CYBER PUBLIC HEALTH REPORT FOR THE ASEAN REGION: AN 18-MONTH REVIEW

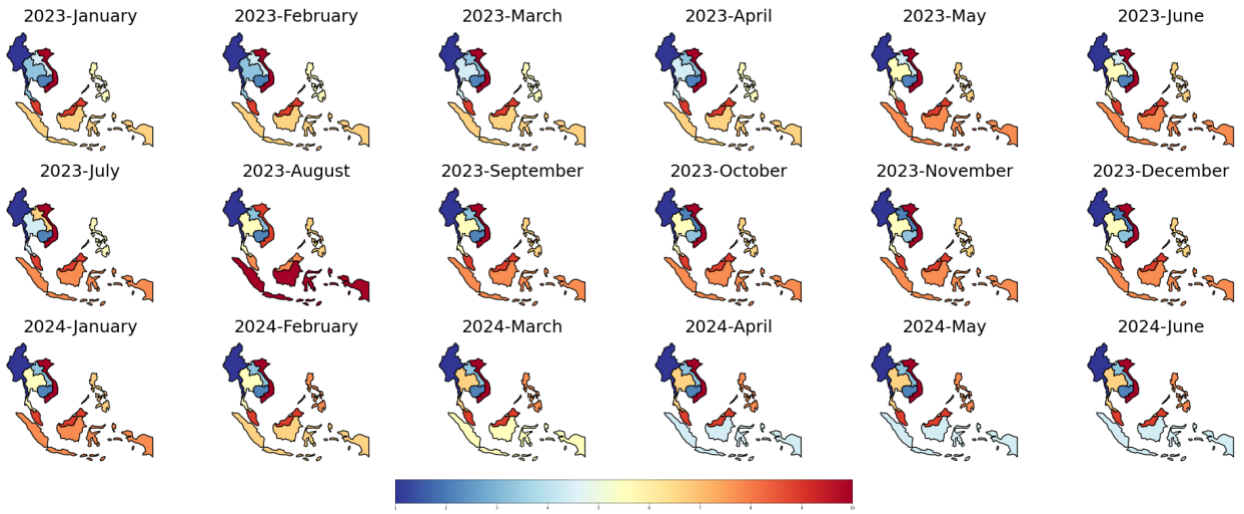
An assessment of the Cyber Public Health of internet infrastructure in ASEAN member states, based on 18 months of measurement from January 2023 to June 2024.

David Conrad, Sudheesh Singanamalla, Arastoo Taslim, Yurie Ito
CyberGreen Institute
October 2024

EXECUTIVE SUMMARY

This Cyber Public Health report provides a view of the cybersecurity risk landscape across the ASEAN region. It highlights the disparities in digital infrastructure health and resilience among member states over an 18-month period, from January 2023 to June 2024. This study identifies critical trends related to core, publicly reachable internet infrastructure services that underlie nearly all users, with particular emphasis on the evolving cyber risk landscape.

Through the collection and analysis of publicly observable data, CyberGreen has established a framework that parallels public health principles, applying those principles to the cyber domain. This innovative approach offers ASEAN member states a means to benchmark and improve their cybersecurity posture, fostering a healthier, more resilient regional internet ecosystem.



Timeline of changes in relative rankings across all components scanned by CyberGreen. The darker blue (lower ranks) indicates better ranking compared to the reds (higher ranks).

The figure presented above indicates the changes in relative rankings for ASEAN countries as identified by the various components in CyberGreen's Internet Infrastructure Health Metrics Framework (IIHMF). Specifically, these relative rankings take into account factors such as security in routing, Domain Name System (DNS) infrastructure, adoption of strong cryptographic protections for web and mail communications, the security of the serving infrastructure, and risks due to services that are open to anyone on the Internet. The darker blue shaded countries in the map indicate higher ranks (which are desirable), compared to the red colors which indicate lower ranks. While this individual rank provides some insight into how a specific country is performing relative to others, it is by no means the only metric that can inform the prioritization of policy development. In this report, we highlight the key actions based on the nuances of the data collected from various components that are actively scanned by CyberGreen and present our detailed findings.

Our analysis of the IIHMF scores has identified improving the security of the routing system as the top priority for ASEAN countries. The most critical actions to affect this improvement would be

the implementation of route validation and, secondarily, the signing of information that identifies the authorized originator of specific routing objects.

Key Actions:

1. **Route Validation**: Validating the origin of routing information is helpful in securing internet infrastructure by preventing mis-origination of routes or when attackers gain access to legitimate IP address blocks announcing it from a different autonomous system in an attempt to redirect traffic and convince the peers to update their routes. Adoption of route validation significantly reduces the risk of misconfiguration in routing information, improving the integrity of the region's cyber infrastructure.
2. **Signing of Routing Information**: Although cryptographically signing the origin of routing information is less important than enabling validation of those signatures, it further strengthens routing security. The initial focus should remain on validation of route origins due to its immediate impact in mitigating misconfigurations.

Other key takeaways from this study include:

- **Open services**, which are internet services that can be reached by anyone, continue to pose significant risks to the region and the internet as a whole, particularly due to the ease by which they can be weaponized. Countries including Myanmar and Cambodia have shown improvement in reducing their availability to attackers, but overall, sustained efforts are necessary to close these vulnerabilities.
- **Naming infrastructure (DNS) security** remains underdeveloped across the region, although some countries, such as Singapore and Thailand, have made notable progress. Indicators of deployment of best practices and proper configuration of naming infrastructure indicate a need for better management practices to ensure resilience and security.
- **Internet routing security**, which can help protect the mechanisms by which internet traffic is directed from source to destination, has improved in some countries but gaps remain, especially in nations with less mature digital infrastructure.
- **Security of communications**, in which individual data exchanges between a source such as a web server and a destination such as a browser are protected, is improving with the adoption of modern protocols and stronger cryptographic algorithms. However, the use of outdated protocols still persists, exposing systems and communications to unnecessary risks.
- **Email security**, which is increasingly adopting the usage of secure communication protocols, shows some countries such as Singapore having successfully enabled secure communications for all incoming mail server communications. However, the adoption of modern standards for email policies that require secure communications (MTA-STS, DMARC) is extremely low – in line with global trends and could improve their security posture.

The results of this study point to the need for continued regional cooperation and the development of unified cybersecurity standards. By leveraging CyberGreen's IIHMF, ASEAN nations can better understand their cybersecurity challenges and allocate resources to address those challenges effectively. The policy recommendations outlined in this report emphasize the importance of public-private partnerships, investment in cybersecurity education, and the adoption of best practices to address specific concerns in the areas of service availability, routing and naming infrastructure, and secure communications configurations.

As ASEAN continues its digital transformation, ensuring the health of its internet infrastructure will be paramount to safeguarding the region's economies and societies. The insights and data presented in this report can inform a roadmap for governments, network operators, and policymakers to work together toward a more secure, stable, and resilient cyber environment.

The journey toward improving Cyber Public Health is an ongoing process, and future research will need to explore additional vulnerabilities and risk areas. By continuing to monitor and address these challenges, ASEAN can strengthen its position in the global cybersecurity landscape and protect its digital future.

1. INTRODUCTION

ASEAN confronts a range of unique challenges in its digital environment that significantly impact its approach to cybersecurity and risk management. The region's varied levels of technological advancement mean that while some member states possess sophisticated technological infrastructure capable of mitigating cyber threats, others lag, creating a gap of internet infrastructure health. This disparity is further complicated by high volumes of cross-border data flows, inherent to ASEAN's diverse economic activities, necessitating robust mechanisms to secure data while ensuring its free movement across national borders.

Moreover, the cybersecurity landscape in ASEAN is not unified, with each member state operating under its distinct set of cyber laws and regulations. This lack of uniformity can hinder the implementation of region-wide cybersecurity measures. As the region undergoes rapid digitalization, it faces an escalation in cyber threats, including cybercrimes and state-sponsored attacks, demanding dynamic and resilient response strategies.

Over the past five years, ERIA and CyberGreen have been collaborating on the development of a science of Cyber Public Health and the Internet Infrastructure Health Metrics Framework (IIHMF), grounded in the shared recognition of the following principles:

- To successfully advance both digital transformation and cybersecurity, it is essential to move beyond traditional security measures and adopt innovative approaches inspired by global public health and international healthcare frameworks.
- Enhancing the resilience of the entire internet ecosystem against risk factors is a critical initiative, directly contributing to the broader cybersecurity strategy of the ASEAN region.
- Given that cyberspace and its associated risks transcend national borders, it is vital to strengthen the resilience of the regional cyber ecosystem in tandem with ASEAN's digital transformation efforts.
- The importance of robust data and statistics-driven policymaking, coupled with effective policy analysis, is a foundational element for sustainable progress.
- ERIA aims to function as ASEAN's equivalent to the OECD, playing a key role in gathering and providing essential data to inform and shape effective policymaking.
- A coordinated and unified approach across the ASEAN region is crucial to avoid heightening geopolitical tensions or fostering competition between nations.

In line with these objectives, CyberGreen has focused on establishing a science of Cyber Public Health, dedicated to making the internet safer and more resilient for all. A key part of Cyber Public Health, like concepts associated with human public health it is modeled after, is establishing a baseline of statistics in order to identify significant deviations away from that baseline. Just as a spike in body temperature (a fever) can suggest an issue of concern in a person, a significant change in observable statistics related to network "health" can suggest areas in which further investigation of the network is warranted. This document presents results based on trends related to five categories of internet components relevant to the state of ASEAN's Cyber Public Health: open services, DNS, routing, email, security protocols and certificates. These components are frequently associated with security incidents or threats and the data collected is plotted and analyzed over the course of the

study period (18 months). This report highlights some key learnings based on the data collected, suggests some possible areas of policy change, and reflects on the improvements in data gathering we aim to make in the future.

2. STUDY DESCRIPTION

For this study, CyberGreen has collected and analyzed publicly available data related to operational security, such as vulnerabilities, exposures, and unhealthy operations, from networks in the ASEAN region, specifically Brunei Darussalam, Indonesia, Cambodia, Laos, Myanmar, Malaysia, The Philippines, Singapore, Thailand, and Vietnam, for 18 months from January 2023 to June 2024. The data collected is broadly categorized as:

- Open Services Exposure
- Internet Routing Security
- Domain Name System (DNS) Infrastructure Security
- Web Protocols Security: TLS & Certificates
- Email Security – Communications and Policy

A brief description of these categories follows.

WHAT IS OPEN SERVICES EXPOSURE?

Open services represent network services that are made available to anyone on the internet capable of reaching the server. This is in contrast to closed services in which the clients that can connect to the service are limited in some way, e.g., by client IP address or by requiring authentication of some sort such as by supplying a userid/password. A simple analogy for an open service exposure would be an unlocked door of a building – if you can get to the door, you can enter the building. Similarly, with open services, if you can initiate a connection to the service, you can access the service. These open services can be used to create Distributed Denial of Service attacks.

WHAT IS INTERNET ROUTING SECURITY?

Internet routing security represents controls that help mitigate the lack of security built into the Border Gateway Protocol (BGP), the common language used by network operators to exchange information used to direct internet traffic from a source to a destination. This information is used by network operators to "announce" the IP addresses they provide service for to their service providers and peers, who propagate those announcements to their service providers and peers, and so on, enabling traffic to be sent from a source to any reachable destination on the internet. Internet routing security provides tools that reduce the risk that those initial announcements are faked, which lessens the probability that traffic gets lost or redirected to malicious sites.

WHAT IS DNS INFRASTRUCTURE SECURITY?

Just as BGP was designed without much consideration to security, the Domain Name System (DNS) was created in a time when securing the information provided by DNS was an afterthought. Unfortunately, a flaw in the original design of the DNS led to a particular vulnerability that would allow a determined attacker to modify the responses to DNS queries, allowing attackers to redirect

connection initiation to malicious attacker-in-the-middle servers. Because DNS is about human-readable names, this is also referred to as "naming security."

DNSSEC

The solution to that particular vulnerability, a protocol enhancement called Domain Name System Security Extensions (DNSSEC), allows the recipient of DNS responses to verify there have been no unauthorized modifications to domain information. CyberGreen measures whether certain government-level domains in its dataset have enabled DNSSEC. Note that, at this time, CyberGreen does not measure all domains in a country's TLD, just a selection of government domains.[1] For example, we might measure within .gov.uk, but not ac.uk (academic) or co.uk (corporate). We may or may not have the ability to ensure complete coverage within .gov.uk, depending on their choice to publish a list of the names within a particular domain (technically, a domain's "zone file").

LAME DELEGATIONS

We also measure the number of lame delegations, which are issues that occur when a nameserver identified to be responsible for a specific domain is unable to authoritatively provide information about that domain. This misconfiguration exposes domains to performance, reliability, and security risks, and is clearly an operational issue. The presence of lame delegations is an indicator that DNS records are not being maintained with sufficient care. This likely correlates with other security issues, possibly more broadly than DNS.

WHAT IS "WEB PROTOCOLS SECURITY": TLS & CERTIFICATES?

Transport Layer Security (TLS) is a set of tools that enable communications to be confidential with strong assurance of the integrity of that communication, i.e., that information exchanged is both kept private and unmodified. These tools are used extensively to reduce the risk of eavesdropping, tampering, and impersonation in both web services and email. CyberGreen measures the use of certificates for both web services and email to show the authenticity of communications, the validity of the certificates, and also scores the configuration of TLS in use.

WHAT IS EMAIL SECURITY?

Email security protocols provide a mix of authentication, integrity, and confidentiality to the exchange of email. Authentication prevents spoofing, integrity prevents tampering, and confidentiality prevents eavesdropping/observing. CyberGreen assesses email security based on the following:

1. **Sender Policy Framework (SPF):** Protocols that help prevent email spoofing and provide authentication. This is done through DNS entries known as SPF resource records, indicating which mail servers and corresponding IP addresses are permitted to send email on behalf of

[1] CyberGreen's dataset consists of over 400,000 unique government hostnames. This list was compiled by combining country domains (such as .ly, .us, .au) with common government extensions (such as .gov, .gob, and .go). Other exceptions (e.g., .fed or .mil) were manually added.

a domain.

2. **Domain-based Message Authentication, Reporting and Conformance (DMARC):** A security protocol that builds on top of SPF and other email authenticity standards such as DomainKeys Identified Mail (DKIM) to report on attempts to impersonate, i.e., spoof, the sender of email.

3. **SMTP MTA Strict Transport Security (MTA-STS):** A security standard that ensures that TLS connections are always used and provides a mechanism allowing servers to refuse message delivery to servers without trusted certificates.

4. **Start-TLS:** An email protocol command that is used to inform the email server to upgrade the plaintext connection between the client and server to a secure TLS enabled connection. Mail servers enable secure connectivity between the sending client and the server by negotiating TLS handshakes after the STARTTLS command is issued by the client.

3. STUDY RESULTS

Results of this study are presented according to the five categories of security-related data CyberGreen has collected and analyzed as discussed previously.

OPEN SERVICES

In the context of the Internet Infrastructure Health Metrics Framework (IIHMF), CyberGreen has created metrics for and tracked some of the most commonly abused open services on the internet: the Domain Name System (DNS), the Character Generator protocol (CHARGEN), the Network Time Protocol (NTP), the Simple Service Discovery Protocol (SSDP), and the Simple Network Management Protocol (SNMP). These services will be described in more detail below.

There are two common contributing factors to the risks associated with open services: source address spoofing and amplification. Source address spoofing is a network issue: when a packet is sent across the internet, it contains both a destination address, i.e., the address of the receiving side of the communication, and a source address, i.e., the sending side of the communication. In many networks, there is no validation that the source address actually corresponds to the address of the device sending the packet. In these cases, an attacker can insert a victim's IP address as the source. When the recipient receives that packet, it will respond by sending data to what it believes to be the source. Because of the spoofing, that's not the actual sender, but the victim.

The second factor, amplification, takes advantage of the difference in the amount of data between a query and the response. In contrast to source address spoofing, amplification is a server side concern. In most services, a source sends a query, e.g., "show me a web page" and the destination provides a response, e.g., "here's the web page". Typically, the query is small, usually a few tens of bytes, and the response is large, on the order of hundreds to millions of bytes or more. In normal

operation, the source is prepared to receive what the destination returns, but when combined with source address spoofing, the source didn't actually request anything from the destination, so it will be unprepared for whatever comes from the destination.

The combination of these two factors means that open services can facilitate "Distributed Denial of Service" (DDoS) attacks, which becomes a potent weapon in the hands of attackers. With enough open services, DDoS attacks, also known as "volumetric attacks", can overwhelm pretty much any infrastructure on the internet and they are hard to defend against since, in many cases, the requests are perfectly valid. While tools and techniques exist to reduce the impact of DDoS attacks, a better solution is to reduce the availability of the open services that the attackers use.

OPEN DNS SERVICES

One of the most important underlying services on the internet is the Domain Name System (DNS). The DNS has been called the "phone book of the internet" as it allows for the translation of a name into information about that name, e.g., how to contact the service(s)associated with the name. For example, if a user wants to view a web page on (say) "example.com", the DNS is the mechanism used to translate example.com into the IP address(es) used for example.com's web server.

One common problem on the internet is that part of the lookup mechanism built into the DNS, known as the "resolver" can be open, i.e., the resolver can answer requests from anyone on the internet instead of just the users of the network operator that is running the resolver. These "open resolvers" can be used by malicious actors to attack any device on the internet by sending lookup requests to the open resolver with source address spoofing. If enough open resolvers are used and/or the queries generate sufficiently large responses, the attacker can overwhelm the victim via a DDoS attack. Other attacks may be possible via open resolvers, particularly if DNSSEC has not been implemented on the resolver, so best practice is for network operators who run DNS resolvers to limit who the resolver will respond to and to enable DNSSEC.

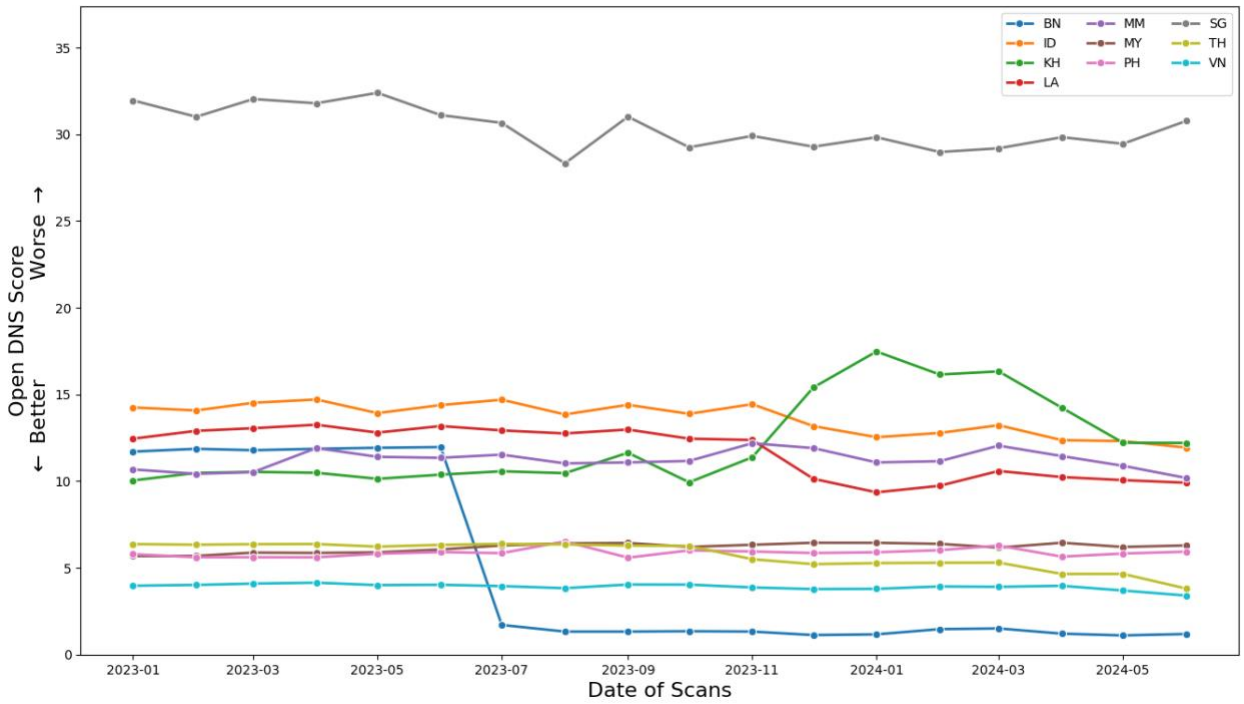


Fig. 1: Changes in open DNS scores over time.

The CyberGreen "Open DNS" scores provide an indication of the presence of open DNS resolvers within networks identified to be within ASEAN countries. The higher the score, the larger the percentage of open resolvers and hence the greater the risk. As shown in Figure 1 above, significantly more open DNS resolvers appear to be found within Singaporean (SG, gray line) networks as compared to networks associated with other ASEAN member nations. Figure 1 also shows that in June 2023, there was a dramatic decrease in the number of open DNS resolvers in Brunei Darussalam (BN, dark blue line) networks, indicating an improvement in their scores beyond the previous lowest, Vietnam's (VN, light blue line). Vietnam maintains a consistent score with essentially no changes to the number of Open DNS services observed during the 18 months of observation. Indonesia (ID, orange line) and Laos (LA, red line) see a slight improvement in their risk scores while Cambodia (KH, green line) sees a temporary increase in January 2024 indicating a worsening of their scores implying an increased risk, but this increase was quickly followed by improvements in May 2024, returning the Cambodia score to just slightly worse than it was prior to the increase.

OPEN CHARGEN SERVICES

CyberGreen's "OpenCHARGEN" scores, similar to the OpenDNS scores, provide an indication of the presence of the Character Generation (CHARGEN) service. CHARGEN is a legacy protocol originally used for testing and debugging that simply responds with meaningless data when it receives a request. Unlike DNS, which must be available to at least some machines on the internet, in today's world CHARGEN is no longer actively used and most modern machines generally turn the service off by default.

Unfortunately, when enabled and available, attackers can make use of CHARGEN for DDoS against victims anywhere on the internet, at least anywhere that allows CHARGEN traffic. As such, best practice is for network operators to disable CHARGEN on all their machines.

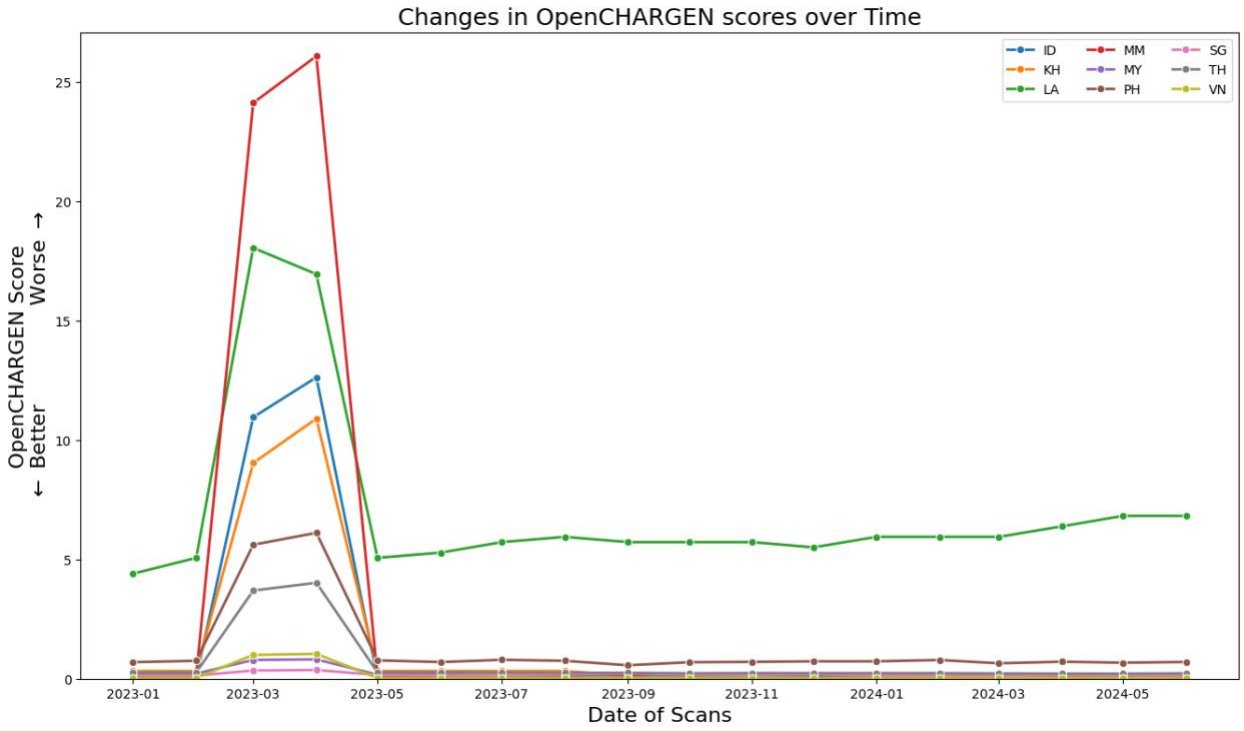


Fig. 2: Changes in open CHARGEN scores over time.

The green line in Figure 2 suggests a lot of infrastructure in Laos (LA) consistently exposes the CHARGEN service, significantly more than in other countries in the ASEAN region and that exposure is growing as indicated by a score which is slowly increasing over time. More generally, there was an anomalous spike in the CHARGEN scores between February - May 2023 for most ASEAN countries, with the highest increase being in Myanmar (MM, red line), and significant increases in Indonesia (ID, blue line), Cambodia (KH, orange line), Philippines (PH, brown line) and Thailand (TH, gray line). This spike disappeared by May, with scores remaining relatively stable thereafter. This observed spike is not just seen in the ASEAN region, but globally, which would suggest a scanner anomaly rather than an actual spike in open CHARGEN services. CyberGreen continues to explore the cause of this anomaly.

OPEN NTP SERVICES

The Network Time Protocol (NTP) service enables devices connected to the internet to have accurate time by allowing those devices to synchronize with highly accurate time sources that are available via the internet. Many, if not most, machines on the internet need to use NTP to have accurate time. However, incorrectly configured Network Time Protocol (NTP) services can be and are used for DDoS attacks. CyberGreen's "OpenNTP" score measures open NTP services, and as with the previous scores, the higher the score, the larger the percentage of open NTP servers, and thus, the higher the risk of facilitating DDoS attacks.

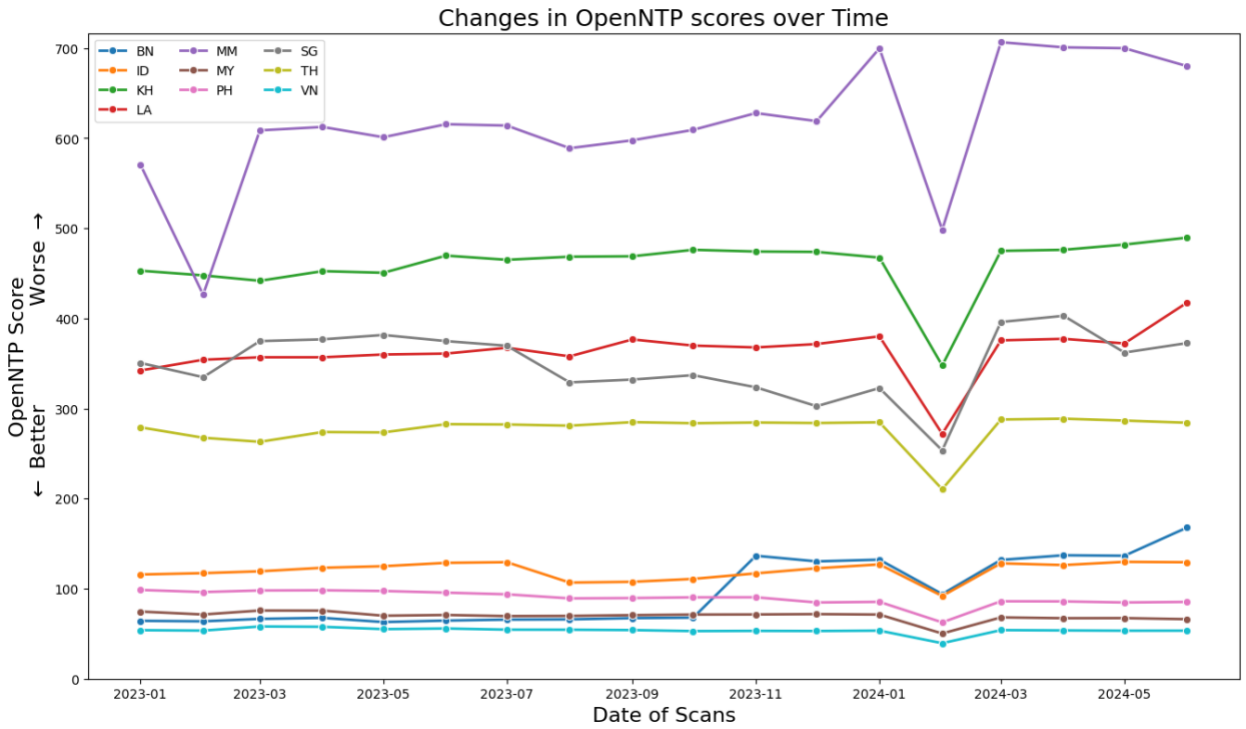


Fig. 3: Changes in open NTP scores over time.

The scores over the observation period indicate Myanmar (MM, purple line) has the highest percentage of exploitable NTP services, and that Myanmar's score is generally increasing over time. Myanmar's score is followed by Cambodia (KH, green line), Laos (LA, red line) and Singapore (SG, gray line), which have also seen a fairly consistent increase over time. Our observations also indicate worsening of scores for infrastructure associated with networks in Brunei Darussalam (BN, blue line). There was an anomalous dip around February 2024 which momentarily affected all countries in the region. The cause of this dip is unknown; it could be a policy change or (more likely) an inconsistency with the scanning infrastructure. More generally, nearly all ASEAN countries indicate a slight upward trend implying higher numbers of accessible NTP servers, increasing overall risk of NTP-based DDoS attacks not just within the ASEAN region but globally since open services can target anywhere on the internet.

OPEN SSDP SERVICES

The Simple Service Discovery Protocol (SSDP), used to help users find resources like printers or media servers on a local network, can be abused for DDoS attacks when an SSDP server is (mis)configured to send responses off the local network.

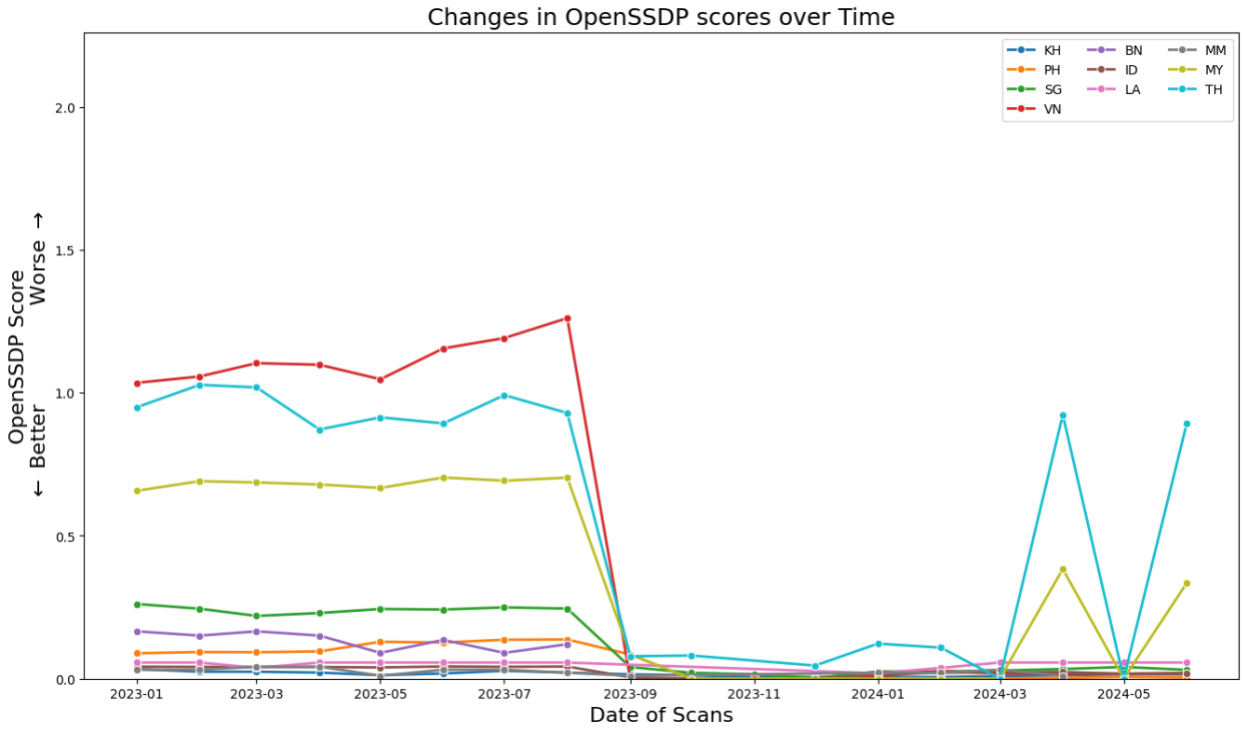


Fig. 4: Changes in open SSDP scores over time.

CyberGreen's "OpenSSDP" score measures these servers, where higher scores indicate greater risk and lower scores are more desirable. In August 2023, our observations indicate sustained and strong improvements across all ASEAN countries indicating a significant reduction in servers exposing SSDP services to the global internet. However, more recent measurements in 2024 (Apr - June) suggest worsening in scores for Thai (TH, light blue) and Malaysian (MY, olive green) networks. These increases indicate SSDP servers within the networks of those countries are again exposed to the internet, implying the risk they may be used for DDoS attacks has risen.

OPEN SNMP SERVICES

The Simple Network Management Protocol (SNMP), as the name implies, allows network operators to manage and monitor the various devices that are connected to their networks. Use of versions of SNMP prior to version 3, misconfiguration of SNMP servers, e.g., with weak credentials, and vulnerabilities in SNMP implementations can allow attackers to gain visibility into and possibly control over an organization's networks. As such, access to SNMP services are ideally isolated to be within a network but may be intentionally exposed to the public internet to allow for remote monitoring and management. As with previous open services scores, a higher score suggests greater risk, with lower scores preferable.

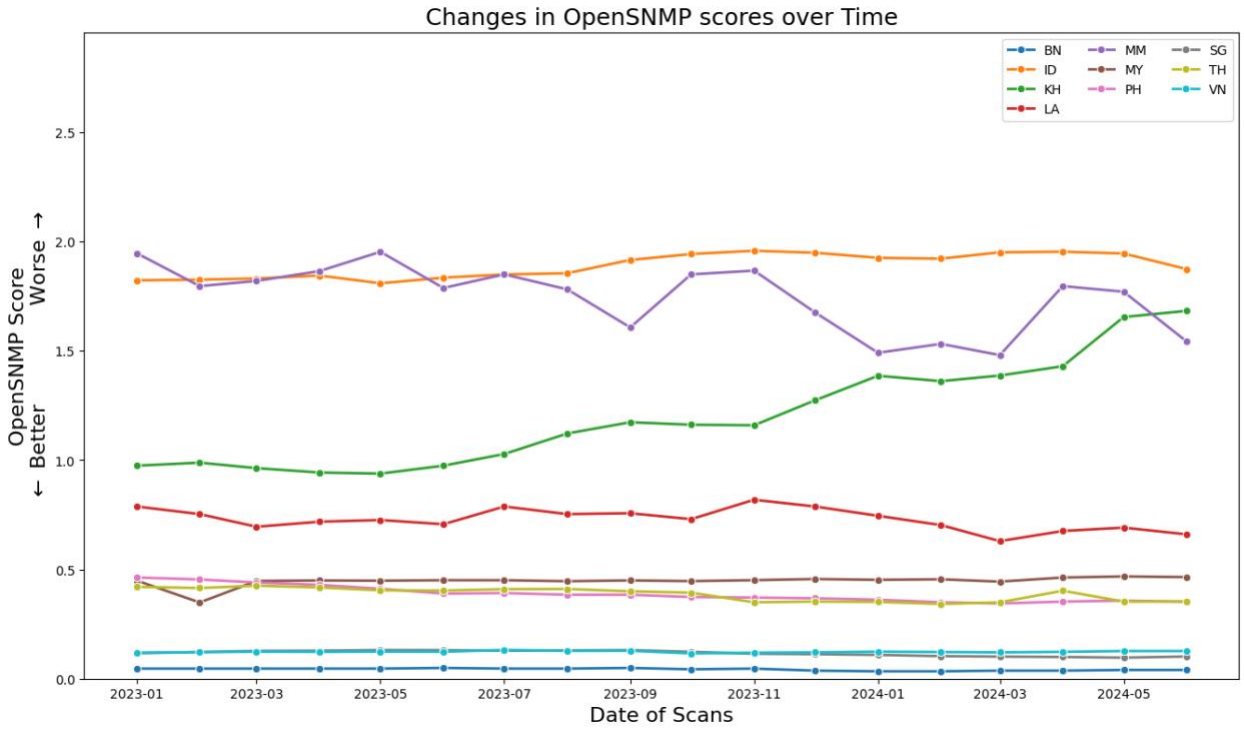


Fig. 5: Changes in open SNMP scores over time.

CyberGreen's "OpenSNMP" score measures the reachability of SNMP services with higher scores indicating higher risk and lower scores being more desirable. We observe higher Open SNMP scores suggesting increased risk due to exposed SNMP services in Indonesian networks (ID, orange line) followed by Myanmar (MM, purple line) and Cambodia (KH, green line). While Indonesia's risk scores have remained steady, Cambodia's score increased during this time implying increasing risk while Myanmar's score improved. Generally, other ASEAN countries have demonstrated slight improvements over time with the lowest scores being observed in Brunei Darussalam (BN, blue line).

SUMMARY OF OPEN SERVICES

In Figure 6, the individual scores for open services are aggregated for each ASEAN country and the rankings for each country are presented, relative to the rest of the world. These rankings help identify the ASEAN countries which could benefit the most from security improvements in their infrastructure to reduce risks due to open services. These rankings could also help to identify nations that have taken effective measures to reduce risks posed by open services. Lower numbered ranks are preferred over higher ones.

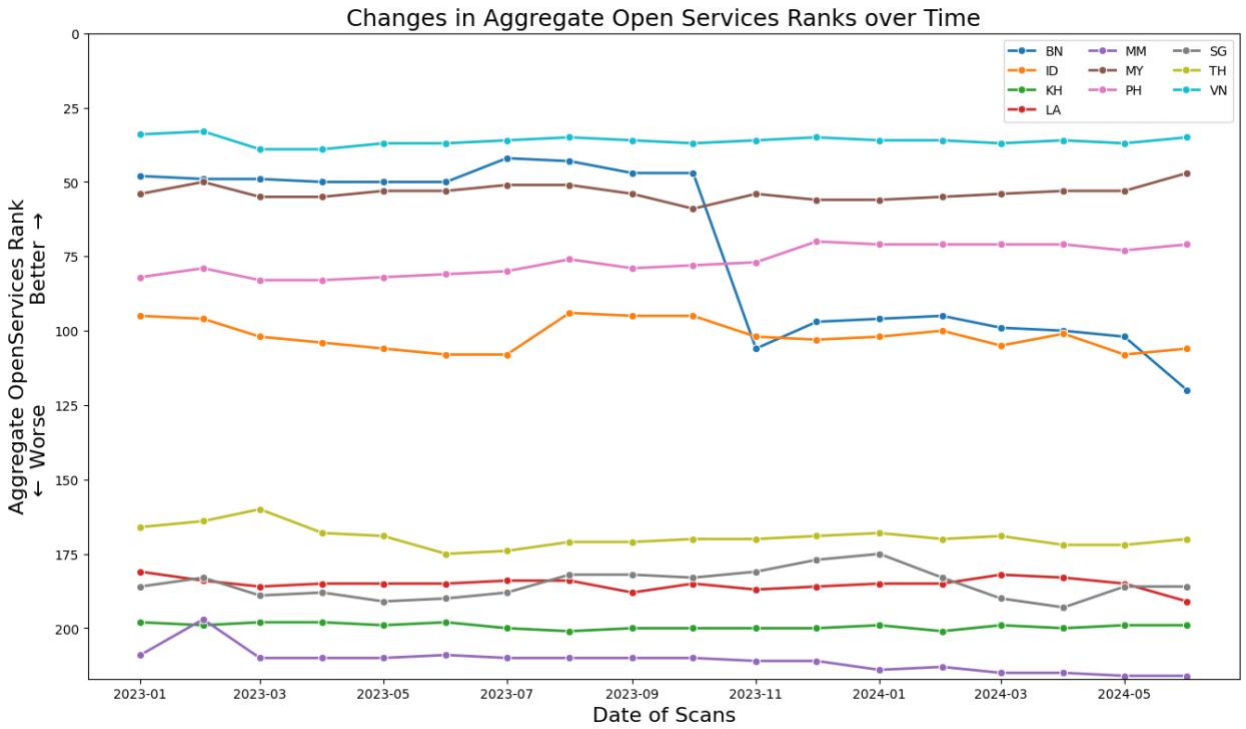


Fig. 6: Changes in global ranking over time due to open services

We observe that Vietnam (VN, light blue line) leads the ranking among ASEAN countries and is remarkably steady over time. Over the last 18 months, we also see improvement in the scores for the Philippines (PH, magenta) and Malaysia (MY, brown). However, Brunei Darussalam (BN, dark blue) witnessed a significant reduction in the rankings due to worsening open NTP scores, eventually putting them below the top 100 ranked countries, which indicates a weaker security posture relative to the rest of the world. The score for Myanmar (MM, purple) has generally been the lowest and continues to worsen with a rank in the 200s despite a momentary improvement in February 2023. Globally, 5 of the 10 ASEAN countries have rankings within the top 100, with 2 being within the top 50. Additionally, two ASEAN countries account for the lowest rankings globally due to the relative risks posed by their networks as a result of various open services. To summarize, we see significant disparity in the region with respect to levels of open services exposure.

In the context of public health, given a globally interconnected world, vaccination and other measures such as establishing "herd immunity" that reduce the chance of infection from viral diseases in one country help protect people in other countries by limiting the opportunities for viruses to spread. Similarly, in the context of Cyber Public Health, as the internet is a global system, improvements in security practices such as closing open services can reduce the risk experienced by networks in other countries.

WHY DO OPEN SERVICES MATTER TO CYBER PUBLIC HEALTH?

Using our analogy of public health, open services can be seen as analogous to people who carry and spread contagious disease but show no symptoms. The disease, i.e., DDoS attacks, is propagated because the disease carrier, i.e., the network operator with the open service, isn't quarantined nor, in many cases, is the carrier even aware they are carrying the disease. CyberGreen's OpenDNS,

OpenNTP, OpenSSDP, OpenSNMP, and OpenCHARGEN scores measure services that pose a risk to third parties due to those services potentially being used for DDoS.

Extending the analogy, some diseases are much more virulent than others, e.g., the Ebola virus is much more dangerous than the rhinovirus, which causes the common cold. Similarly, some open services can be much more damaging than others. The amplification factor of a protocol is an example: if the amplification factor is 1, an attack using that open service would be about the same as the attacker attacking directly, sort of the equivalent of a common cold: annoying, but rarely concerning and easily treated. However, some open services, when sent a request, answer with a response that is many times the size of the request. These sorts of attacks can multiply the impact the victim must withstand, in some cases far beyond what they're capable of withstanding. These "amplification attacks" are analogous to the Ebola virus: they can be extremely concerning and can overwhelm all but the most extreme defenses.

All the CyberGreen open services scores measure the risks of amplified DDoS attacks. These open services can have severe impact when exploited by attackers and are used to target attacks on sensitive and critical infrastructure such as banking, government services, or payment and identity infrastructure.

Open services including DNS resolvers increase the risk of DDoS attacks. Additionally, if an open DNS resolver is controlled by an attacker (rather than simply responding to spoofed source addresses), it can also enable DNS-based redirection attacks. This is because responses from resolvers to client applications are seldom, if ever, verified — even when DNSSEC is in use. Open DNS services can be compared to a potentially contaminated water source in public health, which does not cause illness unless someone drinks from that water source. The existence of open DNS services might not be severely problematic but users communicating with an open resolver may be exposed to severe risks because of their virulent capabilities to quickly activate and infect, e.g., by providing incorrect DNS responses that cause users to navigate to malware or malicious services, or by amplifying an attack against a specific target, potentially causing severe consequences. While identifying these open DNS services is similar to recognizing and identifying a contaminated water source in public health, additional preventive measures need to be put in place to remove the contamination or reduce its risk. This analogy applies for other open services such as those measured with the OpenCHARGEN, OpenSSDP, and OpenNTP metrics.

Open SNMP services on the other hand can be characterized not just as a virus that enables DDoS attacks when infected, but can also result in information leakage due to their ability to provide the network configuration and status to external parties – information which would otherwise not be available to adversaries on the internet. Adversaries can then take advantage of vulnerable clients within these networks, enabling the creation of botnets which can participate in large scale DDoS attacks such as those caused by the Mirai botnet. In the Cyber Public Health setting, the existence of Open SNMP services and the ability to exploit the vulnerabilities it enables increase the risk for interconnected devices which could be compromised and have unintended consequences – possibly resulting in cyber-pandemics.

Public and private network vulnerability scanners operating globally, similar to those provided by CyberGreen, frequently collect information about the risk posed by each independently operated set of networks in a country due to exposed services and malicious request behavior from IP addresses. Some organizations publish this information as "blocklists" that list the IP addresses or domain

names that are deemed risky by the manager of the blocklist. These lists are used by many network administrators around the world to prevent abuse of their systems. However, this practice can have severe consequences for users of these networks as they can experience bounced or discarded email, higher CAPTCHAs, rate limiting behaviors, and blocked access to pages because of firewall rules implemented by various network administrators in other organizations both public and private globally making use of block lists. A public health analogy of this situation would be countries imposing travel bans which have significant economic and social impact in the face of epidemics. As with public health, prevention of the underlying "disease" is far preferable to dealing with the outcomes once the disease has spread.

HOW TO IMPROVE OPEN SERVICES SCORES

The services identified and mapped to each country in our measurements are restricted to registered ISP and organizational networks within each country. Establishing communication and reporting channels between CyberGreen and various network operators within relevant countries would allow direct data sharing with the necessary stakeholders who can take appropriate actions to address identified issues. These actions could include:

- For open DNS services: Limiting access to perhaps unintentionally misconfigured open DNS resolvers and/or identifying and performing take-downs on resolvers behaving maliciously.
- For open NTP services: The increase in open internet time servers running NTP indicates the growing need to serve and synchronize time for millions of clients. This service plays a critical role in global security, e.g., enabling browsers to correctly validate and verify certificates haven't expired. However, the open nature of these services pose a double edged sword and either need to be constrained to a limited customer base, e.g., the users of a network operator's networks or they need to be carefully monitored to prevent abuse. A new protocol known as NTS (or NTPSec), which adds increased security to NTP like DNSSEC did for DNS, is currently being deployed and encouraging its deployment may provide a longer-term answer to the challenge of open NTP services.
- For open CHARGEN services: Disable these services now. CHARGEN is an archaic debug tool that is a hazard on today's internet and should only be available in limited situations or for exceptional circumstances.
- For open SSDP services: Block remote access to SSDP services, as SSDP is intended for local network use only.
- For open SNMP services: If SNMP services are exposed to the internet, especially older versions (SNMPv1, v2c), they pose significant security vulnerabilities. Use only SNMPv3, which offers stronger authentication and encryption, and limit external access. Network administrators should regularly audit SNMP configurations to ensure strong passwords are in use, encryption is enabled, and external access is limited to prevent unnecessary exposure. Since SNMP services provide critical information about network configurations and device statuses, exposing them to external parties is highly risky. Ideally, SNMP services should be restricted to internal network access only, with external access strictly limited or completely blocked.

More generally, in addition to keeping updated with the latest security patches for various software services discussed above, risk mitigation practices such as understanding the need for services to be publicly exposed to the global internet rather than being accessible only from within the network to the users in the network would have significant impact.

The collaborations between organizations that provide public internet scanning infrastructures, such as CyberGreen, and ISPs, either directly or through a mediating organization such as a CERT/CSIRT, would be similar to a medical professional observing certain symptoms and informing the patient or notifying a health agency of a potential outbreak of infection or disease. These notifications would allow the patient (network operators) or the health agency (CERT/CSIRT or other industry body or government agencies) to take mitigating steps that would reduce cybersecurity risks.

INTERNET ROUTING SECURITY

The internet is a globally interconnected set of tens of thousands of networks, each independently managed and maintained. Understanding the connectivity through these networks is a complex and challenging endeavor. The inherent design of the internet requires trust and collaboration between individual networks using a common language that enables network routers to understand each other and allow traffic to flow through or within the various networks. The Border Gateway Protocol (BGP) is that common language and it is used to identify paths from source to destination for network traffic globally. However, it is a protocol developed without much in the way of security and that places heavy reliance and trust on network operators communicating via BGP to provide correct information. Unfortunately, this is a requirement that has time after time been proven to be problematic to meet. Failing to meet this requirement has been disruptive to global internet networks resulting in denial of service, or facilitating phishing and other attacks that have caused economic and reputational damage.

A first step in improving the security of the routing system, known as "Resource Public Key Infrastructure" (RPKI), has recently seen significant uptake. RPKI provides a way in which resources used in the routing of traffic on the network, namely IP addresses and identifiers for networks known as "autonomous systems (ASes)" can be strongly tied to the network operators who have received them, either from their Regional Internet Registry (RIR) or their Internet Service Provider (ISP). RPKI also enables the creation of Routing Origin Authorizations (ROAs) that allow a network operator to securely associate a set of IP addresses, known as a prefix, to that network operator's routing identity, i.e., their AS number. The network operator can then announce via BGP that they provide routing services for the prefix, an act known as "originating the route" for the prefix. Network operators who receive that BGP announcement can then verify the ROA to ensure the originating operator is authorized to provide routing services for the prefix.

When RPKI and ROAs are used, network operators all over the world can verify the information that they are receiving about the route to reach a particular set of IP addresses hasn't been faked, either accidentally or maliciously. This helps prevent traffic from being redirected into unintended networks where the traffic is dropped or worse, intercepted by malicious actors. While a network operator's validation of ROAs via RPKI does not ensure routing is secure, and in particular, cannot protect against a determined attacker, it does provide significant help in avoiding misconfiguration errors due to accidents or lack of understanding of how BGP and routing works.

As noted in Phase 2 of this project, we outline the need for secure routing while measuring the usage of Resource Public Key Infrastructure (RPKI). CyberGreen's "Global Routing Rank" measures routing security at a national level by calculating the number of autonomous systems that use RPKI and create ROAs for their BGP route advertisements.

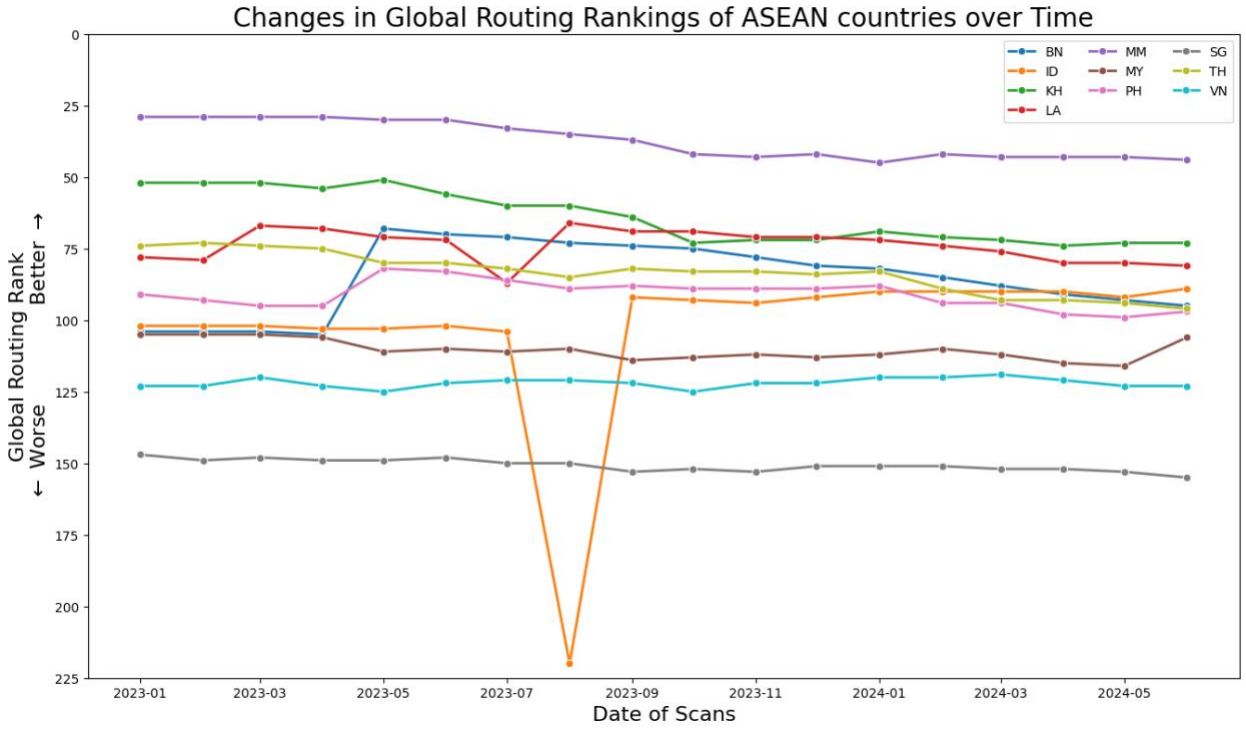


Fig. 7: Changes in global routing ranking over time.

Figure 7 shows the ranks of the ASEAN countries over the last 18 months of this study, with lower numbered ranks indicating better security, i.e., a higher percentage of ASes in the country using RPKI and ROAs. We observe Myanmar (MM, purple line) and Cambodia (KH, green line) have the highest percentage of ASes with ROAs for their IP addresses. Singapore (SG, gray line) has the lowest percentage of ASes securing their BGP advertisements. We observed a sharp decline in signed ROAs by ASes in Indonesia (ID, orange line) in August 2023 but this decline was quickly reversed, improving the ranking of ID during the next month. However, with the exception of Indonesia (ID, orange line), Laos (LA, red line) and Malaysia (MY, brown line), we observe a slight decline in the ranks of ASEAN countries over the observation period. This decrease is in contrast to the usage of RPKI and ROAs globally, which has seen an increase over time.

WHY DOES ROUTING SECURITY MATTER TO CYBER PUBLIC HEALTH?

Correct routing is critical for the security and stability of the internet and keeps users safe by preventing them from navigating to and accessing malicious resources due to routing system hijacks. It also improves global resilience and reduces the impact of a single operator's mistake such as the well-known action by Pakistan's government in 2008 to block YouTube that resulted in disruption of YouTube's services experienced by many other countries and peer networks around the world.

The usage of RPKI and ROAs for providing a way in which BGP advertisements can be validated, while not the silver bullet to addressing insecurities and vulnerabilities in BGP routing, makes the routing system safer operationally, both to the network operator that signs their route advertisements as well as to the users of networks that validate the routing announcements they receive. This is equivalent to the positive impact of vaccination to both protect the individual and the community. The greater the number of people who are vaccinated against a specific disease, the lesser the risk they pose to the vulnerable members of the community.

HOW TO IMPROVE ROUTING SCORES

The following steps should be taken by network operators to improve routing security:

- Implementing RPKI: By adopting RPKI, network operators around the world can verifiably determine who has been allocated which IP addresses and AS numbers. When coupled with ROAs, the integrity of BGP route origin advertisements can be validated. This helps prevent unauthorized route advertisements and reduces the risk of BGP hijacking.
- Enforcing BGP Filtering: Implementing BGP filtering allows network operators to prevent the acceptance of untrusted or misconfigured routes. This mitigates the impact of malicious route advertisements or route leaks and protects other networks from these threats. Regularly updating filtering rules and only accepting routes from trusted sources minimizes the risk of incorrect routes propagating across the internet.
- Regular Validation of ROAs: Network operators should periodically verify that the ROAs for their ASes are correctly configured and up-to-date. Ensuring that these are accurate guarantees that route advertisements are recognized correctly by other networks. Additionally, operators should use RPKI to validate the ROAs of BGP route advertisements received from other networks, ensuring that they are legitimate.
- Utilizing the Internet Routing Registry (IRR): While RPKI is being deployed, network operators can use the IRR to help verify the reliability of BGP route information. The IRR is an older technology that is based on a set of databases in which network operators register their routing information, allowing other operators to query and confirm trusted routes. While imperfect and not without errors and redundancies, using the IRR in those cases where RPKI is not yet available can help reduce the risks of route hijacking and route leaks, improving the overall trustworthiness of BGP routing.
- Following Routing Security Best Practices:
    - The Asia Pacific Network Information Centre (APNIC) offers training, resources, and best practices related to routing security, including the implementation of RPKI and secure BGP practices, particularly for operators in the Asia-Pacific region.
    - Initiatives such as the Global Cyber Alliance's Mutually Agreed Norms for Routing Security (MANRS) can enhance BGP routing security.
    - The White House released a "Roadmap to Enhancing Internet Routing Security" in September 2024 that promotes best practices for BGP and routing security.

DOMAIN NAME SYSTEM (DNS) INFRASTRUCTURE SECURITY

As mentioned previously, the Domain Name System (DNS) is critical infrastructure that allows human memorable hostnames like example.com to be looked up or resolved to machine recognizable information such as IP addresses. This allows users to more easily navigate to various web servers, send email to mnemonic email addresses, and make use of other resources on the internet more naturally. The general purpose nature of DNS has enabled the role of its infrastructure to multiply beyond simply providing name to IP address resolutions and it has become crucial for web and email service location, load balancing, and resiliency, email sender identity, message acceptance/rejection policy, and security, and is even used for other purposes such as physical location.

However, as was the case with BGP, when the DNS was created, little thought was given to security considerations. In particular, there was no mechanism by which a receiver of DNS data could verify the data had not been modified without authorization. This flaw provided a way by which attackers could insert malicious information in responses to DNS lookups that would cause subsequent connections using that information to end up at attacker-controlled machines. While rare, this attack has been successfully implemented on multiple occasions with perhaps the most well known attack, the MyEtherWallet attack in 2018, resulted in the theft of over USD $150,000 from end user crypto wallets.

DNSSEC ADOPTION

To address this risk, a set of DNS protocol enhancements called "DNS Security Extensions" (DNSSEC) was standardized. DNSSEC is in many ways similar to RPKI and ROAs in that the creators of data cryptographically sign information about the information they'll be publishing that consumers of that information can subsequently verify to ensure the information hasn't been modified. However, despite its standardization in the late 1990s and high utilization at the highest levels of the DNS, e.g., the root of the DNS and over 95% of top-level domains are DNSSEC-signed, the usage of the DNSSEC further down the domain name tree is, on average, quite low with only about 8-9% of all names across the internet being DNSSEC-signed.

For the purposes of this study, we measure the adoption of DNSSEC in a selection of government and public sector domains and hostnames scanned by CyberGreen for all ASEAN countries as shown in Figure 8 below.

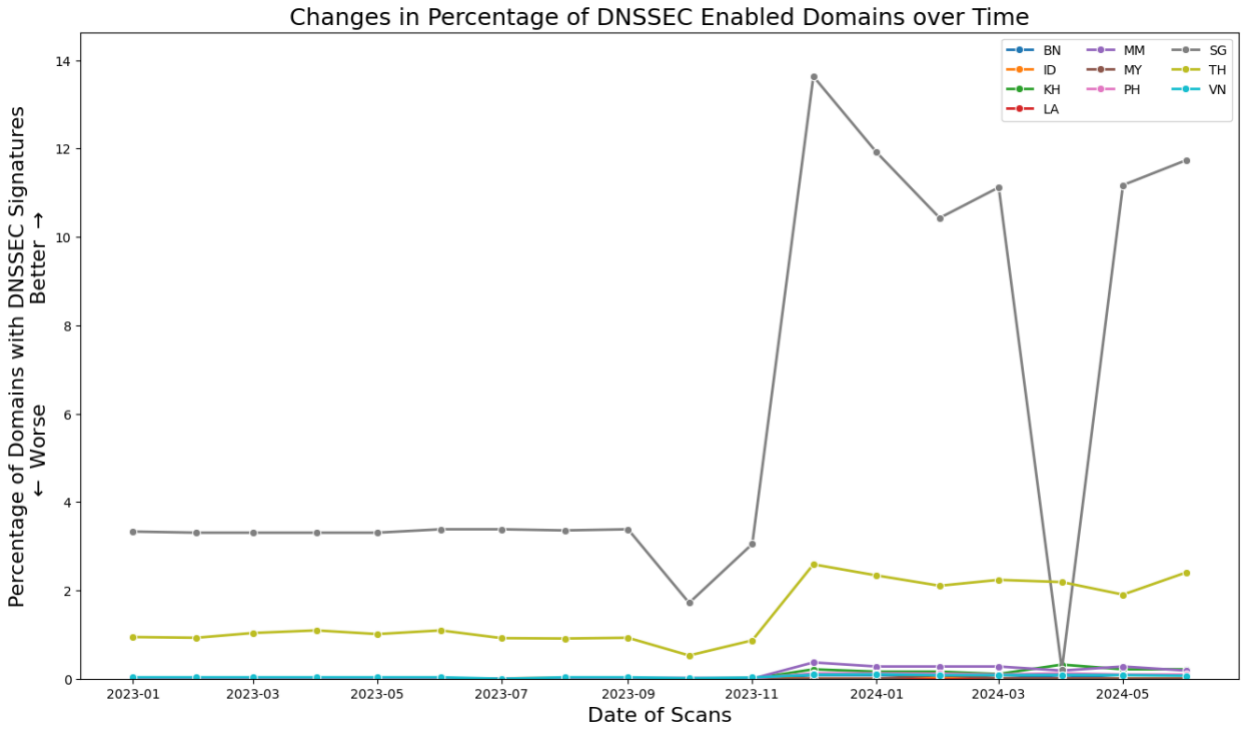


Fig. 8: Changes in percentage of DNSSEC enabled hostnames/domains over time.

While the global average of DNSSEC-signed information is around 8%, at the start of the study, no ASEAN country matched the global average percentage. About 4% of government hostnames in Singapore (SG, gray line) were DNSSEC-signed, followed by Thailand (TH, olive line) at around 1%, with the remaining government hostnames showing essentially no usage of DNSSEC. However, starting January 2024, after a small decline in the percentage of DNSSEC-signed domains that occurred beginning in November 2023, we observed a sharp increase in Singapore, reaching approximately 14% of the total government domains before settling down to about 12% – a 3x increase from December 2023. Similarly, the data show Thailand doubling their number of DNSSEC-signed domains, reaching slightly over 2% by the end of the study period. Our observations in 2024 also indicate changes in Myanmar (MM, purple line), Cambodia (KH, green line), Philippines (PH, pink line), and Vietnam (VN, light blue line) where the respective government domain administrators began signing at least some of their domains.

DNS INFRASTRUCTURE RESILIENCE AND LAME DELEGATIONS

As a best practice for resiliency, domain administrators typically configure multiple authoritative name servers in order to provide responses to recursive resolvers or clients querying for various hostnames within the domain. Sometimes, not all of the designated authoritative name servers respond to queries, a situation known as a "lame delegation." Lame delegations are typically due to temporary lack of connectivity, but are occasionally due to misconfiguration, e.g., forgetting to remove a name server that is no longer providing authoritative name service for a domain, or more consistent connectivity challenges such as a high rate of packet loss or complete unreachability or unavailability of the name server. Lame delegations can impact users and clients attempting a domain name lookup by increasing the time to obtain a response, which can result in degraded experiences, such as taking a long time for a web page beginning to load. In addition, lame delegations can open up potential security risks due to the ability for attackers to exploit

misconfigured nameservers. For the purposes of this study, we measure the percentage of lame delegations in a selection of government domains and hostnames scanned by CyberGreen for all ASEAN countries as shown in Figure 9 below.

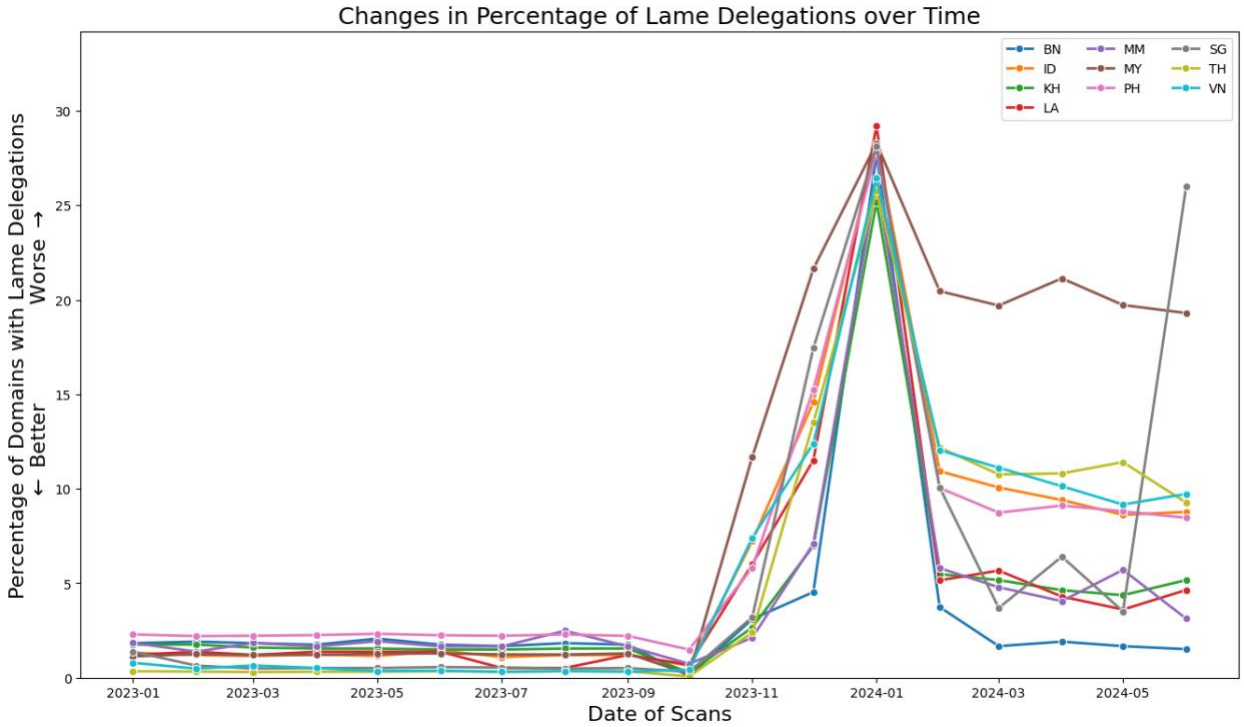


Fig. 9: Changes in percentage of lame delegations over time

Figure 9 shows the changes in the percentage of domains with lame delegations for ASEAN countries. While the percentages typically remain less than 5%, we observed a sharp increase in the number of lame delegations at the beginning of 2024 for all countries monitored. This spike eventually receded somewhat but it did raise the percentage of domains with lame delegations to almost 25% of the country specific hostnames being measured. Malaysia (MY, brown line) shows the highest increase in the number of lame delegations following their general election results, which may suggest the sunsetting of various government domains associated with the dynamic political situation. We are investigating the reasons for significant changes in lame delegations in January 2024 and currently consider it a measurement anomaly.

SUMMARY OF DNS INFRASTRUCTURE SECURITY OF ASEAN COUNTRIES

The IIHMF framework produces a score and rank for the DNS infrastructure security based on the combination of usage of DNSSEC and the number of lame delegations in the country's government DNS infrastructure. Lower rank values indicate better security compared to higher rank values.

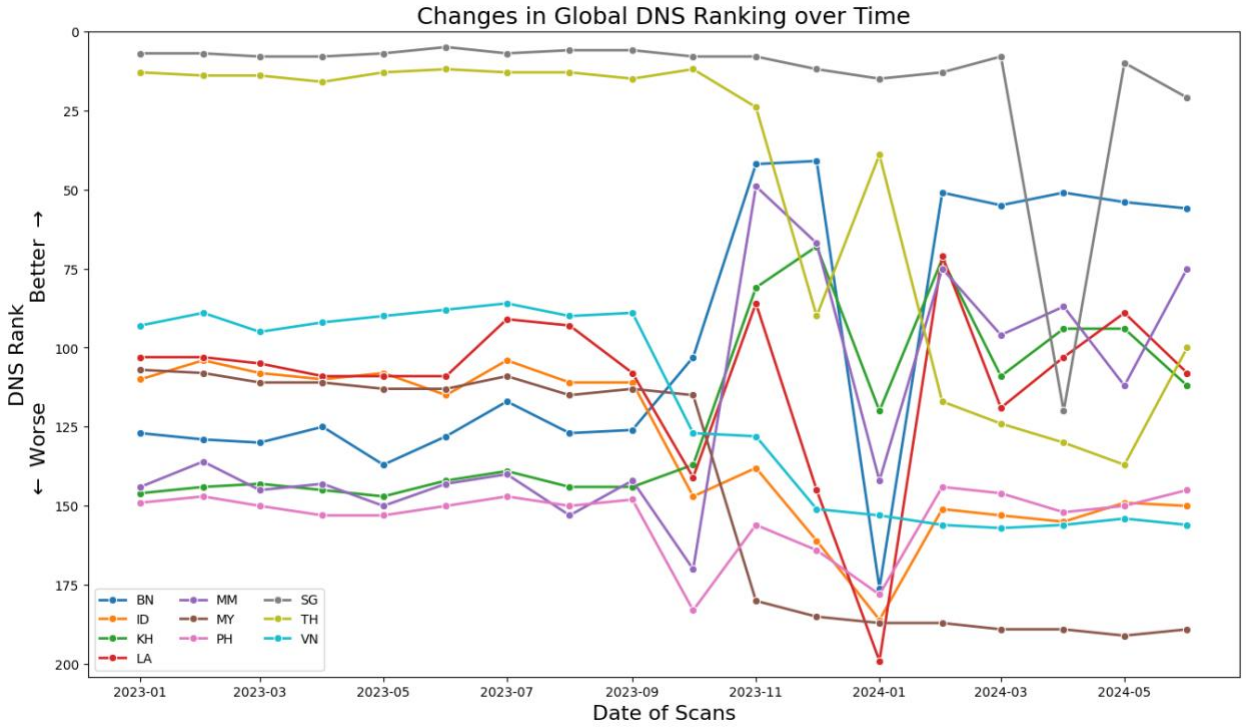


Fig. 10: Changes in DNS Infrastructure security rankings over time

Figure 10 shows Singapore (SG, gray line) ranking the best in terms of DNS infrastructure security among its ASEAN peers with a momentary change in ranking in April 2024. Thailand (TH, olive line) scored second among ASEAN countries but that score, over time, decreased bringing down their ranking to over 100. Cambodia (KH, green line), Brunei Darussalam (BN, dark blue line), and Myanmar (MM, purple line) improved their DNS security scores due to their slight increase in the number of DNSSEC enabled hostnames as shown in Figure 8. Despite the small change in those scores, significant improvements in their overall scores resulted. However, Thailand despite its increase in DNSSEC enabled hostnames, had a drop in ranking because of the increased number of DNS lame delegations observed.

WHY DOES DNS INFRASTRUCTURE SECURITY MATTER TO CYBER PUBLIC HEALTH?

As a critical infrastructure, DNS provides a core part of the environment users interact with in order to communicate via the internet. An insecure DNS can be compared to a polluted environment, e.g., a water supply, that can foster disease. In the case of DNSSEC deployment, DNSSEC-signing a domain and enabling DNSSEC validation in resolvers would be the equivalent to treating (DNSSEC-signing) and filtering (validating DNSSEC signatures and discarding responses that fail validation) water. In the case of addressing lame delegations, the analogy can be made to ensuring there are multiple sources of clean water.

In both cases, the primary consideration is that the resource, be it domain names or water, is secure, stable, and resilient.

HOW TO IMPROVE DNS SCORES

We recommend policymakers make changes to any existing policies and require the deployment and adoption of DNSSEC for critical and sensitive government infrastructure. Additionally, we also recommend mechanisms that allow active monitoring of the quality of the DNS infrastructure such as the adoption of frequent key rollovers and preventing lame delegations. Below, we detail the parties that can implement these recommendations.

- **Configure DNSSEC**: Domain name administrators and network operators should configure DNSSEC (Domain Name System Security Extensions) to protect against DNS spoofing and cache poisoning attacks. DNSSEC ensures that DNS responses are authentic and have not been tampered with. Key actions include:
    - DNSSEC-signing the domain by domain name administrators cryptographically "locks" the domain's information to protect its integrity and authenticity.
    - Enabling DNSSEC validation on recursive resolvers by network operators to check the validity of DNS responses from authoritative servers.
    - Enrolling DNSSEC for the country TLD zones and critical government eTLDs.
- **Monitor and mitigate lame delegations:** Lame delegations occur when authoritative DNS servers fail to respond to queries due to misconfigurations or connectivity issues. To ensure DNS resilience and performance, domain name administrators should take the following steps:
    - Regularly audit DNS configurations to ensure all designated authoritative name servers are responsive.
    - Remove outdated or misconfigured name servers that are no longer authoritative for a domain or which no longer function correctly.
    - Monitor DNS performance to identify and address high rates of packet loss or connection failures that could result in lame delegations.
- **Engage in community and industry best practices**: Collaborating with industry groups and adhering to community best practices for DNS security is essential. Network operators should:
    - Participate in initiatives such as ICANN's Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS) and the Global Cyber Alliance's Mutually Agreed Norms for Routing Security (MANRS) to enhance the overall security of the global DNS infrastructure.
    - Follow recommendations for best practices from organizations like ICANN, DNS-OARC, APNIC, APTLD, and other DNS-focused organizations.

WEB PROTOCOLS SECURITY: TLS & CERTIFICATES

Transport Layer Security (TLS) enables secure communications between a client and a server on the internet. TLS provides authenticity, integrity, and confidentiality of communications between the client and the server. These features prevent attackers from eavesdropping on communications which could lead to an attacker stealing credit card information provided on a web form. TLS also helps prevent connections to an impersonation of web sites, e.g., an attacker creating a duplicate

web page on an attacker controlled machine to implement an man-in-the-middle attack, and also helps to protect the server's content from being corrupted in transit. To provide these features, servers configure their identities through a digital certificate issued to them by a certificate authority. When initiating a connection, clients are provided these server identity certificates, which contain a cryptographic public key and associated signatures of the certificate authority that issued them. These credentials allow the client to validate the contents of the certificate and establish a secure connection with the server they intend to communicate with.

For the purposes of this study, we measure the percentage of hostnames with valid TLS certificates from a selection of government and public domains and hostnames scanned by CyberGreen for all ASEAN countries as shown in Figure 11 below. Higher percentages are preferred.

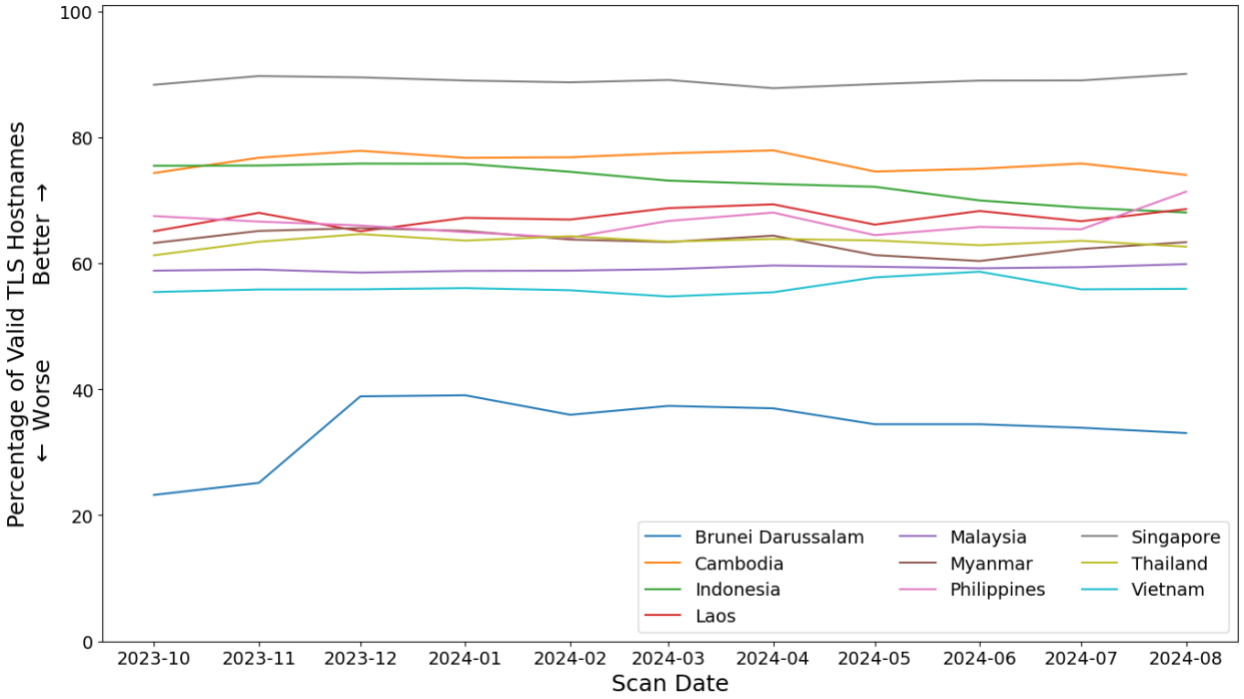


Fig. 11: Percentage of hostnames with valid TLS certificates

On the web, the usage of TLS is presented to the user through the use of "https://". Figure 11 shows that in the study period beginning October 2023, Singapore (gray line) leads the ASEAN region with the highest percentage of hostnames supporting secure connectivity with their web servers. While we observe slight increase in the percentage of hostnames used for servers with TLS enabled for most ASEAN countries, we see the highest increase (almost doubling) its initial number of TLS enabled hostnames in Brunei Darussalam (dark blue line), and a slight decrease in Indonesia (green line).

TLS ALGORITHMS AND PERIOD OF VALIDITY

TLS can be configured by the server administrator to use a variety of cryptographic algorithms to secure the communication. These algorithms have various characteristics that lead to tradeoffs, for example trading the size of the key with the strength of encryption. Given the ability to break encryption generally improves over time and there is always the possibility that a breakthrough in

mathematics (e.g., easily finding prime factors for very large numbers) or computing (e.g., quantum computing) could render a particular algorithm easily broken, new algorithms are frequently developed and deployed with older algorithms deprecated and removed from service. As a result, simply having TLS enabled doesn't necessarily indicate strong protection for communications, rather when evaluating risk associated with TLS communication, it becomes necessary to examine the cryptographic algorithm in use.

In keeping with good security practices, the certificates used in TLS have a period of validity, i.e., a period of time since the certificate was created or issued that it can be considered valid. Server administrators that use TLS must update their certificates before they expire or clients will receive notification indicating the server may not be trustable. On the web, these manifest as error pages presented by the browser with a warning indicating that the connection could be insecure. Other internet infrastructure like mail servers, depending on their configuration, simply reject certificates that fail validation. Modern certificate management tools have mechanisms to automatically monitor expiry of the certificate, and request new certificates through a challenge-response protocol with the certificate authorities.

In TLS usage today, the RSA algorithm with various key sizes is the most common, with a newer algorithm known as elliptic curve cryptography (ECDSA) being increasingly deployed as it provides the same or better cryptographic protection with smaller key sizes.

As shown in Figure 12, during the period of measurements, we observe an increase in the adoption of TLS certificates with ECDSA keys as shown by the increasing solid blue regions in the bar plots. When evaluating the security of TLS configurations, we score algorithms based on their cryptographic strength and efficiency. Elliptic curve (EC) based keys, such as those used with ECDSA/EdDSA, are increasingly favored because they provide strong protection with smaller key sizes, making them both secure and efficient. Although RSA-based keys are still prevalent, the shift toward elliptic curve cryptography is a positive trend that enhances both security and performance. However, both Vietnam and Brunei Darussalam are yet to adopt elliptic curve-based certificates. The change in Brunei Darussalam and Cambodia's rankings, as shown in Figure 11, can be explained by the increased expiration, revocation, or misconfiguration of certificates over time in both the countries.

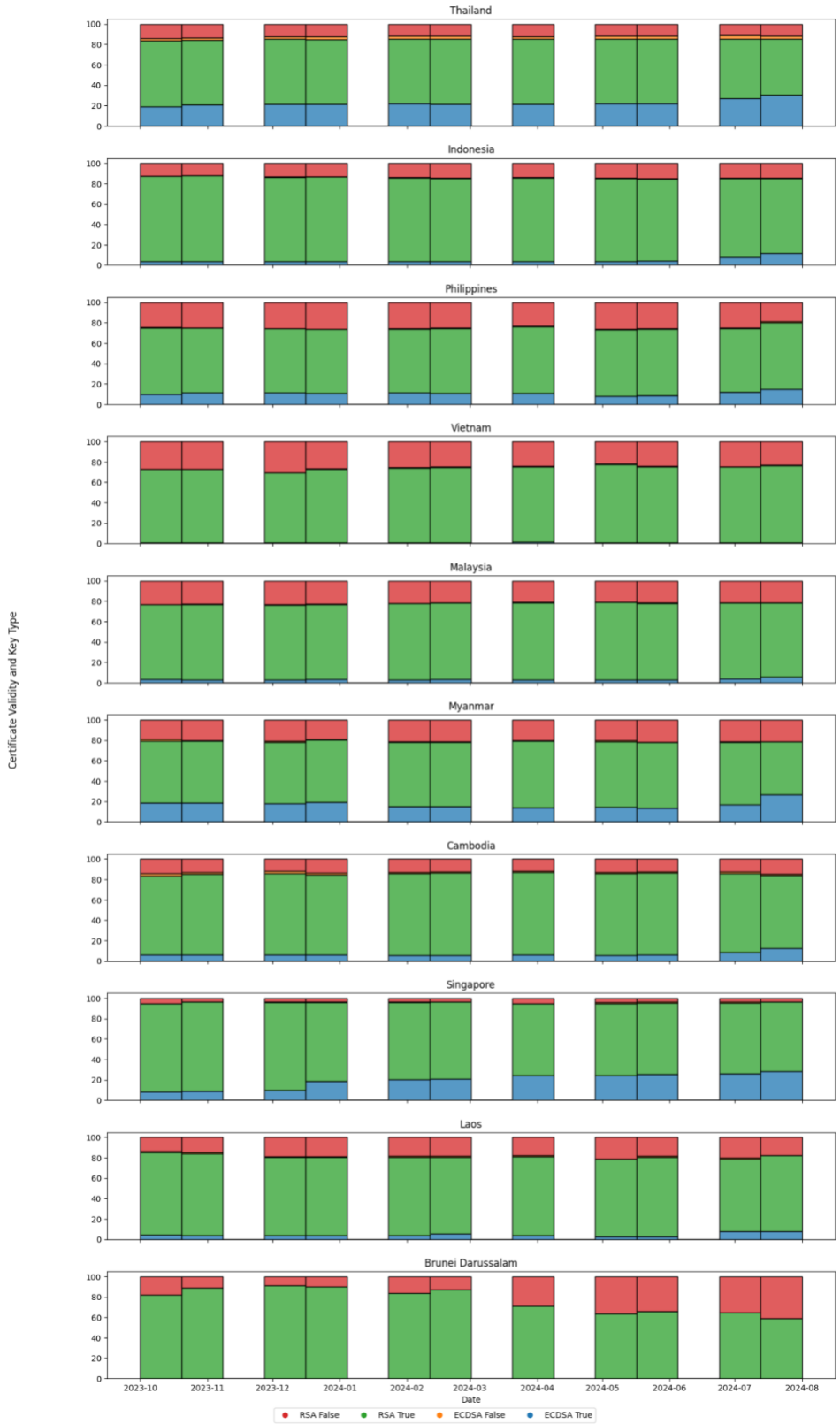


Fig. 12: Percentage of Public Key Types in Certificates and Certificate Validity.

GLOBAL WEB TLS PROTOCOL RANKING SECURITY

Starting in March 2024, CyberGreen began computing an aggregate score and ranking countries based on the utilization of TLS and the cryptographic algorithms used within TLS connections.

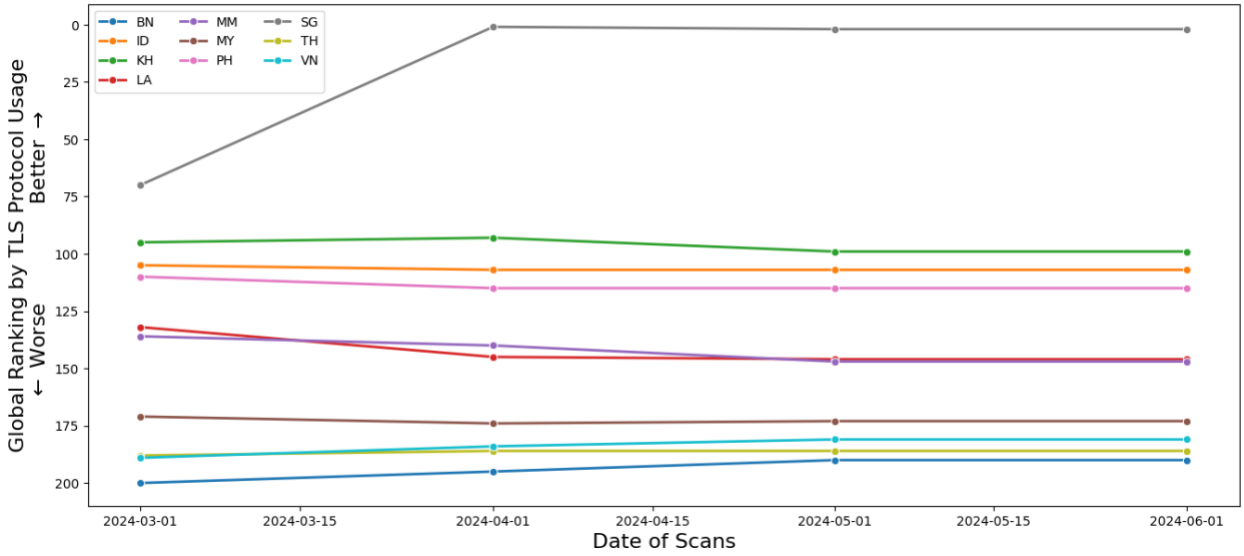


Fig. 13: Changes in ASEAN TLS protocol rankings over time

Figure 13 shows changes in the CyberGreen ranking for TLS protocol usage for ASEAN since data collection began in March 2024. Singapore (SG, gray line) has consistently had the best ranking in the region over the three-month period, with a significant uptick in TLS usage between March and April. Cambodia (KH, green line), Indonesia (ID, orange line), and the Philippines (PH, pink line) were fairly consistent, scoring second, third and fourth respectively. While Brunei Darussalam (BN, dark blue line), Thailand (TH, olive line), and Vietnam (VN, light blue line) saw improvements in their ranking, the remainder of the ASEAN countries experienced a slight reduction in their rankings.

WHY DOES TLS PROTOCOL USAGE MATTER TO CYBER PUBLIC HEALTH?

As with DNS, TLS provides an underlying infrastructure that enables secure communication between clients and servers, permitting trustable communications that facilitates commerce and other services users of the internet depend upon. Utilization of TLS can be compared to vaccinating a population against a disease: the more people within a population who get a vaccine, the less likely a virus will be able to infect people within that population and reproduce, thereby limiting the spread of disease. The ability of TLS to help secure communications against eavesdropping, impersonation, and corruption of data, means that attackers will be less likely to compromise that communication, thereby improving the security of all parties involved in the communication.

VARIANCE IN THE PUBLIC KEY SIZES

RSA 2048, i.e., the RSA algorithm with a 2048 bit key, is the most popular cryptographic algorithm used to establish secure TLS connections and is the public key returned by over 70% of valid certificates in Indonesia, Laos, Brunei Darussalam, Singapore, Cambodia, Malaysia and Vietnam. Over 50% of the government websites in Philippines and Myanmar and 46% of the valid Thai websites use RSA 2048. With the exception of Thailand which using RSA 4096 based keys as the

most popular key size and Brunei Darussalam using RSA 3072, all other countries adopted the more efficient elliptic curves and choose between EC 256/384 bit curve based public keys to be included in their certificates.

UNDERSTANDING TLS PROTOCOLS SUPPORTED

Observations presented in Figure 14 indicate the support of various TLS protocols by the hostnames which serve web content over https. TLS 1.0 was initially an upgrade from the older SSL 3.0 protocol standardized in 1999 however it is now widely considered no longer secure, with active advice being provided to remove support for it from all web servers. Similarly, TLS 1.1 was an upgrade from TLS 1.0 and provided support for resistance from various cryptographic attacks, however it too has now been officially deprecated along with TLS 1.0 in March 2021. TLS 1.2 is currently the most widely accepted version and with the increasing adoption of TLS 1.3, is mostly seen as a backup protocol when TLS 1.3 based communication is not possible due to one side of the communication being unable to support TLS 1.3.

Despite the security challenges and 2021 deprecation of TLS 1.0 and 1.1, the first two subfigures in Figure 14 indicate over 20% of the hostnames scanned continue to support these protocols. While the gradual trend indicates reduction of support over time, almost half of the https enabled hosts in Vietnam support these older protocols, opening them up to serious security risks. We observed major improvements in the hosts associated with Brunei Darussalam despite the intermediate increase. The results indicate that over 95% of the hostnames which make use of TLS support TLS 1.2 based communications. The data shows a generally increasing trend of TLS 1.3, with more hostnames enabling support for the latest version of TLS with the exception of Brunei Darussalam which shows a reduction in the number of hostnames whose servers respond to TLS 1.3 based communications.

The improved security of modern TLS protocols such as 1.2 and 1.3 come from the strong set of cryptographic cipher suites, a collection of algorithms that are used to create and maintain the secure connection. Within these protocols, some cipher suites use weaker cryptographic building blocks, such as a weaker hash function or signature functions which are malleable. Choosing a strong set of cipher suites such as an authenticated encryption scheme (AEAD) like AES GCM 128 with elliptic curves which are available in both TLS 1.2 and 1.3 gives additional security guarantees. TLS 1.3 provides forward secrecy guarantees making analysis of TLS traffic at middleboxes difficult and its use and adoption has therefore been contentious.

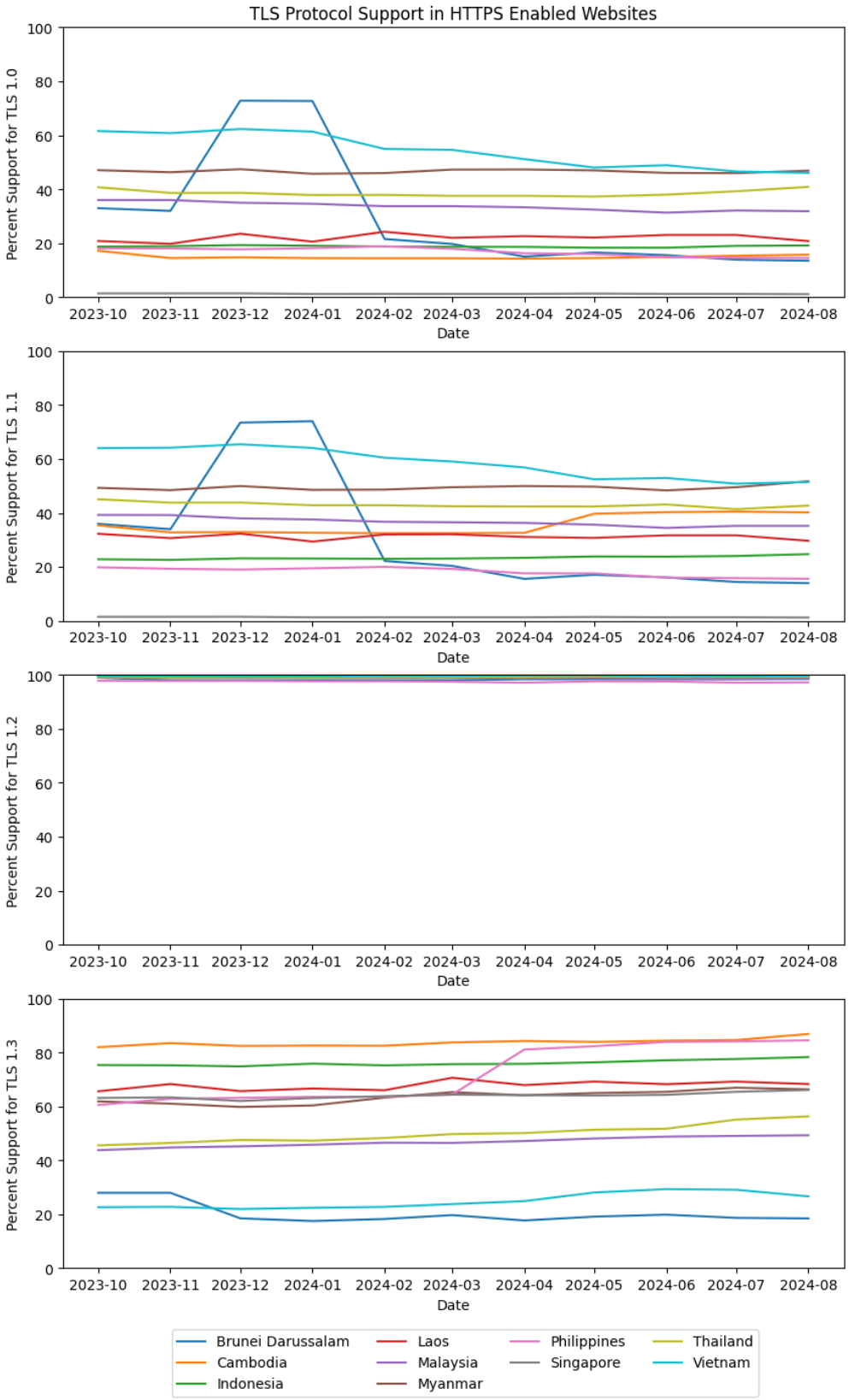


Fig. 14: TLS Protocols Supported by https enabled websites in ASEAN region

HOW TO IMPROVE TLS & CERTIFICATES SCORES

As shown above, there are several takeaways which could be mandated in various policies. However, the exact policy recommendations for this and the mandate of specific algorithms within TLS is context specific. Regulatory efforts should be made to nudge technology services to secure communications to and from the service, irrespective of their Internet connectivity and reachability, while IT departments and/or system administrators should ensure the following:

1. TLS should be enabled wherever possible for securing the communications.
2. TLS certificate validity should be monitored; expiration of TLS certificates generally removes the website protected by that certificate from the internet. The web server's certificate's period of validity should be closely monitored and certificates updated, preferably with automation, with plenty of the validity period remaining to minimize the risk of website disruption.
3. Implement strong cryptographic algorithms with appropriate key sizes: Different TLS algorithms, i.e., versions, exist that balance cryptographic strength with CPU time needed to validate/encrypt/decrypt and amount of data used for signatures. While there is some debate about the "best" algorithm, CyberGreen recommends EC based keys, e.g., EC 256/384, or Edwards curve based keys which are more modern than RSA. Certain RSA algorithms and key size combinations can be sufficient as well.
4. TLS 1.0 and 1.1 are now officially deprecated and considered insecure. TLS 1.2 with modern cipher suites should be supported due to its widespread usage, but TLS 1.3 should be encouraged.

EMAIL SECURITY

Email security protocols provide a mix of authentication, integrity, and confidentiality. Authentication prevents spoofing, integrity prevents tampering, and confidentiality prevents eavesdropping/observing. The effects of email-related attacks can be far-reaching if unauthorized access or impersonation is used with an authoritative domain (e.g. government, critical infrastructure) to glean sensitive information from others. Further, compromised email accounts can be used to send real emails to other related organizations to further spread compromise.

Message Forgery: This active attack is often instantiated in falsification of messages such as emails to create phishing campaigns that seek to make recipients of the email disclose and or verify sensitive information.

Message Diversion/Deletion: An active attack where legitimate messages are removed before they can reach the desired recipient or are redirected to a network segment that is normally not part of the data path.

Message Modification: This active attack is one where a previous message has been captured and modified before being retransmitted. The message can be captured using a man-in-the-middle attack or message diversion.

Message Leakage: Message leaks can happen through active and passive attacks. During an active attack, messages sent in plaintext between mail servers, or between the client and the mail server can be observed by a network adversary to whom sensitive message information is revealed. Passive message leakage attacks happen due to compromise of mail servers, or user accounts which reveal the interactions between mail senders and receivers.

In an effort to assess email security and reduce these risks, CyberGreen measures the usage of TLS, SPF, DMARC, and MTA-STS. While DMARC, and SPF both are DNS-based and help in email authentication, they differ subtly. SPF helps with establishing legitimacy to the sending mail server and describing the policy, while DMARC is useful in combination with SPF to inform further actions that need to be taken when SPF (or DKIM) validation fails.

TLS/CERTIFICATES USAGE IN MAIL SERVERS

Channel encryption, such as Transport Layer Security (TLS), prevents network adversaries from observing or tampering with email in transit.

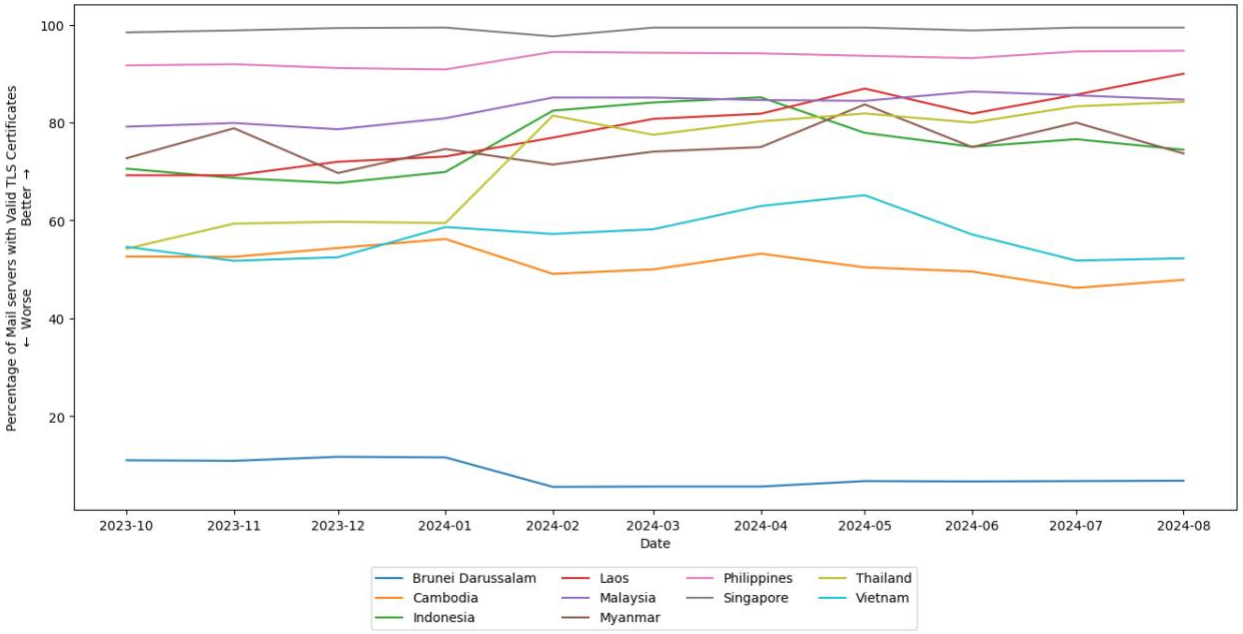


Fig. 15: Percentage of mail servers with valid TLS certificates

Mail transmissions and communications between mail servers rely on the STARTTLS extension and use the standardized TLS protocol to enable secure, and authenticated communications. However, similar to the web TLS certificates on mail servers can also be. In Figure 15, we show the percentage of TLS enabled mail servers which also have a valid TLS certificate. Our observations indicate ~100% of the mail servers managing government emails use secure TLS connections. Thailand saw a dramatic increase over the scan duration and improved the percentage of TLS enabled mail servers from ~55% to ~80%. The percentage of TLS enabled mail servers in Brunei Darussalam on the contrary declined from 10% to 5% during the measurement duration indicating a majority of the mail servers not using valid certificates to enable TLS communications.

SPF

Protocols such as the Sender Policy Framework (SPF) help prevent email spoofing and provide authentication. This is done through DNS entries indicating which mail servers and corresponding IP addresses are permitted to send email on behalf of a domain. SPF is the building block for DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting, and Conformance (DMARC). Testing for correctness of DKIM usage is more intrusive (since it involves sending automated emails as a part of the scan) and nuanced and hence, we do not test DKIM usage but do capture information on alignment.

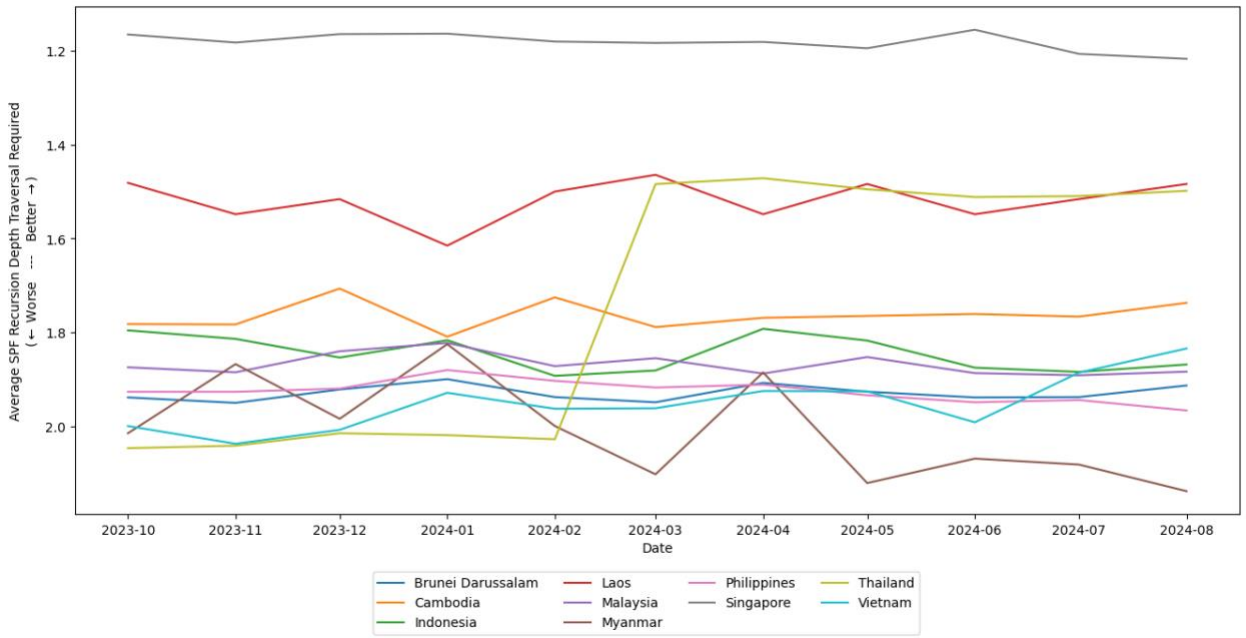


Fig. 16: Average depth of SPF traversal required to obtain the complete sender policy

The standards for SPF indicate that the SPF policy may not require more than 10 levels of additional DNS lookups to evaluate the complete policy. Increase of these recursion depth increases the time required for mail servers to validate the incoming mail senders policy and cause mail deliverability issues. The IP addresses or CIDR ranges obtained from the SPF records are used to validate the sender mail servers' ability to send the email, reducing risk of impersonation or mail forgery. Good SPF practices as a result must have a restricted set of IP addresses owned by the sending organization in the sender policy indicating the set of IPs, the incoming mail could originate from preventing potential abuse. Large allowable IP ranges increase the possibility of the mail being sent to be rejected or classified as spam.

In Figure 16, we observe the changes in the average depth of traversal required to obtain the SPF policy associated with the government hostnames which are configured to send emails. While all the countries have an average of less than 2 SPF lookups, much below the 10 lookups set as the maximum, we observe strong improvements and optimizations on the DNS lookups required for SPF policy by Thailand, while Myanmar worsens and sees an increase in its number of average DNS lookups.

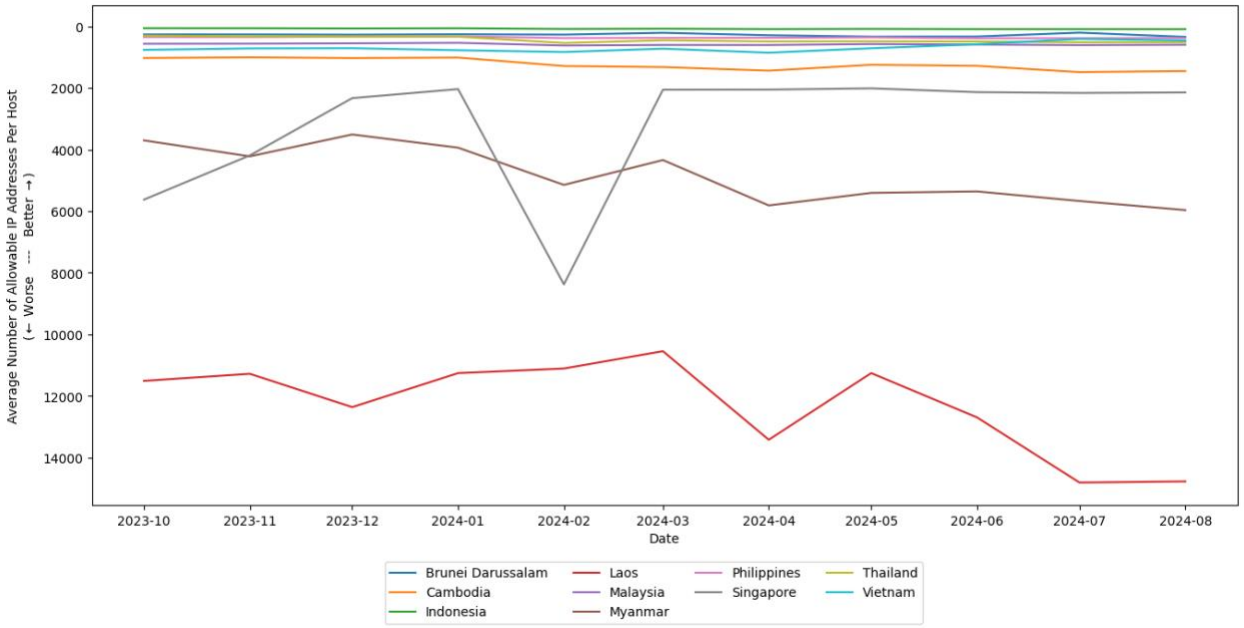


Fig. 17: Changes in average number of allowable mail sender IPs per host.

Figure 17 above presents the average number of IP addresses that a government hostname could send email from, having a large range of IP addresses especially using IP ranges from common cloud services to manage and send emails, enables attackers to spoof email messages affecting the reputation of the mail services. The lower the number of IPs listed in the complete SPF policy indicates a lower security risk but on the flip side might also pose reliability challenges if it's extremely small such as a /30 (containing 4 IP addresses) or /32 (containing a single IP address) IPv4 prefix. We observe many ASEAN countries with the exception of Laos, Myanmar and Singapore have less than 1000 IP (~approximately a /22 prefix worth) addresses on average when normalized by the number of mail hosts. The SPF policies for government mail infrastructure in Laos has worsened over time allowing more IP addresses on an average per host closer to 14000 (~ a /18 prefix).

The qualifier in the SPF record instructs the receiving server to take an action based on the match of the sending mail server IP address with the SPF policy of the hostname. For example, a SOFTFAIL (~all) indicates to the receiving server that if an email is sent from a server that does not match the SPF policy, it should still be accepted but marked as suspicious or be further evaluated before delivery to the intended recipient.

Mail servers with tight controls over the egress mail servers configure hard fail qualifiers (-all) instructing the receiving server to reject the messages if the sender does not match the SPF records. Figure 18 groups the SPF qualifiers and identifies the qualifiers used by various mail enabled domains. We observe the most popular configuration is a SOFTFAIL with the exception of

Singapore which is configured by default to FAIL.

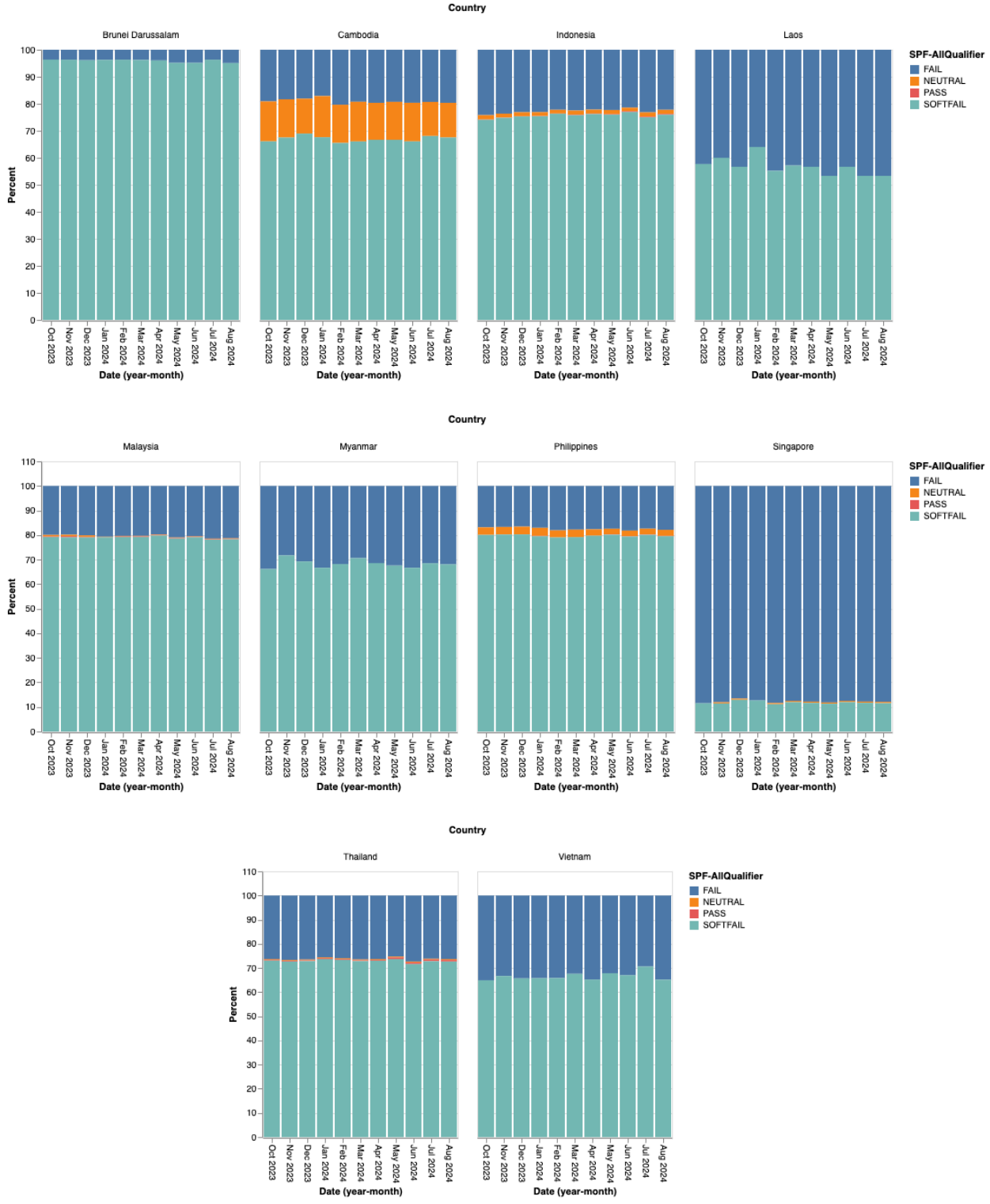


Fig. 18: Changes in Overall SPF Policy Qualifiers for each ASEAN country

DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) is a security protocol that builds on top of SPF and DKIM to report on attempts to spoof. These records play a critical role once the SPF policy and the qualifying criteria for a valid email from a sender is assessed by the receiving mail server. DMARC provides instructional information that enables receiving mail servers to take clearer action on the emails received without necessarily requiring them to be run through additional spam detection filters. These records are important to protect the sending domain from unauthorized use and inform attempts at using the domain to send unauthorized emails or spoofing attacks. The usage of DMARC is highly encouraged as it provides improved security, enables greater visibility into mail usage and prevents reputational damages.

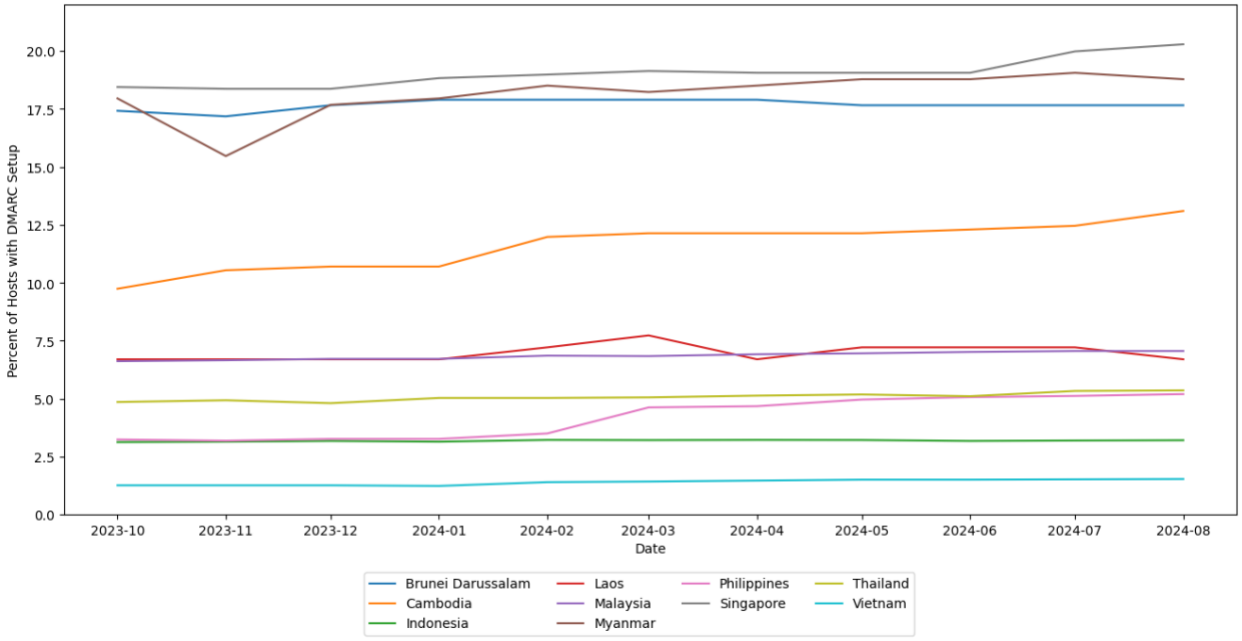


Fig. 19: Percentage of domains with successful DMARC setup.

As shown in Figure 19, we observe that less than 20% of the domains sending mail have DMARC configured and set up. Singapore has the highest adoption of DMARC among ASEAN countries at ~21% improving from 18% in October 2023. Vietnam has the lowest adoption of DMARC with less than 2% of the mail sending domains having DMARC configured.

The best practice is to use the strictest settings for DMARC. This includes setting both the DKIM and SPF alignments used by DMARC to the strictest settings – being applied to all domains and subdomains. However, we observe that the majority (> 80%) of the domains in ASEAN countries that have DMARC enabled (2090 domains i.e. 4.5% of all mail domains scanned) use relaxed settings for both DKIM and SPF alignments in their DMARC configuration. With the increasing adoption of cloud services managing mail infrastructure, it is recommended to eventually modify these settings to be strict.

A receiving mail server uses the sender's DMARC policies to monitor, quarantine (send to spam), or reject (block and notify sender) the incoming email message. On average, 38% of the domains set their policy to quarantine making the receiving mail server accept but mark the message as

spam/junk, 32% have no policy mentioned, and 29% have the policy explicitly requesting the message to be rejected and the domain administrator be immediately notified about 100% of such failed instances.

MTA-STS

SMTP MTA Strict Transport Security (MTA-STS) is a security standard that ensures that TLS connections are always used and provides a mechanism allowing servers to refuse message delivery to servers without trusted certificates or over plaintext SMTP. Globally MTA-STS has very low adoption and the results are similar in the ASEAN region for the government hostnames. We observe 25 hostnames in Indonesia and 3 in Myanmar that have enabled MTA-STS for their mail domains while the remaining have not enabled MTA-STS to force sending mail clients to use secure connections.

WHY DOES EMAIL SECURITY MATTER TO CYBER PUBLIC HEALTH?

In public health, the concept of "Activities of Daily Living" (ADLs) has been fundamental since the 1950s. ADLs encompass essential activities individuals need to perform to live independently, such as eating, bathing, dressing, and managing personal hygiene. These foundational tasks offer a useful framework for evaluating individuals' functional status and designing interventions to enhance health and quality of life. Drawing inspiration from this concept, we can categorize email as a "Digital Activity of Daily Living."

Email "diseases," such as spam and phishing, are significant challenges that hinder the effective use of email for many business and government purposes. Email security is challenging in that there is risk of malicious activity from bad actors but also that it is often contingent on the sender and recipient doing their part to secure their digital environments. For example, if CyberGreen uses DMARC but ASEAN does not check it, ASEAN is less secure. If ASEAN uses DMARC but CyberGreen does not set it, ASEAN is less secure. If many domains neglect or choose not to establish these protocols, it becomes harder to reject mail which is not validated since you may not receive important messages. Email security works best with an organized community (population-level) effort.

HOW TO IMPROVE EMAIL SECURITY SCORES

In order to achieve a higher score for email security, the following steps should be taken by IT departments and/or system administrators as they relate to the different aspects of email security that CyberGreen assesses:

TLS/CERTIFICATES

1. TLS should be enabled and be the preferred default method of mail communications
2. An expired TLS certificate results in a failed secure connection; Modern certificate renewal tools ensure timely and automated management of these certificates and monitoring their validity periods
3. Implementation of strong cryptographic algorithms and key sizes. Different TLS "algorithms" i.e. versions exist. While there is some debate about the gold standard, CyberGreen recommends EC based keys, e.g. EC 256/384, which are more up-to-date than RSA. Certain RSA algorithms and key size combinations can be sufficient as well.

4. TLS 1.0 and 1.1 are now officially deprecated and considered insecure. TLS 1.2 should be a minimum, but TLS 1.3 should be encouraged.

SPF

The RFC 7208 specification for SPF limits the number of DNS lookups to 10. This limit includes all forms of lookups (e.g., include, a, mx, ptr, exists). If an SPF record requires more than 10 lookups, it exceeds the RFC recommendation and becomes non-compliant.

Many mail servers may treat such records as invalid, which can lead to emails being rejected or marked as spam, thus penalizing the sender's deliverability. This restriction helps to prevent excessively long or complex SPF records, which can be a target for DNS-based attacks and negatively impact email performance.

To avoid issues, SPF records should be simplified, limiting the number of mechanisms that require lookups and ensuring compliance with the 10-lookup rule in addition to shrinking the IP ranges that are allowed to send email especially as the usage of cloud services is increasingly becoming popular.

DMARC AND MTA-STS

The setup of additional but optional protocols such as MTA-STS, and DMARC improve security guarantees by forcing secure communications with the mail servers and providing an insight into mail delivery failures or mis-classifications due to policy failures preventing sensitive or important emails from being classified as spam or junk mail. The usage and enrollment of the domain to use MTA-STS, and DMARC improves the country's rankings. Additionally, domain administrators must try to configure them as strictly as possible.

4. OVERARCHING POLICY CONSIDERATIONS

Based on the data collected to date, there are a number of considerations that are applicable in the development of policies that aim to improve ASEAN regional Cyber Public Health. As has been discussed, there are a number of parallels that can be drawn between public health of populations and Cyber Public Health. As has been noted in the public health world, "Public Health focuses on improving the overall health of the group by improving the health of the individuals by various means, including disease prevention, disease screening, and disease treatment, as well as monitoring and modifying the environmental, social, economic, and political environment to improve the health of the public."[2] Many of these concepts can be applied directly to the cyber realm. For example, whereas public health focuses on improving the overall health of the group, Cyber Public Health focuses on improving the overall health of the devices, services, organizations, and people who are part of the cyber environment.

[2] Masters R, Anwar E, Collins B, Cookson R, Capewell S. Return on investment of public health interventions: a systematic review. J Epidemiol Community Health. 2017 Aug;71(8):827-834.

At a high level, the basic functions of public health[3] apply to the cyber world, and these can be used to structure policy formulation to help address the nation's cyber environment. These functions include:

- Monitor health status:
    - In the cyber world, internet-wide scanning services, such as those provided by CyberGreen, can provide this ongoing cyber health assessment and monitoring function to help identify risks, assets, resources, vital statistics, and disparities. Facilitating research of this nature for the common good can help establish an early warning system for cyber attacks and provide data that can be used for predictive modeling of future attacks.
    - To enhance health status monitoring, the creation of regional cybersecurity standards and benchmarks is recommended. Utilizing IIHMF scores as a baseline will enable each ASEAN member state to incorporate these scores into their national cybersecurity strategies**.** This effort will provide a consistent benchmark for evaluating the health of internet infrastructure across the region.
- Diagnose and Investigate:
    - Security researchers, "white hat" hackers, and software and service vendors typically provide these functions. From a policy perspective, encouraging, e.g., via "bug bounty"-type programs, or at least not discouraging through regulation, the investigative efforts, both formal and informal, by third parties has been shown to help improve overall cyber security in the long term.
    - Targeted risk mitigation initiatives should be developed using IIHMF scores, focusing on rapid improvements of cyber hygiene, such as patch management, system upgrades and configurations.
- Inform, Educate, and Empower:
    - The cyber world can be arcane and intimidating, however basic "cyber hygiene" should be easy to understand and implement as long as stakeholders are informed, educated, and empowered to make necessary changes.
    - Increased investment in Cyber Public Health is necessary to build a skilled workforce capable of addressing current and future internet infrastructure health.
- Mobilize Community Partnerships:
    - Given the internet is an interconnection of independently owned and operated networks that encompasses both governmental and non-governmental entities, improvements to a nation's cybersecurity posture will necessarily require public-private partnerships and engaging the wide array of stakeholders.
- Develop Policies and Plans:

[3] Edemekong PF, Tenny S. Public Health. [Updated 2022 Dec 11]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2024 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK470250/

    - Establishing voluntary best practices as guidelines and developing and promulgating plans to mitigate, minimize the impact, and recover from cyber incidents can help reduce the risks associated with those incidents.
    - Using the IIHMF as a central metric will help direct policy action and resource allocation. Allocating funding based on IIHMF scores could ensure that lower-performing countries receive necessary support to enhance their infrastructure health.
- Enforce Laws and Regulations:
    - All nations have laws and regulations that apply to the cyber realm, however enforcing those laws and regulations can be challenging given the difficulty in definitively and accurately attributing cyber incidents. As such, cooperative and collaborative work internationally among national law enforcement bodies must be considered.
    - Strengthening regional cybersecurity cooperation, potentially through an ASEAN-CERT, will allow nations to collaborate on law enforcement and response efforts.
- Link People to Needed Services/Assure Care:
    - In many cases, CERTs/CSIRTs perform the function of providing services to those impacted by cyber incidents, or provide referrals to those who can provide services. Enhancing or promoting CERTs/CSIRTs may be warranted.
- Assure a Competent Workforce:
    - Due to the rapid rate of change within the cyber world and the increasing complexity of the cyber landscape with state-based, state-sponsored, and organized criminal actors, emphasizing the development of a competent workforce is increasingly critical. This development will likely require public-private partnerships and deep involvement with the academic and commercial worlds.
    - Additionally, Cyber Public Health education and training programs should be prioritized, building a skilled workforce to manage the cyber risk landscape.
- Evaluate Health Services:
    - In the context of Cyber Pubic Health, the closest analog to Health Services would probably be the operation of governmental bodies tasked with ensuring the nation's cyber environment is secure, stable, and resilient. In many cases, there is no single agency tasked with this duty. In such cases, it is important that the bodies involved are able to communicate and work together effectively and efficiently, particularly in the event of crises. Tabletop exercises and simulations, particularly involving all stakeholders, that encourage teams to work together may be helpful in improving or ensuring the services can respond appropriately.
    - In countries that do not have a governmental body tasked with securing the nation's cyber environment, exploring the feasibility of establishing such a body would be recommended.
- Research:

- This is arguably the most important function due to the rapidly and ever-evolving cybersecurity landscape. New threats are constantly being discovered, new vulnerabilities constantly being exploited, and new models of assuring and evading cyber protections are constantly being developed and deployed. Research is necessary to keep abreast of these developments and explore new paradigms in which they can be addressed.
- Continuous improvements in methodologies for scoring cybersecurity health, as well as developing new tools and exploring different facets of data related to internet security and operations, can further enhance the accuracy and effectiveness of IIHMF scores. Encouraging academic and private sector collaboration through research funding and support for organizations like ERIA will drive innovation in this area.

This study undertaken by CyberGreen has been primarily focused on providing data for the first and last of these functions. One area in particular in which policy could be beneficial would be in encouraging network operators to collaborate and participate in the data collection needed to gain a better understanding of the national cyber environment. One of the limitations of the current study is that it is necessarily based on publicly available information; information that is internal to networks is, of course, opaque to CyberGreen and similar organizations trying to understand the threat landscape. Policies that can facilitate bonafide researchers, with appropriate anonymization of data, could provide much needed help.

5. FUTURE AREAS OF RESEARCH AND ENGINEERING

As would be expected, in the course of this study, additional areas of exploration have been identified. These areas would include:

- Resolver validation of DNSSEC messages: The DNSSEC portion of CyberGreen's Secure Global DNS scoring is currently based on only one side of the DNS, the publishing side, i.e., checking to see what domains have been DNSSEC-signed. A similar study should be done to see what percentage of resolvers, i.e., the lookup side of the DNS, are validating those signatures. Checking whether open resolvers are validating would be relatively straightforward, however checking the resolvers most end users encounter (e.g., resolvers only reachable by a network operator's customers) is more challenging. This requires the installation of various probes within the various ISP networks run in each country.
- DNSSEC algorithm census: As with TLS, DNSSEC allows for the use of differing cryptographic algorithms, with the same tradeoffs for cryptographic strength vs. CPU time needed for verifying, encrypting, and decrypting vs. amount of data for signatures. Doing further analysis for DNSSEC similar to what has been done for TLS is a logical extension of the current work. CyberGreen already scans for this information.
- HTTP Strict Transport Security usage (requiring TLS instead of just allowing it): While identifying the availability of TLS on the connections to particular services is important, having the ability for connections to those services to still be made without TLS leaves open

the possibility for a variety of attacks. An HTTP header known as HTTP Strict Transport Security, when used, forces all connections to the server providing that header to be protected by TLS. It may be interesting to see what percentage of websites' security via TLS can be bypassed by falling back to non-TLS connections.

- Census of SNMP versions: SNMP version 3 introduced encryption and authentication to SNMP communications, thereby making it less risky than earlier versions of SNMP. However, versions of SNMP earlier than 3 remain publicly available over the internet. Including the version of SNMP in the OpenSNMP scoring may provide a more accurate assessment of OpenSNMP risk than the current analysis.
- Expansion of Domain List: CyberGreen is currently limited in its assessment of security around domains by the list of government domains that it has manually populated. Expanding and updating this list, in conjunction with relevant organizations that could provide zone files would aid in creating a more accurate, up-to-date version of this list. Additionally, the ethical usage of certificate transparency infrastructure to discover and learn newer government hostnames poses strong opportunities for expanding the current list.
- Expansion of open services scanned for: Currently, CyberGreen has focused on the most commonly abused open services. Future research will increase the number of open services scanned, thereby providing a more in-depth assessment of risks associated with open services.

A note on engineering: While many research directions exist, CyberGreen currently faces challenges around streamlining the transformation and analysis of the existing measurement infrastructure and protocols. While a large portion of the scanning and archiving infrastructure operated by CyberGreen is automated, there is limited visibility into the *immediate* accuracy of the measurements. These momentary blips, typically caused by the network (such as the sudden spikes in some results presented in this report), would be more valuable to analyze immediately than at a later time. Significant engineering efforts need to be prioritized to improve such observability and inspection into the various in-house, and external tools that CyberGreen relies on. The maintenance of transformed databases from the current archival format would significantly improve and speed up analysis, and enable CyberGreen to share and integrate data directly with external partners and stakeholders. This would also serve as a milestone towards enabling interactive and exploratory user interfaces presenting the scores and measurements from all the components currently being measured and to be measured in the near future.

6. CONCLUSION

A defining characteristic of the risk landscape in ASEAN is the significant variation in technological maturity and cyber readiness among its member states. This disparity in digital infrastructure poses challenges, particularly as the region experiences high volumes of cross-border data flows and increasingly interconnected economies. The study highlights that countries with more developed digital infrastructures, such as Singapore, are better equipped to mitigate risks, while others, like Myanmar and Cambodia, face higher levels of vulnerability due to outdated or less well managed infrastructure.

Particularly concerning are the risks posed by open services such as Open DNS, NTP, and SNMP, which remain prominent across the region. While some countries have made strides in addressing these risks, the presence of open services still creates opportunities for amplification-based DDoS attacks that could have widespread impacts across the globe. Additionally, the low of adoption of DNSSEC and the presence of "lame delegations" in many ASEAN countries indicate gaps in DNS infrastructure security that could expose nations to external threats.

Internet routing security is another area where significant improvements are needed. While some countries have embraced RPKI to reduce the risk of unauthorized BGP route advertisements, others continue to experience vulnerabilities in routing, which leaves them exposed to potential traffic hijacking or redirection. Similarly, the ongoing use of outdated security protocols like TLS 1.0 and 1.1 poses risks, even as newer, more secure cryptographic methods, such as elliptic curve cryptography, are slowly being adopted.

The report emphasizes the critical importance of developing a comprehensive digital infrastructure risk management strategy for ASEAN. The findings from the analysis highlight the varied cybersecurity capabilities across member states and the notable risks posed by open services, outdated DNS infrastructure, and insecure routing operations. To effectively address these challenges, it is crucial to establish a unified Cyber Public Health framework that brings together all ASEAN member states, while offering flexibility for customization based on each country's specific needs and capabilities.

A key takeaway from this report underscores the urgency of adopting a public health style approach to cybersecurity. Just as public health focuses on collective responses to shared risks, the Internet Infrastructure Health Metrics Framework (IIHMF) offers a similar model for measuring and improving cybersecurity health across the region. The IIHMF can serve as a baseline for national cybersecurity assessments, providing a transparent and consistent method to track progress, evaluate policy effectiveness, and foster collaboration between member states.

The continued usage of IIHMF data enables nations to proactively mitigate vulnerabilities, assess the impact of interventions, and prioritize areas for improvement. This structured approach also encourages ASEAN members to adopt evidence-based policymaking and promotes regional cooperation. By using the IIHMF national scores, governments can compare cybersecurity health, share best practices, and engage in joint efforts to manage cross-border cyber threats.

The IIHMF framework not only helps identify individual weaknesses but also supports collective risk management. This collective framework is essential in managing the inherently interconnected risks of cyberspace, where vulnerabilities in one country can pose risks to others. By fostering collaboration and creating mechanisms for sharing cyber public health metrics, ASEAN nations can build a more resilient and secure regional digital infrastructure.
Continued utilization of the IIHMF ensures that each member state has access to the data necessary for proactive risk mitigation. It also serves as a valuable tool for allocating resources and support to countries that need it the most, thus driving the overall security of the region forward. A regular review of the IIHMF metrics and scores ensures that policies remain relevant in the face of evolving cyber threats, while promoting transparency and accountability.

Moreover, integrating the IIHMF scores into a regional cybersecurity strategy, such as Digital Economy Framework Agreement (DEFA), will be instrumental in building ASEAN-wide

cybersecurity standards and benchmarks. These benchmarks will encourage member states to enhance their cybersecurity posture through healthy competition, thereby improving the region's resilience to cyberattacks. Incentives tied to improvements in IIHMF scores, such as technical assistance or capacity building, can further motivate states to engage actively in risk mitigation efforts.

Ultimately, the IIHMF framework offers a robust foundation for the development of national and regional strategies aimed at reducing cybersecurity risks. As digital transformation accelerates in ASEAN, maintaining a strong focus on cybersecurity health will be critical to ensuring the stability and security of the region's digital infrastructure. Through collaborative efforts, transparency, and data-driven decision-making enabled by the IIHMF, ASEAN can position itself as a leader in regional Cyber Public Health and resilience.

ACKNOWLEDGEMENTS

This report was written by the CyberGreen Institute, a non-profit organization that conducts and supports research to establish a science of Cyber Public Health, dedicated to making the internet safer and more resilient for all. Production of this report was made possible through generous funding and support from the Economic Research Institute for ASEAN and East Asia (ERIA).

We would like to thank the following reviewers:

Michuki Mwangi, Distinguished Technologist, Internet Society
Budi Rahardjo, Head, ITB Microelectronics Center (Pusat Mikroelektronika)
Adam Shostack, Lead Scientist, CyberGreen Institute