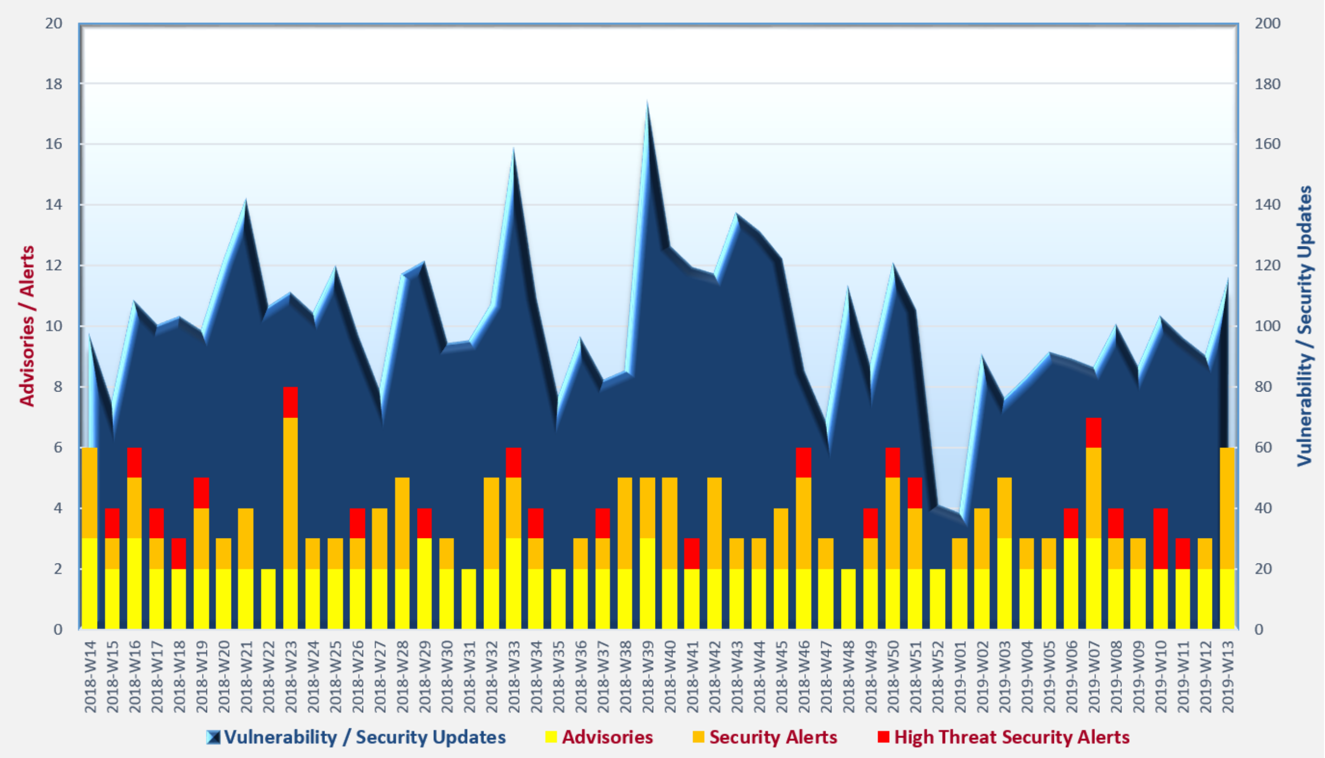
Cyber Security Threat Trends 2019-M03

March 2019

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:

- ✧ **Account compromise** thrives with voluminous passwords leaking from misconfigured open databases and massive identity breaches. Multi factor authentication and privileged access management should be the keys to the defence.
- ✧ **Extensible components** including add-on modules and plugins, become popular attack targets as underlying software. Timely patching and secure configurations should be enforced.
- ✧ **Malware** is more agile to develop new variants to evade detection and add the capabilities. Enterprises should implement multi-layers of security protection to mitigate the growing risks.

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

CERT Advisories

Facebook stored user passwords in plain text. Users were advised to change their passwords for Facebook and Instagram accounts

Facebook confirmed that the company stored hundreds of millions account passwords in plain text format on their internal company servers. This implied that more than 20,000 Facebook employees could access these passwords. HKCERT[2] advised users should change their Facebook and Instagram account passwords, and should not reuse the same password for other online services. Besides, users should use strong passwords for all accounts.

Organisations and end users should take actions to protect against credential stuffing and password spraying attacks

SingCERT[3] noticed an increase in credential stuffing and password spraying attacks successfully compromising user accounts. End users were advised to use strong and different passwords for different online accounts, periodically change their passwords and if possible, use multi-factors authentication. System owners were advised to perform regular checking on their systems including check and remove user accounts that were unauthorised, suspicious, or inactive; monitor for multiple unsuccessful login attempts; and so on.

Patch your Google Chrome

GovCERT.HK[4], Australian Cyber Security Centre (ACSC)[5], MyCERT[6], SingCERT[7] and US-CERT[8] issued alerts on a vulnerability of Google Chrome which has been exploited in the wild. Successful exploitation could allow attackers to run arbitrary code on the affected system. Users were advised to update their Google Chrome immediately.

[2] https://www.hkcert.org/my_url/en/blog/19032201
[3] https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-credential-stuffing-and-password-spraying-attacks
[4] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=370
[5] https://cyber.gov.au/business/news/chrome-security-update/
[6] https://www.mycert.org.my/en/services/advisories/mycert/2019/main/detail/1333/index.html
[7] https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-critical-vulnerability-cve-2019-5786-in-google-chrome
[8] https://www.us-cert.gov/ncas/current-activity/2019/03/07/Google-Releases-Security-Updates-Chrome

Industry Insight on Cyber Security Threat Trends

Fortinet's Threat Landscape Index reached a record high in the 4th quarter but subsided toward 2018 year end

Fortinet analysed billions of threat events and incidents collected and presented their findings on exploit trends, malware trends and botnet trends in its publication "Threat Landscape Report Q4 2018"[9]. The report also recommended some measures to cope with the ever changing cyber threat landscape nowadays. The key contents were:

- **Despite Fortinet's Exploit Index dropped 0.3% as compared with last quarter, the unique exploits detected and the exploits detected per firm grew by 5% and 10% respectively.** The top detected exploit remained the Apache Struts exploit related to CVE-2017-5638. Moreover, six out of the twelve most prevalent exploits targeted Internet of Things (IoT) devices.

- **Fortinet's Malware Index dropped by 4.3%, with unique variants dropped 1.5% and cryptojacking malware dropped 1%.** The most prevalent malware variant detected was an adware, with more detections in Northern America, Oceania and Europe. At the second place was Coinhive, which was used for mining cryptocurrency, with more detections in Latin America and Middle East. The third one, W32/Agent.AJFK!tr, was a keylogger/downloader Trojan, and was mostly detected in Middle East, Asia and Europe.

- **Fortinet's Botnets Index dropped by 1.5% but the unique botnets detected, infection days per firm and average volume per day/firm increased by 2%, 15% and 7% respectively.** Gh0st was the most prevalent botnet and leaded the second place by a wide margin.

- **Open source tools were weaponised by the cyber-criminals.** Sharing of malware information, for example, the availability of proof-of-concept ransomware or Trojan, could facilitate cyber security professionals to perform testing and analysis. However, adversaries could also utilise these open resources to perform malicious activities.

- **Threat actors used steganography to perform malicious acts.** They hid the payloads in social media memes. Examination on the malware samples indicated that, besides trying to contact Command and Control host, the malware also tried to download images from social media feeds and search for commands hidden within the images for malicious activities.

- **Organisations were recommended to implement multiple layers of security protection.** They could consider measures such as monitoring system processes and stopping those suspicious resource-consuming processes, using separate network segments for IoT devices and production network, proactively reducing external accessible attack surface, and so on.

Source: Fortinet

[9] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q4-2018.pdf

Industry Insight on Cyber Security Threat Trends

WordPress was the most infected website content management system (CMS) and Search Engine Optimization (SEO) spam related attacks increased in 2018

Sucuri analysed 18,302 infected websites and more than 4.4 million cleaned files, and published their study results on the latest trends, and tactics, techniques and procedures (TTPs) on attacks to website CMS in its "Hacked Website Report 2018"[10]. The major observations in the report were:

- **WordPress was the most hacked (90%) CMS in 2018.** The next came Magento (4.6%), Joomla! (4.3%), and Drupal (3.7%). As a comparison, the figures for these four CMS in 2017 were 83% (WordPress), 6.5% (Magento), 13.1% (Joomla!) and 1.6% (Drupal). Most of the infections to the CMS were rooted from the vulnerabilities of the add-on modules, plugins, themes and extensions and other factors such as improper deployment or security configuration, lack of security knowledge or resources, issues on website maintenance and broken authentication and session management.

- **44% of CMS were found to be out-of-date (i.e. not patched with the latest version) in 2018.** The top 5 outdated infected CMS were PrestaShop (97.2%), OpenCart (91.3%), Joomla! (87.5%), Magento (83.1%), and phpBB (72.6%). For WordPress, the most hacked CMS product, the figure was only 36.7%. This could be related to the auto-update features of WordPress. However, the extensible components of WordPress (e.g. plugins) were very often the primary attack vectors. For Drupal, the fourth most hacked CMS, 63.1% of them were found outdated.

- **PHP-based backdoors were found in 68% of all hacked sites.** The second and third places on this infection trend analysis were browser-side malware code to create drive-by downloads (56.4%) and SEO spam (51.3%) respectively. SEO attacks injected spam content to the victim websites, or redirect visitors of the victim websites to other spam webpages.

- **The analysis found the top 3 files modified by malware in compromised websites: "index.php" (34.5%), "functions.php" (13.5%) and "wp-config.php" (10.6%).** All these files have some common properties making them mostly targeted by attackers: they were loaded every time the websites were accessed; they were core files which were not replaced by WordPress update; and they were more likely ignored by file integrity monitoring systems.

Source: Sucuri

[10] https://sucuri.net/reports/19-sucuri-2018-hacked-report.pdf

Industry Insight on Cyber Security Threat Trends

Study revealed after Internet of Things (IoT) devices were connected to the Internet, they were under attack within five minutes.

Findings on the trends on attacks targeting IoT devices, Distributed Denial of Service (DDoS) attacks, Commercialisation of Crimeware and advancement of state actors were included in the "NetScout Threat Intelligence Report"[11]. The report revealed that the attackers improved their strategies and attack efficiency, and adopted better business models to expedite their rate and coverage of attack. The key findings from the report were:

- **IoT devices were subject to brute-force attack on usernames and passwords within five minutes after they were online in the Internet.** Besides, they were aimed by specific exploits within 24 hours. Attackers used readily available lists of factory default usernames and passwords to conduct the brute-force attack and infected the devices with malware after they gained access to the devices successfully. Administrators of the devices should change the factory default passwords as early as possible. A trend has been observed that attackers were using their experience in attacking IoT devices to attack other Linux servers.

- **The number of DDoS attacks in the second half of 2018 was increased by 26 percent compared to the same period of previous year.** Regarding the attack size, although there was no new record on the maximum attack volume, attacks in the range of 100–200 gigabits per second (Gbps), 200–300 Gbps and 300–400 Gbps grew rapidly by 1.69 times, 25 times, and 36 times respectively. In the second half of 2018, Asia Pacific region and EMEA (Europe, the Middle East and Africa) region encountered 37 and 2 DDoS attacks over 400Gbps respectively.

- **Attackers diversified their DDoS attacks portfolio.** The number of attacks of some previously less used amplification attack types were found increased in the second half of 2018. The attack size of some of these less used types also grew significantly. For example, the number of attacks using mDNS amplification increased by 233%, and the maximum attack size rose remarkably from 8.28 Gbps to 186 Gbps. On the other hand, both the attack frequency and volume of some amplification attack types commonly used previously (DNS, NTP, and Chargen) dropped in the same period.

Source: NetScout

[11] https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901 - NETSCOUT Threat Intelligence Report 2H 2018.pdf

Industry Insight on Cyber Security Threat Trends

Identity breaches from government sector grew the most in 2018, up 291% from 2017

Security vendor 4iQ collected identity breaches and leaks cases from both open domains as well as from the deep web and dark web. Analysis on collected information indicated that in 2018, the attacker not only targeted those large companies, but also attacked those small businesses and supply chain vendors that had fewer resources on security protection. The findings were published in the "2019 4iQ Identity Breach Report"[12]. The following were highlights from the report:

- **There were 12,449 new authentic breaches and leaks in 2018, which increased by 424% as compared with 2017.** However, the average breach size was 216,884 records in 2018, which was 4.7 times smaller as compared with 2017, indicating there was a shift of trending to more but smaller scale breaches.

- **There were 14.9 billion raw identity records found in the Internet in 2018, which increased by 71% as compared with 2017.** Out of these records, 3.6 billion were found to be real and new, which increased by 20% than that of 2017. The exposed identity information were used in illegal activities, such as business email compromise, account takeover, etc.

- **The number of identity breaches from public sector increased by 291%.** The exposed citizen data included voter records, citizen identity information, Identity Card and passport images, tax return data, etc. There was a rising trend that threat actors combined personal identifiable information (PII) from various sources and packaged the information for sale.

- **These was a keen increase in the distribution of "Password Combo List" (i.e. username and password databases) in 2018.** The information could be used by attackers to launch automatic brute-force attacks on website authentication, taking the chance users re-using the same password for different websites.

- **There were 9.4 billion records, or 18.9 GB storage, leaked from open devices and databases in 2018.** Organisations left their databases or servers open to the Internet. Threat actors could make use of automated crawlers to discover these opened database and obtain the data. System administrators should well protect their databases and minimise the attack surface as much as practicable.

Source: 4iQ

[12] https://4iq.com/2019-identity-breach-report/

Summary of Microsoft March 2019 Security Updates

10
Product Families with Patches

6
Critical

4
Important or below

Product Family	Impact[13]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4489868, KB4489871, KB4489872, KB4489882, KB4489886, KB4489899
Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1709)	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4489882 Windows Server 2019: KB4489899 Windows Server v1803: KB4489868 Windows Server v1709: KB4489886
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4474419, KB4489876, KB4489878, KB4489880, KB4489881, KB4489883, KB4489884, KB4489885, KB4489891
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4489871, KB4489872, KB4489868, KB4489882, KB4489886, KB4489899
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4489873, KB4489880 IE 10: KB4489873, KB4489891 IE 11: KB4489868, KB4489871, KB4489872, KB4489873, KB4489878, KB4489881, KB4489882, KB4489886, KB4489899
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore
.NET Core SDK, Nuget, and Mono Framework	Tampering	Important ★★★	.NET Core, Mono Framework, Nuget
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010 SP2: KB4462226 Microsoft Lync Server 2013: KB2809243 Microsoft SharePoint Enterprise Server 2016: KB4462211 Microsoft SharePoint Foundation 2013: KB4462208 Skype for Business Server 2015: KB3061064

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

Product Family	Impact[13]	Severity	Associated KB and / or Support Webpages
Microsoft Visual Studio	Remote Code Execution	Important ★★★	Microsoft Visual Studio 2017: CVE-2019-0809 Visual Studio for Mac: CVE-2019-0757
Team Foundation Server	Spoofing	Low ★	Azure DevOps Server

Learn more:
High Threat Security Alert (A19-03-03): Multiple Vulnerabilities in Microsoft Products (March 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=371)

Sources:

🗎 Microsoft March 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/ac45e477-1019-e911-a98b-000d3a33a34d)