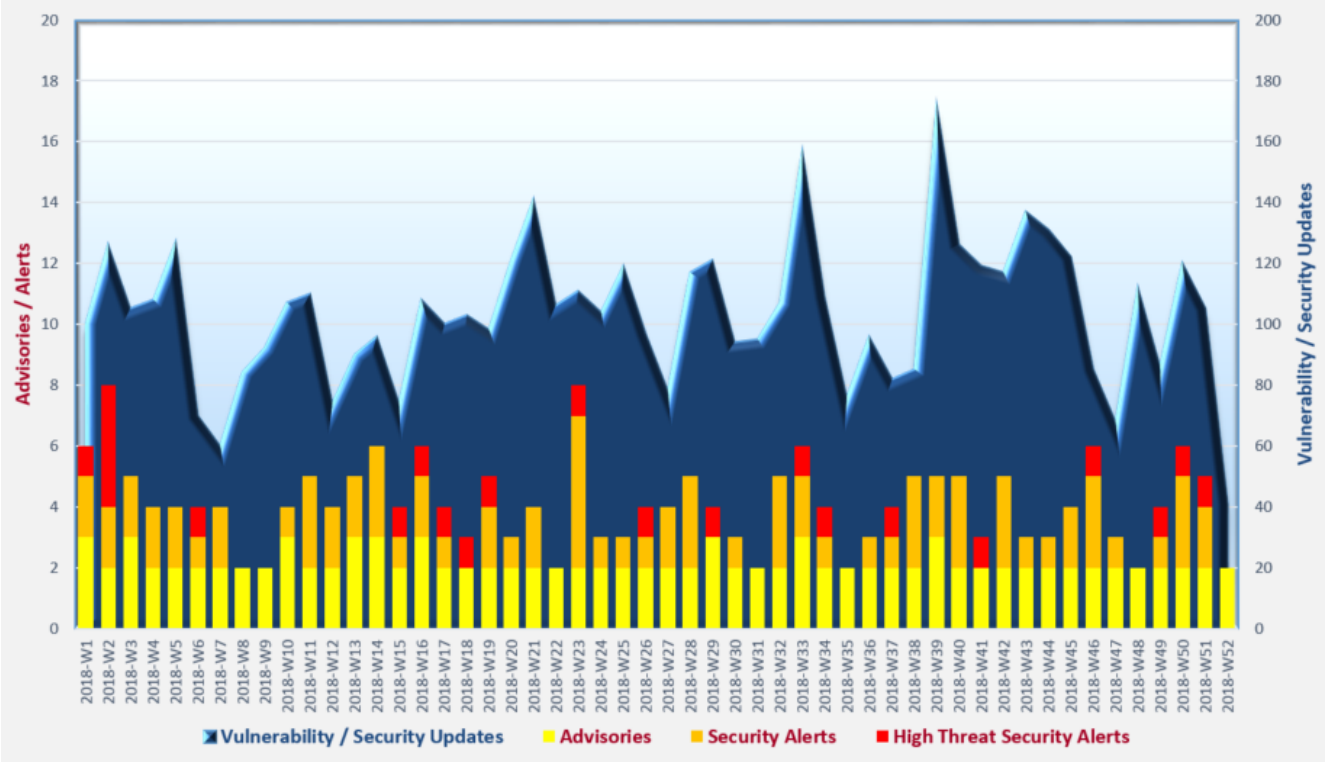
TLP:WHITE

Cyber Security Threat Trends 2018-M12

December 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:

- **Big data breaches** involving personal information of millions of customers kept being disclosed. Businesses should realise that their customer information will always be targeted by attackers and impose stringent protective measures against potential breaches**.**
- **Remote Desktop access** is abused by Ransomware to infect Windows computers. End users and system administrators should restrict the remote access to their desktops or servers.
- **Internet of Things (IoT) botnets** thrive with increasing exploitations of vulnerabilities in IoT devices. Device owners are advised to keep their devices updated with latest firmware.

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

CERT Advisories

HKCERT[2] issued a "Best Practice Guide of Remote Desktop". Remote Desktop is to control a computer remotely. Remote Desktop should be disabled as poor configuration will expose risk to the computer. If Remote Desktop is geniunely needed, user should follow the best practices to use it in a secure manner.

HKCERT[3] issued Security Newsletter for December 2018, which covers security over mobile payment service, security and privacy by design to handle customer information with caution, and the Google Play Store's Apps Security Risk Report.

US-CERT[4] published on its website a security tip on what questions every CEO should ask about cyber risks, including what cybersecurity threats they were facing, and what they should do to mitigate the cybersecurity threats. The article also listed out some recommended organisational cybersecurity best practices for reference, e.g. engaging senior management in cybersecurity risk management and policy formulation, preparing and rehearsing cybersecurity incident response plan and procedures, and so on.

US-CERT[5] issued an alert on SamSam ransomware and its variants. SamSam actors exploited Windows servers using Remote Desktop Protocol (RDP). They might use brute force attacks, stolen login credentials or even purchase stolen RDP credentials from known darknet marketplaces. To mitigate the risk, best practices to strengthen the security posture of IT systems were recommended in the article.

US-CERT[6] issued an advice on "Securing New Devices" on 2018.12.28. Measures such as securing the devices with strong passwords, reviewing the security settings, applying software updates timely and connecting the devices to the Internet with care have been recommended.

SingCERT[7] issued an alert on EternalSilence, which was a new variant of EternalBlue and EternalRed. EternalSilence abused Universal Plug and Play (UPnP) services on routers. Attackers could then create a "UPnProxy" to spread spam, malware and launch DDoS attacks. End users were told to reset their routers to their original factory settings, disable the routers' UPnP feature and upgrade the router firmware to the latest available version. Network administrators were advised to block off Internet access on TCP port 139 and 445 to the routers.

[2] https://www.hkcert.org/my_url/en/guideline/18120501
[3] https://www.hkcert.org/my_url/en/blog/18120301?nid=255931
[4] https://www.us-cert.gov/ncas/tips/ST18-007
[5] https://www.us-cert.gov/ncas/alerts/AA18-337A
[6] https://www.us-cert.gov/ncas/current-activity/2018/12/28/Securing-New-Devices
[7] https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-eternalsilence-a-new-variant-of-eternalblue-and-eternalred-abusing-upnp-services-on-routers

Industry Insight on Cyber Security Threat Trends

Malwarebytes Labs:

Malwarebytes Labs published its **"Under the Radar – The Future of Undetected Malware"**[8] which studied the new attack methods used by malware, making them difficult to be detected and remediated, remain out of sight and silently spread across an organisation. The key observations were:

- **Fileless malware was one of the latest threats accounting for 35 percent of all attacks in 2018**. It had around 10 times higher chance of success over file-based attacks because most of the security solutions deployed were using file-based detection, and were unable to detect malware in memory.

- **Emotet and Trickbot used "mutation" to make themselves difficult to be identified.** They were commonly distributed by email with malicious office documents and used PowerShell for downloading and execution. Since the downloaded malicious files were frequently changed, they were difficult to be detected. They exploited the same vulnerabilities used by WannaCry and NotPetya to spread over the network. There were more than 1.5 million Emotet detections during January and September 2018. Most detections were found in the US, but there were growing trends of infections in other countries including UK, Philippines, and Canada.

- **Sorebrect was one of the fileless ransomware** that also targeted network share drives. Users might need to check with their anti-malware solution providers to see if the solution could monitor process memory and had the capability of behavioural identification and detection to detect and stop these kind of fileless malware.

- **SamSam was a ransomware launched by attackers using batch scripts after it broke into misconfigured or vulnerable networks.** Attackers first gained administrative access of the compromised information system by Remote Desktop Protocol (RDP) exploit, and then manually disable any security software before executing the malware. This made the malware difficult to be detected and removed. It was reported that there were 67 different SamSam targets predominately located in the US in 2018, and the situation would be continued in the year of 2019. System administrators should take precautionary actions such as disabling all unnecessary RDP services and access, or applying protection measures if RDP access was genuinely needed.

- **PowerShell itself was not a malware, but it could be misused by attackers to conduct malicious operations.** It was commonly used together with macro scripts in malicious Office documents or VBScript in PowerShell attack. It was expected this kind of attack would be more common owing to the high success rate of its fireless nature.

[8] https://resources.malwarebytes.com/resource/under-the-radar-the-future-of-undetected-malware/

Industry Insight on Cyber Security Threat Trends

Proofpoint:

Proofpoint published its **"Protecting People: A Quarterly Analysis of Highly Targeted Cyber Attacks"**[9] which revealed the threats of email, social media, and the web. The key findings were:

- **The number of email fraud attacks kept growing since Q3 2017.** The study compared the figures from Q2 2018 and Q3 2017 and observed the growth continued throughout the period. In Q3 2018, there were 36 email fraud attacks per targeted organisation on average, an increase of 4% and 80% when compared with Q2 2018 and Q3 2017, respectively.

- **Attackers targeted people at all career levels and their targets were always changing.** The study collected most-targeted email addresses from Fortune Global 500 companies. 40% of the highly targeted employees were contributors, 27% were managements, another 27% were upper managements and 6% were executives. 99% of the email addresses ranked as most targeted in this quarter report did not rank as such in last quarter. It revealed that the attackers could shift their targets from time to time.

- **Large and small organisations could be targeted by email fraudsters.** There was no relationship on the size of organisations and their chance of encountering email fraud attack.

- **Attackers changed the way they spoofed, from spoofing a wide range of identities to focusing on impersonating people with higher authority.** Despite there was an increase of the volume of email fraud, the number of spoofed identities dropped by 68% when compared with last quarter. Besides, credential phishing increased three-fold since last quarter and the number of emails with malicious URLs was far more than emails with malicious attachments.

- **The sender name displayed in more than 99% of fraudulent emails were fake**. User should check the actual sender address rather than the display name of email to prevent reading spoofed email. Email administrators should have sender authenticity checking mechamism in place and flagged suspicious email to draw users' attention. Moreover, email fraudsters fabricated timebound requests using subject with "Request", "urgent" and "payment", which accounted for 58% of fraudulent emails. Payroll-related scams increased by 549% compare to previous quarter.

- **Customer-support fraud, or angler phishing on social media increased 486% compared to Q3 2017.** Attackers used fake customer support accounts to con those seeking for assistance to phishing web sites for capturing credentials.

- **Web-based social engineering attacks were on the rise.** These attacks tricked users to download malware, visit phishing or malicious web sites by displaying fake antivirus or software updates notifications. It increased by 233% compared to previous quarter.

[9] https://www.proofpoint.com/us/resources/threat-reports/quarterly-threat-analysis

Industry Insight on Cyber Security Threat Trends

FORTINET:

Fortinet published its **"Quarterly Threat Landscape Report"**[10]. The report reviewed trends of infrastructure, exploit, malware and botnet in Q3 2018. The report summarised the statistics of billions of threat events observed by devices around the world. The findings were:

- **Infrastructure Trends.** Over 72% of web browsing traffic were encrypted using HTTPS. The increased adoption of encryption was probably due to an increased need for secure communication channel. However the encryption could impose challenges to threat monitoring and detection as well. The usage of cloud applications also increased. Users should ensure their cloud resources were properly managed and protected.
- **Exploit Trends.** The exploit threats increased in Q3 2018. The top 3 most popular exploits were the Apache Struts exploit which related to the Equifax breach; the exploit against a PHP vulnerability first found in 2012 and the exploit targeting the buffer overflow bug in WebDAV service of Microsoft IIS 6.0 which was found being used for distribution of Cryptojacking malware. Internet of Things (IoT) exploits increased during Q3 2018 which included various consumers use Routers, IP Camera, Digital/Network Video Recorder (DVR, NVR), Network Attached Storage (NAS), Telephony and Printers. Attacks to industrial IoT devices on Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) technologies were less than consumer devices. However, the potential impact was higher for its value to disrupt business operations.
- **Malware Trends.** The malware activity increased in Q3 2018. Cryptojacking accounted for 19.31% of malware detected. There were much more mobile malware in Android than iOS platform, and variants of Android mobile malware had very high activity in Q3, 2018. The report also revealed the VPNFilter threat were still evolving. Threat actors added seven additional modules for various malicious activities in Q3 2018.
- **Botnet Trends.** The botnet activity also increased in Q3 2018. The seven most popular botnets were the same as Q2 2018. They were Gh0st, Pushdo, Andromeda, Necurs, Sality, ZeroAccess and Conficker. There was new development in IoT botnets that switched from centralised command and control infrastructure to decentralised one via peer to peer (P2P) protocol. IoT botnets would keep growing and spreading. It might use machine learning to refine itself for seeking the most efficient exploits and most vulnerable devices.
- **Recommendations.** The report suggested users and administrators to keep abreast of threat information, review vulnerability status in their environment, secure their IoT devices and systems, review system processess, implement mobile security strategies, and so on, in order to maintain a healthy computing environment in their organisations.

[10] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf

Industry Insight on Cyber Security Threat Trends

FireEye:

FireEye published its **"Facing Forward: Cyber Security in 2019 and Beyond"**[11]. The report summarised views from security experts on the cyber security arena in 2019 as below:

- **Increasing nation-state offensive activities would be expected.** It was observed that the nation-state threat actors became more aggressive in launching cyber operations.
- **Breaches would continue to grow**, as currently there was seldom deterrent to the attackers and they would continue to victimise their targets.
- **Growth of supply chain attack.** Small to medium-sized enterprises (SMEs), which were also supply chains for larger companies, did not have sufficient security resources. When these SMEs were compromised, the supply chains were compromised. Moreover, it was also attractive to attackers as they could infect multiple targets and was difficult to be detected.
- **Insufficient manpower to fill the increasing cyber security job vacancy.** This would lead to less experience or skilful personnel filling security roles.
- **The cloud platform attracted interest from attackers.** More companies migrated their data to the cloud platform. However, the protection to their cloud platform were found insufficient, leaving more opportunities to the attackers. Organisations should focus on business logic and visibility of operation, and always grasp the information on users' action.
- **More attacks on E-commerce web sites and online banking portals would be expected.** Number of gift card fraud would also increase.
- **Business Email Compromise (BEC), or CEO fraud, would be more commonly used by attackers.** All kinds of phishing attacks would continue to be used as they were hard to defend. Users should pay extra attention to check if email was genuinely sent by the sender.
- **Threat actors would use new techniques to evade detection.** They could commingle threat activities with normal network activities, use misleading data to confuse machine learning security solutions or use new evasion methods to overcome sandbox environments.
- **Threat activities related to Tokyo 2020 Olympics would be expected.** These activities included phishing, fake ticket websites, Distributed Denial of Service (DDoS) and ransomware attacks targeting organisations and industries related to the Olympics.
- **In longer terms, the development of artificial intelligence (AI) and quantum computing could have significant impact to cyber security.** New types of attack could emerge. Increase in computation power could greatly reduce the time to break the encryption which was considered as secured nowadays.

[11] https://content.fireeye.com/predictions/rpt-security-predictions-2019

Summary of Microsoft December 2018 Security Updates

13 Product Families with Patches

7 Critical

6 Important or below

Product Family	Impact[12]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4471332, KB4471324, KB4471329, KB4471321 and KB4471323.
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4471321, KB4471323, KB4471324 , KB4471327, KB4471329, and KB4471332.
Windows Server 2016, 2019 and Server Core installations 2016, 2019, v1803, v1709	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4471321; Windows Server 2019: KB4471332.
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4471318, KB4471319, KB4471320, KB4471322, KB4471325, KB4471326, KB4471328 and KB4471330.
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4471325, KB4470199, IE 10: KB4470199, KB4471330 IE 11: KB4470199, KB4471318, KB4471320, KB4471321, KB4471344723, KB4471324, KB4471327, KB4471329, and KB4471332
Microsoft .NET Framework	Remote Code Execution	Critical ★★★★	.NET Framework security update release
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	KB4092468, KB4092472, KB4461465, KB4461541, KB4461548, KB4461549, KB4461558 and KB4461580.
Microsoft Exchange Server	Tampering	Important ★★★	KB4468741
Microsoft Dynamics NAV	Spoofing	Important ★★★	KB4479232 and KB4479233.

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

Product Family	Impact[12]	Severity	Associated KB and / or Support Webpages
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010, 2013, 2016, 2016 for Mac, 2019, 2019 for Mac, Compatability Pack: KB3114565, KB4022232, KB4022237, KB4032218, KB4461518, KB4461524, Click to Run, Office for Mac; Office 365 ProPlus: Click to Run; Microsoft Online Server: KB4011027; Microsoft Excel 2010, 2013, 2013RT, 2016, Viewer: KB4461542, KB4461559, KB4461566 and KB4461577; Excel Services: KB4461569; Microsoft Project 2010, 2013, 2013RT, 2016, Viewer: KB2597975, KB4461481, KB4461521 and KB4461532; Microsoft Outlook 2010, 2013, 2016: KB4461576, KB4461556 and KB4461544; Microsoft Office 2010, 2016 for Mac, 2019, 2019 for Mac, Office Compatibility, Web Apps 2010, Web Apps 2013: KB2965312, KB4011207, KB4461551, KB4461565, KB4461570 and Click to Run.
Microsoft Visual Studio	Elevation of Privilege	Important ★★★	KB4469516.
Windows Azure Pack	Remote Code Execution	Important ★★★	KB4480788.

Learn more:
High Threat Security Alert (A18-12-03): Multiple Vulnerabilities in Microsoft Products (December 2018) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=347)

Sources:

- Microsoft December 2018 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/6c54acc6-2ed2-e811-a980-000d3a33a34d)