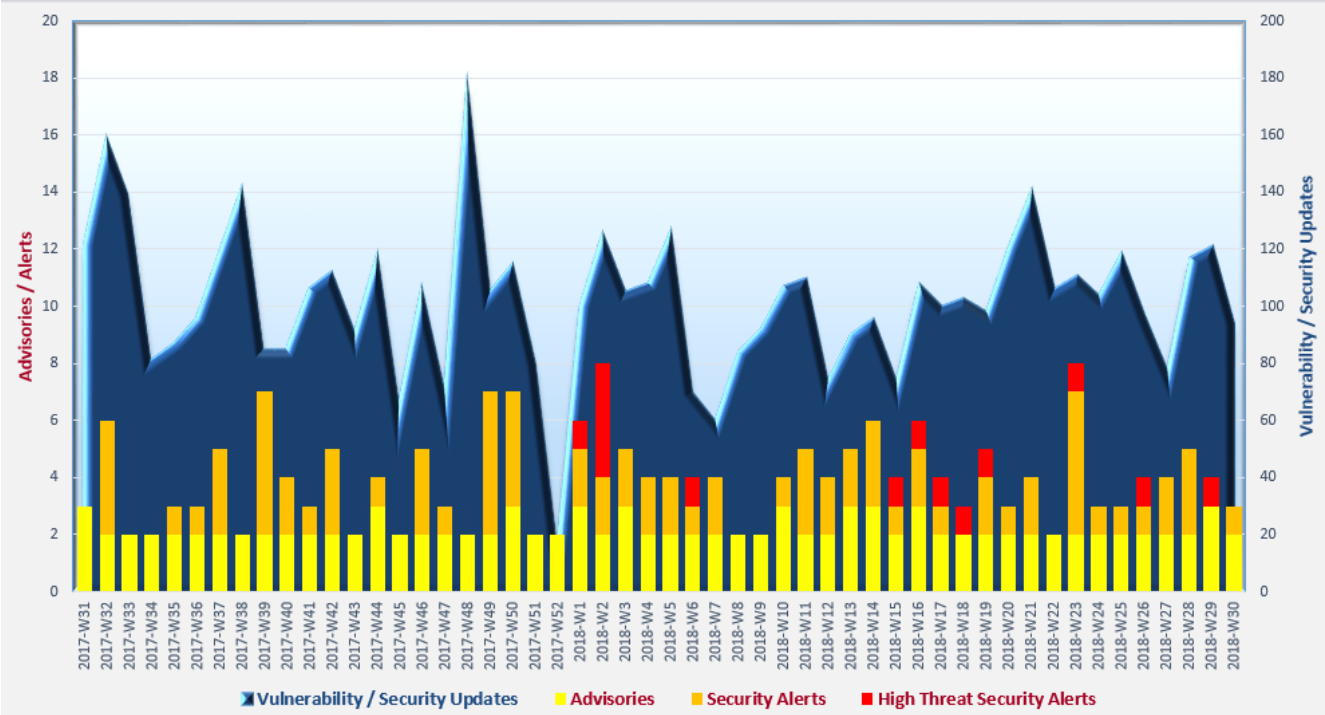
Cyber Security Threat Trends 2018-M07

July 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:

- ✧ **Malware attacks** continue to affect computer users globally. Users are highly recommended to install security protection tools and apply latest security patches without delay to guard against possible attacks.
- ✧ **Phishing threat** has been around for a long time and has always proved an effective way to steal personal information. Users are advised to be cautious on all kinds of bait that could end up with data loss and even ransomware attacks.
- ✧ **Mining cryptocurrencies** are still profitable and users are advised to scan and clean their computers to avoid being hijacked by hackers for mining**.**

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

CERT Advisories

SingCERT[2] published on 20 July 2018 a Technical Advisory on measures for protecting customers' personal data. It was reported that SingHealth's database containing patient personal particulars and outpatient dispensed medicines has been the target of a major cyber attack. SingCERT recommended companies that collect personal data to review their systems and be vigilant to suspicious activity.

The recommended security measures include reviewing domain administrator accounts, disabling PowerShell for standard workstations, monitoring for unauthorised remote access or database access, tightening control for long-running or decommissioned endpoints, employing strong endpoint protection, and keeping systems up-to-date.

HKCERT[3], in response to the SingHealth's incident, also published on 23 July 2018 a Security Blog to advice organisations to observe the recommendations promulgated by SingCERT.

HKCERT[4] released on 25 July 2018 its "Hong Kong Security Watch Report" for the second quarter of 2018. The report provided an analysis of the activities of compromised computers in Hong Kong which suffer from or participate in various forms of cyber attacks.

The report highlighted that the number of phishing events identified in Q2 2018 increased exponentially compared to the previous quarter. The number of malware hosting events also increased significantly. HKCERT urged all system and application administrators to secure their servers and regularly health check their computers to ensure they would not become a part of the botnets. HKCERT warned that major botnet family – WannaCry, Avalanche, XCode Ghost, Pushdo, Citadel, Mumblehard, Ramnit, ZeroAccess and GameOver Zeus are still in action.

[2] https://www.csa.gov.sg/singcert/news/advisories-alerts/measures-for-protecting-customers-personal-data
[3] https://www.hkcert.org/my_url/en/blog/18072301
[4] https://www.hkcert.org/my_url/en/blog/18072501

McAfee:

The **"McAfee Labs Threats Report June 2018"**[5, 6] highlighted the following trends in malware and also reviewed the tactics of a few key campaigns in Q1 2018:

- **Attackers became more active to harvest cryptocurrencies.** They chose a simpler and more direct way to monetise the infections, resulting in a drastic 1,189% increase in the number of new coin miner malware. The number of total coin miner malware known samples also skyrocketed a 629% increase from around 400,000 in Q4 2017 to more than 2.9 million in Q1 2018.

- **Be cautious on LNK shortcut files.** There was a 59% increase in the number of new LNK malware in Q1 2018, showing that threat actors were increasingly leveraging Microsoft Windows LNK shortcut files to deliver malicious PowerShell scripts and other malware. Users should keep their anti-malware solution updated and stay vigilant to any suspicious LNK file in particular those received via email.

- **The emergence of new malware slowed down but the tactical and technological advancement did not.** Although new malware recorded declined by 31% in Q1 2018 (from around 63 million in Q4 2017 to around 44 million), the researchers noticed that the bad actors were improving their technology and tactics. Users should always stay alert to the emerging cyber threats.

- **Three major threat campaigns were highlighted in the report:** the attack targeted organisations involved in the Winter Olympics in South Korea; a campaign dubbed Operation GhostSecret which targeted a wide range of sectors; and the Bitcoin-stealing phishing campaign, HaoBao, which was launched by Lazarus, targeted the financial sector and Bitcoin users. It was worthy to be noted that phishing email was a common infection channel for threat campaigns. Users should be aware of spam / phishing email and not to click suspicious links.

[5] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf
[6] https://www.mcafee.com/enterprise/en-us/assets/infographics/infographic-threats-report-jun-2018.pdf

Positive Technologies:

The Positive Technologies unveiled its **"Web Application Vulnerabilities: Statistics for 2017"**[7], which was compiled based on the results of 23 web application assessed in 2017 from various industries such as finance, IT, E-commerce, telecom, mass media, manufacturing and government. The key findings were:

- **All tested web applications contained vulnerabilities of medium-severity level at least.** The average number of medium-severity vulnerabilities per tested web application was 7.5 in 2017, dropped from 17.3 in 2016. 52% of tested web applications had high-severity vulnerabilities, compared to 58% in 2016. On average, two high-severity vulnerabilities per tested web application were found. Web application owners should conduct web application security assessment regularly to identify and rectify flaws.

- **Critical information leakage threat was found in 70% of tested web applications and 48% of them were vulnerable to unauthorized access.** In addition, 17% of tested web applications were vulnerable to be exploited to gain full control over application and server and 25% of tested web applications could be a vector for penetrating the intranet.

- **High-severity vulnerabilities were found in 60% of PHP web applications**, followed by 50% of Java-based web applications and 33% of ASP.NET-based web applications. The top 3 prevalent vulnerabilities in web applications were cross-site scripting (XSS) which was found in 74% of the tested web applications, followed by fingerprinting, and information leakage, which were detected in 61% and 52% of web applications, respectively. 65% of the detected vulnerabilities were caused by errors in application development, while incorrect configuration of web servers accounted for the remaining 35%. 21% of the tested web applications used outdated software such as web servers and content management systems. Web application owners should always apply the latest security patches to operating system and application software to fix the known vulnerabilities.

- **The report graded the average level of web application security as poor** and suggested adopting secure software development lifecycle and conducting web application security assessment during development to prevent vulnerabilities at the early stage. The report also recommended adoption of white-box testing with source code analysis during web application security assessment.

[7] https://www.ptsecurity.com/ww-en/premium/web-vulnerabilities-2018/

Rapid7:

Rapid7 released the third annual **"National Exposure Index 2018"**[8] report which surveyed 187 countries and regions through port scanning. The key results were:

- **The top 5 most exposed countries were the U.S., China, Canada, South Korea and UK.** Over 61 million servers were found listening on at least one port out of the 38 TCP ports and 9 UDP ports surveyed in these 5 countries.

- **13 million exposed endpoints were found allowing direct database access over the Internet, which were highly risky of being abused and leading to data breach.** More than 6 million of these exposed endpoints were using MySQL database. Other exposed database services included PostgreSQL, Oracle Database, Microsoft SQL Server, Redis, DB2 and MongoDB.

- **Although the number of exposed Microsoft SMB Servers was significantly reduced after the WannaCry attack in 2017, there were still about a half million exposed Microsoft SMB Servers**. These servers were still exposed to the SMB-based attacks.

- **Amplification-based distributed denial of service attacks remained dangerous.** The study found that there were about 40,000 unpatched TCP memcached servers running out-of-date software versions of which around 4,000 of them were also UDP-based memcached servers. All these servers were at risk of being utilised in future DDoS attack.

- **Hong Kong was ranked as the 13th most exposed countries/locations.** The study found that there were around 3,800 SSH servers with vulnerable SSH version 1.99, and around 900 memcached servers with weak and unmaintained configurations in Hong Kong.

[8] https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf

Link11:

Link11 Security Operation Center (LSOC) issued the **"Distributed Denial of Service Report for Q1 2018"**[9] in June 2018. The report was based on the data collected from the attacks on the web pages and servers protected by Link11. It revealed the following security trends in Distributed Denial of Service (DDoS) attacks in Central Europe in the first quarter of 2018:

- **The number of DDoS attacks increased by almost 10% in Q1 2018 as compared with Q4 2017,** from 13,452 to 14,736. That means an average of 160 attacks per day in Q1 2018. The affected industry included hosting/IT, gaming, retail, e-commerce, logistics, media, and finance.

- **There were 12 attacks recorded with an attack volume of more than 100 Gbps during the period.** The greatest attack volume involved bandwidth amounted to 212 Gbps caused by a memcached reflection attack, which was an attack method not observed in Q4 2017. The attack made use of vulnerable memcached servers to amplify the attack, with an amplification factor of, according to US-CERT, 10,000 to 51,000. Website administrators should secure their memcached servers by restricting inbound access from the Internet and disabling unnecessary TCP and UDP ports.

- **The most common attack vector was UDP Floods (49.3%),** with the second to the fifth places being Simple Service Discovery Protocol (SSDP) Reflection (27.2%), TCP SYN Floods (9.9%), UDP Fragments (7.7%), and DNS Reflection (2.0%) respectively. Both UDP Floods and SSDP Reflection recorded an increase of more than 18% as compared with Q4 2017.

- **The attackers stopped within 60 minutes in most of the attack cases.** On average, attacks lasted for around 6 minutes, which was slightly decreased from the 7 minutes in Q4 2017. The longest recorded attack lasted for 321 minutes.

[9] https://www.link11.com/en/ddos-report/

Summary of Microsoft July 2018 Security Updates

18 Product Families with Patches

4 Critical

14 Important

Product Family	Impact[10]	Severity	Associated KB and / or Support Webpages
Windows Edge	Remote Code Execution	Critical ★★★★	KB4338819, KB4338825, KB4338826, KB4338829, KB4338814
Internet Explorer	Remote Code Execution	Critical ★★★★	IE9: KB4339093; IE10: KB4338830, KB4339093; IE11: KB4338815, KB4338818, KB4339093, KB4338819, KB4338825, KB4338826, KB4338829, and KB4338814.
PowerShell Editor Services, PowerShell Extension for Visual Studio Code	Remote Code Execution	Critical ★★★★	PowerShell Editor Services, PowerShell Extension for Visual Studio Code.
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore
Windows 10 and Windows Server 2016 (including Microsoft Edge)	Elevation of Privilege	Important ★★★	Windows 10: KB4338819, KB4338825, KB4338826, KB4338814, KB4338829; Windows Server 2016: KB4338814.
Windows 8.1 and Windows Server 2012 R2	Elevation of Privilege	Important ★★★	KB4338815, KB4338824.

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

Product Family	Impact[10]	Severity	Associated KB and / or Support Webpages
Windows Server 2012	Elevation of Privilege	Important ★★★	KB4338830, KB4338820.
Windows RT 8.1	Elevation of Privilege	Important ★★★	KB4284815.
Windows 7 and Windows Server 2008 R2	Elevation of Privilege	Important ★★★	KB4338818, KB4338823.
Windows Server 2008	Elevation of Privilege	Important ★★★	KB4293756, KB4339854, KB4291391, KB4339291, KB4295656, KB4339503, and KB4340583.
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010, 2016, 2016 for Mac, Click to Run, Compatibility Pack: KB4011202, KB4022200, Click to Run, 2016 for Mac; Microsoft Word 2010, 2013, 2016, Microsoft Office Word Viewer: KB4022202, KB4022218, KB4022224, KB4032214; Microsoft Excel Viewer, Microsoft PowerPoint Viewer: KB4011202; Microsoft Access 2013, 2016: KB4018338, KB4018351.
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	KB4022235, KB4022228, and KB4022243.
Skype for Business, Microsoft Lync	Remote Code Execution	Important ★★★	Skype for Business: KB4022221 Microsoft Lync: KB4022225
.NET, .NET Core, ASP.NET, ASP.NET Core	Remote Code Execution	Important ★★★	.NET Framework, .NET Core, GitHub.

Product Family	Impact[10]	Severity	Associated KB and / or Support Webpages
Microsoft Visual Studio	Remote Code Execution	Important ★★★	KB4336919, KB4336946, KB4336986, and KB4336999.
Microsoft Research JavaScript Cryptography Library	Remote Code Execution	Important ★★★	MSR JavaScript Cryptography Library, Download Center.
Microsoft Wireless Display Adapter	Remote Code Execution	Important ★★★	Microsoft Wireless Display Adapter
Web Customizations for AD FS	Remote Code Execution	Important ★★★	AD FS user sign-in customization, AD FS Web Customization.

Learn more:
Security Alert (A18-07-04): Multiple Vulnerabilities in Microsoft Products (July 2018) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=308)

Sources:

- Microsoft July 2018 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/1c26eff2-573f-e811-a96f-000d3a33c573)