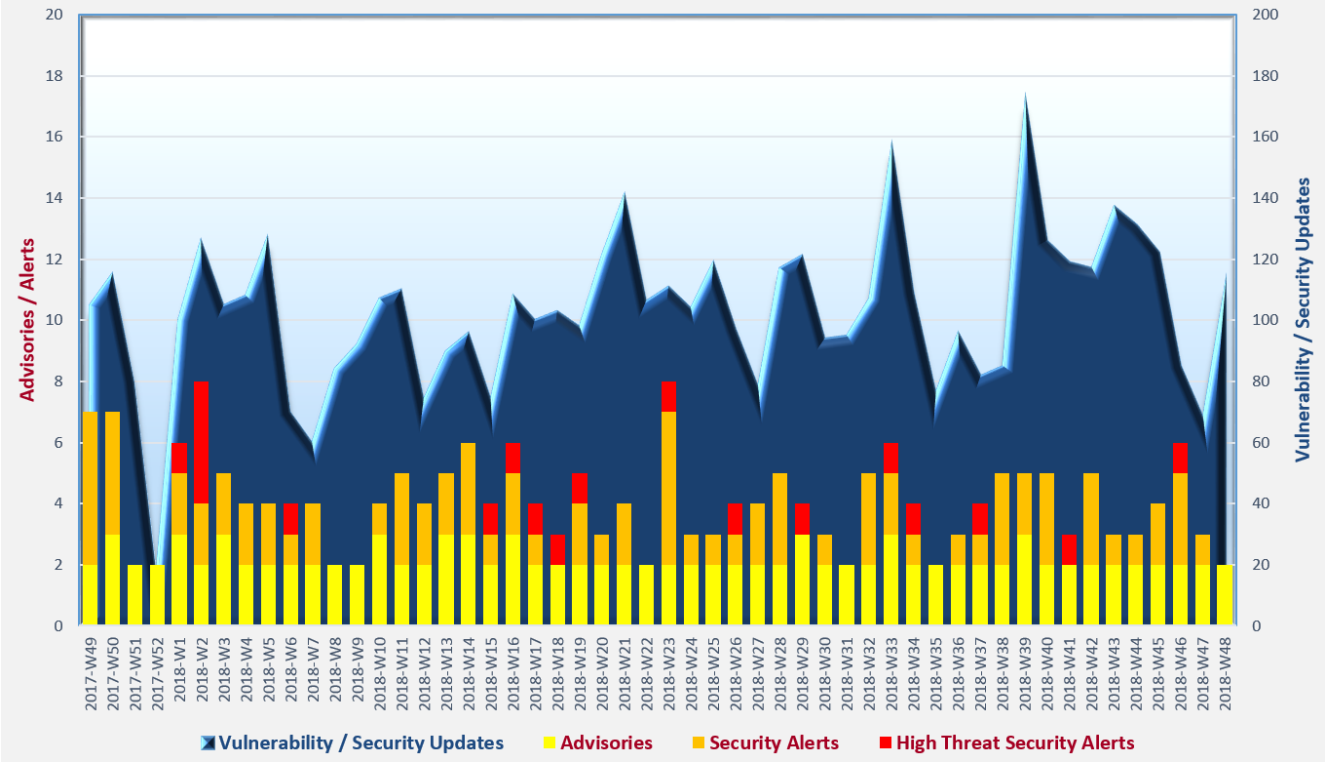
TLP:WHITE

Cyber Security Threat Trends 2018-M11

November 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:

- ✧ **Data breach** affecting personal information continues to happen. Organisations should review how sensitive information is stored and flowed across their systems to mitigate the risks**.**
- ✧ **Ransomware and cryptomining malware** are targeting both individuals and businesses. Cyber security hygiene and best security practises help protect Internet users at home and offices.
- ✧ **Phishing** attacks are getting more sophisticated. Anti-phishing campaigns demanding high user awareness and well-trained responses should become more essential than ever.

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

CERT Advisories

HKCERT[2] issued an advisory in response to the report that mentioned 257,256 Facebook user profiles were compromised and 81,208 private messages were leaked. Users were reminded to take security measures to protect their accounts including use two-factor authentication, install software from trusted sources, etc.

HKCERT[3] issued an advisory regarding the security incidents related to mobile payment. Users were reminded to take security measures in using email service such as use strong password and two-factor authentication, check the login activity of their accounts, beware of suspicious or phishing email, and so on.

HKCERT[4] issued an advisory about the sensitive data leakage of an online application system of a sport event. Organisations and web application developers were reminded of the importance of securing web applications and protecting privacy. They should also adopt "Security and Privacy by Design" in software development and follow PCPD's Six Data Protection Principles ("DPPs").

US-CERT[5] published on its website a security tip on the protection of public-facing websites from cyberattacks. The best practices include implementing the principle of least privilege, using multifactor authentication, do not use default vendor usernames and passwords, disabling unnecessary accounts, and so on.

[2] https://www.hkcert.org/my_url/en/blog/18110301
[3] https://www.hkcert.org/my_url/en/blog/18110901
[4] https://www.hkcert.org/my_url/en/blog/18111001
[5] https://www.us-cert.gov/ncas/tips/ST18-006

Industry Insight on Cyber Security Threat Trends

Group-IB:

Group-IB published its **"Hi-Tech Crime Trends 2018"**[6] which analysed the global cybercrime trends and forecast on hardware and firmware vulnerabilities, sabotage and espionage activities, targeted attacks on banks, attacks on bank clients, and threats to cryptocurrency and blockchain projects. The key observations were:

- **Hardware, firmware vulnerabilities, and related side-channel attacks emerged as a new security threat.** Examples of hardware vulnerabilities included Meltdown, Spectre, TLBleed, Rowhammer, etc. were mentioned. Proof of Concepts (PoCs) on exploits for these vulnerabilities already existed. The study forecast that the number of such attacks would increase.

- **On sabotage and espionage, Southeast Asia was the region being attacked most.** Windows, Mac OS and other mobile operating systems were all being targeted by hackers. Open-source tools and new techniques were used to hide the connection with Command and Control (C&C) servers, making detection and analysis more difficult. Moreover, hackers increasingly targeted vulnerabilities in home routers and spent a lot of resources on zero-day exploits.

- **Several APT groups were found targeting on banks.** These groups included Silence, MoneyTaker, Lazarus, and Cobalt, who infiltrated into the victim banks' networks, gained access to their isolated financial systems, and withdrew money via different channels embracing interbank transfer system to automatic teller machines (ATMs).

- **Attacks on bank clients were observed worldwide.** Card data of about 686,000 compromised bank cards and 1.1 million card dumps were available for sale every month. On the other hand, new banking Trojans kept being discovered. It was expected that the use of self-propagating Trojans would continue to increase. Besides PC based Trojans, Android banking Trojans such as Exobot 2.0, Cannabis, Loki v2, etc. were also mentioned in the report. These Trojans could propagate via SMS/MMS messages, while Exobot 2.0 could be distributed by some dropper apps in Google Play store.

- **There were threats to cryptocurrency and blockchain projects too.** 14 cases of hacking on cryptocurrency exchanges were reported from January 2017 to September 2018, causing a total loss of US$ 882 million. In the first half of 2018, there were five successful attacks where hackers controlled more than 51% of the network mining power and captured control of the cryptocurrency.

[6] https://www.group-ib.com/resources/threat-research/2018-report.html

Industry Insight on Cyber Security Threat Trends

Tenable:

Tenable published its **"Vulnerability Intelligence Report"**[7] which outlined the vulnerability trends, and the insights on how organisations assess and respond to the vulnerabilities:

- **The number of new vulnerabilities kept growing since 2016.** The study compared the figures from 2016 to 2018 and observed the growth continues throughout recent years. In the first half of 2018, an increase of around 27% was observed when compared to the first half of 2017. The number was estimated to be around 18,000–19,000 by end of 2018. The study also projected that around 8% of the Common Vulnerabilities and Exposures (CVEs) would have public exploits available.

- **Same vulnerability may have different classifications in Common Vulnerability Scoring System version 2 (CVSSv2) and version 3 (CVSSv3).** CVSSv3 was published in June 2015 and intended to replace CVSSv2. There were some differences on the way the two versions classify a vulnerability. When comparing those CVEs with both CVSSv2 and CVSSv3 scores available, it was found that CVSSv3 rated 60% of them with severity High or Critical, while CVSSv2 only classified 31% of them as High. Moreover, some CVEs rated as Medium in CVSSv2 became High or Critical in CVSSv3.

- **There are 22,625 distinct vulnerabilities and 23% of them were found impacting enterprises.** An organisation would face 870 vulnerabilities every day. 61% of the vulnerabilities had a CVSSv2 score of 7.0 or above and 12% got a score of 9.0 or above. Even if an organisation only remediated vulnerabilities scoring higher than 9.0, there were still be more than a hundred vulnerabilities to be handled per day.

- **Old, legacy, unused, discontinued and end-of-life software should be removed.** The study revealed that a number of years-old vulnerabilities were found in web browsers (e.g. Firefox, Microsoft Internet Explorer, etc.) or applications (e.g. Oracle Java, Adobe Flash, Microsoft Office, etc.), due to the existence of unmanaged, dormant versions of the software. The report recommended that system administrators should remove these obsolete versions of software. The study also revealed that 27% of organisations were still using the insecure SSLv2 and SSLv3. These insecure protocols should be disabled. 63% (675 out of a total of 1,065) web browser vulnerabilities had a high severtity. Users should upgrade their web browsers to the latest versions to ensure that all known vulnerabilities are patched timely.

[7] http://static.tenable.com/translations/en/Vulnerability_Intelligence_Report-ENG.pdf

High-Tech Bridge:

High-Tech Bridge published its **"Abandoned Web Applications: Achilles' Heel of FT 500 Companies"**[8]. Their analysis results were based on the data collected from various Internet resources for the 1,000 companies rated by the Financial Times as FT US 500 and FT Europe 500. The findings were:

- **For proper configuration, patching and security management, business owners should have correct and up-to-date inventory on all IT assets.** IT assets could be classified into:

  Shadow IT - system built for legitimate business purposes but poorly maintained and protected due to no proper coordination with IT security and central management staff;

  Legacy IT - systems built long time ago and still in operation to serve legitimate business purposes but without proper maintenance due to complexity, and lack of resources, skills or knowledge; and

  Abandoned IT - systems built for legitimate business previously but forgotten and cast aside.

- **Exploitable SSL/TLS vulnerabilities** – Almost 30% of the companies under study have at least 2 servers exposed to these vulnerabilities. System owners should ensure the latest security protocols with proper configuration and implementation have been used.

- **Expired or untrusted SSL certificates or domain names** – More than 30% of the companies under research were using invalid SSL certificates such as certificates issued by untrusted Certificate Authority (CA) or expired certificates. **More than 40% of the 1,000 companies had one or more web applications that referred to external resources such as Javascript library, image, font, etc. on expired or non-existing domain names.** If threat actors registered these domain names, they could seize the opportunity to place malicious codes or contents to the web applications.

- **Around 77% of the companies under study failed to harden their web servers properly.** More than 8% of the web applications were using outdated or vulnerable Content Management Systems (CMS) or libraries. For those web applications running WordPress, over 94% were using the default admin location (i.e. adding /wp-admin at the end of URL of the web site) without additional protection measures, making them more vulnerable to attacks. Moreover, more than 98% of the web applications were either not protected by Web Application Firewalls (WAFs) or using improperly configured WAFs.

- **19% of the companies used external cloud storage without authentication.** Strong authentication and access control should be enforced for external cloud storage to avoid data leakage.

[8] https://www.htbridge.com/blog/FT500-application-security.html

Industry Insight on Cyber Security Threat Trends

AGARI:

The AGARI published its **"Q4 2018 Email Fraud & Identity Deception Trends"**[9] reporting email fraud trends from July to October 2018 including inbound attacks against businesses and outbound attacks against their customers through domain spoofing and phishing. The key observations were:

- **Inbound Attack – Display Name Deceptions dominate.** In 54% of the cases, Display Name Deception with impersonated brands was used in the attack. These emails had looking friendly and trustable senders such as "Support Team" and reasonable subjects. For attacks targeting executives, Microsoft was the most common brand (more than 70% of attacks) being impersonated. Dropbox was in the second place, probably due to their file sharing service making it "natural" to have link in the email body, and cybercriminals could use the link to entice user to access files embedded with malware.

- **Inbound Attack – Look-a-like Domain.** 35% of the attack cases used email with look-a-like domain. Manufacturing and logistics/transportation sectors received the most attacks on the type of look-a-like domain when compared with other industry sectors.

- **Outbound Attack – Defence.** Email authentication standard, Domain-based Message Authentication, Reporting and Conformance (DMARC), could help email exchange to recognise whether an email was coming from approved domains. DMARC also instructs how to handle those unauthenticated email. As of October 2018, more than 5.3 million domains had adopted DMARC.

- **Outbound Attack – Analysis.** It was found that for the Fortune 500 companies in US, almost 49% of them did not publish DMARC policy, only 5% of them had implemented quarantine policy (put in spam folder), and 8% implemented Reject Policy (blocking). For FTSE 100 (top 100 companies listed on the London Stock Exchange) and ASX 100 (top 100 large and mid-cap securities in Australia's stock market index), 56% and 60% of them did not have DMARC policy, 1% (for both) had Quarantine Policy, and 9% and 7% had Reject Policy respectively. The importance of DMARC could be shown by the experience of a public-listed global ecommerce company. Before DMARC was implemented, it received more than 100 million email impersonating its brand every day. After the implementation of DMARC, 99% of these emails have been blocked.

[9] https://www.agari.com/bec/whitepapers/Agari_Q4_EmailFraudTrends_20181031.pdf

Summary of Microsoft November 2018 Security Updates

16 Product Families with Patches

10 Critical

6 Important or below

Product Family	Impact[10]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4467708, KB4465664, KB4467702, KB4465663, KB4467686, KB4465661, KB4467696, KB4465660, KB4467691, KB4465659, KB4467680 and KB4093430.
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4467708, KB4467702, KB4467686, KB4467696, KB4467691 and KB4467680.
Windows Server 2016, 2019 and Server Core installations 2016, 2019, v1803, v1709	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4467691, KB4465659; Windows Server 2019: KB4467708, KB4465664.
Windows 8.1 and Windows Server 2012 R2	Remote Code Execution	Critical ★★★★	KB4467697, KB4467703 and KB3173424.
Windows Server 2012	Remote Code Execution	Critical ★★★★	KB4467701, KB4467678 and KB3173426.
Windows RT 8.1	Remote Code Execution	Critical ★★★★	KB4467697, KB4467703.
Windows 7 and Windows Server 2008 R2	Remote Code Execution	Critical ★★★★	KB4467107, KB4467106 and KB3177467.
Windows Server 2008	Remote Code Execution	Critical ★★★★	KB4467706, KB4467700 and KB3020369.
Microsoft Dynamics 365	Remote Code Execution	Critical ★★★★	Dynamics 365 documentation.
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore

[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
Internet Explorer	Remote Code Execution	Important ★★★	IE 9: KB4467706, KB4466536 IE 10: KB4467701, KB4466536 IE 11: KB4467107, KB4467697, KB4466536, KB4467686, KB4467708, KB4467691, KB4467696, KB4467702, KB4467680, KB4465661, KB4465664, KB4465659, KB4465660 and KB4465663.
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 Word 2010, 2013, 2016: KB4461526, KB4461485, KB4461504; Microsoft Excel 2010, 2013, 2016, Viewer: KB4461530, KB4461488, KB4461503, KB4461519; Excel Services: KB4011190; Microsoft Project 2010, 2016, Server 2013: KB4022147, KB4461478, KB4461489; Microsoft Outlook 2010, 2013, 2016: KB4461529, KB4461486, KB4461506; Microsoft Office Web Apps 2010, Server 2013: KB4461527, KB4092473.
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	KB4461520, KB4461501, KB4461483, KB4461513 and KB4461511.
Microsoft Exchange Server	Elevation of Privilege	Important ★★★	CVE-2018-8581.
PowerShell Core	Remote Code Execution	Important ★★★	PowerShell Core, GitHub.
Team Foundation Server	Spoofing	Important ★★★	Azure DevOps Server documentation.

Learn more:

High Threat Security Alert (A18-11-04): Multiple Vulnerabilities in Microsoft Products (November 2018) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=340)

Sources:

- Microsoft November 2018 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/ff746aa5-06a0-e811-a978-000d3a33c573)