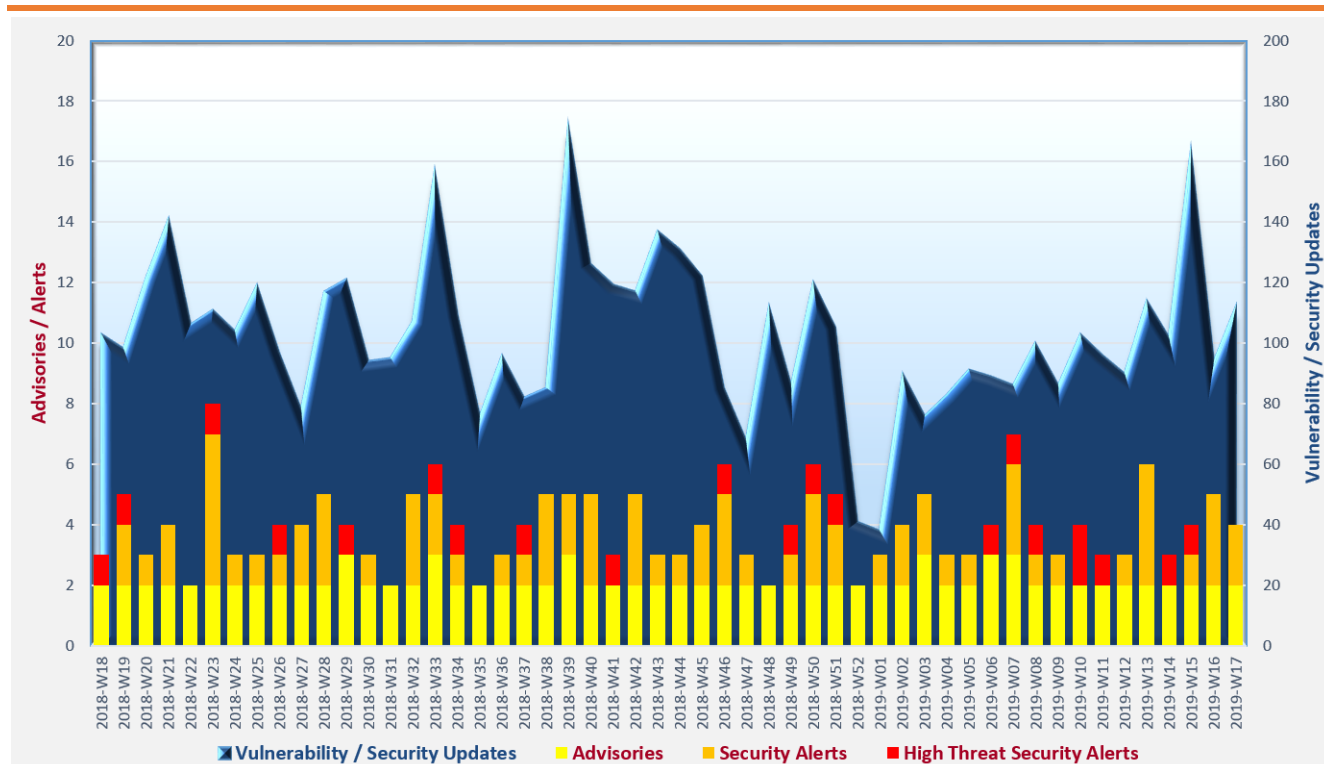


Cyber Security Threat Trends 2019-M04

April 2019

With reference to the FIRST Traffic Light Protocol (TLP) standard¹, 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:

- ✧ **Ransomware** grows in attacks on businesses. Organisations should improve security awareness of their staff in defence against attacks via phishing emails and malicious websites.
- ✧ **Botnets** are actively built up by criminals to launch cyber attacks or for sale to do so. Owners of Internet-facing devices should secure their systems from being compromised into bots.
- ✧ **User credentials** are favourable attack targets since they are keys to gain unauthorised access. System administrators should enforce strong password policy and multi-factor authentication to minimise the risk of credential stealing.

¹ <https://www.first.org/tlp/>

CERT Advisories



Users and organisations should take actions to protect against ransomware

US-CERT issued a Security Tip on protecting against ransomware². It provided a brief introduction on ransomware and the infection channels. Users should **back up computers files frequently and regularly, and store the backups in devices separated from the computers and networks** to protect data and networks against ransomware. To prevent ransomware infection, **application and operating systems should be updated and patched**. Users should be **cautious with links to websites and opening email attachments**. **Anti-malware software, email filters and firewalls should be used and properly maintained**.



Patch your Apache HTTP Server

GovCERT.HK³, HKCERT⁴, SingCERT⁵ and US-CERT⁶ issued alerts on multiple vulnerabilities of Apache HTTP Server which have been exploited in the wild. Successful exploitation of the vulnerabilities could lead to system crash, access control restrictions bypass, arbitrary code execution and privilege escalation on an affected system. System administrators were advised to **patch the affected Apache HTTP Servers immediately**.



Attackers are exploiting a remote code execution vulnerability in Oracle WebLogic Server. Patch your system immediately.

GovCERT.HK⁷, HKCERT⁸ and US-CERT⁹ issued alerts on a remote code vulnerability in Oracle WebLogic Server which has been exploited in the wild. Remote attackers could send specially crafted HTTP requests to exploit the vulnerability. System administrators should **patch the affected systems immediately**.

² <https://www.us-cert.gov/ncas/tips/ST19-001>

³ https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=377

⁴ https://www.hkcert.org/my_url/en/alert/19040302

⁵ <https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-privilege-escalation-vulnerability-cve-2019-0211-affecting-apache-web-server>

⁶ <https://www.us-cert.gov/ncas/current-activity/2019/04/04/Apache-Releases-Security-Update-Apache-HTTP-Server>

⁷ https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=383

⁸ https://www.hkcert.org/my_url/en/alert/19042603

⁹ <https://www.us-cert.gov/ncas/current-activity/2019/04/26/Oracle-Releases-Security-Alert>

CERT Advisories



There was a sharp increase in number of security events in Q1 2019, mentioned in the latest HKCERT quarterly report

HKCERT released its Hong Kong Security Watch Report (Q1 2019)¹⁰. There was a 389% increase in number of security events when compared with Q4 2018, which largely caused by a significant increase in malware hosting events. Detail analysis result on the trend for defacement, phishing, malware hosting and botnet were presented in the report.



Re-using password is risky. Users could check if the passwords they use are on the list of passwords disclosed in previous security breaches

The UK National Cyber Security Centre (NCSC) released a security blog¹¹ on password blacklists, explaining the reasons why password re-use was risky for both individuals and companies, and how the password blacklists could help on the area of password selection. A list of top 100,000 passwords from a security consultant's compromised password data set was included in the post. **Users were advised to change their passwords immediately if they could locate their passwords in the list.**

¹⁰ https://www.hkcert.org/my_url/en/blog/19043003

¹¹ <https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere>

Industry Insight on Cyber Security Threat Trends

Botnet-based attacks included not only Distributed Denial of Service (DDoS), but also stealing of information such as user credentials, credit card information, etc.

Kaspersky studied the commands collected from more than 60,000 Command and Control (C&C) servers and published the analysis results in its “Bots and botnets in 2018”¹² report. The report covered attacks which aimed to capture user credentials and card data, or perform malicious operations or transactions at the client machines of organisations. Major observations were:

- **The number of unique attacks detected in 2018 decreased by 23.46% as compared with 2017.** 39.35% of the detected attacks were new in 2018, due to the emergence of new banking Trojans such as Danabot and BackSwap, and the shift of threat actors’ targets.
- **Financial services, including online banking services and online stores, were the top targets of attacks in both 2017 and 2018.** Over 73% of attacks targeted these services in 2017 and 2018. Attacks targeted cryptocurrency services such as cryptocurrency exchanges, cryptocurrency wallets, etc. increased significantly from 2.3% in 2017 to 7.25% in 2018, making cryptocurrency services became the second most targeted by threat actors in 2018.
- **Organisations in the United States remained as the top attack targets in both 2017 (31.29%) and 2018 (34.84%).** The composition of the top 10 countries were the same in both 2017 and 2018, although the positions were different, except for the United States. There were conspicuous drops in number of unique attacks targeted Germany (from 11.15% in 2017 to 3.88% in 2018) and Australia (from 4.67% in 2017 to 2.29% in 2018) due to significant drop of attacks by some of the bots such as BetaBot for Germany and Gozi for Australia.
- **13.25% of the unique attacks were from BetaBot, the most active Trojan in 2018.** The malware targeted organisations in 42 countries, 73.6% of its targets were in US. Financial services, global portals and social networks were its most attacked targets. Trickster (also known as TrickBot), Panda, SpyEye and Ramnit ranked as the second to fifth places in terms of the most active Trojans in 2018 and accounted for 12.85%, 9.84%, 8.05%, and 7.97% of all unique attacks in 2018 respectively.

Source: Kaspersky

¹² <https://securelist.com/bots-and-botnets-in-2018/90091/>

Industry Insight on Cyber Security Threat Trends

In Q4 2018, the number of phishing attack campaigns and zero day malware increased. Number of detected malware increased in both the Americas (AMER) and Europe, the Middle East and Africa (EMEA) regions but declined in Asia-Pacific (APAC)

WatchGuard collected anonymised information on threat detected from 42,069 globally deployed appliances and summarised the latest malware and exploit trends observed from the collected threat data in its "Internet Security Report - Q4 2018"¹³. Samples of phishing and extortion email were also included in the report. The highlights from the report included:

- **Phishing attacks increased in Q4 2018.** Attackers used bank-related phishing emails or sextortion emails to entice users to click malicious links, visit fake web sites, open mal-formed attachments or pay ransom. In the example quoted in the report, attackers used alarming email subjects such as threatening the victims their accounts were hacked. They also spoofed the sender address in the email headers or showed the victims' password in the emails to make the emails appeared to be more "real". *Users were reminded to be cautious on links or attachments in the emails and examine the links carefully. Users should also be aware of extortion scams.*
- **Mimikatz, a password stealer, was the most detected malware in Q4 2018 (18% of total number of detections).** It mainly targeted AMER and EMEA regions. An increase in zero day malware was observed in Q4 2018. The malware was never seen before, and hence was more evasive from detection by signature-based anti-malware solution. *Organisations were recommended to, in addition to the traditional signature-based malware detection solution, adopt multi-layered approach on malware detection for better protection.*
- **EMEA recorded most malware detection (47.2%) in Q4 2018.** AMER and APAC recorded 35.4% and 17.4% respectively. As compared to Q3 2018, the number of malware in EMEA and AMER increased slightly, while that for APAC had a significant decrease.
- **Network attack (i.e. exploitation of vulnerabilities of network-accessible servers or client software) in Q4 2018 increased for 46% as compared with Q3 2018 in terms of attack volume.** "Remote File Inclusion /etc/passwd" attack, which aimed to steal user login information, was the top network attack (19.3%) in Q4 2018. There was also a sharp increase for the "Cisco WebEx Chrome Extension Remote Code Execution" attack, which targeted a vulnerability disclosed in 2017. Similar to the observations for malware detection, EMEA recorded the highest network attack volume (66%). The attack volume for AMER and APAC were 32.6% and 1.4% respectively.

Source: WatchGuard

¹³ <https://www.watchguard.com/wgrd-resource-center/security-report-q4-2018>

Industry Insight on Cyber Security Threat Trends

An 85% drop in Distributed Denial of Service (DDoS) average attack size in Q4 2018 was observed due to FBI crackdown on 15 large DDoS-for-hire websites

Nexusguard analysed threat information collected from sources such as attack data, research, open information, honeypots, logs, etc. and published the analysis results in its "DDoS Threat Report Q4 2018"¹⁴. The key observations in the report included:

- **The number of DDoS attacks, the maximum and average attack sizes in Q4 2018 were dropped by 10.99%, 23.91%, and 85.36% respectively when compared with Q4 2017.** The maximum and average attack sizes were 176 Gbps and 1.008 Gbps respectively. The sharp decline was mainly due to the takedown of 15 large DDoS-for-hire websites by FBI in December 2018.
- **On the contrary, compared with Q3 2018, the number of DDoS attacks, the maximum and average attack sizes increased by 36.08%, 49.15%, and 3.75% respectively.** It was due to the adoption of "Bit-and-Piece" technique by attacker, which bypassed detection by spreading attack traffic across large numbers of IP addresses.
- **SSDP (Simple Service Discovery Protocol) Amplification attack was the top attack vector (48.26 %) in Q4 2018, increased by 3,122.22% and 91.21% comparing with Q4 2017 and Q3 2018 respectively.** This kind of attacks had a bandwidth amplification factor of up to 30.8 times. The attacks were launched by sending malicious UDP packets to exploitable Universal Plug and Play devices, causing these devices to generate a large amount of replies to the attack target.
- **42.80% of the attacks lasted shorter than 90 minutes, but the maximum attack duration was 18 days, 21 hours and 59 minutes.** Average attack duration was 452.89 minutes. 15.58% of the attacks lasted for more than 1,200 minutes.
- **90.37% of the attacks were smaller than 1Gbps.** 6.47% of the attacks with attack size between 1Gbps and 10Gbps, and the largest attack size was 176 Gbps. The overall smaller attack size was related to the popularity of the "Bit-and-Piece" attack technique.
- **China (22.68%), the United States (18.01%) and France (7.06%) were the top 3 regions with the most attacks originated from.** If only considered sources from Asia Pacific area, the top 3 source regions were China (61.16%), Vietnam (9.52%) and India (7.33%).

Source: Nexusguard

¹⁴ <https://www.nexusguard.com/threat-report-q4-2018>

Industry Insight on Cyber Security Threat Trends

Compliance, coin mining, web-based attacks, and credential theft were the major cyber security challenges identified in 2018, and were expected to continue in 2019

NTT Security analysed global attack data collected from over 10,000 clients during October 2017 to September 2018. The analysis was presented in its "2019 Global Threat Intelligence Report"¹⁵. The observations of the report included:

- **Both finance sector and technology sector were the top targets of attacks in 2018, each of them accounted for 17% of total number of attacks.**
- **From the source of attack point of view, 22% of attacks were originated from IP addresses in the United States, making the region became the top source of global attack.**
- **General Data Protection Regulation (GDPR) became effective in 2018, it was expected that more similar regulations would be introduced. Organisations should adopt the data protection by design approach, and draw the Board's attention on the importance of data protection and regulation compliance.**
- **The number of coin mining detections increased by 459% from 2017 to 2018.** 75% of these attacks were host-based, meaning that the coin mining occurred on the system which the malicious application resided. The remaining 25% were web-based which consume the computation power of client machines visiting the infected websites. The report recommended defense measures such as **applying least privilege controls for different accounts, implementing firewall restrictions, limiting browser-based cryptomining, disabling Stratum protocol, segregating network environment**, and so on, to mitigate the threat.
- **The percentage of web-based attacks increased slightly from 29% in 2017 to 32% in 2018.** These attacks targeted vulnerabilities of organisations' Internet facing applications. The report recommended **adoption of effective patching mechanisms, segregation of network environment, adoption of secure coding practice, implementation of application gateway firewalls, and perform regular vulnerability scanning** as defensive measures.
- **67% of credential theft attacks used phishing as attack method, while the remaining 33% used credential stealing malware.** Organisations should consider implementing measures such as **multi-factor authentication, segregation of network environment, enforcing "least privilege" and segregation of duties, monitoring for data exfiltration or leakage, and conducting awareness training on phishing attacks.**

Source: NTT Security

¹⁵ <https://www.nttsecurity.com/en-uk/landing-pages/2019-gtir/2019-global-threat-intelligence-report-download>

Summary of Microsoft April 2019 Security Updates

12

Product Families
with Patches

6

Critical

6

Important or
below

Product Family	Impact ¹⁶	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4493441 , KB4493464 , KB4493470 , KB4493474 , KB4493475 , KB4493509
Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1709)	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4493470 Windows Server 2019: KB4493509 Windows Server v1709: KB4493441 Windows Server v1803: KB4493464
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4493446 , KB4493448 , KB4493450 , KB4493451 , KB4493458 , KB4493467 , KB4493471 , KB4493472
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4493441 , KB4493464 , KB4493470 , KB4493474 , KB4493475 , KB4493509
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4493471 , KB4493435 IE 10: KB4493451 , KB4493435 IE 11: KB4493435 , KB4493441 , KB4493446 , KB4493464 , KB4493470 , KB4493472 , KB4493474 , KB4493475 , KB4493509
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010: KB4464520 , KB4462223 Microsoft Office 2013: KB4464504 Microsoft Office 2013 and 2013 RT: KB4462204


¹⁶ The Impact and Severity are the maximum impact and severity assessment of the vulnerabilities in the associated knowledgebase (KB) by Microsoft.

Product Family	Impact ¹⁶	Severity	Associated KB and / or Support Webpages
			<p>Microsoft Office 2016: KB4462242, KB4462213</p> <p>Microsoft Office 2019 Security Update: Click to Run</p> <p>Microsoft Office 365 ProPlus Security Update: Click to Run</p> <p>Microsoft Excel 2010: KB4462230</p> <p>Microsoft Excel 2013 and Excel 2013 RT: KB4462209</p> <p>Microsoft Excel 2016: KB4462236</p> <p>Microsoft SharePoint Server 2010: KB4464525</p> <p>Microsoft SharePoint Server 2019: KB4464518</p> <p>Microsoft SharePoint Enterprise Server 2013: KB4464511</p> <p>Microsoft SharePoint Enterprise Server 2016: KB4464510</p> <p>Microsoft SharePoint Foundation 2010: KB4464528</p> <p>Microsoft SharePoint Foundation 2013: KB4464515</p>
Microsoft Exchange Server	Spoofing	Important ★★★	<p>Microsoft Exchange Server 2010: KB4491413</p> <p>Microsoft Exchange Server 2013, 2016, 2019: KB4487563</p>
ASP.NET Core	Denial of Service	Important ★★★	ASP .NET Core: Download
Windows Admin Center	Elevation of Privilege	Important ★★★	Windows Admin Center: Information & Download
Team Foundation Server, Azure DevOps Server	Elevation of Privilege	Important ★★★	Azure DevOps Server: Information
Open Enclave SDK	Information Disclosure	Important ★★★	Open Enclave SDK: Information

Learn more:

High Threat Security Alert (A19-04-02): Multiple Vulnerabilities in Microsoft Products (April 2019)
(https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=378)

Sources:

 Microsoft April 2019 Security Updates
(<https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/18306ed5-1019-e911-a98b-000d3a33a34d>)

Data analytics powered by  in collaboration with 