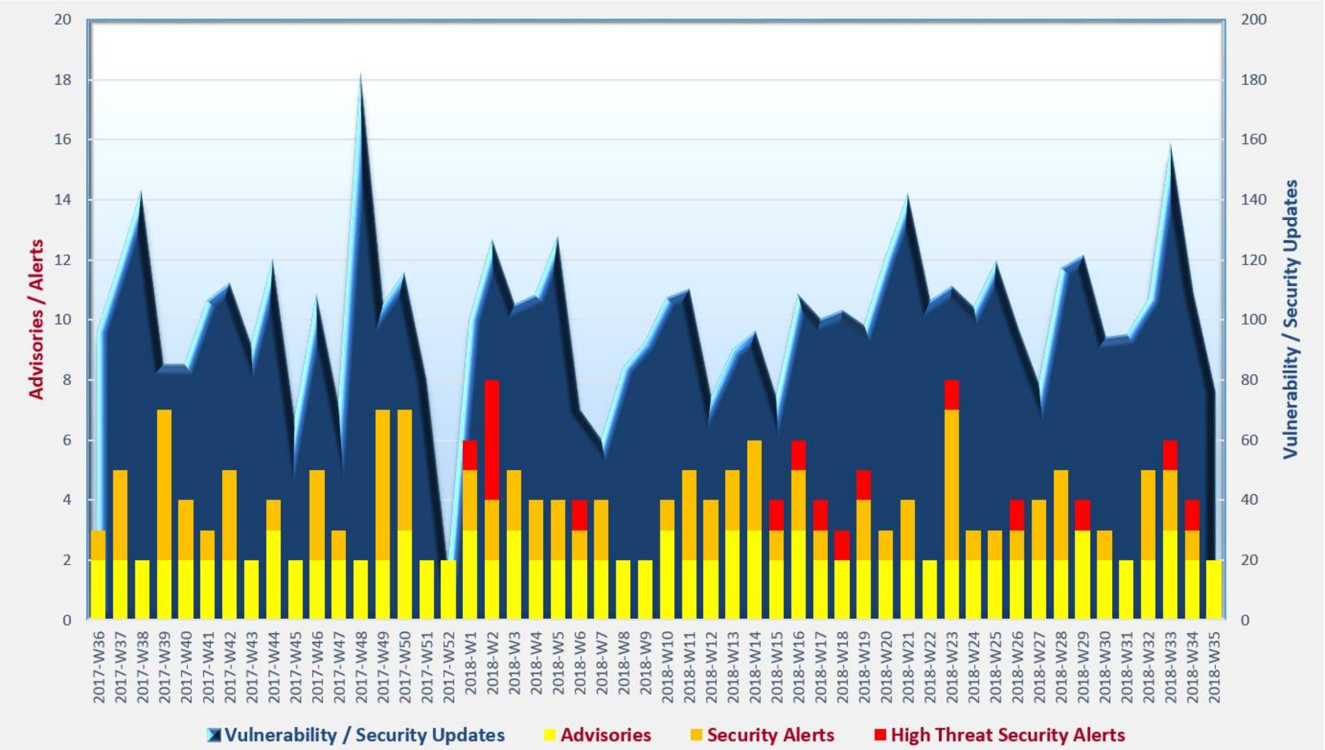
Cyber Security Threat Trends 2018-M08

August 2018

With reference to the FIRST Traffic Light Protocol (TLP) standards[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:

✧ **Ransomware attacks** targeting enterprises still prevail. Enterprises should harden systems, strengthen perimeter defences, and raise user awareness to guard against the attacks.

✧ **Email scam** comes in a form threatening computer users to pay ransom while there may not be real intrusion into the computers. Users are advised to stay alert with any tricks that could lead to data loss, ransomware attacks, and even direct financial loss.

✧ **Cryptomining malware** keeps making its way through others' computers to reap profits and users should stay away from suspicious email attachments and web links to avoid to be infected.

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

CERT Advisories

HKCERT[2] reminded users to be aware of a new wave of email scam that request for ransom. Recipient of the mail was advised to stay calm, do not pay the ransom, delete the email and immediately change the password. Recommendation were also given in the areas of password security, system security, physical security, and security awareness.

UK NCSC[3] published a guidance on setting up two-factor authentication (2FA) to protect online accounts. The guidance explained the importance of using 2FA and advised how to set up 2FA for extra protection.

MYCERT[4] issued an alert on cryptomining. It pointed out the adverse impacts caused by cryptojacking such as degraded system and network performance and more frequent system failures. Recommendations were provided for protection against cryptojacking, including keeping software and operating systems up-to-date, using strong passwords instead of default passwords.

Both GovCERT.HK[5] **and SingCERT**[6] issued alerts on a critical vulnerability on Apache Structs 2. Attackers could exploit the vulnerability to conduct remote code execution on the affected system. System administrators should upgrade Apache Structs to version 2.3.35 or 2.5.17 immediately.

[2] https://www.hkcert.org/my_url/en/blog/18080201
[3] https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa
[4] https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1314/index.html
[5] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=319
[6] https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-critical-apache-struts-2-remote-code-execution-vulnerability-cve-2018-11776

Industry Insight on Cyber Security Threat Trends

Proofpoint:

The **"Proofpoint Quarterly Threat Report Q2 2018"**[7] highlighted the company's observed cyber threats including email-based threats, web-based attacks and social media threats. It revealed how cyber criminals seized the chance to launch attacks in the World Cup 2018. The key findings were:

- **In Q2 2018, there was a 36% increase in malicious email volume over Q1 2018. 11% of the malicious emails were found containing ransomware in Q2 2018, an increase of more than 10% compared with Q1 2018.** The percentage of Downloader (malware for the purpose of downloading other malicious software to victims' devices) and Remote Access Trojans (RATs) also increased. On the contrary, the percentage of banking Trojans and credential stealers were dropped. Attackers were found more frequent to include malicious URLs than malicious file attachments in emails. There was a 26% increase in Business Email Compromise (BEC, or Email Fraud) in Q2 2018, as compared to Q1 2018. Email was one of the most common malware infection channels. Users should always be vigilant about handling emails from unknown sources and in particular should not open suspicious attachments and don't click suspicious links in emails.

- **Web-based attacks: social engineering and detected Coinhive events were both skyrocketed by 500% and 460% over Q1 2018, respectively.** One of the techniques used in web-based social engineering attack was that attackers leveraged fake anti-virus and browser plugins to deceive users. For Coinhive, attackers inserted malicious code to compromised websites to consume processing power of equipment visiting the websites for cryptocurrency mining.

- **Scam on social media platform was on the rise.** In Q2 2018, support fraud (also known as angler phishing) grew by 38%. Cyber criminals created fake social media profiles of companies, attempting to deceive customers and redirecting them to phishing web sites to obtain their sensitive information. Users should pay attention when using social media to avoid falling into the trap.

- **Around 250 potentially risky or malicious social media accounts related to World Cup 2018 were found.** Malicious activities associated with these accounts included phishing, links to web sites with malicious contents, stealing users' credential and so on.

[7] https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q218-quarterly-threat-report.pdf

AV-TEST:

The **"AV-TEST Security Report 2017/2018"** [8] has the following key findings on malware development:

- **Cryptomining malware grew tremendously, as more cybercriminals adopted this less risky and lower overhead approach.** The development of new cryptomining malware skyrocketed from an average of 3,700 new samples per month for the first nine months in 2017 to 470,000 new samples per month in March 2018. In Q1 2018, 84.69% of cryptomining malware targeted Windows platform, a growth of almost 30% when compared with 55.44% in 2017. Browser miner was the second most common cryptomining malware (about 15%).

- **Trojans had the largest share in malware under Windows platform, followed by viruses and malicious scripts.** Trojans accounted for 40.90% and 51.48% of malware under Windows platform in 2017 and Q1 2018, respectively. The share for password and banking Trojans also grew from 4.50% in 2017 to 8.03% in Q1 2018.

- **Android device users should keep vigilant.** Android platform was another attackers' target after Windows platform. In Q1 2018, around 5.63% of all detected malware targeted Android platform. More than 80% of the detected Android malware were Trojans. In particular, the share of password and banking Trojans increased to more than 9% in Q1 2018. Another noteworthy finding was that one-third of Android devices operated in obsolete Android version from version 1.1 to 5.1.1, of which security patch was no longer available.

- **macOS-based malware was on the rise.** In Q1 2018, 22,453 new malware samples were found, an increase of 500% and 35% when compared with Q1 2017 and Q4 2017 respectively. Trojans accounted for 40.93% of all macOS-based malware in 2017 and more than 86% in Q1 2018.

- **Users should stay alert and perform precautionary measures, no matter what platforms they used.** They should employ anti-malware solution whenever possible, and apply the latest security patches to the operating system and applications to fix known vulnerabilities, and update any obsolete software to the latest version.

[8] https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2017-2018.pdf

APWG:

The Anti-Phishing Working Group (APWG) issued its **"Phishing Activity Trends Report 1st Quarter 2018"**[9] in July 2018. Based on the phishing attack cases reported to APWG, the following phishing trends in Q1 2018 were found:

- **Number of phishing sites detected increased 46%** from 180,577 in Q4 2017 to 263,538 in Q1 2018. Over the first quarter of 2018, the number has grown rapidly from 60,887 in January, through 88,754 in February, to 113,897 in March.

- **The online payment industry was mostly targeted by phishing (39.4%).** An increase was observed for phishing targeted service providers of Software as a Service (SAAS), webmail, cloud storage and file hosting. The report also indicated that phishers were increasingly using one-time phishing URLs, which were unique phishing URLs generated by phishers for individual victims, trying to evade detection and blocking.

- **13,954 unique domains were identified as being used in phishing attacks in Q1 2018.** Around 47% or 6,608 phishing sites belong to the .com top-level domain.

- **The phishing sites hosted on HTTPS infrastructure were found to be increasing.** In Q1 2017, there were only around 10% of phishing sites hosted on HTTPS infrastructure, but the proportion had raised to more than 33% in Q2 2018. The report explained this increasing trend from two aspects. Firstly, more and more websites used HTTPS, however, this did not mean that these websites were immune to being compromised. When these HTTPS websites were compromised by phishers, they became HTTPS phishing sites. Secondly, phishers were taking advantage of users' misunderstanding on HTTPS and the misleading "Secure" labels provided by the browsers on HTTPS web sites.

- **Phishing emails were not the only channel used by phishers.** The report referred to the situation in Brazil to elaborate how phishers used multiple means to phish such as by sending Short Text Messages (SMS) with phishing URLs to victims, by scam web sites, by scam mobile apps, distributing phishing URLs by malware, by social media scams, etc.

[9] https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf

Rapid7:

Rapid7 produced its report **"Under the Hoodie: Lessons from a Season of Penetration Testing"**[10] based on data gathered from 268 penetration testing service engagements from September 2017 to June 2018. The report revealed the following:

- **At least one software vulnerability could be identified in 96% of internal engagements and 80% of external engagements**. Internal engagements focused on testing systems within the internal network while external engagements were for testing Internet-accessible systems. Common vulnerabilities found included SMB relaying (25.8%) and broadcast name resolution (24.2%) for internal networks, cross-site scripting (13.6%) and cross-site request forgery / clickjacking (11.7%) for Internet-accessible systems.

- **96% of internal engagements and 65% of external engagements detected at least one misconfiguration.** Common configuration issues identified included service misconfiguration, password reuse, lack of least-privilege principles for accounts, lack of patch management, service accounts as Domain Administrators, lack of detection controls, lack of network segmentation, default account access and outdated firewall rules.

- **86% of internal penetration tests and 33% of external penetration tests could compromise at least one credential**. According to the report, the most common method used by the penetration testers to gain user credential was "manual guessing".

- **The penetration testers commented that the choice of password by human was, to a certain extent, predictable.** They analysed a collection of 130,000 real passwords from different organisations and were able to identify some common password patterns:
  - Around 46% passwords were 8-character in length.
  - Around 5% users used the name of the organisation as part of their passwords.
  - Around 3% passwords were related to the word "password" or its derivative.
  - Around 1.4% passwords were created by combining the season and the year.
  - Among the choice of uppercase letter, lowercase letter, special character and digit, passwords ended with a digit were found to be the most common.

  When choosing password, users should not use patterns which could be guessed easily.

- **The penetration testers were undetected in 61% of the engagements.** The report suggested organisations should review their detection capabilities against cyber attacks.

[10] https://www.rapid7.com/globalassets/_pdfs/research/rapid7-under-the-hoodie-2018-research-report.pdf

Summary of Microsoft August 2018 Security Updates

15 Product Families with Patches

11 Critical

4 Important

Product Family	Impact[11]	Severity	Associated KB and / or Support Webpages
All versions of Windows 10 and Windows Server 2016 (not including Microsoft Edge)	Remote Code Execution	Critical ★★★★	Windows 10: KB4343909, KB4343897, KB4343885, KB4343887, KB4343892; Windows Server 2016: KB4343887.
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4343897, KB4343892, KB4343909, KB4343887, KB4343885.
Windows 8.1 and Windows Server 2012 R2	Remote Code Execution	Critical ★★★★	KB4343898, KB4343888.
Windows Server 2012	Remote Code Execution	Critical ★★★★	KB4343901, KB4343896.
Windows RT 8.1	Remote Code Execution	Critical ★★★★	KB4343898.
Windows 7 and Windows Server 2008 R2	Remote Code Execution	Critical ★★★★	KB4343900, KB4343899.
Windows Server 2008	Remote Code Execution	Critical ★★★★	KB4340937, KB4344104, KB4340939, KB4338380, KB4343674, and KB4341832.

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

Product Family	Impact[11]	Severity	Associated KB and / or Support Webpages

Internet Explorer	Remote Code Execution	Critical
		★★★★
			IE9: KB4343205;
			IE10: KB4343901, KB4343205;
			IE11: KB4343900, KB4343898, KB4343205, KB4343899, KB4343897, KB4343892, KB4343909, KB4343887, and KB4343885.

Microsoft Exchange Server	Remote Code Execution	Critical ★★★★	KB4340733, KB4340731.
Microsoft SQL Server	Remote Code Execution	Critical ★★★★	KB4293801, KB4293808, KB4293803, KB4293805, KB4293807, and KB4293802.
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore

Microsoft Office-related software	Remote Code Execution	Important
		★★★
			Microsoft Office 2010, 2013, 2016, 2016 for Mac, Click to Run, Compatibility Pack: KB3213636, KB4022198, KB4032212, KB4032233, KB4032239, Click to Run, 2016 for Mac;
			Microsoft Office Word Viewer: KB4092433, KB4092434;
			Word Automation Services: KB4032215;
			Microsoft Excel 2010, 2013, 2016, Viewer: KB4022195, KB4032213, KB4032223, KB4032229, KB4032241, Click to Run;
			Microsoft PowerPoint 2010: KB4018310;
			Microsoft Outlook 2010, 2013, 2016: KB4032222, KB4032235, KB4032240, Click to Run;
			Microsoft Office Web Apps 2010, 2013: KB4032220, KB4022238.

Microsoft SharePoint-related software	Information Disclosure	Important ★★★	KB4018392, KB4022234, KB4032256, and KB4022236.

Product Family	Impact[11]	Severity	Associated KB and / or Support Webpages
Microsoft .NET Framework	Information Disclosure	Important ★★★	.NET Framework, .NET Core, GitHub.
Microsoft Visual Studio	Elevation of Privilege	Important ★★★	KB4456688.

Learn more:
High Threat Security Alert (A18-08-05): Multiple Vulnerabilities in Microsoft Products (August 2018) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=316)

Sources:

- Microsoft August 2018 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/ecb26425-583f-e811-a96f-000d3a33c573)