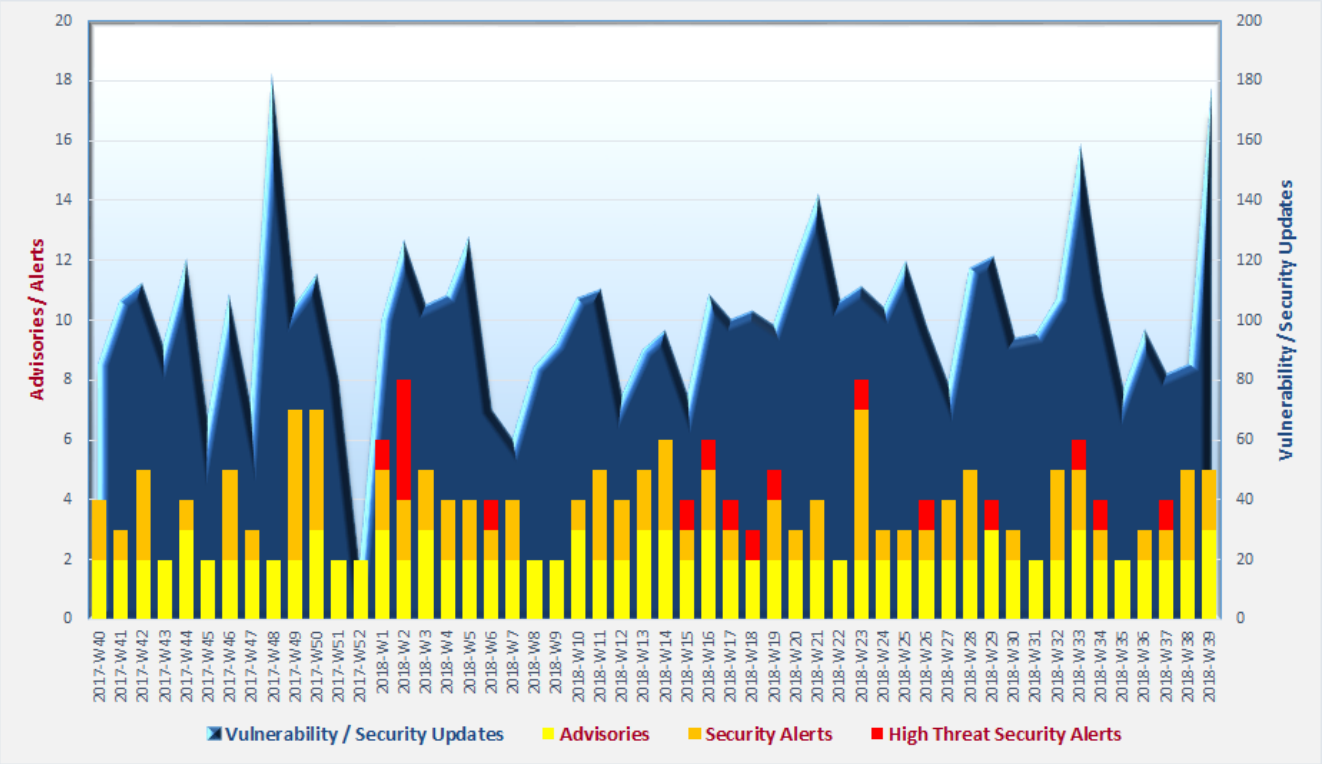
TLP:WHITE

Cyber Security Threat Trends 2018-M09

September 2018

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:

- ✧ **Newly published vulnerabilities** are quickly exploited to compromise any vulnerable systems. System owners should take timely patching as their essential security defence.
- ✧ **Ransomware** changes rapidly to evade detections and carry new exploit code. Multiple layers of defence at networks, end points and user awareness should be always on guard.
- ✧ **IoT malware** keeps infecting network devices to form botnets for further attacks. Device owners are advised to change the default passwords and disable access to admin functions via the Internet.

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

CERT Advisories

GovCERT.HK[2] issued a security advisory on how to protect routers from VPNFilter malware attack. VPNFilter is a malware which could infect small office and home office (SOHO) network equipment such as routers and network-attached storage (NAS) devices. Hackers could use the malware to perform man-in-the-middle attacks, stealing credentials, and taking control of vulnerable devices. Users could reboot their routers and NAS devices to temporarily stop the activity of the malware and update the devices with the latest firmware. Users should avoid using the routers' default password. For better security, user could also disable remote management settings of the devices.

HKCERT[3], SingCERT[4], and Australian Cyber Security Centre (ACSC)[5] issued security advisories on the Facebook security breach, in which a vulnerability in Facebook's "View as" function was found and exploited. Attackers could gain access to the victims' Facebook account, as well as those third party online services which used Facebook account as authentication. Users were advised to safeguard their Facebook accounts, by following the steps stipulated in the advisories.

SingCERT[6] posted an advisory that the Internet Corporation of Assigned Names and Numbers (ICANN)[7] scheduled the Root Zone Key Signing Key (KSK) rollover on 2018.10.11 to strengthen the security of Domain Name System Security Extensions (DNSSEC). It recommended the resolver operators to refer to the guidance issued by ICANN for the event.

US-CERT[8] published tips on how to secure enterprise wireless networks. Some of the recommended best practices included using strong Wi-Fi encryption standards, deploying wireless intrusion detection or prevention system, updating equipment with latest applicable security updates and patches, using securely configured equipment, isolating the guest Wi-Fi network from the organisation's main network, and so on.

2 https://www.govcert.gov.hk/en/advisories.html
3 https://www.hkcert.org/my_url/en/blog/18092901
4 https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-facebook-security-breach
5 https://cyber.gov.au/infrastructure/news/facebook/
6 https://www.csa.gov.sg/singcert/news/advisories-alerts/singcert-technical-advisory-on-dnssec-root-zone-key-signing-key-rollover
7 https://www.icann.org/resources/press-material/release-2018-09-18-en
8 https://www.us-cert.gov/ncas/tips/ST18-247

CERT Advisories

US-CERT[9] published on its website a security alert on Remote Desktop Protocol (RDP) exploitation, which was issued by the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation (FBI). Cyber threat actors abused remote administration tools by identifying vulnerable RDP sessions and exploiting them to perform malicious activities such as credential stealing or spreading ransomware. Users and administrators were advised to use strong passwords, well protect their passwords and disable RDP access if not necessary.

The UK National Cyber Security Centre (NCSC)[10] published an advisory for defending Trickbot banking Trojan. Trickbot was a credential stealing Trojan and could infect targets through phishing emails or by other infected devices on the same network. Mitigation measures included applying latest security updates to software, keeping anti-malware solutions up-to-date, implementing measures to detect and prevent lateral movement of malware in company networks and so on.

9 https://www.us-cert.gov/ncas/current-activity/2018/09/28/IC3-Issues-Alert-RDP-Exploitation
10 https://www.ncsc.gov.uk/alerts/trickbot-banking-trojan

Kaspersky:

The **"Kaspersky Spam and Phishing Report in Q2 2018"** [11] highlighted the company's observations on cybercriminals' tactics in spam and phishing, and the statistics in Q2 2018 as below:

- **Threat actors seized the opportunity of abusing General Data Protection Regulation (GDPR) for phishing.** They sent fake notification mails with malicious links to customers of companies, quoting the requirements of GDPR and requesting them to update their user accounts. The cybercriminals could then obtain personal information of the victims.

- **Cybercriminals used social media networks such as WhatsApp, Facebook, Twitter and Instagram as distribution channels for disseminating fraudulent content or distributing malware.** They often used lotteries, advertisements, giveaways, discounts such as airplane tickets or hotels promotion, etc. to attract users to visit their fraudulent website which might further redirected the victims to other resources, eventually stole victims' credentials or installed malware to victims' devices. Even worse, the victims might forward or "share" the spam messages to others through social media.

- **Cybercriminals aimed at cryptocurrency.** They created fake websites of cryptocurrency wallet and market to collect victims' credentials and private information. In addition, cybercriminals used fake Initial Coin Offerings (ICO) projects to tempt victims to pay them.

- **There was a 2.16% decrease in spam email volume over Q1 2018.** Most of the spam came from China, USA and Germany which accounted for 14.36%, 12.11% and 11.12% respectively. The top three countries targeted by malicious email in Q2 2018 were Germany, Russia and the United Kingdom with 9.54%, 8.78% and 8.57% respectively. 10.35% of malicious attachments sent by email contained Exploit.Win32.CVE-2017-11882 malware family, which targeted Microsoft Word's CVE-2017-11882 vulnerability. Another finding during Q2 2018 was that threat actors, trying to evade detection, started using Microsoft Excel Web Query (IQY) files as email attachments to perform malicious activities.

- **IT related organisations and financial organisations were mostly targeted by phishing attacks.** The percentage of phishing attacks to global Internet portals; banks, financial and e-pay organisations; and IT companies were 25.01%, 21.10% and 13.83% respectively.

[11] https://securelist.com/spam-and-phishing-in-q2-2018/87368/

Fortinet:

Fortinet published its **"Threat Landscape Report Q2 2018"**[12] which revealed the observations of exploits, malware and botnets. The key observations were:

- **In Q2 2018, 5.7% of vulnerabilities published on the CVE List (5,898 out of 103,786) were exploited in the wild.** The report mentioned some noteworthy exploits during the period such as the exploit related to Microsoft IE, Apache Struts, Oracle WebLogic Server, "Drupalgeddon 2" and some other exploits targeting Industrial Control Systems (ICS) and Internet of Things (IoT) devices. Many attacks targeted IoT devices for cryptocurrency mining. The report pointed out that knowing what vulnerabilities were exploited in the wild could give system administrators an insight on making their decision on remediation prioritisation.

- **Volume of cryptojacking malware followed the price of cryptocurrency.** 23,945 unique malware variants were found in Q2 2018. In particular, 23.3% of malware were cryptojacking malware. Researchers observed that the volume of cryptojacking malware decreased in first half of 2018 might have a correlation with the drop of the market price of cryptocurrencies such as Bitcoin and Monero. Although volume of cryptojacking malware was dropped, attackers still aimed to infect IoT devices for mining cryptocurrencies since many IoT devices were kept powered on and connected.

- **Malware developers adopted agile development approach to modify the malware within a short period of time**, to avoid being detected by anti-malware software. A notable example was GandCrab v4.1.2 which was released just within one to two days after a temporary solution to GandCrab v4 was developed. The report also pointed out that threat actors were increasingly using PowerShell to perform malicious activities. It was crucial to update system and anti-malware software timely.

- **Botnets infected different platforms.** There were 265 active botnets detected in Q2 2018, targeting various platform. For instance, the Monero mining malware/botnet, Smominru, targeted Microsoft Windows platform, and the EternalBlue exploit. The Bankbot botnet, which aimed to steal credentials, targeted Android devices. Its new member, Anubis variant, added several new features, including ransomware, keylogger, Remote Access Trojan (RAT) functions, and so on. A new Mirai botnet variant, Wicked, added at least three exploits to attack vulnerable IoT devices in a more effective way.

[12] https://ready.fortinet.com/q2-2018-threat-landscape-report/q2-2018-threat-landscape-report

NETSCOUT:

NETSCOUT Threat Intelligence issued its **"2018 Threat Intelligence Report"**[13]. The report analysed the trends on DDoS attack and Advanced Threat attack in the first half of 2018. It also highlighted some noteworthy DDoS attacks, Threat Actor groups and Crimeware.

- **2.8 million DDoS attacks were observed in first half of 2018.** Compared with the first half of 2017, the average size of attacks increased by 37%. The number of attacks with over 300 Gbps traffic and 500 Gbps traffic increased from 7 to 47 and from 2 to 19 respectively. In terms of regional attacks, Asia Pacific recorded the highest number of attacks while Latin America got the lowest. The largest DDoS attack attained 1.7 Tbps and was detected in North America in March 2018.

- **2 million Internet-connected devices could be abused for Simple Service Discovery Protocol (SSDP) reflection / amplification attack**, among which 1.2 million devices could also be abused for SSDP diffraction attack, which was more difficult to mitigate as the source and destination ports of the UDP packets were ephemeral.

- **The largest DDoS attack size was 1.7 Tbps by Memcached attack on 5 March 2018.** Number of servers vulnerable to Memcached attack decreased from 17,000 in March 2018 to 550 in June 2018, according to the report. However, it was found that some attackers were setting up their own vulnerable servers to launch attacks.

- **There would be 125 billion IoT devices by 2030.** If these devices were not properly managed and patched, they could be abused by threat actors to form IoT botnets. The researchers expected the number and size of IoT botnets would increase, as threat actors would utilise the IoT-based malware in an automated way for spreading and exploiting vulnerabilities. The report also highlighted the characteristics of Mirai, a malware targeting IoT devices, and its variants such as IoTrojan, JenX, OMG, Satori and Wicked.

- **The report highlighted a number of Advanced Persistent Threat (APT) Groups, namely Donot Team, Fancy Bear, Hidden Cobra, Ocean Lotus and OilRig.** It also mentioned the techniques and tools used by these threat groups and their targets.

- **Crimeware was found to become more capable to self-propagate and spread. Some of them switched their focus to cryptocurrency mining.** The report highlighted some of the crimeware such as Emotet, Kardon Loader, Panda Banker and Trickbot and their characteristics.

[13] https://www.netscout.com/pdf/threat_intelligence_report/

Tripwire:

The **"Tripwire State of Cyber Hygiene Report 2018"**[14] surveyed organisations on how they implemented the top 6 of the 20 Critical Security Controls (the "cyber hygiene") that established by The Center for Internet Security (CIS). The key findings were:

- **Control 1 - Inventory and Control of Hardware Assets:** Researchers advised organisations to have accurate network inventory and be able to detect newly connected devices quickly. The up-to-date inventory gives visibility of the attack surface so that appropriate protection measures could be applied.

- **Control 2 - Inventory and Control of Software Assets:** The report suggested organisations should properly implement this control to prevent malware or unauthorised software running in their IT environment. The report also pointed out that organisations could consider applying "application whitelisting" in implementation of this control.

- **Control 3 - Continuous Vulnerability Management:** While security breaches with high impact were often caused by known vulnerabilities, organisations should deploy applicable patches timely. Running vulnerability scans frequently (at least weekly) and comprehensively (using authenticated scans) was also recommended.

- **Control 4 - Controlled Use of Administrative Privileges:** The credentials of administrative accounts were highly targeted by attackers. Organisations could consider restricting execution of administrative tasks from dedicated workstations in dedicated network segments. Moreover, default passwords must be changed and multi-factor authentication could be considered.

- **Control 5 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** All systems should be configured and hardened according to companies' security policies as well as cybersecurity best practices. Organisation should consider using configuration monitoring tools for fast detection on any unexpected changes in configurations.

- **Control 6 - Maintenance, Monitoring and Analysis of Audit Logs:** The report suggested that logs should be reviewed more frequently. Organisations should enable logging at endpoints and network and store the logs in a centralised log server as attackers might leave traces of activity at endpoint and network devices.

[14] https://www.tripwire.com/misc/state-of-cyber-hygiene-report-register/

Summary of Microsoft September 2018 Security Updates

13 Product Families with Patches

11 Critical

2 Important or below

Product Family	Impact[15]	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: KB4457128, KB4457142, KB4457138, KB4457131, KB4457132; Windows Server 2016: KB4457131.
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4457131, KB4457132, KB4457138, KB4457142, KB4457128.
Windows 8.1 and Windows Server 2012 R2	Remote Code Execution	Critical ★★★★	KB4457129, KB4457143.
Windows Server 2012	Remote Code Execution	Critical ★★★★	KB4457135, KB4457140.
Windows RT 8.1	Remote Code Execution	Critical ★★★★	KB4457129.
Windows 7 and Windows Server 2008 R2	Remote Code Execution	Critical ★★★★	KB4457144, KB4457145.
Windows Server 2008	Remote Code Execution	Critical ★★★★	KB4458010, KB4457984.
Internet Explorer	Remote Code Execution	Critical ★★★★	IE9: KB4458010, KB4457426; IE10: KB4457135, KB4457426; IE11: KB4457129, KB4457144, KB4457426, KB4457128, KB4457132, KB4457131, KB4457138, and KB4457142.

[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-related software	Remote Code Execution	Critical ★★★★	Microsoft Office 2016 for Mac, Click to Run, Compatibility Pack: KB4092466, Click to Run, 2016 for Mac; Microsoft Word: KB4032246, KB4092447; Microsoft Excel 2010, 2013, 2016, Viewer: KB4092460, KB4092467, KB4092479, KB4227175;
.NET Framework	Information Disclosure	Critical ★★★★	.NET Framework.
ChakraCore and ASP.NET Core	Remote Code Execution	Critical ★★★★	ChakraCore, .NET Core, GitHub.
Microsoft SharePoint-related software	Elevation of Privilege	Important ★★★	KB4092470, KB4092459, and KB4022207.
Microsoft Lync	Security Feature Bypass	Moderate ★★	Mac 2011: CVE-2018-8474.

Learn more:
High Threat Security Alert (A18-09-02): Multiple Vulnerabilities in Microsoft Products (September 2018) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=321)

Sources:

- Microsoft September 2018 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/498f2484-a096-e811-a978-000d3a33c573)