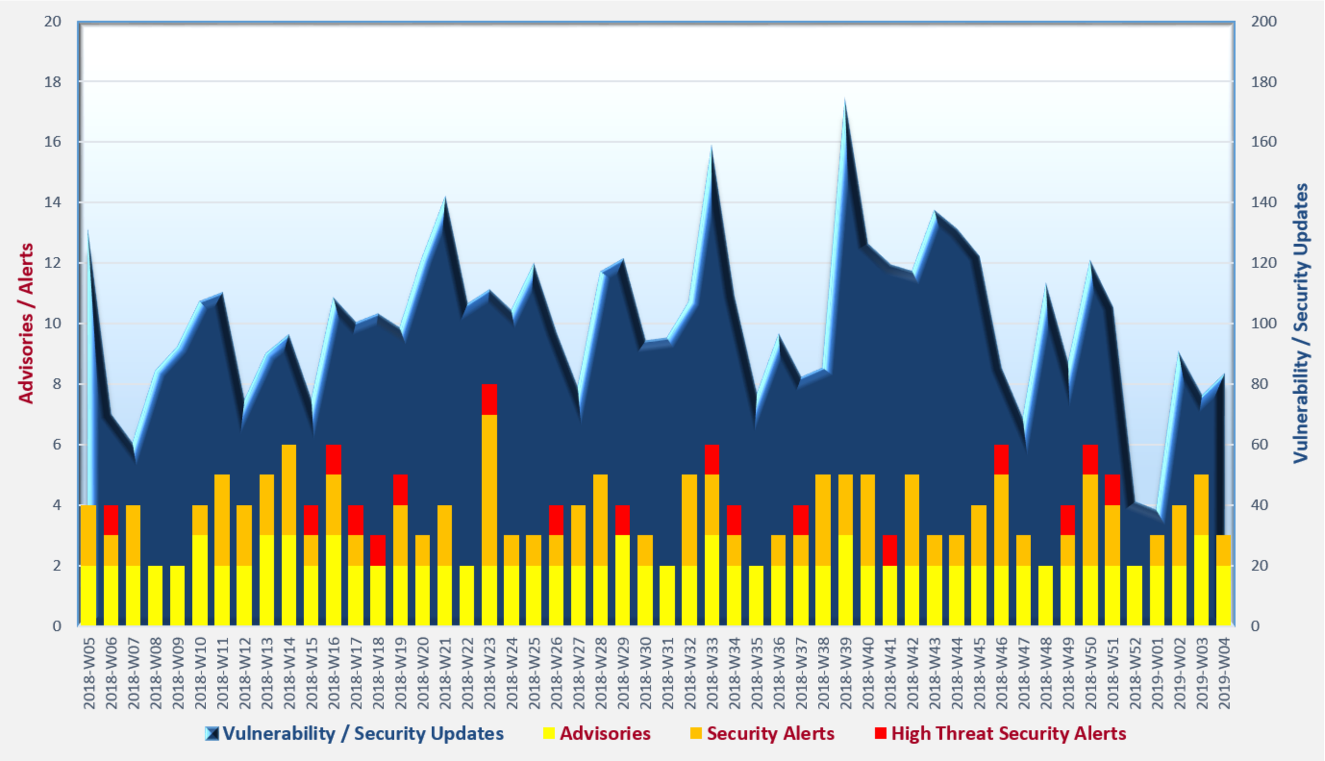
Cyber Security Threat Trends 2019-M01

January 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:

- **Cryptographic ransomware** continually disrupts operations by forcing its ways with various attack channels including phishing emails, online ads, compromised websites and remote desktop accesses. Users should back up data regularly and offline to prevent data loss.
- **Password compromise** either through credential leakage or brute-force attack frequently leads to further system intrusions and information disclosure. Multi-factor authentication should be adopted for accounts to access sensitive information or personal data.
- **Evasion techniques** become common for malware to infect systems. Multi-layers of defense and detection mechanisms should be implemented to mitigate the risks.

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

CERT Advisories

🗎 E-mail extortion scam could threaten victims to pay ransom

SingCERT[2] issued an advisory on e-mail extortion scam, in which the scammer deceived victims that their computing device or accounts were compromised, and asked for a ransom. Users were advised not to pay the ransom, and take necessary actions to protect their accounts such as changing passwords regularly, using strong passwords, using different password for different accounts, enabling two-factor authentication and so on. Besides, their computing device security should be kept up-to-date, equipped with updated anti-malware software and performed anti-malware scans.

🗎 Organisers could consider including processes and measures for cyber risk management in event planning

The UK National Cyber Security Centre (NCSC)[3] published the guidance on cyber security for major events, which set out how to manage the cyber risk in major events usually relied on digital systems and technology. The document included discovery phase, risk management, cyber incident management, and event preparation action list.

🗎 HKCERT[4] urged organisation to adopt the "security by design" approach in developing new services to prevent data breaches and cyber attacks

The threat trends observed by HKCERT in 2018 were also reported. There were a total of 10,081 security incident reports, an increase of 55% when compared with 2017.

🗎 Securing the account of online services should always be in high priority

HKCERT[5] recommended protection measures in its security advisory “Online Account Security”. Users have been advised that the email accounts, financial services and social network should be secured by strong password with periodical change. Password manager service/software might be used to better manage passwords. Users should be aware of any phishing websites and emails which asking for login credentials.

[2] https://www.csa.gov.sg/singcert/news/advisories-alerts/advisory-on-e-mail-extortion-scam
[3] https://www.ncsc.gov.uk/guidance/cyber-security-major-events
[4] https://www.hkcert.org/my_url/en/articles/19012201
[5] https://www.hkcert.org/my_url/en/blog/19011801

CERT Advisories

Emerging campaign on Domain Name System (DNS) hijacking attacks were noticed recently

Some government and business organisations in areas such as Middle East, Europe and the United States have been targeted. Attackers used compromised credentials to modify the records of DNS of victim organisations, with a view to redirect their Internet traffic. Attackers could also use the credentials to obtain valid encryption certificates for the domain names, so as to launch man-in-the-middle attacks. Organisations should examine their DNS records to ensure the correctness, and use strong password as well as multi-factor authentication for DNS accounts. HKCERT[6], US-CERT[7], SingCERT[8], Australian Cyber Security Centre (ACSC)[9] and the UK National Cyber Security Centre (NCSC)[10] have issued alerts on this matter.

[6] https://www.hkcert.org/my_url/en/blog/19012502

[7] https://www.us-cert.gov/ncas/alerts/AA19-024A

[8] https://www.csa.gov.sg/singcert/news/advisories-alerts/advisory-on-mitigating-dns-records-tampering

[9] https://cyber.gov.au/business/news/combat-dns-hijacking/

[10] https://www.ncsc.gov.uk/alerts/alert-dns-hijacking-activity

Industry Insight on Cyber Security Threat Trends

Cybercriminals change approaches on their ways of attack

Cybercriminals kept improving their tactics and techniques on attack and evade detection. DataVisor studied more than 42 billion attack events during July to September 2018, and observed that attackers made use of a great variety of finesse, altered their attack approaches skillfully, and employed flexible and specialised proxy services. Reactive security solutions which based on previous labels or rules would be insufficient for fraud detection and protection. Security solutions with proactive capability in detecting unknown fraud would be needed. The study results were published in their "DataVisor Fraud Index Report: Q3 2018"[11]. More details of the report were listed below:

- **Low sophistication fraud attacks were generally short-term but with sharp increase in attack volume.** Fraudsters normally adopted a one-off disposable approach in these attacks. 80% of these attacks were performed within one day after creation of the fraudulent accounts. The attackers might be less concern about being detected. During the attack, they created an observable amount of malicious activities and used a number of different fraudulent accounts but with similar profile characteristics and behaviour. All these characteristics made such attacks had higher chance of being discovered and blocked. Around 60% of fraud attacks on social platforms were this kind of attacks.

- **High sophistication attacks were usually more stealthy and difficult to be detected.** Fraudsters tried to hide the fraudulent accounts among those normal accounts. The attack durations were longer, and could potentially cause more damage. Around 56% of fraud attacks on financial platforms were this kind of attacks.

- **Fraudulent accounts using diverse IP subnets (71%) and diverse user-agents strings (29%) were the two most common means of attack evasion.** By using specialised proxy services, fraudulent accounts could use residential or educational networks that sounded more trustful to avoid detectors. Moreover, by using different cloud services and anonymous proxies, attacker could assign different IP address for the fraudulent accounts, making them appeared to be more "different" and thus more difficult to be detected.

- **Multi-stage attacks were adopted.** In some attacks, the attack was conducted in different phases, from different geolocations, using different devices and by different means such as automated tools, manually launched or through other fraud services providers to avoid detection. For instance, the major attack might be executed after a prolonged period (from days, weeks, or even months) of trials and camouflaging the fraudulent accounts. This multi-stage approach were more commonly adopted in high sophistication attacks. 20% of them launched their peak attack after more than a month since last attack.

Source: Datavisor

[11] https://www.datavisor.com/resources/special-reports/Fraud-Index-Report-Q3-2018

Industry Insight on Cyber Security Threat Trends

“Growth in botnet”, “Upsurge in coinming”, and “Rise of Maldoc” are 3 threat trends

Boost in botnet activities, an upsurge in coinmining, and the growing popularity of Malicious Document (Maldoc) downloader propagation were the three major threat trends in 2018 identified by eSentire, which published the “2018 Annual Threat Report”[12]. The details were:

- **The use of botnet increased by 5 times in 2018, with intrusion attempts by botnet increased by 2.5 times in the period.** The wide deployment of Internet of Things (IoT) devices provided potential building blocks for large scale botnet when such IoT devices were compromised by attackers. Among the threats given rise by botnet, Mirai was the most identified threat. There were notable growth in CoinMiners (15 times), DNSChangers (5 times) and Emotet (3 times).

- **During 2018, coinmining by malware on the infected victims, and in-browser mining which persisted in browsing session, were the most notable.** Cyber criminals preferred coinmining as the return on investment of coinmining was faster than ransomware or banking Trojans. Once the malware was deployed, the attackers could start consuming the victims’ processing power for mining. Compared with other methods such as ransomware, which required the victims to carry out some tasks (e.g., paying a ransom) before the attackers could achieve financial gains.

- **Several Maldocs downloaders were observed to be prevailing in 2018, including Marap, Ursnif and Emotet.** These malware were embedded in Office and PDF files and distributed by email. To deal with Maldocs, organisations could consider applying measures such as preventing macro execution, restricting usage of PowerShell, and so on.

- **DocuSign, Office365 and OneDrive were the top 3 observed enticements for phishing.** Such enticements usually pretended to be common office application (such as Adobe, DocuSign and Office 365), social network (such as Facebook), on-line storage (such as Dropbox, OneDrive and Google), and shipping companies (such as FedEx). “Invoice” were observed to be the most successful enticement for phishing in 2018.

- **Attacks targeting IoT devices and home routers were increasing.** There were a number of these devices found to be using default credentials. Cameras, door controllers, surveillance equipment, media devices, home routers were all targeted.

Source: eSentire

[12] https://www.esentire.com/resources/knowledge/2018-annual-threat-report/

Industry Insight on Cyber Security Threat Trends

"Cryptomining", "Machine Learning", "EU GDPR", and "Home Assistant Devices" are 4 cybersecurity trends in 2019

ESET reviewed the trends in 2018 and made predictions for 2019 on the areas of cryptomining, machine learning, European Union (EU) General Data Protection Regulation (GDPR) and data security, and home assistants devices in the report "Cybersecurity Trends 2019: Privacy and Intrusion in the Global Village"[13]. The key findings were:

- **The cases of cryptomining increased significantly in 2018 and expected to continue to grow in 2019.** As more smart devices connected to the Internet, they would become targeted by attackers to misuse for cryptomining. Organisation were recommended to deploy security solution that could detect and block coin-mining executable files and coin-mining web browser scripts, and could detect suspicious system processes. Also, they should not neglect those malware identified as "Possibly unwanted" or "Possibly unsafe", which in fact could be coin-mining malware. Organisation were also reminded to safe-keep the backups.

- **Machine learning has been a double edged sword.** Machine learning could be used to train security solutions to learn to identify malicious files and behaviours, by making use of a large amount of threat related data collected by the anti-malware industry. On the attacking sides, cyber-criminals could use machine learning to acquire target, exploit victims, evade detection, evolve new malware variants, and so on.

- **Organisations should review their data strategies to comply with GDPR.** It was predicted that "GDPR-style" legislation would likely to be enacted in different countries, as there were growing global concerns on data privacy and data protection on sensitive information. In fact, number of records breached in 2016 and 2017 reached 6.3 and 7.8 billion respectively. 1.8 billion records were exposed in the first half of 2018 by just 5 organisations only.

- **Attacks on home assistants devices would grow, both in terms of numbers and variety of attacks.** Home assistants devices, similar to routers, were main targets for the attackers, as they were most likely interacted with other smart devices and the Internet. In addition, attackers were particularly interested in the sensitive data exchanged and collected by these devices. Users should not only consider the features of these devices but also their security implementations.

Source: ESET

[13] https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET_Trends_Report_2019.pdf

Industry Insight on Cyber Security Threat Trends

Cybercriminals got cleverer, using different methods to infiltrate targets faster

Cybercriminals became smarter, more creative, coordinated and effective. They were no longer bounded geographically. "Cybersecurity can no longer be considered as IT problem. It is a business problem.", as quoted from the "Cyber Intrusion Casebook 2018"[14] published by CrowdStrike Services. The report outlined trends on cyber intrusion: attackers used more innovative techniques, infiltrated the targets faster and more immersed, used commodity malware as forerunner during the course of an attack, and shammed as genuine users to hide their identities.

- **Attackers used more innovative techniques, with a changing ecosystem.** They used remote access tools to real time monitor their victims to acquire more information. Besides, different attackers or malware that used to work independently became working in cooperative manners, such as sharing the use of dedicated malware or droppers, for launching attacks.

- **Attackers infiltrated the targets faster and more immersed, and were more persistent, especially for those nation-state attackers.** This led to the incident response consideration. Organisations were reminded that incident response should adopt a holistic approach. Just focus on a single system in incident response might not be able to solve the problem completely, as the attacker might still persist and re-infect the system instantly right after the incidents were seemed to be settled.

- **Commodity malware was used as forerunner to test the defence capability of an organisation.** Threat actors used these commodity malware as stepping stones to perform further attacks. TrickBot was one of the example of this kind of attack. In 2018, it was also observed that bot networks were used for the delivery and spreading of infections.

- **The tactic for an attacker to sham as genuine users was considered to be the most effective.** Attacker made use of uncontrolled, misconfigured or compromised user credential to pretend as a genuine user to compromise the target system. Single sign-on (SSO) and multi-factor authentication (MFA) were practical measures to protect user credentials. However, improper configuration on these measures could lead to a false expectation on the security protection of an organisation.

- The report suggested some best practices including proper implementation of multi-factor authentication, application-level log monitoring, effective and timely patch management and security control of cloud applications for organisations' consideration.

Source: CrowdStrike

[14] https://crowdstrike.lookbookhq.com/casebook-web-download/cs-services-casebook-2018

Summary of Microsoft January 2019 Security Updates

13 Product Families with Patches

5 Critical

8 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 ★★★★	KB4480116, KB4480961, KB4480962, KB4480966, KB4480973 and KB4480978.
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4480116, KB4480961, KB4480962, KB4480966, KB4480973 and KB4480978.
Windows Server 2016, 2019 and Server Core installations 2016, 2019, v1803, v1709	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4480961; Windows Server 2019: KB4480116.
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4480965, KB4480968, KB4483187, IE 10: KB4480965, KB4480975, KB4483187 IE 11: KB4480116, KB4480961, KB4480962, KB4480963, KB4480965, KB4480966, KB4480970, KB4480973, KB4480978, KB4483187, KB4483228, KB4483229, KB4483230, KB4483232, KB4483234 and KB4483235.
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Important ★★★	KB4480960, KB4480963, KB4480964, KB4480968, KB4480970, KB4480972, KB4480957 and KB4480975.
Microsoft .NET Framework	Information Disclosure	Important ★★★	.NET Framework security update release
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	KB4461589, KB4461591, KB4461596, KB4461598 and KB4461634.

[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 Exchange Server	Information Disclosure	Important ★★★	KB4468742 and KB4471389

Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010, 2013, 2016, 2016 for Mac, 2019, 2019 for Mac: KB2553332, KB3172522, KB4022162, KB4461535, KB4461537, KB4461614, KB4461617, Click to Run, Office for Mac;
			Office 365 ProPlus: Click to Run;
			Mirosooft Office Online Server: KB4461633;
			Microsoft Word 2010, 2013, 2013 RT, 2016, Viewer: KB4461543, KB4461594, KB4461625, KB4461635 and KB4462112;
			Word Automation Services: KB4461612;
			Microsoft Excel Viewer 2007: KB2596760;
			Microsoft Outlook 2010, 2013, 2013 RT, 2016: KB4461595, KB4461601 and KB4461623;
			Microsoft Business Productivity Server: KB4461624;
			Microsoft Web Apps Server 2010: KB4461620.

Microsoft Visual Studio	Information Disclosure	Important ★★★	KB4476698 and KB4476755.
.NET Core	Information Disclosure	Important ★★★	GitHub.
ASP.NET Core	Denial of Service	Important ★★★	GitHub.

Learn more:
High Threat Security Alert (A19-01-02): Multiple Vulnerabilities in Microsoft Products (January 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=355)

Sources:

🗎 Microsoft January 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/b4384b95-e6d2-e811-a983-000d3a33c573)

Data analytics powered by CRisP in collaboration with GovCERT.HK