Global Threat Intelligence Report 2022

First Half 2022 Publication

SysArmy

Content

Executive Summary

SysArmy regularly notify our valued clients regarding the security incidents, threat indicators, as well as security news surfacing on the web. This is to provide timely updates on the most relevant cyber threats. This biannual series of Global Threat Intelligence Report summarizes threat insight from the first half of 2022. The intelligence and analysis formed a perspective of threat landscape that can guide management, IT security professionals and incident responders to strategize their efforts on securing their defence layers. For the past 6 months alone, SysArmy had processed over **3150 Indicator of Compromise (IOC)**, and out of these data, it was derived that **malware (73.9%)** remains a huge threat for individuals and organization to deal with, followed by **ransomware (18.8%)** and **botnet (5.9%)**.

We've segmented the content of the report into three main area: **Key Findings;** where we provide insights from our global security monitoring and our proprietary threat intelligence platform, **Threat Landscape;** summaries of emerging threats and **Cybersecurity360;** a section dedicated for education and knowledge sharing. SysArmy is committed to continuously help you overcome the challenges that we observed and gain advantage over increasingly sophisticated cyber threats actors. Our cybersecurity operation team work round-the-clock to ensure our clients environments are proactively monitored and potential threats are detected before it's leveraged by threat actors.

Key Findings

Cyber threats in the period between January till June of 2022 were identified, extracted and analyzed from various security appliances and intelligence data. These data are then associated across industry verticals to observe an overall overview of the cyber threat landscape. Over this period, SysArmy Cyber Intelligence and Monitoring Center (CIMC) had gathered over **3150 unique IoC** and sent out **76 Global Threat Notification (GTN)** and **124 Global Security Notification (GSN)**. Clients can use this data to better protect their system from malicious threats. Out of these data points, it was concluded that malware remain a prominent threat, in which a surge of **56** different **malware** variants were identified, **13** different **ransomware** variants, as well as **5 botnet** campaigns were under observation. The statistics says it all and organization's data confidentiality, integrity and availability are potentially at risk if they play catch-up with latest threat advancement. In order to address the imminent risks of cyber threat, CISOs need to transition their roles from technologists who prevent breaches to corporate strategists who manage cyber risks. A good way to plan for cyber risk management via the top-down approach is to expect the whole business unit to be breached at any point of time.

9 out of 10

Data breach incidents are caused by employee mistakes[1]

73.9%
Malware

2135 unique IoC were analyzed and correlated against the security data of all clients for proactive detection

18.8%
Ransomware

13 different ransomware variants were analyzed, comprising a total of 556 unique IoC

5.9%
Botnet Campaign

Apart from the typical DDoS operation, threat actors utilized botnet to spread crypto-mining software

Trend Analysis

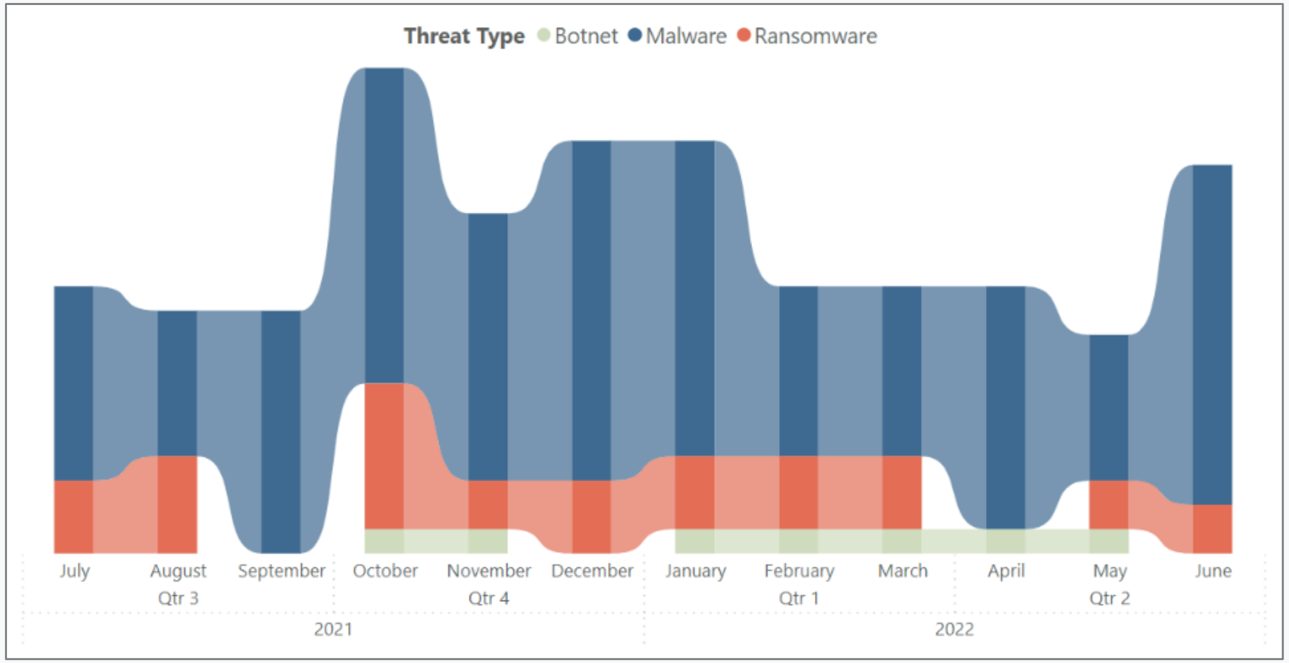


Figure 1: Threat Trend Analysis Q3Q4 2021 and Q1Q2 2022

From the last 6 months of 2021 going into the first 6 months of 2022, **overall threat attempts are down slightly** by **8%**. Similarly, moving from Q1 to Q2 of 2022, **overall threat attempts are down by 11%**. This statistics may be due to certain factors. For instance, COVID-19 disease is still around, and yet some countries are already transitioning to endemic phases. As a result, governments and private sectors had shifted their business mode and encouraged employees to resume working arrangement - return to office. As a result, this had slightly reduced overall threat exposure of remote working. Statistically, the theme had changed as there is no reported phishing campaign directly related to COVID-19 in the past 6 months. However, phishing as vector of attack remains a huge concern for organization, regardless of their size and nature of business. Malware campaigns, however remains a major threat. As we witnessed in majority of high-profile breaches, threat actors leverage third parties to reach their desired victims.

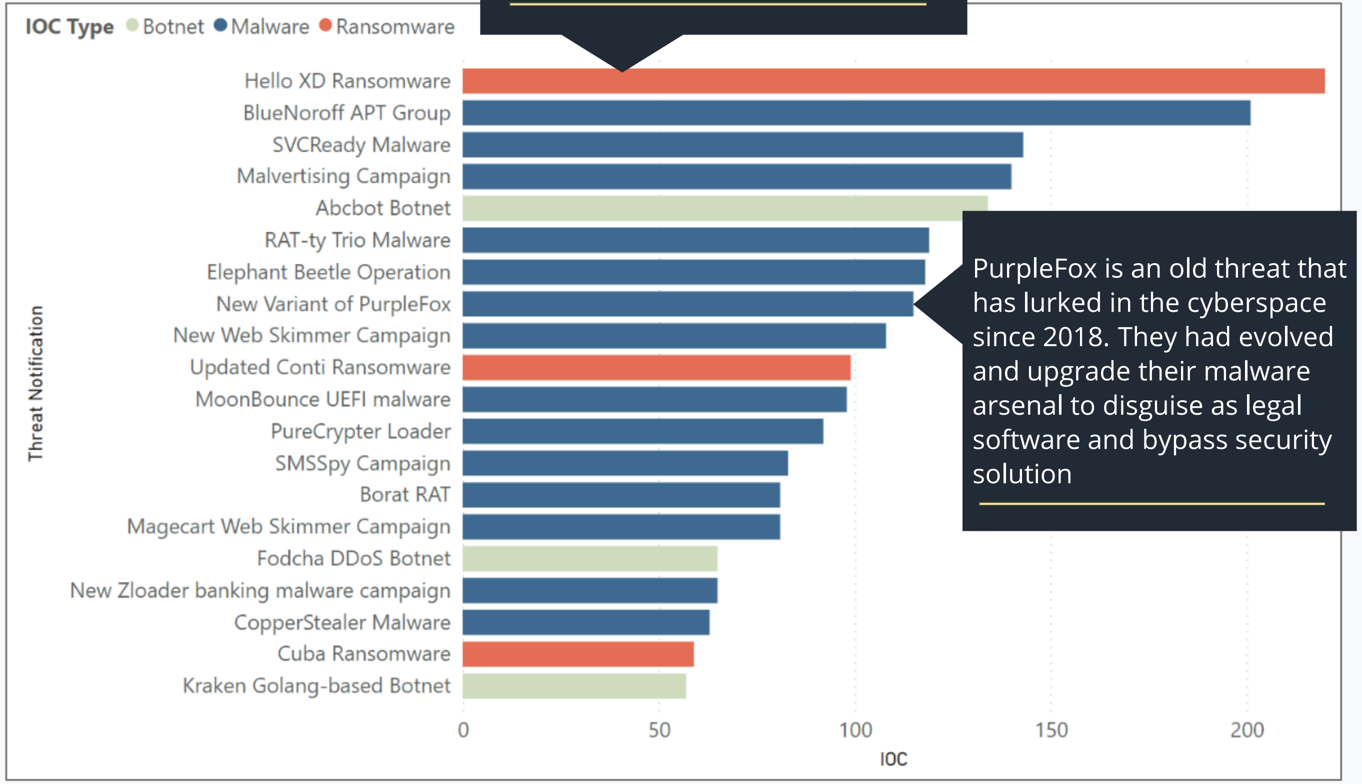
Trend Analysis

The top 5 threat notification alone generated over **3600 unique IOC**, indicating huge attack volume from these threat actors. In order to protect from such threats, organization should proactively detect threats before they spread to critical system. This can be done with threat hunting or setting up a team of threat intelligence analysts to monitor and keep malicious threats at bay. Organizations can leverage IOC by proactively incorporating them with existing security solution such as Security Information and Event Management (SIEM) and Intrusion Prevention System (IPS).

41

The average number of IOC per threat notification sent by SysArmy CIMC

There has been an upsurge in threat activities from Hello XD ransomware group. Other than its payload that encrypt file systems, the threat actor also drop backdoor to navigate maintain persistence.

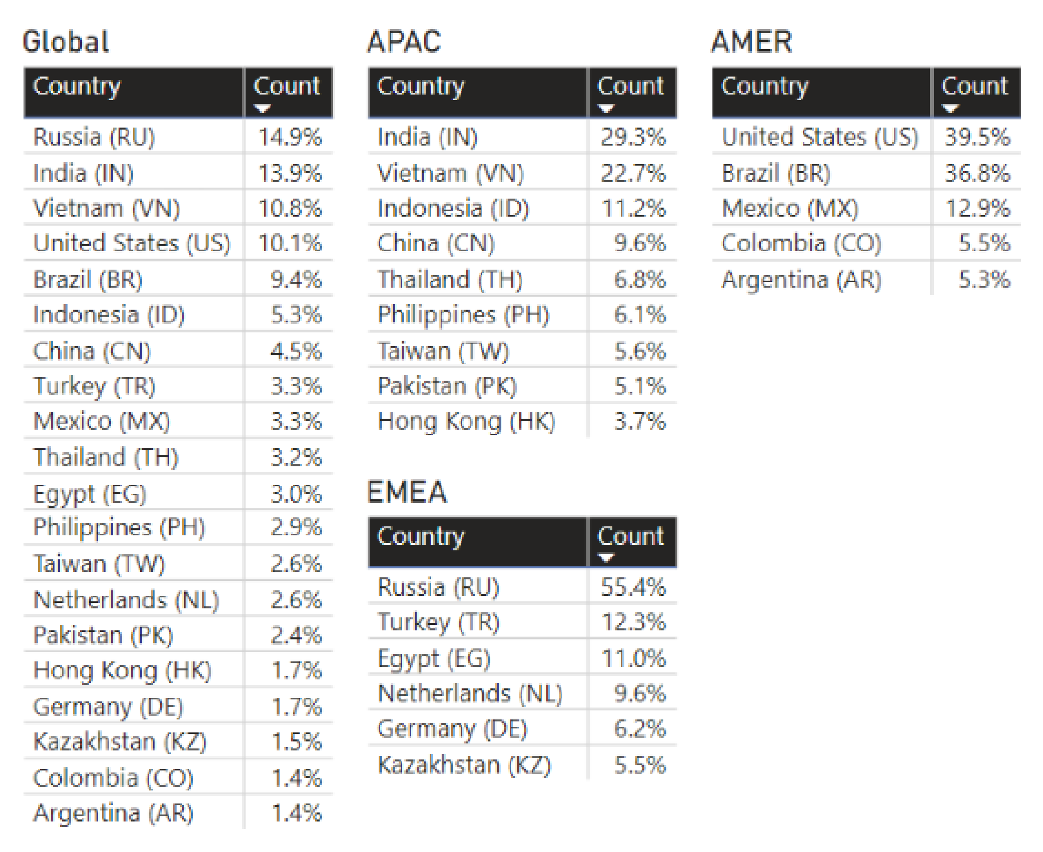


PurpleFox is an old threat that has lurked in the cyberspace since 2018. They had evolved and upgrade their malware arsenal to disguise as legal software and bypass security solution

Figure 2: Threat Volume in Q1Q2 2022

Threat Origins

Globally, we discovered that Russia (**14.9%**), India (**13.9%**) and Vietnam (**10.8%**) were at the top of the list for origins of threat. Any form of actions taken in the geopolitical scenario would have a significant impact on the cybersecurity landscape too. This was evident as we seen on multiple occasion such as the Russian invasion of Ukraine. In today's scene, cybersecurity has become part of the arsenal in geopolitical conflicts and attacks can be sophisticated and persistent. As such, in times of crisis, organizations need to lower the thresholds for detecting intrusion. This is where detection and protection pillar need to be thoroughly reviewed as part of preparation for unprecedented cyber attacks.



Global

Country	Count
Russia (RU)	14.9%
India (IN)	13.9%
Vietnam (VN)	10.8%
United States (US)	10.1%
Brazil (BR)	9.4%
Indonesia (ID)	5.3%
China (CN)	4.5%
Turkey (TR)	3.3%
Mexico (MX)	3.3%
Thailand (TH)	3.2%
Egypt (EG)	3.0%
Philippines (PH)	2.9%
Taiwan (TW)	2.6%
Netherlands (NL)	2.6%
Pakistan (PK)	2.4%
Hong Kong (HK)	1.7%
Germany (DE)	1.7%
Kazakhstan (KZ)	1.5%
Colombia (CO)	1.4%
Argentina (AR)	1.4%

APAC

Country	Count
India (IN)	29.3%
Vietnam (VN)	22.7%
Indonesia (ID)	11.2%
China (CN)	9.6%
Thailand (TH)	6.8%
Philippines (PH)	6.1%
Taiwan (TW)	5.6%
Pakistan (PK)	5.1%
Hong Kong (HK)	3.7%

EMEA

Country	Count
Russia (RU)	55.4%
Turkey (TR)	12.3%
Egypt (EG)	11.0%
Netherlands (NL)	9.6%
Germany (DE)	6.2%
Kazakhstan (KZ)	5.5%

AMER

Country	Count
United States (US)	39.5%
Brazil (BR)	36.8%
Mexico (MX)	12.9%
Colombia (CO)	5.5%
Argentina (AR)	5.3%

Figure 3: Threat of Origins

Targeted Industries

As evident in our datasets, financial services **(56.5%)** are the primary target for threat actors, whereby threat attempts are majorly motivated by the prospect of financial gain. This is followed by retail (**14.5%**), digital services (**9%**), manufacturing (**6.2%**), Government-Linked Companies (**5.0%**), Critical Infrastructure (**4.8%**), Corporate (**3%**) and Education (**1%**). As the world is rapidly digitizing and connecting customers (individuals), organization, devices and governments; enabling seamless transactions, work collaborations, and social interactions, so are the exposure to risks and cyber threats. As such, to stay ahead of cyber threat actors, SysArmy highly encourage the practice of open threat intelligence sharing between government agencies, regulators, Managed Security Service Providers (MSSP), and across all vertical of industries. By exchanging threat intelligence among the community, organization would benefit from the collective knowledge, experience and capabilities to better understand the threats they face.

The Financial Sector Blueprint 2022-2026 released by Bank Negara Malaysia had outlined their consideration to integrate intelligence-sharing with third party service providers[2]

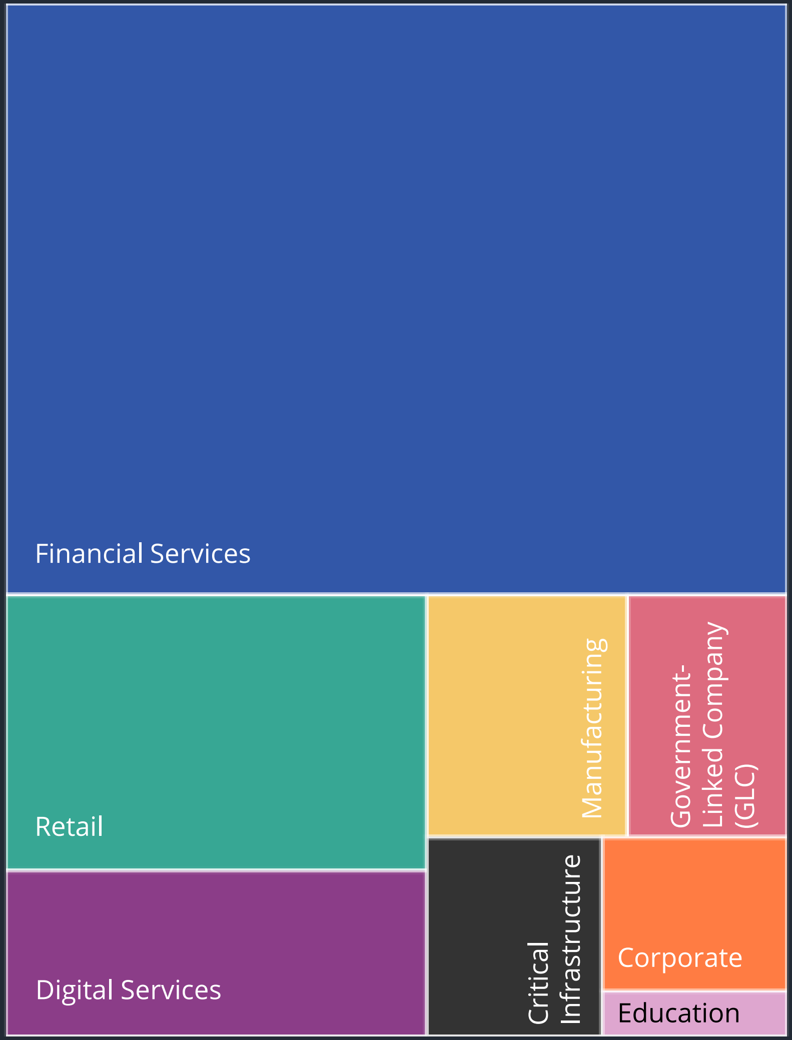


Figure 4: Top Attempts by Industries

Threat Landscape

The following are some key trends highlighted in this report, including a disruptive supply chain risk, evolving trend of ransomware, vulnerabilities exploitation and the impact of Russia-Ukraine Conflict on cybersecurity.

Digital Supply Chain Risk

Disruptions are inevitable. But when it comes to supply chain, the technology that we used today are part of the big ecosystem. One slip up and your critical data could be in the hand of threat actors

Ransomware Trend

The Ransomware as a Service (RaaS) model has only sparked more threat actor group to target high profile organization. We witness a **25%** hike in threat from **Q4 2021 to Q1 2022**

Vulnerability Exploitation

Many router product are exposed to vulnerabilities which involve SME and home router users. Threat actors also take advantage of zero day, causing major outbreak in the wild.

Russia-Ukraine Conflict

The geopolitical tension between Russia and Ukraine have adverse effect on the threat landscape, especially within this two conflicting entity, as well as their allies.

Digital Supply Chain Risk

A digital supply chain refers to leveraging advanced technologies and capabilities, such as sensors, robotics, automation and predictive analysis, to improve transparency and efficiency across the chain. The actor across the chain may range from manufacturers, retailers, distributors, wholesalers to end users. As cross-border and global supply chain linkages deepen, so will new interdependencies and potential blind spots. In these networks, each of the nodes is a possible target. Unlike most operational risks, cyber security breaches in one node can quickly propagate to others in a short period. The cyber security strength of any single 'node' or institution is therefore only as strong as the weakest link in that network. As a matter of fact, Gartner predicts that **by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021**[3]. In the next few pages, we'll look into one of the most relevant cases impacting the digital supply chain.

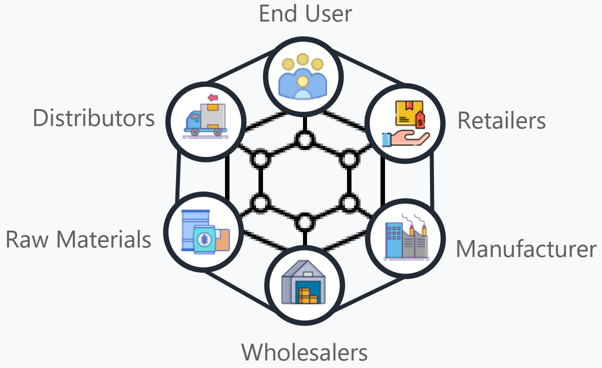
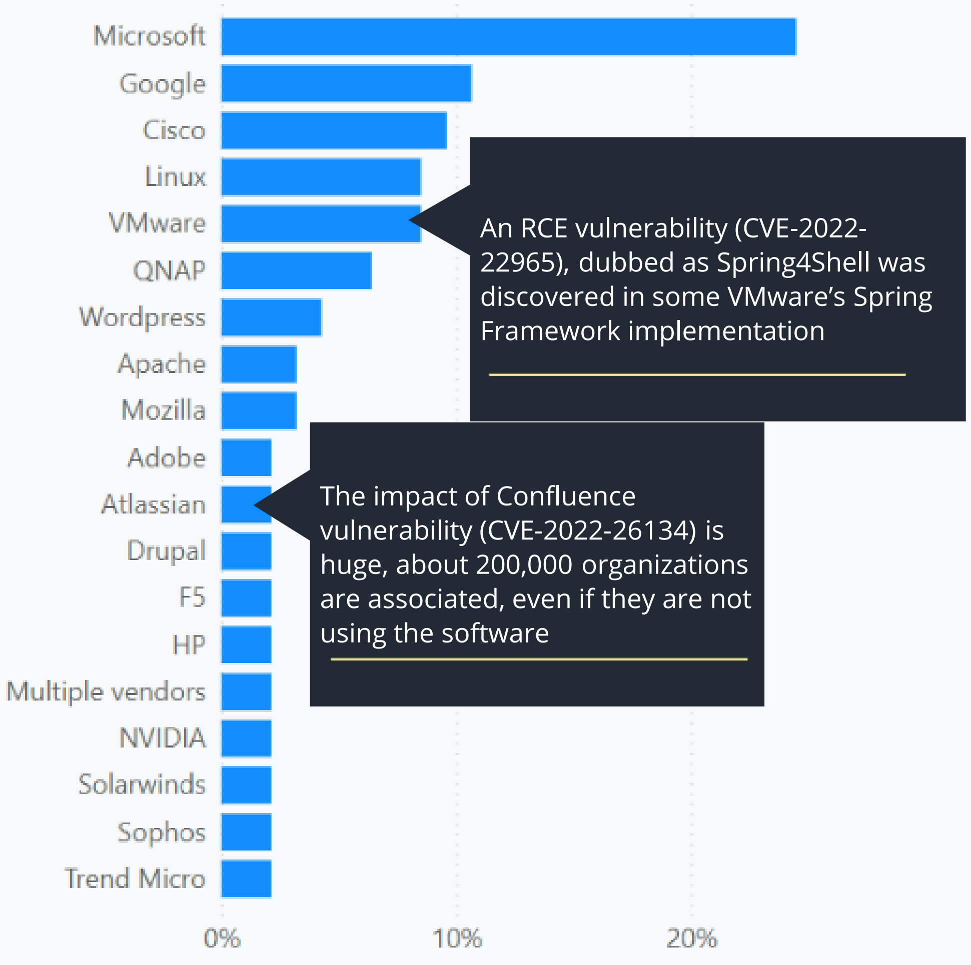


Figure 5: Supply Chain Actors



An RCE vulnerability (CVE-2022-22965), dubbed as Spring4Shell was discovered in some VMware's Spring Framework implementation

The impact of Confluence vulnerability (CVE-2022-26134) is huge, about 200,000 organizations are associated, even if they are not using the software

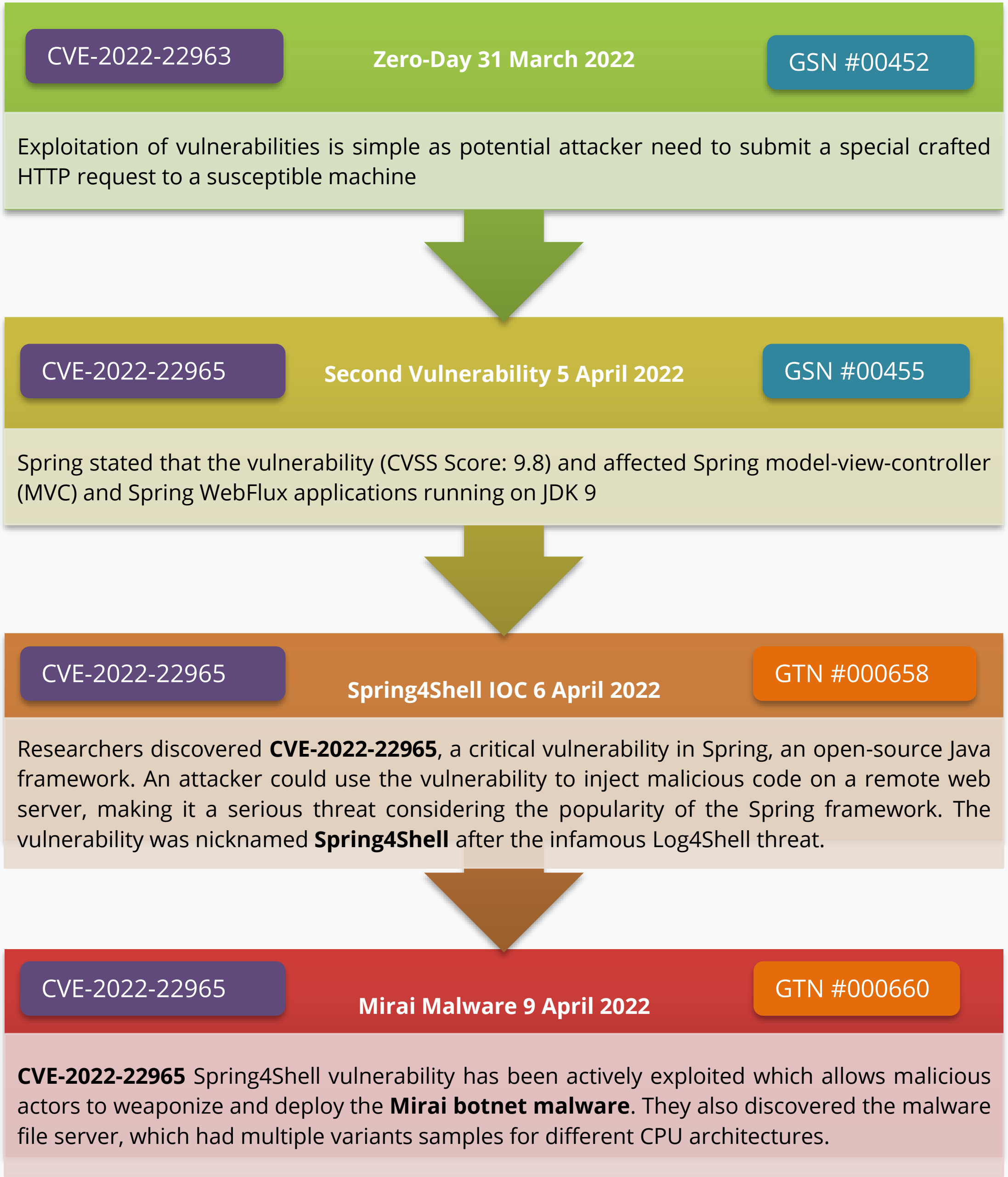
Figure 6: Vendors Affected by Vulnerabilities

Spring4Shell

CVE-2022-22965 | GSN #00455 | GTN #000658

Sping4Shell is a critical vulnerability with **CVSS Score of 9.8** impacting Java's most popular framework, Spring. Java Spring Core is a popular application framework that enables software developers to create enterprise-level Java applications fast and efficiently. On March 21st, 2022, a new zero-day vulnerability named 'Spring4Shell' has been disclosed in the Spring Core Java framework that allows unauthenticated remote code execution upon applications. The impact of RCE on this framework could be identified as a serious impact similar to Log4Shell back in late 2021. SysArmy has notified four security notifications related to this attack. These are the chronology of the exploit.

About 70% of all Java applications use Spring Framework to develop their applications [5].



CVE-2022-22963 | **Zero-Day 31 March 2022** | GSN #00452

Exploitation of vulnerabilities is simple as potential attacker need to submit a special crafted HTTP request to a susceptible machine

CVE-2022-22965 | **Second Vulnerability 5 April 2022** | GSN #00455

Spring stated that the vulnerability (CVSS Score: 9.8) and affected Spring model-view-controller (MVC) and Spring WebFlux applications running on JDK 9

CVE-2022-22965 | **Spring4Shell IOC 6 April 2022** | GTN #000658

Researchers discovered **CVE-2022-22965**, a critical vulnerability in Spring, an open-source Java framework. An attacker could use the vulnerability to inject malicious code on a remote web server, making it a serious threat considering the popularity of the Spring framework. The vulnerability was nicknamed **Spring4Shell** after the infamous Log4Shell threat.

CVE-2022-22965 | **Mirai Malware 9 April 2022** | GTN #000660

CVE-2022-22965 Spring4Shell vulnerability has been actively exploited which allows malicious actors to weaponize and deploy the **Mirai botnet malware**. They also discovered the malware file server, which had multiple variants samples for different CPU architectures.

Figure 7: Spring4Shell Exploitation Timeline

Spring4Shell

CVE-2022-22965 | GSN #00455 | GTN #000658

@RequestMapping is the most common and widely used annotation in Spring MVC. It is used to map incoming application requests into their appropriate handler functions.

ClassLoader manipulation allows an attacker to access and modify the underlying applications server settings. On certain applications servers like Tomcat 8, an attacker may tweak these settings to upload a web shell and execute arbitrary commands.

Threat Chronology

1. It started when there is a vulnerability disclosure in Spring framework and gave opportunity to attacker to send other Objects known to the application instead of the expected User object. It occurred when RequestMapping function is used together with POJO
2. The vulnerability abused a functionality of RequestMapping annotation and Spring Framework accepts any other Object input and map it according to their classes. From here, it allows the injection objects into the legitimate request handlers and led to server exploitation
3. As the door has opened, it was the time for the threat actor to trigger the vulnerability by injecting payload. The payload sorted the Tomcat server's logging properties via ClassLoader
4. The payload straight away redirect the logging logic to the ROOT directory and drops the file payload which enables the threat actors to modify the Tomcat log files names and location into an exposed web path
5. From here, the actor just need to craft a payload where the content of the request will include .jsp code
6. The last step, the threat actor need to browse to "`/springshell/attack.jsp`" to execute the malicious code. Once it has started to browse, the command **`"vi test.txt"`** will run at the same time. But the actor may prefer to upload webshell to grant the full command and control on the compromised server

Spring4Shell

CVE-2022-22965 | GSN #00455 | GTN #000658

Recommendation

Spring4Shell vulnerability involved millions of systems and majorities of them are unpatched systems. Despite the urgency to upgrade the current version of Java Spring versions, it is important to understand the fundamental concept of the framework from the perspective of a developer. By keeping the code proper and implement security features in the code, this may help to enhance the protection shield against any forms of attacks. To reduce the risk of a backdoor exploitation, it is advisable to practice the following :

It is recommended to implement **zero trust security** in all aspects, including structuring organizations, applications, software and hardware. Zero Trust Security will give ideas to put full efforts preventing attack of all forms.

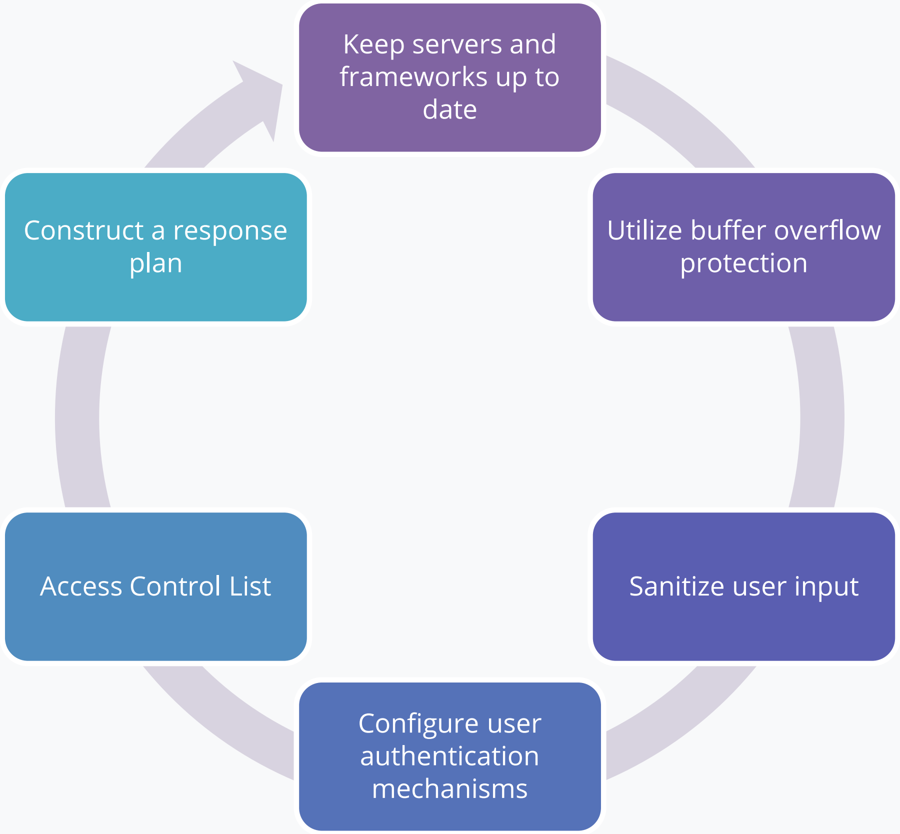

Keep servers and frameworks up to date
Utilize buffer overflow protection
Sanitize user input
Configure user authentication mechanisms
Access Control List
Construct a response plan

Figure 8: Spring4Shell Mitigation Plan

Ransomware Trend

The trend for ransomware remains a huge concern for many. What's more worrying, threat actors have a business model they could capitalize to cause even more chaos to their targets; Ransomware as a Service (RaaS) scheme has become a profitable gig-economy for threat actors to take advantage on the loophole left behind by system administrators in their IT assets. CIMC had generated multiple GTN related to ransomware threat, alongside its attributes, methodologies and IOCs. Amongst the most notable ransomware variant detected in Q1Q2 of 2022 is **Hello XD**, **Conti** and **Cuba** variant where it has contributed to **12%** of overall ransomware IOC sample. In March 2022, CISA updated their advisory with a list of domains used by groups that distribute **Conti** ransomware, as well as some IP addresses previously used to communicate with their C&C server. Their notable attack vectors include Trickbot and Cobalt Strike. In April 2022, a new RaaS group, **Black Basta** stormed onto the ransomware scene, where the community speculate that they could be a similar entity to Conti group after the group's shut down. In May 2022, researchers discovered **Nokoyawa**, a new strain of Windows operating system ransomware. Once infected, victims would be instructed to contact with the ransomware operators via a TOR browser.

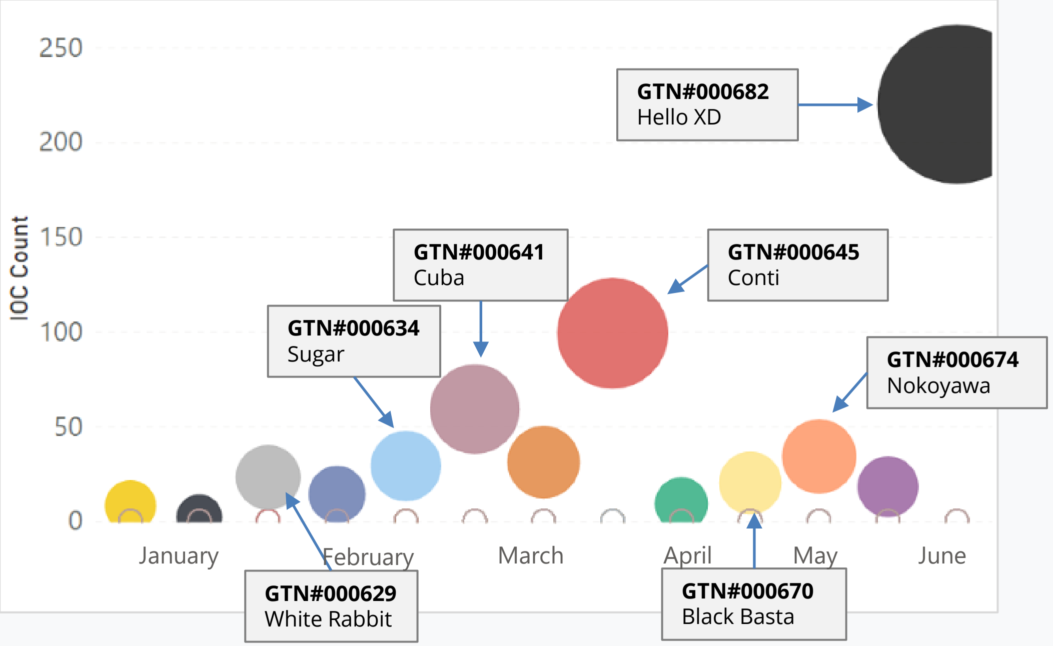


Figure 9: Ransomware Discovery in Q1Q2 2022

Ransomware Trend

In revelation with the Russia-Ukraine conflict, **Wizard Spider** group suffered a data leak by their members, believed to be a Ukraine nationality as a result of voicing support for Russia. This has resulted in unprecedented cyber warfare. Apart from that, several other group identified as **Lockbit Gang**, **Twisted Spider** and **Viking Spider**, which is thought to be originated from Eastern European region, forming one of the most prolific ransomware cartel[5] today which was suspected of several high-profile attack such as Ireland's Health Service, SolarWinds, Accenture, and bunch other small and medium sized businesses.

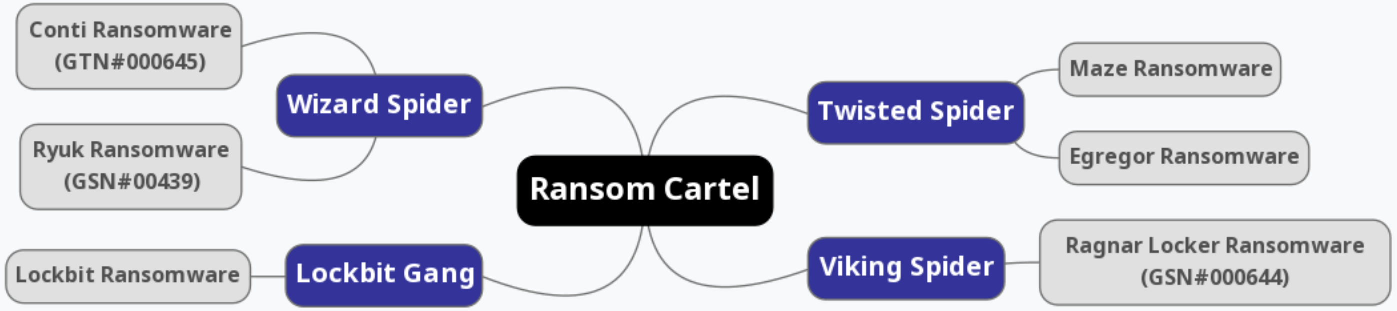


Figure 10: Cluster of Ransomware Group

Organization or individual who responded by paying the ransom would eventually incentivizes threat actors to commit this crime. SysArmy strongly advise individual and organization to never pay cybercriminals in ransomware exploitation since there absolutely no basis of guarantee that they will provide a decryption for data recovery. In fact, by paying cybercriminals, it will only encourage their operation and provide more capital for them to grow this criminal scheme to a larger extent. As mentioned by Gartner[6], for those who paid the ransom, only **65% of the data is recovered**, and only **8% of organizations manage to recover all data**. In truth, organizations cannot 100% prevent ransomware attacks. The best thing to do is assume that you will be hit and formulate plans in place that enable swift response.

Russia-Ukraine Conflict

The geopolitical unrest between Russia and Ukraine have an adverse effect on the threat landscape, especially within this two conflicting entity, as well as their allies. Cyber attacks between the two nation have persisted ever since Russia's illegal annexation of Crimea in 2014, the attack intensifies going into the 2022 invasion. As highlighted in the scatter chart below, CIMC notifies clients of all industry verticals of the threat related to the conflicting region. Early in the year, a wiper malware known as **WhisperGate** was discovered by researchers targeting government, non-profit organization and information technology groups in Ukraine. The impact of the intrusions were huge as numerous government websites in the country were defaced with a message warning Ukrainians that their personal data was being uploaded to the internet. The threat was believed to be attributed to an emerging group codenamed "**DEV-0586**".

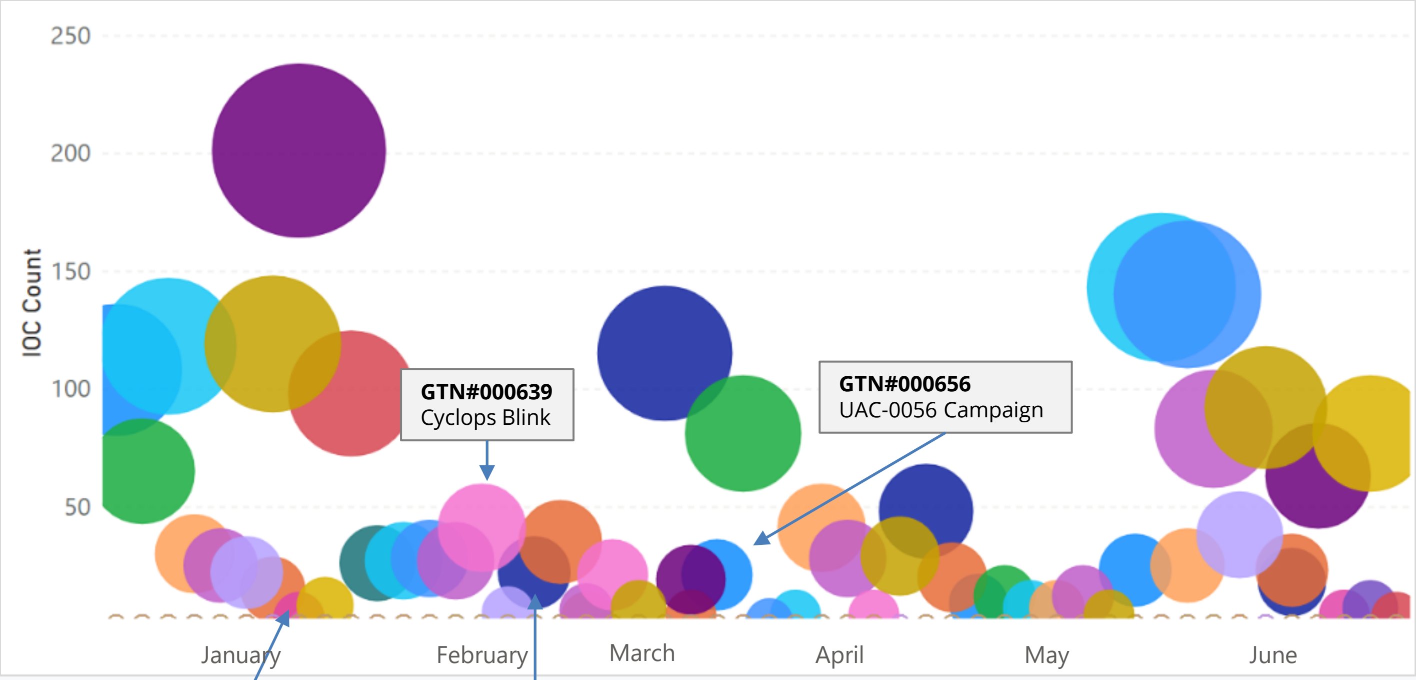


Figure 11: Threat Volume in Q1Q2 2022

Russia-Ukraine Conflict

Sandworm, a notorious Russian threat group have resurfaced in February 2022. As reported by a joint security advisory published by US and UK cybersecurity and law enforcement agencies, the group utilized **Cyclops Blink.** The threat is believed not directly linked to the situation in Ukraine, however it may be an attempt to build an army of compromised routers for cyberwarfare. In the advisory, the malware has appeared to be sophisticated and professionally developed, given its modular design approach. As a preventive measure, it is recommended that system administrators follow the mitigation advice released by product principals. There were also cases of data-wiping malware being used, targeting Ukrainian entities before and during the conflict. **HermeticWiper**, one of the most highly distributed wiper has one and only purpose; to cause disruptions to the availability of data by making storage drive unusable. Often deployed together with **WhisperGate**, the impact are devastative as computer systems would be render inoperable. The wiper would misuse legitimate drivers of popular disk management software in order to corrupt data. In April 2022, researchers have observed cyber espionage activities from **UAC-0056** or **Ember Bear** an entity that has mainly targeted Ukraine and Georgia since early 2021. The typical kill chain process that this group typically adopt consist of weaponizing with lure files in Microsoft Office file formats, and delivering via targeted, spear-phishing emails containing these malicious attachment and links. CIMC highly encourage end users to actively track IOC and any indicator of future attacks from these threat actors as it would cause major disruption if they slipped past your environment.

Sandworm have been attributed to the following disruptions in the past:

- **BlackEnergy** trojan disruption of Ukrainian electricity in 2015
- **Industroyer** disruption of Ukrainian electricity in 2016
- **NotPetya** in 2017
- **South Korea Winter Olympics and Paralympics** in **2018**
- **Georgian web hosting defacement** in 2019

Vulnerabilities Exploitation

The exploitation could be happened due to the disclosure of vulnerability by deploying significant tools and crafted script used by APT groups. The negligence of system provider may increase the risk in facing cyber attacks which may involve their end users' credentials. Most of critical vulnerabilities (CVSS 9.0 and above) may have higher chances to get attacks and being injected with numerous payloads by the threat actors to be granted in command-and-control attack towards the compromised devices. CIMC notifies more than **500 CVE** involving various type of devices, software, network services which influenced by many factors such as geopolitics crisis, campaigns in supply chain attacks, the rise of specific malware throughout the months and many more.

The spike in January was a result of internet **browsers vulnerabilities** which involved Google Chrome and Firefox in different versions.

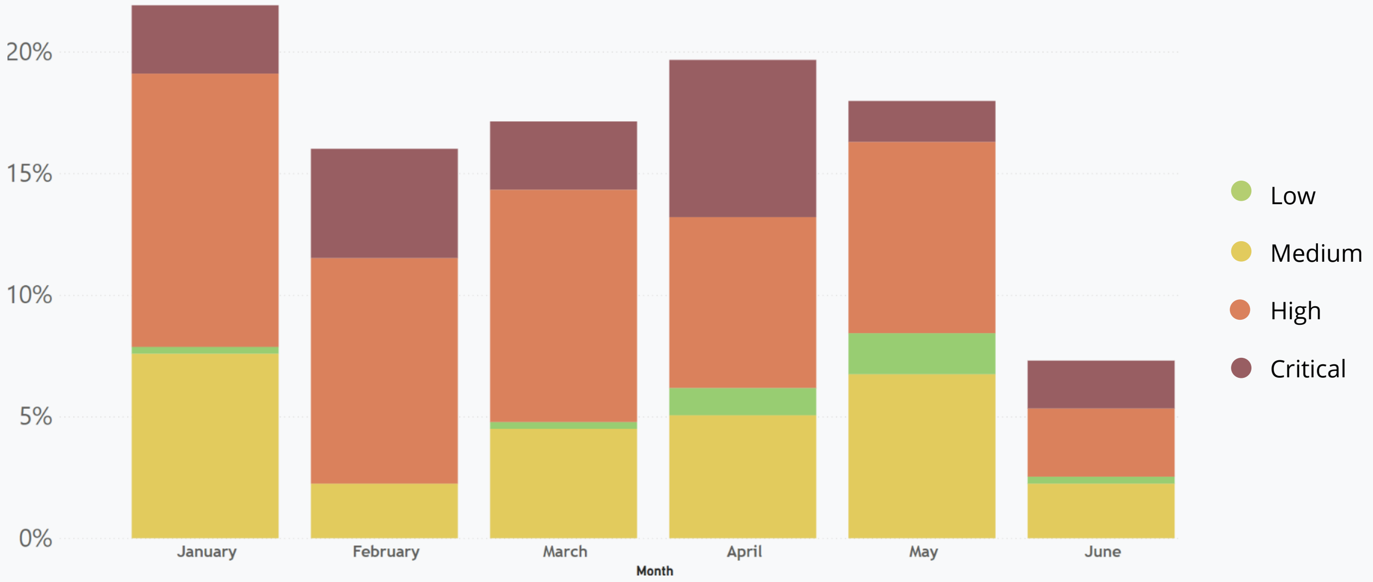
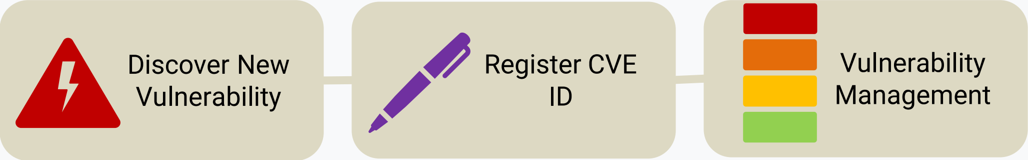


Figure 12: CVE by severity over Q1Q2 2022

CVSS Calculation Component

How does It Works?

CVSS Calculation will begin once there is a new vulnerability discovered in a specific system or hardware which connected to the Internet. These calculation will be made by security researcher. This is how the process flow:

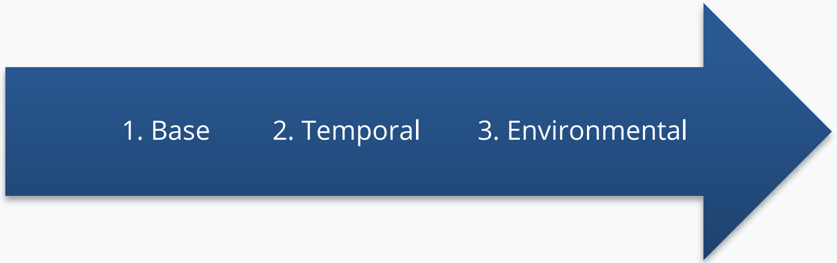


Discover New Vulnerability

Register CVE ID

Vulnerability Management

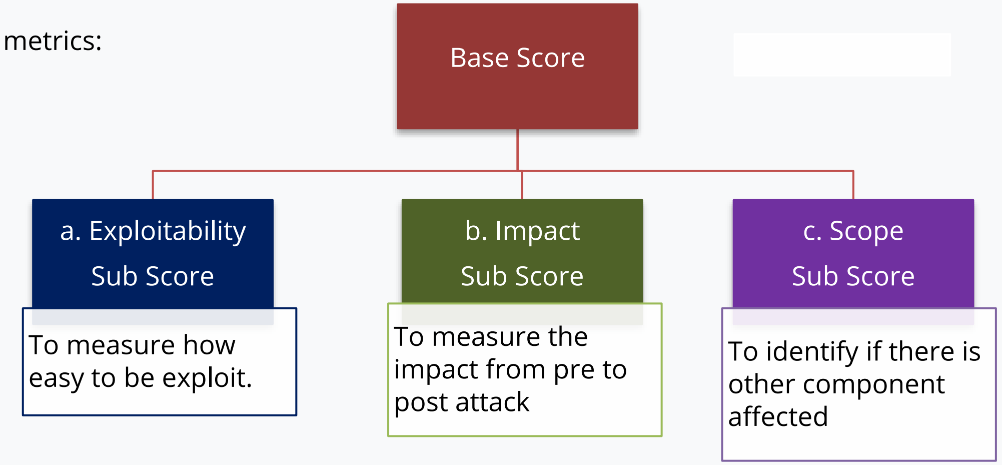
To identify the vulnerability score of a system, here is a standard used by security researchers to plot the severity of the vulnerabilities which called as Common Vulnerability Scoring System CVSS. There are 3 main scores in CVSS:



1. Base 2. Temporal 3. Environmental

1. Base Score

Base score measures the inherent qualities of vulnerability which should not change over time nor dependent on certain environments. To get the base score, it needs to calculate 3 sub scores where each sub scores contains its metrics:



Base Score

a. Exploitability Sub Score

To measure how easy to be exploit.

b. Impact Sub Score

To measure the impact from pre to post attack

c. Scope Sub Score

To identify if there is other component affected

a. **Exploitability Sub Score –** To measure the level of vulnerable **component.**

Metric	Description
Attack Vector (AV)	How easy to access the vulnerability
Attack Complexity (AC)	What prerequisites are necessary for exploitation
Privileges required (PR)	The level of privileges needed to exploit the vulnerability
User Interaction (UI)	Whether exploitation requires actions from a tertiary user

CVSS Calculation Component

b) **Impact Sub Score** – to analyze the impact made by the exploitation on the affected component or environment. It defines from pre to post exploit. The metrics are following the CIA Triads Components:

Metrics	Descriptions
Confidentiality	The lost of data confidentiality in the component and system involved
Integrity	The lost of data integrity throughout the system functionality
Availability	The lost of availability of the component and system

c) **Scope Sub Score** – to identify the vulnerability impact involved other than current affected environment. This sub score will be using binary (either Changed or unchanged).

2. Temporal

Temporal score analyzed based on current status as a well-known vulnerability. These follow the below metrics:

Metrics	Descriptions
Exploit Code Maturity (E)	The current existence of components, tools or code that can be used to exploit the vulnerability
Remediation Level (RL)	The level of remediation available for the end users
Report Confidence (RC)	The accuracy degree on the vulnerability report

3. Environmental

Environmental metric is to calculate the current severity degree of the vulnerability which has impacted on individual systems. This metric is a customized based on the base score metrics. Environmental metrics are most powerful tools when applied internally by security teams calculating severity in relation to their own systems.

Key takeaway

Vulnerabilities within software/hardware are here in cybersecurity threat landscape. The most important part for any organization to stay ahead in the game is to implement a robust Cybersecurity framework as outlined by the National Institute of Standards and Technology (NIST).

Zero Day Exploitation

Attacker groups always seek for opportunities to access vulnerable system Zero day is a known term used to described a new discover related to security vulnerabilities that attackers use to attack system. The term "zero-day" describes the fact that the vendor or developer has only just learned of the flaw – which means they have “zero days” to fix it. A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it. Zero-day exploitation could be in any forms of attack as shown below.

SysArmy team had notified client **19 alerts** related to zero-day vulnerabilities in several categories which are:

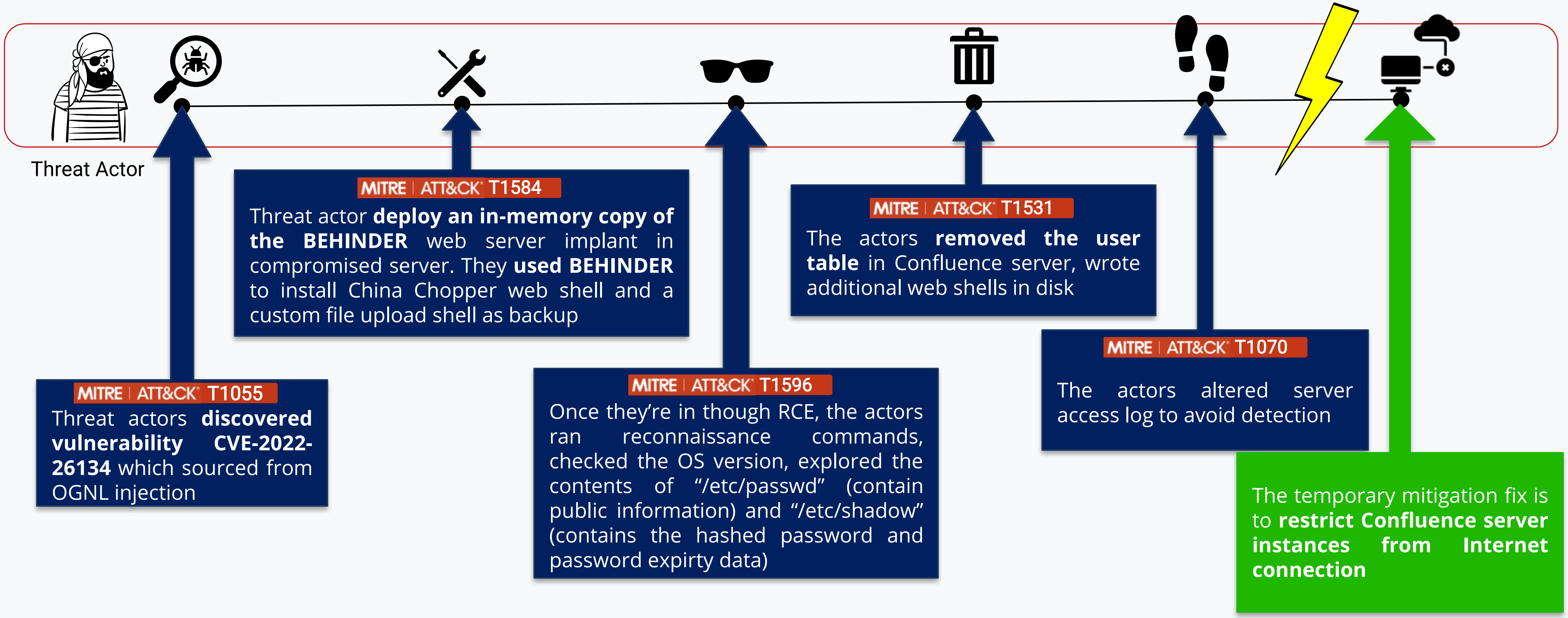
- Hardware (servers, routers, printers)
- Browser applications
- Language Frameworks
- Operating systems

QNAP NAS Devices Zero-Day Exploit	Google Chrome Zero-Day Exploit	Spring Java Framework Zero-Day Exploit	Exploits Zero-Day Exploitation of Atlassian Confluence
25 January 2022	14 February 2022	31 March 2022	4 June 2022
GSN #00415	GSN #00425	GSN #00452	GSN #00495
CVE-2022-27588	CVE-2022-0609	CVE-2022-22963	CVE-2022-26134
Deadbolt Ransomware	Execute Damaging Code	Mirai Malware	Remote Code Execution

Atlassian Confluence Zero Day Vulnerability Exploitation

CVE-2022-26134 | GSN #00495 | GTN #00676 | T1195.003

How Does Attack Happen?



Threat Actor

MITRE | ATT&CK® T1055

Threat actors **discovered vulnerability CVE-2022-26134** which sourced from OGNL injection

MITRE | ATT&CK® T1584

Threat actor **deploy an in-memory copy of the BEHINDER** web server implant in compromised server. They **used BEHINDER** to install China Chopper web shell and a custom file upload shell as backup

MITRE | ATT&CK® T1596

Once they're in though RCE, the actors ran reconnaissance commands, checked the OS version, explored the contents of "/etc/passwd" (contain public information) and "/etc/shadow" (contains the hashed password and password expirty data)

MITRE | ATT&CK® T1531

The actors **removed the user table** in Confluence server, wrote additional web shells in disk

MITRE | ATT&CK® T1070

The actors altered server access log to avoid detection

The temporary mitigation fix is to **restrict Confluence server instances from Internet connection**

Atlassian Confluence Zero Day Vulnerability Exploitation

CVE-2022-26134 | GSN #00495 | GTN #00676

Mitigation and Response Plan

- Upgrade to a fixed version of Confluence as soon as possible.
- Updating mitigation information to include replacement jar and class files.
- Ensure that you have locked down the internet-facing access to the Confluence server and the data center.
- As you monitor your Internet-facing web services, ensure that log retention policies and robust monitoring capabilities are in place.
- Using a SIEM or Syslog server, send appropriate log files from each web server that has access to the Internet.
- Keep an eye out for suspicious child processes or processes that are part of web applications
- Construct a secure Connection - Every connection to an external network, no matter how well monitored, is a potential avenue for an attack into the network. To be safe in a security architecture of an organization, IT managements should identify which devices should implement unsegmented and segmented network in organization.

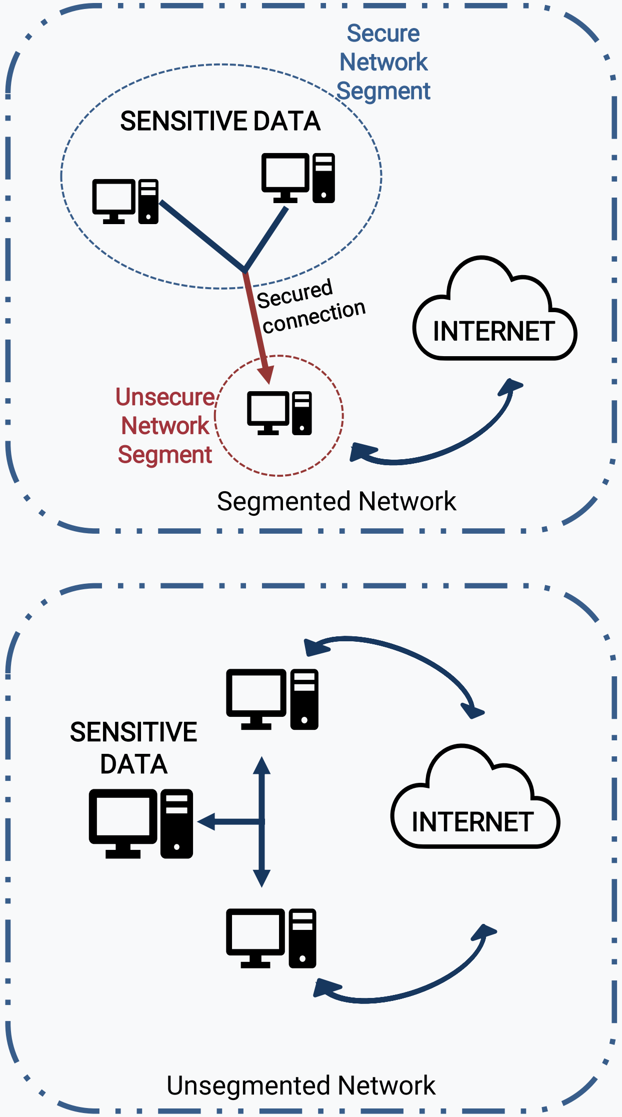


Figure 13: Segmented and Unsegmented Network

Vulnerabilities Exploitation

Router Exploitation

The increasing usage of internet around the globe has put the priority of securing routers and VPN at the top of the list. The installation of routers and internet are not only involved home users, but also Small and Medium-sized Enterprises (SME) as digitalized business and marketing offer huge demands from the market. In first half of 2022, CIMC has generated threat and vulnerabilities notifications on different attack methods used to exploit routers. Common methods used by threat actors are DDoS, remote code execution (RCE), brute force and many more.

The security threats related to network security devices so far in first half of 2022:

13 January 2022 **GSN #00397**

KCodes NetUSB Kernel Module

Remote Exploitation

4 February 2022 **GSN #00419**

Cisco Small Business RV Series Routers

Vulnerability Exploitation

18 February 2022 **CVE-2022-20653** **GSN #00429**

Cisco Secure Email

Routing Exploitation using DOS

16 April 2022 **CVE-2021-22205** **CVE-2021-35394** **GTN #000663**

Android, GitLab, Realtek Jungle SDK, MVPower DVR, LILIN DVR, TOTOLINK Routers, ZHONE Router

Fodcha DDoS Botnet

20 April 2022 **CVE-2022-20685** **GSN #00467**

SNORT IDS and IPS

Exploiting vulnerabilities

28 April 2022 **CVE-2022-23121** **CVE-2022-0194** **GSN #00474**

QNAP Routers

Exploiting vulnerabilities

21 May 2022 **GSN #00487**

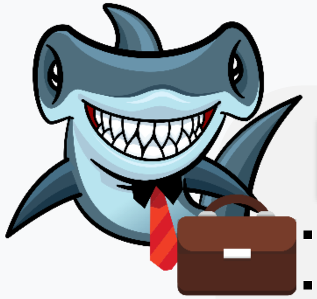
IOS XR Routers

Exploiting vulnerabilities

Cybersecurity360

Phishing

Phishing is an initial attempt by cybercriminals by sending fraudulent communication that appear to come from legitimate source(s). This crime can be categorized as one of the most dangerous threat in social engineering attacks, with a plan to trick a victim into doing what they are not supposed to do while creating a sense of urgency and panic towards victims. Phishing are often used to steal data and it is often motivated by financial gain. The following highlights 6 type of phishing and how to identify them.



Business Email Compromise

- Unusual financial transactions
- Create sense of urgency/obligation
- Create pressure/fear
- Self-promotion/Displaying power

Masquerading Phishing

- Generic salutation
- Grammar mistakes
- Spelling errors
- Unexpected/surprising event
- Irrelevant context

Smishing

- Texts from unknown numbers
- Contains links (normally shortened URL)
- Inducement rewards

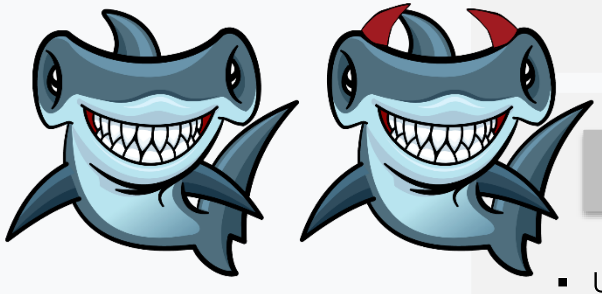
Spear Phishing

- Unusual communication channel
- Feign ignorance
- Create sense of urgency/ obligation

Phishing

Vishing

- Calls from unknown numbers
- Feign ignorance/Equivocation
- Claims to be calls from government authorities
- Create sense of obligation/guilt/conformity

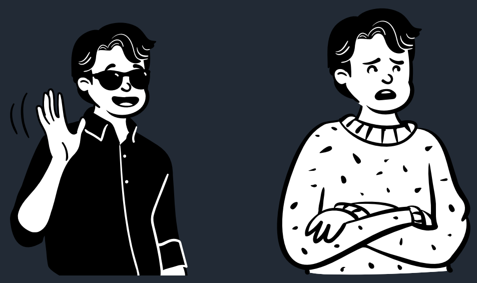


Pharming / DNS Poisoning

- Unusual behavior of browsing
- Website without HTTPS/Issued to different entity

Remember!

Whenever someone requested you to do something



1. Always **verify** authenticity
2. Put a **pause** to think twice
3. **Create** and **follow** trusted channel to verify
4. **Double confirm** with different communication method

A Safer Digital World

SysArmy had been in operation since 2014. Apart from the security monitoring pillar, the organization also provide other services in the area of risk management and security assessment. Our team had since then grown rapidly by five-fold to provide professional services to over **200+ businesses globally**.

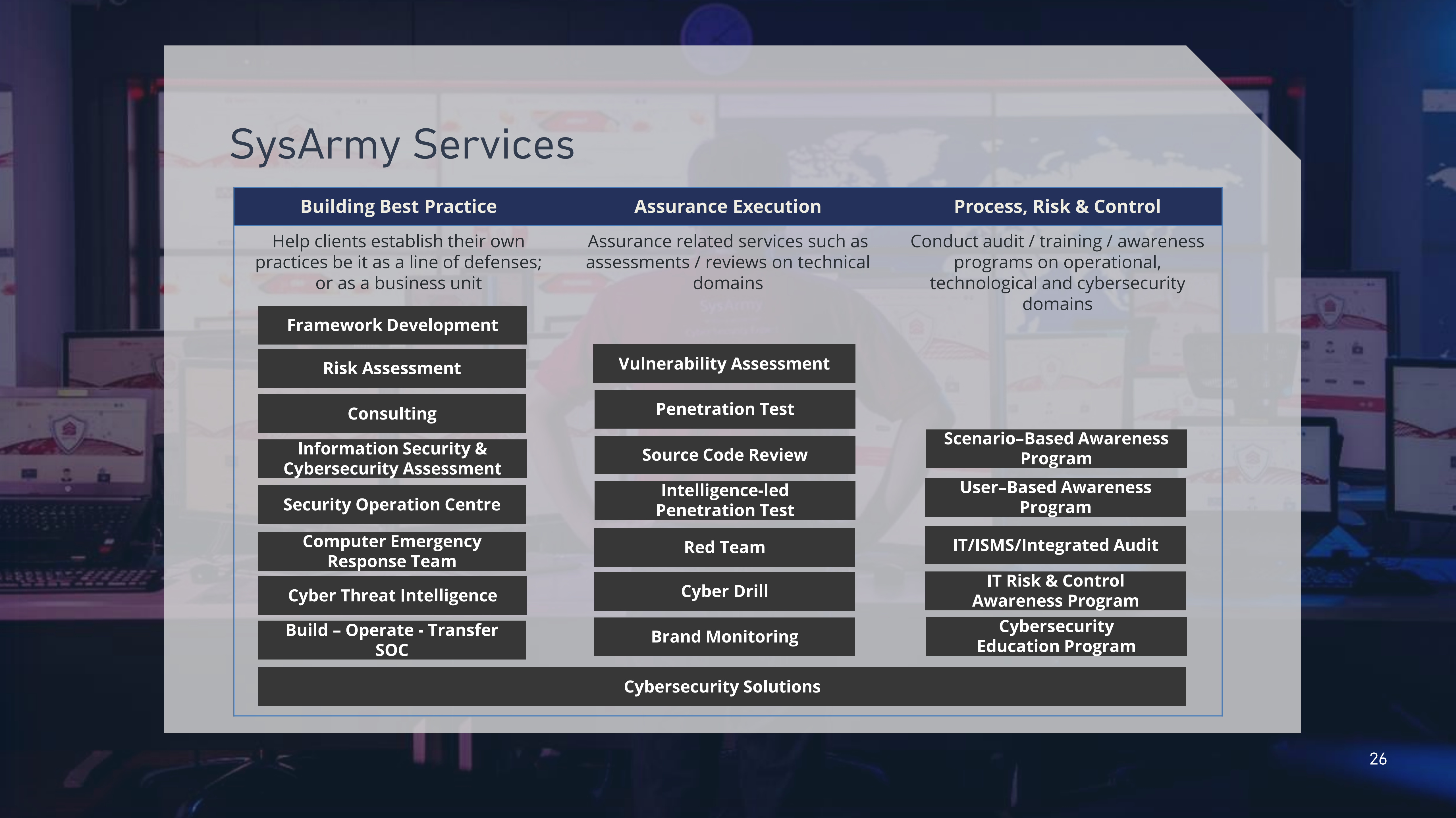
ISO 27001:2013 Certified

CREST Penetration Testing Certified

Core Philosophy

We believe that cybersecurity is the culmination of several elements to achieve maximum visibility in any environment. Instead of relying solely on security endpoint products, SOC pursues a methodology that requires intervention of people and formulated process, as the cyber-attacks are originated by the perpetrators who are also human.

People **Process** **Technology**



SysArmy Services

Building Best Practice

Help clients establish their own practices be it as a line of defenses; or as a business unit

- Framework Development
- Risk Assessment
- Consulting
- Information Security & Cybersecurity Assessment
- Security Operation Centre
- Computer Emergency Response Team
- Cyber Threat Intelligence
- Build – Operate - Transfer SOC

Assurance Execution

Assurance related services such as assessments / reviews on technical domains

- Vulnerability Assessment
- Penetration Test
- Source Code Review
- Intelligence-led Penetration Test
- Red Team
- Cyber Drill
- Brand Monitoring

Process, Risk & Control

Conduct audit / training / awareness programs on operational, technological and cybersecurity domains

- Scenario–Based Awareness Program
- User–Based Awareness Program
- IT/ISMS/Integrated Audit
- IT Risk & Control Awareness Program
- Cybersecurity Education Program

Cybersecurity Solutions

Glossary

APT – Advanced Persistent Threat is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time.

C&C – Command and Control server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.

CIMC – Cyber Intelligence and Monitoring Center is the operation team in SysArmy which operates on a 24x7x365 basis to detect threats on the clients' digital environment.

CVSS - The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities.

GTN – Global Threat Notification is any information related to client nature of business or threat impacting client critical asset list that warrant a notification to be send to client.

GSN – Global Security Notification is a notification to client using the information from security portal, forum, to share news about the latest discovered in software/hardware security vulnerabilities and threats as our client can plan and take immediate actions to mitigate before being exploited wild by intruder.

IoC – Indicator of Compromise is an artifacts from intrusion that are identified on organizational information system. It provides valuable information on systems that have been compromised.

RCE – Remote Code Execution is an attacker's ability to run any commands or code of the attacker's choice on a target machine.

Appendix

[1] CISOMAG – https://cisomag.eccouncil.org/psychology-of-human-error-could-help-businesses-prevent-security-breaches/

[2] Bank Negara Malaysia – Financial Sector Blueprint 2022-2026 - https://www.bnm.gov.my/publications/fsb3

[3] Gartner - https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

[4] Security Boulevard - https://securityboulevard.com/2022/03/spring4shell-what-happened-whos-vulnerable-and-how-to-mitigate/

[5] Ransom Mafia: Analysis of the world's first ransomware cartel - https://analyst1.com/whitepaper/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

[6] Gartner - https://www.gartner.com/en/articles/when-it-comes-to-ransomware-should-your-company-pay

SysArmy

A Safer Digital World