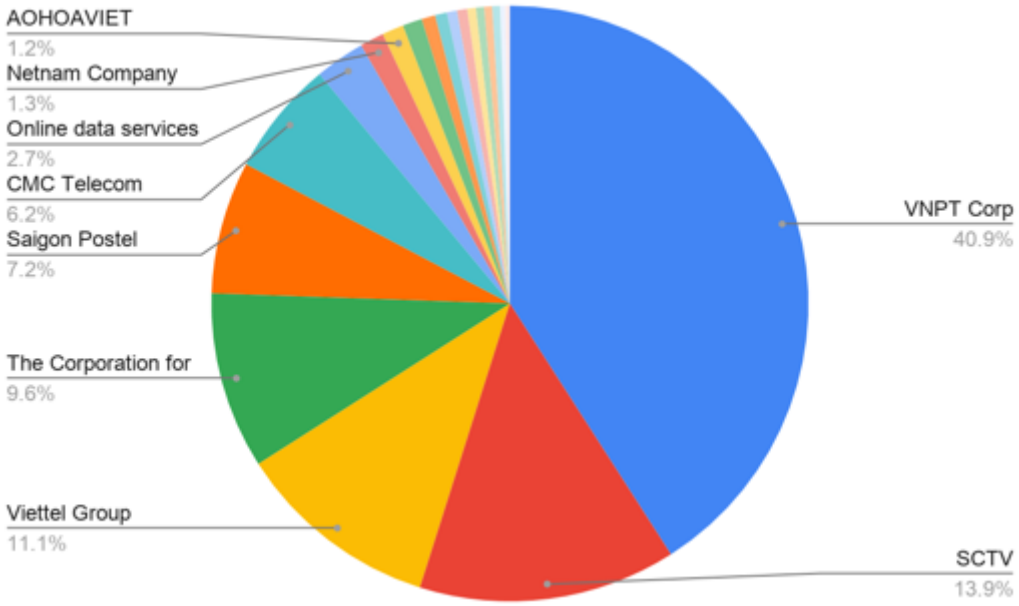


MAJOR SNMP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SNMP is the third most prevalent of those risks in Vietnam. Of the 7,098 open SNMP services nationwide, 6,919 of them (97%) are hosted by the top twenty Vietnamese ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	VNPT Corp	2832	Telecom	Vietnam
2	SCTV	965	Telecom	Vietnam
3	Viettel Group	766	Telecom	Vietnam
4	The Corporation for Financing & Promoting Technology (FPT)	664	Telecom	Vietnam
5	Saigon Postel Corporation	498	Telecom	Vietnam
6	CMC Telecom Infrastructure Company	432	Telecom	Vietnam
7	Online data services	187	Cloud	Vietnam
8	Netnam Company	90	Telecom	Vietnam
9	AOHOAVIET	81	Cloud	Vietnam
10	Hanoi Telecom Joint Stock Company - HCMC Branch	73	Telecom	Vietnam
11	Rainbow E-Commerce Company Limited (Bizmac)	51	Cloud	Vietnam
12	VNDATA	45	Cloud	Vietnam
13	NhanHoa Software company	38	Cloud	Vietnam
14	TIEN PHAT TECHNOLOGY CORPORATION (TPCOMS)	38	Cloud	Vietnam
15	Mobifone Global JSC	33	Telecom	Vietnam
16	BKHOST	30	Cloud	Vietnam
17	VTC	30	Telecom	Vietnam
18	TLSoft	29	Software dev	Vietnam
19	Information Technology Park - Vietnam National University Ho Chi Minh City	19	University	Vietnam
20	SUPERDATA	18	Cloud	Vietnam

The pie graph below illustrates, among those 6,919 open SNMP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a substantial reduction of potential DDoS infrastructure.



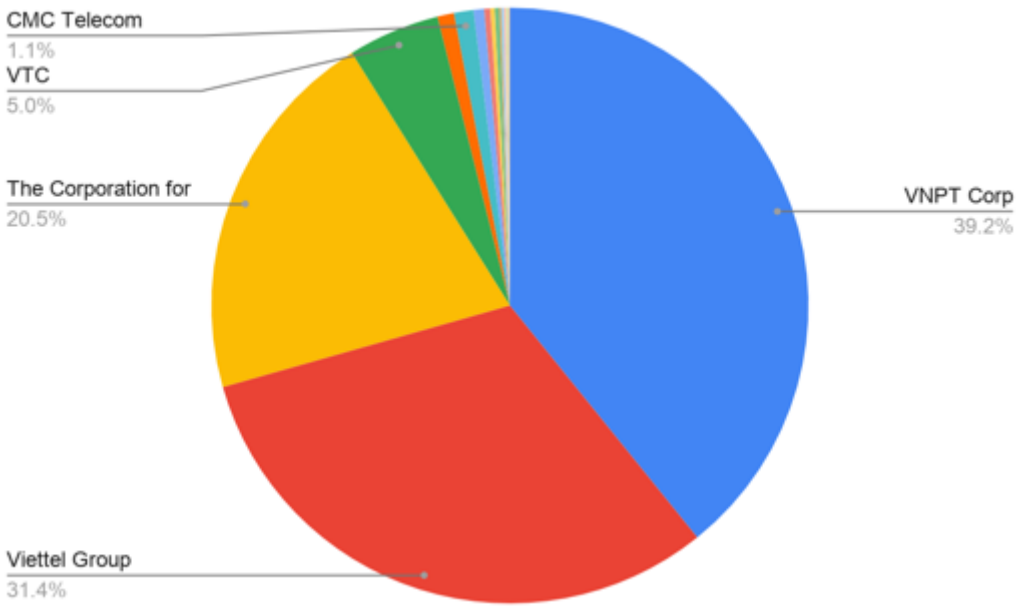
MAJOR SSDP CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, SSDP is the fourth most prevalent of those risks in Vietnam. Of the 1,227 open SSDP services nationwide, all of them (100%) are hosted by the 17 ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	VNPT Corp	481	Telecom	Vietnam
2	Viettel Group	385	Telecom	Vietnam
3	The Corporation for Financing & Promoting Technology (FPT)	252	Telecom	Vietnam
4	VTC	61	Telecom	Vietnam
5	SCTV	11	Telecom	Vietnam
6	CMC Telecom Infrastructure Company	13	Telecom	Vietnam
7	Netnam Company	7	Telecom	Vietnam
8	MOBIFONE Corporation	4	Telecom	Vietnam

9	Maxdata	3	Cloud	Vietnam
10	Vietnam Technology and Telecommunication JSC	3	Telecom	Vietnam
11	Hanoi Telecom Joint Stock Company - HCMC Branch	1	Telecom	Vietnam
12	Hanel Communication JSC	1	Cloud	Vietnam
13	Saigon Postel Corporation	1	Telecom	Vietnam
14	TIEN PHAT TECHNOLOGY CORPORATION	1	Cloud	Vietnam
15	Telehouse international corporation of vietnam	1	Cloud	Vietnam
16	Viet Online trading service corporation	1	Cloud	Vietnam
17	Securebit AG	1	Cloud	European Union

The pie graph below illustrates, among those 1,227 open SSDP services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs - and especially the top 3 which host nearly over 90% of the open SSDP services nationwide - to mitigate could result in a substantial reduction of potential DDoS infrastructure.

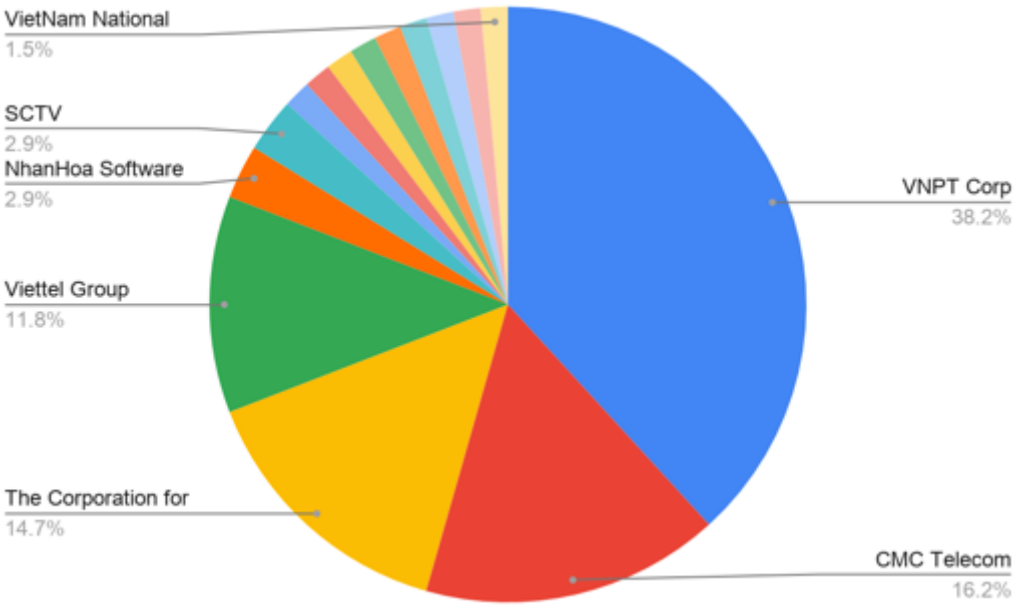


MAJOR CHARGEN CONTRIBUTORS

Of the 5 open services that are scanned by CyberGreen, CHARGEN is the least prevalent of those risks in Vietnam. Of the 68 open CHARGEN services nationwide, all of them (100%) are hosted by the fifteen Vietnamese ISPs listed in the table below.

Rank	ISP	Count	Type	Allocated Country
1	VNPT Corp	26	Telecom	Vietnam
2	CMC Telecom Infrastructure Company	11	Telecom	Vietnam
3	The Corporation for Financing & Promoting Technology (FPT)	10	Telecom	Vietnam
4	Viettel Group	8	Telecom	Vietnam
5	NhanHoa Software company	2	Cloud	Vietnam
6	SCTV	2	Telecom	Vietnam
7	Ocean Commercial Joint Stock Bank	1	Bank	Vietnam
8	Branch of Long Van System Solution JSC - Hanoi	1	Cloud	Vietnam
9	Vietnam Technology and Telecommunication JSC	1	Telecom	Vietnam
10	Ha Noi University of Technology	1	University	Vietnam
11	Saigon Postel Corporation	1	Telecom	Vietnam
12	Netnam Company	1	Telecom	Vietnam
13	Viet Solutions Services Trading Company Limited	1	Cloud	Vietnam
14	Maxserver Company Limited	1	Cloud	Vietnam
15	VietNam National University Ha Noi	1	University	Vietnam

The pie graph below illustrates, among those 68 open CHARGEN services quantified in the table above, the contribution of each ISP. Reaching out and collaborating with the top 5 ISPs to mitigate could result in a reduction of potential DDoS infrastructure.


VietNam National
1.5%
SCTV
2.9%
NhanHoa Software
2.9%
Viettel Group
11.8%
The Corporation for
14.7%
VNPT Corp
38.2%
CMC Telecom
16.2%

WHO WE ARE

The CyberGreen Institute (CyberGreen) has produced this comprehensive report on vulnerabilities and threats within and facing the Internet ecosystems of the ASEAN nations. The outputs of this report show, quantitatively and based on actual data, the cyber risk posture of those ten nations and the steps needed to reduce and mitigate exposure to both the ASEAN region and global Internet ecosystems.

CyberGreen was the main contributor of data, analysis, and recommendations related to open services for this report.

ABOUT CYBERGREEN

CyberGreen is a global non-profit and collaborative organization that serves the global public benefit by supporting a more resilient and healthier global Internet Ecosystem. CyberGreen is a trusted player in that Ecosystem following transparent ways of working, and identifying sources of risk and best practices for the community. We are committed to evidence-driven metrics and measurements.

Practices include:

- For community members: Providing reliable metrics, measurements, analysis, and mitigation best practices
- For policymakers: Ensuring that policy development and capacity building have the insight to focus on reducing systemic risk conditions
- For CERTs/CISOs: Facilitating operational clean-up of systems.

More information and statistics can be found at https://www.cybergreen.net and https://stats.cybergreen.net.

DATA & ANALYSIS CONTRIBUTORS

GLOBAL CYBER ALLIANCE

The Global Cyber Alliance (GCA) provided data and analysis related to email infrastructure for this report.

GCA is an International nonprofit 501(c)(3) organization that focuses on making the Internet safer by developing and deploying practical and real-world solutions that measurably improve our collective cybersecurity. GCA was founded in 2015 by law enforcement and research

organizations, namely, the District Attorney of Manhattan, the City of London Police, and the Center for Internet Security.

DOUBLE SHOT SECURITY

Double Shot Security provided analysis and recommendations related to open services and routing infrastructure for this report.

Double Shot Security is a company whose expertise lies in creating and leading global cybersecurity initiatives. Through a combination of education, analysis, and design, the organization focuses on creating strategies and frameworks to improve online safety and trust for evolving digital economies.

PACKET CLEARING HOUSE

Packet Clearing House (PCH) provided data and narratives related to routing infrastructure for this report.

PCH advises policy makers and government ministries on issues related to Internet development and cyber-security. Using its extensive research and service network, PCH measures key indicators of the development and independence of a nation's Internet ecosystem, and provides recommendations for policies to improve them.

ACKNOWLEDGEMENT

We would like to express our gratitude to the following individual for his input and advice:

Gaus Rajnovic