TLP:WHITE

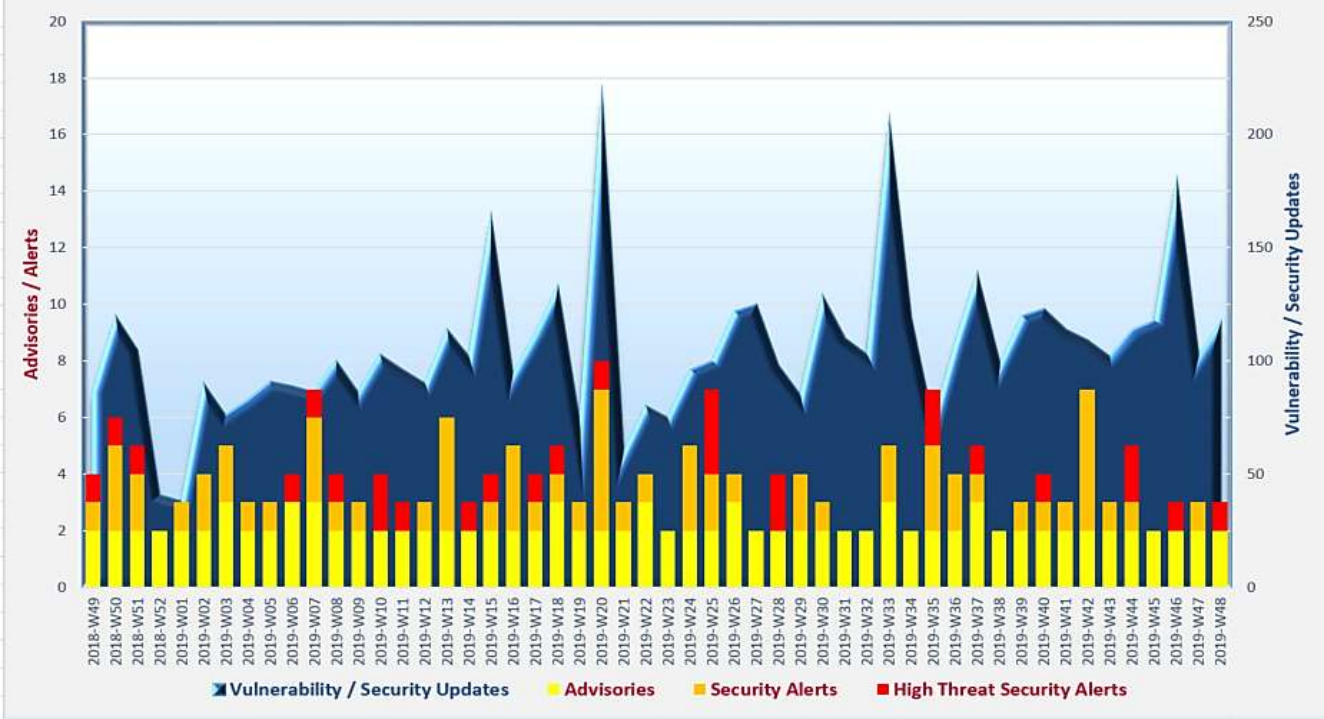
Cyber Security Threat Trends 2019-M11

November 2019

Last Revised: 2020.01.15

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:

- ✧ **Phishing emails, malware attacks and human errors** are the three major causes of security breaches. Organisations should arrange cyber security training, deploy advanced anti-malware solutions, and conduct regular security checks to prevent the breaches.
- ✧ **Artificial intelligence (AI) and machine learning (ML)** make coming malware more destructive and evasive. Organisations should review their cyber security measures and catch up with the latest security solutions to leverage AI and ML instead of being victimised by the technologies.
- ✧ **Security misconfiguration on cloud-based systems** is a prevailing issue leading to security incidents. System administrators should adopt the principle of least privileges in configuring their systems and third-party assessments should be carried out to assure secure settings.

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

CERT Advisories

Countdown to End-of-Support for Windows 7 and Windows Server 2008

GovCERT.HK[2], HKCERT[3], Australian Cyber Security Centre (ACSC)[4,5] and US-CERT[6], issued advisory/alert on the ceasing of support for Windows 7, Windows Server 2008 and Windows Server 2008 R2 operating systems after 13 January 2020 by Microsoft. According to the latest StatCounter figures[7], with only less than two months till the end of support, Windows 7 still accounted for 28% of desktop Windows market share in Hong Kong. System administrators should upgrade any Windows 7, Windows Server 2008 and Windows Server 2008 R2 to supported Windows operating systems before January 2020. Failing to upgrade in time, system administrators could acquire the Extended Security Update (ESU) program for continual security updates up to a maximum of three years[8].

Implement cyber supply chain risk management if using third-parties' product or service

ACSC[9] issued guidelines on how to implement cyber supply chain risk management for securing the supply of products and services for systems throughout their lifetime. These included identifying the cyber supply chain, understanding cyber supply chain risk, setting cyber security expectations with suppliers, auditing suppliers for compliance, and continual monitoring and improvement of cyber supply chain security practices.

Follow the vendor-recommended configurations for all deployed hardware and software

The Cybersecurity and Infrastructure Security Agency (CISA)[10] in the United States issued a reminder on protecting against the malware which exploited improper configurations. CISA also issued the Cyber Essentials guide for small businesses and government agencies to enhance their security posture.

[2] https://www.govcert.gov.hk/pdfjs-flipbook/web/viewer.html?file=../../weekly_report/2019w48.pdf
[3] https://www.hkcert.org/my_url/en/blog/19112201
[4] https://www.cyber.gov.au/publications/end-of-support-for-microsoft-windows-7
[5] https://www.cyber.gov.au/publications/end-of-support-for-microsoft-windows-server-2008-and-windows-server-2008-r2
[6] https://www.us-cert.gov/ncas/alerts/aa19-290a
[7] https://gs.statcounter.com/windows-version-market-share/desktop/hong-kong
[8] https://support.microsoft.com/en-hk/help/4487594/prepare-now-for-end-of-support-in-2019-and-2020
[9] https://www.cyber.gov.au/publications/cyber-supply-chain-risk-management
[10] https://www.us-cert.gov/ncas/current-activity/2019/11/15/reminder-malware-can-exploit-improper-configurations

Industry Insight on Cyber Security Threat Trends

Machine learning and automation technologies showed the offensive face

Sophos published its "Sophos 2020 Threat Report"[11] which revealed the new attack methods used by malware, the changes in the threat landscape over the past 12 months, and uncovered trends likely to impact cybersecurity in 2020. The key observations were:

- **Smart automation technologies evolved into new key threats.** The legitimate automated tools and other "living off the land" utilities ranging from the nmap network scanner to PowerShell, were leveraged for moving laterally in the victims' network to target assets, escalating the privileges, stealing data and evasion. Automated scans and probes posed threats to devices exposing specific ports online**.**
- **Ransomware attacks continued to evolve to increase damage and evade security controls.** Attackers tried to disable or destroy backups so as to incur maximum damage. They also attempted to stop the security controls of the infected machines or restricting the malware to be run on specific time period only to evade detection.
- **Deepfakes would boost more automated social engineering attacks.** Deepfakes relied on generative artificial intelligence (AI) to generate realistic human artefacts like pictures, voices, and text. With the advancement on technology, more automated fraud scams, phishing, vhishing, and deepfake-enabled video attacks were expected.
- **Potentially unwanted applications (PUAs) were not malware, but could be misused by attackers to conduct malicious operations.** For example, browser plug-ins could be turned into brokers for delivering and executing malware and fileless attacks.
- **Misconfiguration could lead the data and system on cloud vulnerable to malicious activities.** Many data breaches involving large quantity of data were caused by misconfiguration of cloud storage. Misconfiguration of cloud computing instances could also lead to malicious code modification such as Magecart.
- **Mobile attacks on smartphone were found to be diversified and primarily for Android operating system**. Attackers resorted to means from SIMjacking to adware and 'fleecing' apps that charge users with exorbitant amounts.
- Organisations were recommended to implement cyber hygiene practices thoroughly including software patching, strict access policies, proper system and network monitoring, and user education.

Source: Sophos

[11] https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf

Industry Insight on Cyber Security Threat Trends

Advanced Persistent Threats tended to be more targeted, sophisticated and diversified with the advanced development of machine learning and artificial intelligence

Kaspersky uncovered the vision on Advanced Persistent Threats (APTs) in 2020 and specified the changes of targeted threats landscape in its "Advanced threat predictions for 2020"[12] report. The following were the highlights from the report:

- **Artificial intelligence (AI) could facilitate the abuse of personal information from deepfakes to DNA leaks.** Video and audio deepfakes, together with AI's automated and profiling support, allowed attackers to launch social engineering and other malicious schemes for enticing the victims of personal data abuse. Besides personal information, biometric data could be the new target for more sensitive data breaches.

- **Attack tactics would be more sophisticated with new data exfiltration ways (e.g. signaling data, Wi-Fi/4G) and interception capabilities (e.g. Quantum insert).** DNS over HTTPS (DoH) could keep the malicious activities out of sight. Supply chain attacks would continue to be the security concern through manipulating the software containers including packages and libraries.

- **New attack vectors could be arisen from accessing banks' data and infrastructure due to the introduction of European Union's Payments Services Directive (PSD2).** Adversaries could attempt to exploit new services and channels for new fraudulent schemes.

- **Attacks against infrastructure and non-PC targets would increase as more attack toolsets extended their coverage beyond Windows to networking hardware.** VPNFilter and Slingshot could be performed as a massive botnet-style or selected targets compromise. A growth in targeted attacks against critical infrastructure facilities would be expected.

- **Mobile APTs would grow at a fast pace due to higher penetration rate of mobile devices and increasing amount of valuable information stored in the mobile devices.** The report forecast that more mobile APTs would be uncovered as well as their advanced tactics.

- **False flag attacks evolved from hiding the trait to divert the suspected authorship.** Commodity malware, scripts, publicly available security tools and administrator software would be used with false flags to distract the investigation.

Source: Kaspersky

[12] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/11/20151759/KSB2019_APT-predictions-2020_web.pdf

Industry Insight on Cyber Security Threat Trends

Good cybersecurity regulatory framework improves organisation cybersecurity

ESET surveyed 1,835 managers and chief level executives in Asia Pacific (APAC) region, including India, China, Hong Kong, Taiwan, Japan, Thailand and Indonesia. By analysing and correlating the survey responses and the data from the vendor's own products and services, the research result was published in the "ESET Enterprise Survey 2019 report"[13]. Findings of the report included:

- **63% of respondents deemed a strong cybersecurity regulatory framework was the foremost for protecting the data against potential breaches**. More than 70% of the respondents from Indonesia, India and China supported this view. However, only 41% and 48% respondents of Japan and Hong Kong agreed this view. 71% of Hong Kong respondents supported the review of Hong Kong's Personal Data (Privacy) Ordinance to enhance cybersecurity and better compliance.

- **In the past 24 months, more than six data breaches were encountered by nearly one in five organisations because of phishing emails, malware, and human error**. These security breaches cost more than HKD 0.78 million per organisation in average. 17% of Hong Kong respondents suffered a data breach incident. Organisations were recommended to adopt up to date cybersecurity solutions to keep up with the evolving cybersecurity landscape.

- **Regular security checks, use of good cybersecurity solutions, cybersecurity training and adoption of stronger encryption were the top cybersecurity measures against data breaches opined by the respondents.** Furthermore, better control on data and services, higher service reliability and minimising disruption to business were the top three benefits of using additional cybersecurity solutions perceived by the respondents.

- **92% of the respondents from Hong Kong considered their encryption solution covered all endpoints, followed by China and India with 91% and 90% respectively.** For data encryption, 91% of respondents planned to encrypt partial or all of their data files whereas 93% of respondents from Hong Kong had such planning.

- **91% of respondents had a cybersecurity awareness programme,** whereas 84% of respondents from Hong Kong claimed that they had such awareness programme. Organisations should understand that lack of proper cybersecurity knowledge and delay in adopting cybersecurity solutions could hinder the improvement of their business infrastructure to meet the requirements of new regulations.

Source: ESET

[13] https://www.eset.com/sg/business/apac-enterprise-survey-2019/

Industry Insight on Cyber Security Threat Trends

Phishing becomes more target-oriented and sophisticated

Akamai solicited telemetry data from their products and analysed more than 2 billion phishing domains, and prepared the "2019 State of the Internet Security: Phishing - Baiting the Hook"[14] report. The observations of the report included:

- **Less than 40% of the phishing kits monitored were active for more than 20 days. The mean lifespan of most phishing URLs was shorter than 2 days.** Cybercriminals used the phishing kits to offer phishing as a service (PaaS) for making the phishing more organised, business-liked and sophisticated. Phishing kits typically targeted the consumer products, banking or finance, and gaming sectors.

- **Social media and mobile devices became the common vectors other than email for phishing.** Cybercriminals leveraged the continuous growth on usage of social media and mobile devices as a means of rapid propagation to reach more victims in shorter timeframe.

- **Users of well-known brands such as Microsoft, PayPal, DHL and Dropbox, were common phishing targets.** After analysing the phishing domains detected, 3,897 domains were found targeted Microsoft users, followed by PayPal and DHL with 1,669 and 1,565 domains respectively. Dropbox users were also targeted by 461 domains. More than 60 global brands were targeted during the monitoring period.

- **High technology, finance, e-commerce and media were the four most targeted commercial sectors.** Almost 120 phishing kit variants and 6,035 phishing domains were identified targeting the high technology sector. The financial services sector was targeted by 83 phishing kit variants and 3,658 domains. 19 phishing kit variants were found for e-commerce and media sectors, which were targeted by 1,979 and 650 domains respectively. Organisations should consider to adopt the multi-layered defense solutions and comprehensive endpoint protection to defend against phishing.

- Phishing threat has always proved an effective way to steal personally identifiable information (PII) which is the valuable product in identity theft scams. Phishing attacks are getting more sophisticated. High user awareness and well-trained responses should become more essential than ever. Phishing simulations could help organisations to improve employee's awareness on potential phishing attacks.

Source: Akamai

[14] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-phishing-baiting-the-hook-report-2019.pdf

Summary of Microsoft November 2019 Security Updates

12 Product Families with Patches

7 Critical

5 Important or below

Product Family	Impact[15]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4523205, KB4524570, KB4525232, KB4525236, KB4525237, KB4525241
Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1903)	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4525236 Windows Server 2019: KB4523205 Windows Server v1803: KB4525237 Windows Server v1903: KB4524570
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4525233, KB4525234, KB4525235, KB4525239, KB4525243, KB4525246, KB4525250, KB4525253
Microsoft Edge (EdgeHTML-based)	Remote Code Execution	Critical ★★★★	KB4523205, KB4524570, KB4525232, KB4525236, KB4525237, KB4525241
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4525106, KB4525234 IE 10: KB4525106, KB4525246 IE 11: KB4523205, KB4524570, KB4525106, KB4525232, KB4525235, KB4525236, KB4525237, KB4525241, KB4525243
Microsoft Exchange Server	Remote Code Execution	Critical ★★★★	Microsoft Exchange Server 2013, 2016 & 2019: KB4523171
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore: Security Update
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010 SP2: KB4484127, KB4484160

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

Product Family	Impact[15]	Severity	Associated KB and / or Support Webpages
			Microsoft Office 2013 and 2013 RT: KB4484119, KB4484152 Microsoft Office 2016: KB4484113, KB4484148 Microsoft Office 2019 Security Update: Click to Run Microsoft Excel 2016, Office 2016 & 2019 for Mac Security Update: Release Notes Microsoft Office 365 ProPlus Security Update: Click to Run Office Online Server: KB4484141 Microsoft Excel 2010: KB4484164 Microsoft Excel 2013 SP1 & 2013 RT SP1: KB4484158 Microsoft Excel 2016: KB4484144 Excel Services: KB4484159
Microsoft SharePoint-related software	Information Disclosure	Important ★★★	Microsoft SharePoint Foundation 2010 SP2: KB4484165 Microsoft SharePoint Foundation 2013 SP1: KB4484157 Microsoft SharePoint Enterprise Server 2013: KB4484151 Microsoft SharePoint Enterprise Server 2016: KB4484143 Microsoft SharePoint Server 2019: KB4484142, KB4484149
Azure Stack	Spoofing	Important ★★★	Azure Stack: Security Update Guide
Microsoft Visual Studio	Elevation of Privilege	Important ★★★	Visual Studio 2017 version 15.9: Download Visual Studio 2019 version 16.0 & 16.3: Download Visual Studio Code: Download
Open Enclave SDK	Information Disclosure	Important ★★★	Open Enclave SDK: Security Update

Learn more:

High Threat Security Alert (A19-11-02): Multiple Vulnerabilities in Microsoft Products (November 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=434)

Sources:

- Microsoft November 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2019-Nov)

Revision History	
17 December 2019	First release
15 January 2020	Additional information provided on P.2 (Paragraph 1) Textual amendment on P.5 (Paragraph 1 & 5)