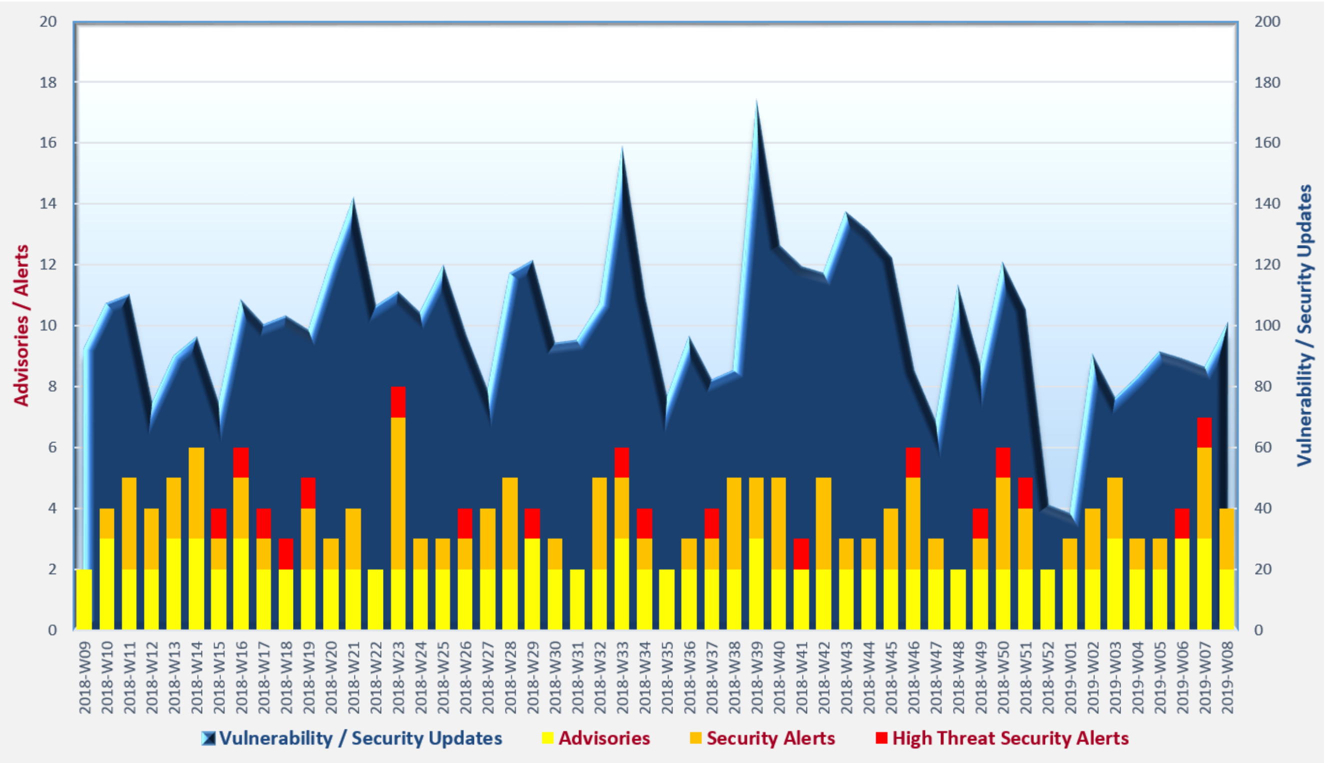
Cyber Security Threat Trends 2019-M02

February 2019

With reference to the FIRST Traffic Light Protocol (TLP) standard[1], this document is classified as TLP:WHITE information. Recipients may share with peers and partner organisations without restriction.

Cyber Security Threat Landscape of the past 12 months (source: GovCERT.HK)



Trending:

- **Cloud platforms** become popular targets of attackers who are attracted by the platforms' large volume of sensitive data and strong computational power. Enterprises should assure secure configurations and strong authentication for their cloud deployments.
- **Exploit code** is often readily available after disclosure of vulnerabilities. Enterprises must patch the known vulnerabilities timely before attackers could exploit them.
- **PowerShell** is increasingly abused by malware for fileless attacks and lateral movement. LAN administrators should restrict PowerShell script execution on end user computers.

[1] https://www.first.org/tlp/

CERT Advisories

Organisations could consider using IPsec to protect the confidentiality and integrity of their data

Organisations that want to deploy or buy network encryption using IPsec could reference to a guidance “Using IPsec to protect data”[2] published by the UK National Cyber Security Centre (NCSC) for recommendations on how to select and configure the relevant networking equipment, and how a network encryption service could operate to provide an understood level of security.

Certificates play a vital role in encryption, organisations should be aware of the proper provisioning and securing of the certificates

The NCSC published the guidance[3] on how to initially provision certificates, and to securely operate the certificates supporting infrastructure. The topics included how to manage certificates, the related Certificate Policy (CP) / Certification Practice Statement (CPS) requirements, and the shared Public Key Infrastructure (PKI) services.

[2] https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data
[3] https://www.ncsc.gov.uk/guidance/provisioning-and-securing-security-certificates

Industry Insight on Cyber Security Threat Trends

The rise of "DeepAttacks" with Artificial Intelligence (AI), attacks on Internet of Things (IoT) and malicious mobile apps and browser extensions are the predictions on cybersecurity threats in 2019

Apart from Adversarial AI, IoT attacks, and "fake apps", other key predictions include elevated sophistication of the malware used by attackers, the increasing scale of malicious cryptomining, resurgence of banking Trojans and increase of targeted ransomware attacks. Increasing Advanced Persistent Threat (APT) attacks due to supply chain attacks on chipsets or firmware or other components of smart devices would be another threats trend in 2019. Avast published their predictions in their "Avast Threat Landscape Report 2019 Predictions"[4]. Details of the report were:

- **A new type of attack, known as "DeepAttacks", which used AI to automatically generate malicious content, would be more common.** By virtue of the deep learning ability of AI, attackers could use DeepAttacks to evade AI security controls. For example, DeepAttacks could generate fake network traffic in botnets, and learn how to evade detection by firewalls or intrusion detection system. It could be trained to evolve malware to avoid detection. DeepAttacks could also be used to generate phishing sites by imitating the appearance of the legitimate web sites. AI would also be effective in launching smart attack on home network. It could be deployed to scan and profile the targets with information such as type of devices used, number of vulnerable devices and subsequently launch attack on targeted vulnerable devices automatically. Another application of AI in attack would be to break text-based captchas so as to defeat the purpose of differentiating humans and machines.

- **While there were rapid growth of IoT devices, some manufacturers put little emphasis on the security protection of their IoT products, making the devices more vulnerable.** Attack on routers would increase. 60% of users never updated the router firmware or change the default password, making these routers vulnerable to be compromised. Moreover, once an attacker compromised the router in a network, all the devices connected to the network could be accessed, and the attacker could perform various malicious activities, such as stealing credentials, launching DDoS, cryptomining, and so on.

- **Fake apps, ad-based malware and smishing (phishing by SMS) would be major mobile threat in 2019.** For Android platform, fake mobile apps were found not only in those third party download channels, but also in the legitimate Google Play Store. Such fake apps could aggressively push advertisement to user, or dispensing malicious payloads such as banking Trojans or SMS stealers to victims' device. Another growing threat would be malicious browser extensions, would could lead to credential theft, malicious cryptomining, etc.

Source: Avast

[4] https://cdn2.hubspot.net/hubfs/486579/Avast_Threat_Landscape_Report_2019.pdf

Industry Insight on Cyber Security Threat Trends

40% of Enterprises were hit by Cryptominers in 2018

The observations and insights in the 2018 cyber security landscape, included cryptomining, ransomware, malware techniques, data breaches, mobile attacks, and nation state cyber attacks, were reviewed by Check Point, which published the "Cyber Attack Trends Analysis Security Report 2019"[5]. The details were:

- **Cryptomining attacks affected over 40% of organisations in 2018, up from 20.5% as at 2017.** A wide range of devices and platforms were targeted. Cryptomining attacks became more advance, with improved evasion mechanism, fast leverage of exploits for infection, ability to deploy other malware and conceal the malware in legitimate installers.

- **Ransomware attacks became more targeted.** They selectively aimed at the critical assets of organisations for a higher chance of ransom being paid, instead of conducting large-scale undirected mass attacks, which could lead to higher exposure and attract the focus of security vendors.

- **Malware evolved from single-objective design to multi-purpose implementation.** The report quoted some examples such as a ransomware could also steal user credentials, or collect sensitive information from the victims; a botnet could be used for cryptomining as well as sending spam; a banking Trojan, in addition to credential theft, could be used for malware distribution; and so on. Increase in collaboration among attackers to conduct multi-stage attacks were also observed.

- **The popularity of public cloud adoption attracted attackers.** Cloud environments stored a large amount of sensitive data, and provided strong computational power, which offered very good incentives for threat actors to attack the cloud environment. It was observed that many of these attacks were due to poor security setting, such as system misconfigurations, and use of weak credentials. Successful attacks caused massive information leakage or the cloud services being abused for malicious activities such as cryptomining or launching DDoS attacks.

- **In 2018, attackers shown increasing interest in iOS devices.** The number of exposed iOS vulnerabilities in 2018 were observed to be increased. Moreover, a number of malware were found targeted iOS devices.

- **The participation of nation state cyber attacker in cyberspace became more prominent in 2018.** In the past, the operations by nation states in cyberspace were usually carried out in a secret manner. However, it was observed that some state actors aborted such approach, and operate in a relatively apparent and unconcealed way.

Source: Check Point

[5] https://www.checkpoint.com/downloads/resources/cyber-attack-trends-analysis-security-report-2019.pdf

Industry Insight on Cyber Security Threat Trends

Credential theft became the most common impact to organisation by phishing attack, overtaking malware infections in 2018

Based on survey replies from around 15,000 infosec professionals and more than 7,000 users, and the results from tens of millions of simulated phishing emails, Proofpoint presented the trends and statistics on phishing and other social engineering attacks and shared the findings of simulated phishing campaigns in their "2019 State of the Phish Report"[6]. The report also included regional highlights for North America, EMEA (Europe, Middle East, & Africa Countries) and APAC. The details were:

- **83% of infosec professionals responded their organisations encountered phishing attacks in 2018, an increase from 76% in 2017.** Besides, 64% of them encountered spear phishing (53% in 2017), 49% encountered vishing (voice phishing) and/or smishing (SMS/text phishing) (45% in 2017), and 4% encountered USB-based social engineering attacks via infected USB drives (3% in 2017).

- **58% of infosec professionals in Asia Pacific considered that phishing attacks were increased in 2018.** Only 50% from the North America and 33% from the EMEA had the same response.

- **The top 3 impacts of phishing to organisations were compromised accounts (65%), malware infections (49%), and data loss (24%).** The percentages of these 3 impacts in 2017 survey were 38%, 49% and 13% respectively. The increases were due to, according to the report, not only the growth of the phishing threat, but also the improved awareness of these threats to organisations. Survey results also indicated that organisations of APAC respondents were more likely to experience account compromise and data loss, while the EMEA counterparts were more likely to encounter malware infection.

- **10% of infosec professionals responded their organisations encountered ransomware attack in 2018.** However, 21% of EMEA respondents indicated their organisations experienced ransomware attack in 2018.

- **The results of simulated phishing campaigns indicated that, on average among various type of simulated phishing emails, 9% of the users clicked on the links or attachments.** 11% of users clicked the links to data entry forms and 4% submitted credentials or requested data.

- **The awareness of end user on suspicious emails increased.** There were 5.5 million emails reported by user as suspicious, an increase of 180% over the same period in 2017, reflecting users became more cautious about the emails sent to them. In fact, 59% of the reported emails were found to be potential phishing emails. Organisations could consider to implement suspicious email reporting mechanism and perform automated analysis on reported messages.

Source: Proofpoint

[6] https://www.proofpoint.com/sites/default/files/pfpt-us-tr-state-of-the-phish-2019.pdf

Industry Insight on Cyber Security Threat Trends

There were 1 million cyberattack attempts per day, a finding based on 15 million global endpoints

Carbon Black pointed out in its report "Global Threat Report: The Year of the Next-Gen Cyberattack"[7] that cyberattacks were more and more stoked by geopolitical factors. Attackers used various measures to hide themselves, such as lateral movement, island hopping, and counter incident response. Other findings of the report included:

- **$1.8 billion loss were caused by cryptocurrency-related thefts.** 27% of these were stemmed from attacks to cryptocurrency exchanges. Monero was used in 44% of all the incidents. It was observed that some ransomware attackers tried to search for cryptocurrency wallets from their victims first before carried out the ransomware attack.

- **Kryptik was the top ransomware variants found in ransomware attacks in 2018.** After infected victim systems, Kryptik tried to modify the system registry so that it could be executed every time the victim systems were started. It tried to delete the executable file after it started running, making the malware hard to be detected. Moreover, it could download and update to new version by itself.

- **Emotet was the most common commodity malware families used in the malware attack in 2018.** Emotet was a banking trojan but evolved to have the capability to deliver malware, making use of Microsoft Word documents and PowerShell.

- **More lateral movement on cyber attacks would be expected.** Cybercriminals were not just attacking one victim system in an organisation, but would try to find and compromise more targets. They abused legitimate tools such as PowerShell, Windows Management Instrumentation (WMI) and Secure File Transfer Protocol to perform lateral movement for further infection.

- **50% of cyberattack campaigns used island hopping approaches.** Attackers, instead of attacking the targeted organisation directly, they first attacked the organisation's affiliates which could be smaller or less protected organisations as springboard for further attacks.

- **32% of attacks were found to be conducted by nation-state cyber-attackers and were increasingly destructive.**

Source: Carbon Black

[7] https://www.carbonblack.com/wp-content/uploads/2019/01/carbon-black-global-threat-report-year-of-the-next-gen-cyberattack-012419.pdf

Summary of Microsoft February 2019 Security Updates

14 Product Families with Patches

7 Critical

7 Important or below

Product Family	Impact[8]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4487018, KB4487020, KB4487044, KB4487026, KB4487017
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4487017, KB4487018, KB4487020, KB4487026, KB4486996, KB4487044
Windows Server 2016, 2019 and Server Core installations 2016, 2019, v1803, v1709	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4487026 Windows Server 2019: KB4487044
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4486474, KB4487023 IE 10: KB4486474, KB4487023, KB4487025 IE 11: KB4486474, KB4486563, KB4486996, KB4487000, KB4487017, KB4487018, KB4487020, KB4487026, KB4487044
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4487000, KB4487028, KB4487025, KB4486993, KB4486563, KB4486564, KB4487023, KB4487019, KB4486996, KB4487017
Microsoft SharePoint-related software	Remote Code Execution	Critical ★★★★	KB4461630, KB4462139, KB4462143, KB4462155, KB4462171
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore
Microsoft Exchange Server	Elevation of Privilege	Important ★★★	KB4345836, KB4471391, KB4471392, KB4487052
Microsoft .NET Framework	Remote Code Execution	Important ★★★	.NET Framework, .NET Core, GitHub
Java SDK for Azure IoT	Information Disclosure	Important ★★★	CVE-2019-0729, CVE-2019-0741

[8] The Impact and Severity are the maximum impact and severity assessment of the vulnerabilities in the associated knowledgebase (KB) by Microsoft.

Product Family	Impact[8]	Severity	Associated KB and / or Support Webpages
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010, 2013, 2016, 2016 for Mac, 2019, 2019 for Mac: KB4018294, KB4018300, KB4018313, KB4462138, KB4462146, KB4462174, KB4462177, Click to Run, Office for Mac Office Compatibility Pack: KB4092465, KB4461607 Office 365 ProPlus: Click to Run Microsoft Excel 2010, 2013, 2016, Viewer: KB4092465, KB4461597, KB4461608, KB4462115, KB4462186 Microsoft Office Word Viewer: KB4462154 Microsoft PowerPoint Viewer: KB4092465
Microsoft Visual Studio	Remote Code Execution	Important ★★★	Microsoft Visual Studio 2017: CVE-2019-0657, CVE-2019-0613 Microsoft Visual Studio 2017 version 15.9: CVE-2019-0657, CVE-2019-0613 Visual Studio Code: CVE-2019-0728
Skype for Business Server 2015 CU 8	Spoofing	Important ★★★	KB3061064
Team Foundation Server 2018	Spoofing	Important ★★★	Team Foundation Server 2018 Update 3.2: CVE-2019-0742, CVE-2019-0743, CVE-2019-0646, CVE-2019-0647 Team Foundation Server 2018 Updated 1.2: CVE-2019-0647 Team Foundation Server 2017 Update 3.1: CVE-2019-0647

Learn more:
High Threat Security Alert (A19-02-02): Multiple Vulnerabilities in Microsoft Products (February 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=362)

Sources:

- 🗎 Microsoft February 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/51503ac5-e6d2-e811-a983-000d3a33c573)