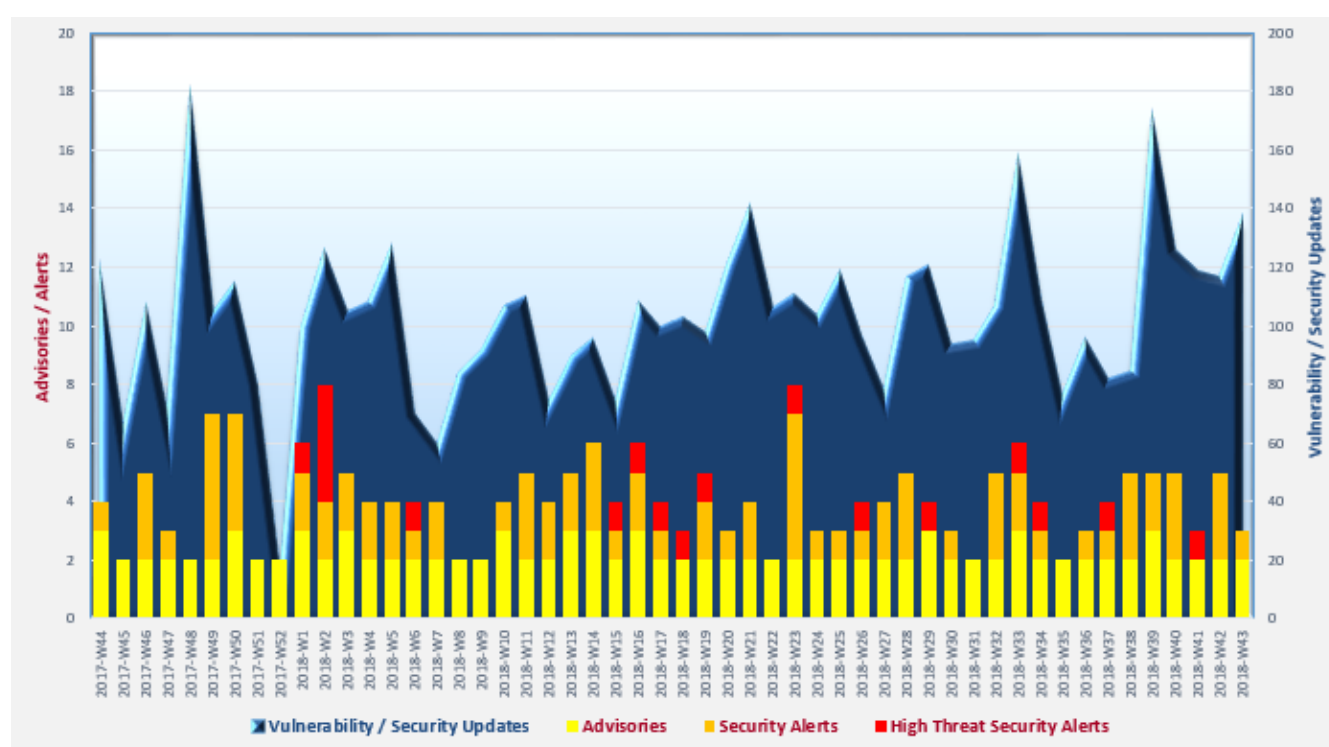


Cyber Security Threat Trends 2018-M10

October 2018

With reference to the FIRST Traffic Light Protocol (TLP) standard¹, 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:


- ✧ **Compromised systems** causing bulk volume of personal data stolen hit the headlines. Enterprises should be well prepared for that hackers are always following their customers' data.
- ✧ **Ransomware and cryptomining malware** are ongoing threats to businesses. System protection and user awareness are both key to the defence.
- ✧ **Phishing** keeps being a major initial attack vector. Employees should be trained to counter the phishing attack and regular phishing drills should be arranged to strengthen their defence capabilities.


¹ <https://www.first.org/tlp/>


CERT Advisories


-  **HKCERT²** issued an advisory on the passenger data breach of Cathay Pacific and Cathay Dragon, where unauthorised access to the airlines' 9.4 million passenger data was discovered in early March 2018. Organisations were urged to improve and enhance their data protection and security, so as to prevent and detect any unauthorised access and data breach. End users were reminded to stay vigilant of scam and phishing messages taking advantage of this event.

-  **HKCERT³** issued an advisory on the webapp programming vulnerability related to the website of Hong Kong Airline that led to personal information leakage. Webmasters and web application developers were advised to ensure security measures were in place, including strong authentication, security and privacy by design, static code scanning, penetration testing and vulnerability scanning, application log monitoring, etc.

-  **HKCERT⁴** issued an advisory on the reported unauthorised money transfer between bank accounts and stored value facilities (SVF). Users of such payment facilities were advised not to disclose personal information, and to secure their online banking login accounts and email accounts with strong passwords and multi-factor authentication.

-  **The UK National Cyber Security Centre (NCSC)⁵** published a guidance on the secure configuration for the 1803 "April 2018 Update" of Windows 10 Enterprise. The areas covered included administrators' deployment guide, recommended network architecture, user account hardening, system hardening, device firmware management, etc.

-  **The NCSC⁶** published an updated guidance on email security and anti-spoofing for IT managers and systems administrators to secure their organisations' email by using Transport Layer Security (TLS), Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF) and Domain-Keys Identified Mail (DKIM).

-  **US-CERT⁷** published on its website a security tip on the proper disposal of electronic devices, including computers, smartphones, tablets, digital media, external hardware and peripheral devices, as well as gaming consoles. Some methods for sanitization were introduced in the tip.

² https://www.hkcert.org/my_url/en/blog/18102501

³ https://www.hkcert.org/my_url/en/blog/18103001

⁴ https://www.hkcert.org/my_url/en/blog/18102502

⁵ <https://www.ncsc.gov.uk/guidance/eud-security-guidance-windows-10-1803>

⁶ <https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing>

⁷ <https://www.us-cert.gov/ncas/tips/ST18-005>

CERT Advisories



US-CERT⁸ published a research report on the following five publicly available tools which have been used in worldwide cyber security incidents recently:

1. Remote Access Trojan: JBiFrost
2. Webshell: China Chopper
3. Credential Stealer: Mimikatz
4. Lateral Movement Framework: PowerShell Empire
5. C2 Obfuscation and Exfiltration: HUC Packet Transmitter

The research was performed by cyber security authorities of Australia, Canada, New Zealand, the United Kingdom and the United States. The report revealed the associated threats, capabilities, related incidents, detection and counter-measures of each tool.

⁸ <https://www.us-cert.gov/ncas/alerts/AA18-284A>

Industry Insight on Cyber Security Threat Trends

SiteLock:

SiteLock published its “**SiteLock Website Security Insider Q2 2018**”⁹ highlighted their analysis results based on the data collected from 10 million protected websites of different company sizes:

- **Cybercriminals became stealthier on website attack.** Attackers used smaller, less noisy, and more profitable attacks such as deploying JavaScript for cryptojacking. From Q1 to Q2 2018, there was a 16% increase in deploying malicious JavaScript to websites. Website owners should scan and review the website directories and files for malicious and suspiciously changed content.
- **60% of visits to websites were from bots.** Some were search engine crawlers for indexing but far more were for malicious activities including exploiting common vulnerabilities such as cross-site scripting or deploying backdoor for future attack. Implementing web application firewall, which allows blacklisting malicious and suspicious bots, could be one of the measures to protect websites.
- **9% of the 6 million sampled websites had vulnerability found.** Cross-site scripting, SQL injection and cross-site request forgery vulnerabilities were found in 2%, 7% and 0.2% of the sampled websites respectively. Websites with these vulnerability would have higher chance of malware infection. Website owners were recommended to use code analysis and vulnerability scanners to check their websites for vulnerabilities periodically and upon website update. Patches should be applied accordingly.
- **In Q2 2018, 61 vulnerabilities were found in three common website Content Management Systems (CMS): WordPress, Joomla! and Drupal.** 1,099 patches were required to address these vulnerabilities, a 48% increase compared to Q1 2018. Website owners should apply the latest patches to the CMS to address the vulnerabilities and update the themes, add-ons and plugins used in their websites timely. Configuration files should be well protected and reviewed regularly. Strong password should be used and sent over secured networks.
- **Website owners should note that website connecting to one social media platform doubled its chance to be infected with malware,** as the social media platform could be an additional attack surface available to cybercriminals. The chance would be tripled if connecting to three or more social media platforms.

⁹ <https://www.sitelock.com/website-security-report-2018q2>

Industry Insight on Cyber Security Threat Trends

eSentire:

The eSentire Threat Intelligence team published its "**Quarterly Threat report Q2 2018**"¹⁰ revealed the analysis results based on data collected from more than 2,000 worldwide distributed network and host based sensors. The key observations were:

- **Phishing continued as a popular attack vector. An increase in imitating shipping and eFax was observed in Q2 2018.** DocuSign was the most common lure in phishing attacks, although there was a 70% decrease already. Decrease in other Internet services (e.g. Google, Dropbox, etc.) phishing attacks were also observed. However, there was an increase in phishing attack using "invoice" as bait.
- **Major exploit campaign aiming IIS, Drupal, WebLogic web technologies and GPON home routers were observed in Q2 2018.** The number of IIS attacks increased from around two thousand to 1.7 million, a 782 times increase from Q1 to Q2 2018. The researchers studied the attack sources observed in the IIS and WebLogic attacks and found that the attacks were mainly from compromised Apache servers and other servers running RDP, SQL, IIS and HTTP API services. On the other hand, attacks to exploit Drupalgeddon and GPON were found to be high volume of attacks originated from a relatively small number of IP addresses.
- **Endpoint solutions detected the use of PowerShell-based attacks increased by 50% when compared to Q1 2018.** 32% of detected attacks on endpoints were by PowerShell, 21% were by VBA Scripting and around 16% were by abusing the regsvr32 system process. Most attacks using PowerShell adopted the usage of obfuscated command lines to evade detection.
- **Emotet was a self-propagating banking Trojan, which also had malware downloading capability.** It became a dangerous threat to organisations. To defend Emotet, SMB connections should be restricted. Organisations could consider blocking spam email from known malicious domains and IP addresses. They should also follow the least privilege principle in assigning user access rights. Administrative rights should be restricted to designated system administrators only.

¹⁰ <https://www.esentire.com/resources/knowledge/q2-2018-quarterly-threat-report/>

Industry Insight on Cyber Security Threat Trends

Malwarebytes Labs:

Malwarebytes Labs published its “**Cybercrime tactics and techniques Q3 2018**”¹¹, which outlined the key developments in cybercrime in the quarter. The key observations were:

- **There was a greater percentage increase in malware targeted business sector.** In terms of total detection count, there was an increase of 1.7 million, 55% more detections in Q3 when compared with the previous quarter. The percentage increase in malware detection in consumer sector was 4%.
- **Trojan was the top detected malware for both the business and consumer sectors.** The increase in number of detection of Trojan for business sector and consumer sector over the last quarter was 84% and 27% respectively. The increase was mainly due to the outburst of Emotet, a self-propagating information stealer, in August 2018. Spam email with malicious attachments were the main infection source of Emotet.
- **Cryptomining malware decreased 26% for business sector and 32% for consumer sector.** Despite of the decrease in cryptomining activities, cybercriminals switched their ways of attack by targeting popular websites or Internet of Things (IoT) and server vulnerabilities.
- **Ransomware increased 88% for business sector but decreased 24% for consumer sector.** Majority of ransomware infection in business sector was by GandCrab, which could encrypt files without communicating to command and control server. It was also noted that around 40 new ransomware families were discovered, and some families have undergone vigorous updates which could lead to more dangerous and powerful variants.
- **Activity of multi-purpose Remote Access Trojans (RATs) slightly increased in Q3 2018.** These RATs, including Gh0st RAT, njRat, FlawedAmmyy RAT, etc., could perform different kinds of attacks such as information stealing, keystrokes and screen contents capturing, accessing connected webcam and microphones, and so on.
- **Sham ad-blocking browser extensions were found to be bots.** They captured victims’ browsing habits, sent to the command and control servers and received commands to perform malicious actions.
- **Exploit kits were found more infective in Asia Pacific region, in particular South Korea and Taiwan.** One reason was the higher usage rate of Internet Explorer in these regions than other regions of the world.

¹¹ <https://go.malwarebytes.com/CTNTQ3FY19.html>

Industry Insight on Cyber Security Threat Trends

Cofense:

Cofense published its “**The State of Phishing Defense 2018: Susceptibility, Resiliency, and Response to Phishing Attacks**”¹² which analysed user susceptibility, reporting behaviour, and resiliency to phishing attacks from 1,400 organisations in 50 countries and 23 major industries. Data referred were based on 48,000 real phishing campaigns, one-year of simulated data from July 2017 to June 2018 including 135 million simulated phishing email and 800,000 email reported to Cofense Phishing Data Centre from January 2018 to July 2018. The key observations were:

- **On average, 10% of reported email were malicious.** The malicious email could bypass email gateway and reached users’ inbox. 53% and 21% of reported malicious email were related to credential phishing and malicious attachment, respectively.
- **Phishing attackers liked to mimic Microsoft and popular authentication providers in credential phishing.** To harvest credentials, attackers created fake Microsoft login pages or phishing pages that allowed user to login with a credential such as Dropbox, Facebook, Gmail, Hotmail, LinkedIn, or Yahoo. A typical phishing email example was email that claimed the target’s account had abnormal activities and urged the target victim to click a link or button to verify the account. Another example was email asking the target victim to login a website to download a document.
- **Phishing attackers crafted PDFs, Microsoft Office documents, and even Microsoft Publisher files in phishing email.** In order to bypass URL scanning and email security measure, attackers often embedded malicious URLs inside PDF files. Malicious macros could be embedded in Microsoft Office documents and Microsoft Publisher file (.PUB extension) to perform harmful actions such as installing malware. Organisation could consider blocking or gray-listing email attachment from unknown or untrusted source and conducting continuous security awareness training for users.
- **The term "Invoice" was one of the top phishing subjects and appeared in six out of the ten most effective phishing campaigns in 2018.** Other common subjects used were “Payment Remittance”, “Statement”, etc. Researchers recommended organisations to train employees in finance and account department and anyone authorised to conduct financial transaction the proper handling for these phishing email and attachments repeatedly. Researchers also reminded employees to be more cautious on dates such as end of month, end of year since phishers could take chance to launch phishing attacks during these busy days.

¹² <https://cofense.com/state-of-phishing-defense-2018/>

Summary of Microsoft October 2018 Security Updates

14

Product Families
with Patches

10

Critical

4

Important or
below

Product Family	Impact ¹³	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4464330 , KB4462919 , KB4462918 , KB4462937 , KB4462917 and KB4462922 .
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4464330 , KB4462919 , KB4462918 , KB4462937 , KB4462917 and KB4462922 .
Windows Server 2016, 2019 and Server Core installations 2016, 2019, v1803, v1709	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4462917 ; Windows Server 2019: KB4464330 .
Windows 8.1 and Windows Server 2012 R2	Remote Code Execution	Critical ★★★★	KB4462926 and KB4462941 .
Windows Server 2012	Remote Code Execution	Critical ★★★★	KB4462929 and KB4462931 .
Windows RT 8.1	Remote Code Execution	Critical ★★★★	KB4462926 .
Windows 7 and Windows Server 2008 R2	Remote Code Execution	Critical ★★★★	KB4462923 and KB4462915 .
Windows Server 2008	Remote Code Execution	Critical ★★★★	KB4463097 and KB4463104 .
Internet Explorer	Remote Code Execution	Critical ★★★★	IE11: KB4462923 , KB4462926 , KB4462949 , KB4464330 , KB4462937 , KB4462922 , KB4462919 , KB4462918 , and KB4462917 .
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore .

¹³ The Impact and Severity are the maximum impact and severity assessment of the vulnerabilities in the associated knowledgebase (KB) by Microsoft.

Product Family	Impact ¹³	Severity	Associated KB and / or Support Webpages
Microsoft Office-related software	Remote Code Execution	Important ★ ★ ★	Microsoft Office 2010, 2013, 2016, 2019: KB4092437 , KB4092444 , KB4092483 , KB4461437 , KB4461445 , KB4461466 and Click to Run ; Office 365 ProPlus: Click to Run ; Microsoft Excel 2010, 2013, 2016, Viewer: KB4092444 , KB4461448 , KB4461460 and KB4461466 ; Microsoft Word 2010, 2013, 2016, Viewer KB4092439 , KB4092464 , KB4461449 and KB4461457 ; Microsoft PowerPoint 2010, 2013, 2016, Viewer 2007 and 2010: KB4022138 KB4092444 , KB4092453 , KB4092482 and KB4461434 ; Microsoft Outlook 2010, 2013, 2016: KB4092477 , KB4227170 and KB4461440 ; Microsoft Office Web Apps 2010: KB4227167 .
Microsoft SharePoint-related software	Elevation of Privilege	Important ★ ★ ★	KB4461450 , KB4461447 , and KB4092481 .
Microsoft Exchange Server	Remote Code Execution	Important ★ ★ ★	KB4459266 and KB2565063 .
SQL Server Management Studio	Information Disclosure	Important ★ ★ ★	Microsoft SQL documentation .

Learn more:

High Threat Security Alert (A18-10-04): Multiple Vulnerabilities in Microsoft Products (October 2018) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=331)

Sources:

- Microsoft October 2018 Security Updates (<https://portal.msrmc.microsoft.com/en-us/security-guidance/releasenotedetail/aa99ba28-e99f-e811-a978-000d3a33c573>)

Data analytics powered by  in collaboration with 