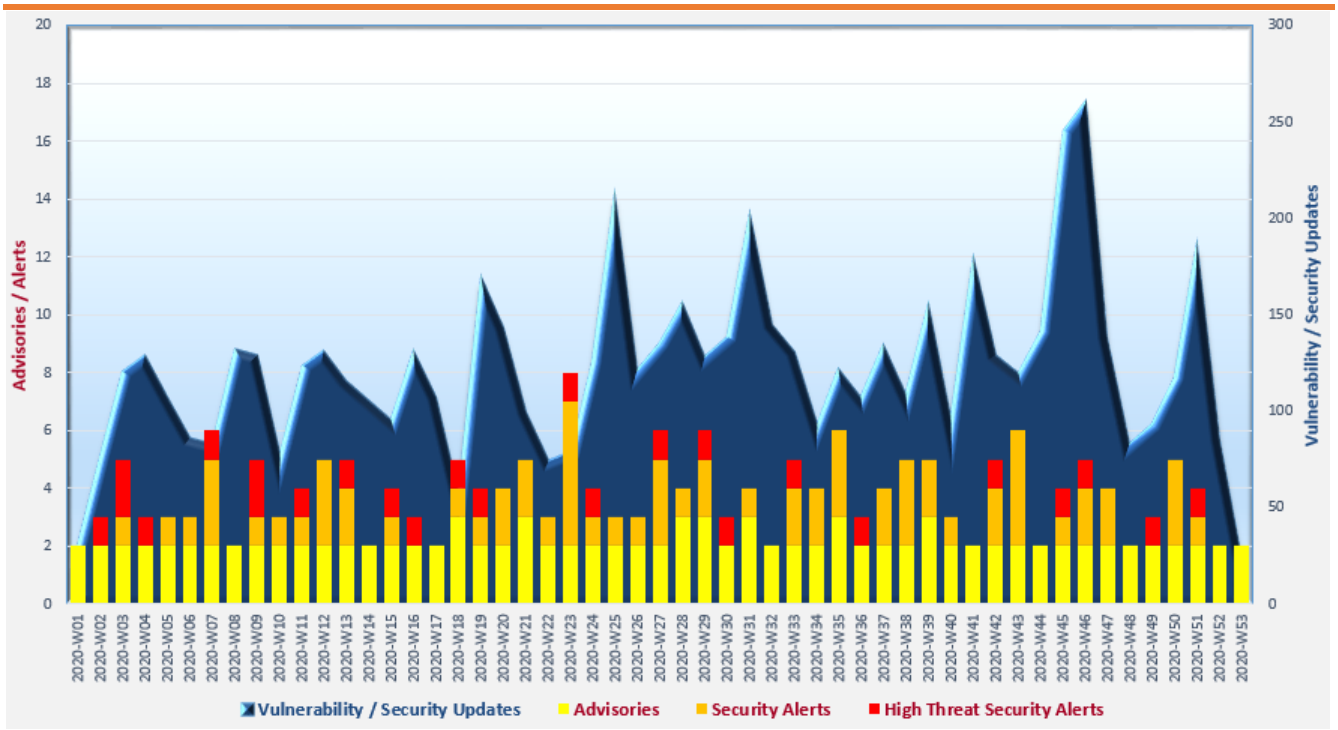
TLP:WHITE

Cyber Security Threat Trends 2020-M12

December 2020

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:

- **Distributed Denial of Service (DDoS) attack** continues causing adverse impact to organisations' networks and operations. Organisations should endeavour to protect their critical services by adopting appropriate anti-DDoS measures.
- **Supply chain attack** can lead to serious damage to organisations such as data theft or service interruption. Organisations should assure a defence-in-depth strategy and proper privileged access management with least privilege enforcement are in place for their systems and networks.
- **Phishing** continuously evolves with new attack tactics and phishing themes. Organisations could implement advanced threat detection and protection technology to protect against the threat. Security awareness training should be provided regularly to refresh end users with defence techniques on newly emerging phishing tactics.

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

CERT Advisories

Cyber attack targeted SolarWinds Orion Platform

GovCERT.HK[2], HKCERT[3], SingCERT[4], CERT NZ[5], Australian Cyber Security Centre (ACSC)[6], Cybersecurity and Infrastructure Security Agency (CISA)[7], National Cyber Security Centre (NCSC)[8], Canadian Centre for Cyber Security[9] issued alerts reminding organisations and system administrators to patch SolarWinds Orion Platform which was exploited actively in a global intrusion campaign. The affected versions were 2019.4 HF 5, 2020.2 with no hotfix installed or 2020.2 HF 1. System administrators should patch their affected products immediately. If for any reasons the patch could not be applied immediately, system administrators should disconnect or completely shut down SolarWinds Orion products. System administrator should also refer to product vendor's advisory and mitigation measures.

Red Team security assessment tools were stolen in security breach

ACSC[10], CISA[11] and Canadian Centre for Cyber Security[12] issued alerts regarding security breach incident of FireEye, in which the company's Red Team tools were stolen by threat actor. The tools could be abused by threat actor to gain unauthorised access or even take control of targeted systems. The stolen tools did not contain zero-day exploits. FireEye released countermeasures for detection on the use of the stolen tools.

Security events in Hong Kong dropped in Q3 2020

HKCERT[13] released its Hong Kong Security Watch Report (Q3 2020). The number of security events declined from 13,365 in Q2 2020 to 6,753 in Q3 2020, contributed by the drop in malware hosting, phishing, defacement and botnet events. There were 934 malware hosting events, 552 phishing events, 571 defacement events and 4,696 botnet events in Q3 2020, recorded a decrease from Q2 2020 by 88%, 70%, 46% and 21% respectively. There was no Botnet Command and Control Centre (C&C) security event for four consecutive quarters. Mirai was the most numerous botnet family though it dropped 28% in Q3 2020.

---

2 https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=535
3 https://www.hkcert.org/my_url/en/alert/20121501
4 https://www.csa.gov.sg/singcert/alerts/al-2020-049
5 https://www.cert.govt.nz/it-specialists/advisories/solarwinds-orion-vulnerability-being-actively-exploited/
6 https://www.cyber.gov.au/acsc/view-all-content/alerts/potential-solarwinds-orion-compromise
7 https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software
8 https://www.ncsc.gov.uk/guidance/dealing-with-the-solarwinds-orion-compromise
9 https://www.cyber.gc.ca/en/alerts/solarwinds-security-incident
10 https://www.cyber.gov.au/acsc/view-all-content/news/theft-fireeye-red-team-tools
11 https://us-cert.cisa.gov/ncas/current-activity/2020/12/08/theft-fireeye-red-team-tools
12 https://www.cyber.gc.ca/en/alerts/fireeye-security-incident
13 https://www.hkcert.org/my_url/en/blog/20120701

CERT Advisories

Apply patch to address vulnerability in FortiOS

HKCERT[14, 15] and CERT NZ[16] issued alerts reminding organisations and system administrators to patch Fortinet's FortiOS software. Vulnerability CVE-2018-13379 was published in 2019 which, when exploited, could allow an attacker to steal SSL VPN credentials. FortiOS versions 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 were affected. About 1,000 Hong Kong IP addresses might be vulnerable to CVE-2018-13379. System administrators should patch their affected products immediately.

Exploitations against vulnerability in VMware products

CISA[17, 18] and Canadian Centre for Cyber Security[19] issued alerts stating that threat actors actively exploited a command injection vulnerability, CVE-2020-4006, in VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector. System administrators should apply software patches timely and monitor any suspicious connections to the administrative configurator on port 8443.

End of support for Adobe Flash Player

HKCERT[20] published an article to remind users that Adobe Flash Player was no longer supported after 31 December 2020 and Flash content was blocked from running in Flash Player from 12 January 2021. Users should uninstall Adobe Flash Player from their devices and update the web browsers to latest version. Web developers could adopt open standards such as HTML5, WebAssembly and WebGL, etc.

14 https://www.hkcert.org/my_url/en/blog/20120801
15 https://www.hkcert.org/my_url/en/alert/19100802
16 https://www.cert.govt.nz/it-specialists/advisories/vulnerability-in-fortinet-firewalls-being-exploited/
17 https://us-cert.cisa.gov/ncas/current-activity/2020/12/07/nsa-releases-advisory-russian-state-sponsored-malicious-cyber
18 https://us-cert.cisa.gov/ncas/current-activity/2020/12/03/vmware-releases-security-updates-address-cve-2020-4006
19 https://www.cyber.gc.ca/en/alerts/active-exploitation-vmware-vulnerability
20 https://www.hkcert.org/my_url/en/blog/20121601

Industry Insight on Cyber Security Threat Trends

Almost 77% of Distributed Denial of Service (DDoS) attacks in Q3 2020 targeted online gambling and online gaming industries

Nexusguard published the "DDoS Threat Report 2020 Q3"[21], which included the analysis result and observation on DDoS attacks detected in the third quarter of 2020. The key findings were:

- **In Q3 2020, there were less than 40,000 DDoS attacks recorded, a decrease of 51.28% from Q2 2020, and was the lowest volume among the first three quarters of 2020.** UDP Attack (30.11%) and DNS Amplification Attack (22.22%) were the most prominent attack vectors, recorded a decrease of about 78% and 12.9% from Q2 2020 respectively. However, TCP SYN Attack (20.66%), the third most common attack vector, had an increase of more than 470% since Q2 2020. In terms of application attack source distribution, Hong Kong ranked the fourth (6.54%) worldwide and ranked the second (10.45%) in Asia-Pacific region.

- **The majority (over 72%) of DDoS attacks was single-vector.** The highest number of attack vector recorded in the period was 13. Over 93% of the detected DDoS attacks had attack sizes less than 1 Gbps. The largest attack size was 71.7 Gbps, roughly halved against Q2 2020 and diminished by almost 75% from Q3 2019. The average attack size was 0.55 Gbps, 63.78% lower than Q2 2020.

- **Most of the DDoS attacks (72.76%) lasted less than 90 minutes.** The average duration of attacks was 137.57 minutes, grew by 30.81% from Q2 2020 and 42.90% from Q3 2019. The longest attack continued for more than 575 hours, dropped by 45.81% compared to Q2 2020 but rose by 12.65% from Q3 2019.

- **44 Autonomous System Numbers (ASNs) were targeted by sophisticated bit-and-piece attacks in Q3 2020.** The attacks injected small pieces of junk traffic across a wide pool of IP addresses to evade detection, but the accumulated junk traffic were significantly large to cause adverse impact to the targets.

- **In Q3 2020, more than 45% of DDoS attacks targeted online gambling industry and almost 32% targeted online gaming industry.** The largest attack size recorded in Q3 2020 for online gambling industry and online gaming industry were 57.4 Gbps and 23.57 Gbps respectively. Adoption of network segregation, resource compartmentalisation and secure coding practice; formulation and periodic drilling of incident response plan; and engaging third party DDoS mitigation services were recommended measures to protect against DDoS attack.

Source: Nexusguard

[21] https://blog.nexusguard.com/threat-report/ddos-threat-report-2020-q3

Industry Insight on Cyber Security Threat Trends

Attackers adapted new tactics quickly in conducting spear-phishing

Barracuda published the "Spear Phishing: Top Threats and Trends"[22], which included the analysis of over 2.3 million spear-phishing attacks during August 2020 to October 2020 and the trends of social engineering attacks. The key findings were:

- **50% of the analysed attacks were phishing, followed by scamming (36%) and business email compromise (12%).** Business email compromise (BEC) increased from 7% in March 2019 to 12%. Extortion dropped from 11% in 2019 to 2% of all analysed spear-phishing attacks due to a slower growth than other types of spear-phishing attacks.
- **13% of all spear-phishing attacks emails were sent from potentially compromised internal email accounts.** This type of attack was dangerous since the emails were sent from legitimate email accounts which were more likely to be trusted. Moreover, the attacks did not only targeted users within the same organisation of the compromised accounts. 85% of phishing emails from these compromised accounts were sent to recipients with different email domains. Organisations should improve their detection and remediation mechanism on compromised accounts and train their employees to increase the awareness on suspicious messages from compromised accounts.
- **Malicious URLs were found in 71% of spear-phishing attacks.** 71% of the malicious URLs used ".com" as domain, but attackers also customised the malicious URLs for different targets. For example, ".edu" domain was commonly used in spear-phishing attacks to education sector targets. 4% of spear-phishing attacks used URL redirection or URL shortening for detection evasion since those domains were more likely to be permitted by security solutions. 64% of analysed attacks with shortened URLs used "t.co", link shortening service from Twitter.
- **Attackers continued to leverage COVID-19 in spear-phishing attacks** although the growth in overall volume was not significant since March 2020. 72% of COVID-19 themed spear-phishing attacks during June to October 2020 were scamming attacks on fake cures and donations.
- Organisations could consider implementing detection and protection technology which could analyse normal communication patterns and detect abnormal email conversations and compromised accounts to tackle attackers' evolving evasion tactics on bypassing gateways and spam filters. Domain-based Message Authentication, Reporting and Conformance (DMARC) could be adopted for prevention of domain spoofing and brand hijacking.

Source: Barracuda

[22] https://www.barracuda.com/spear-phishing-report-5?utm_source=42964&utm_medium=blog

Industry Insight on Cyber Security Threat Trends

Network attacks and scams skyrocketed in Q3 2020

WatchGuard collected anonymised information on threat detected from 47,866 globally deployed appliances and summarised the latest malware and exploit trends observed from the collected threat data in its "Internet Security Report – Q3 2020"[23]. The highlights from the report included:

- **Both network attacks and unique attack signatures recorded two-years high with over 3.3 million attack attempts and 438 signatures respectively in Q3 2020.** Compared to Q2 2020, network attack volume increased 90%. The Asia Pacific region (APAC) got 11% growth in global share in terms of attack volume, from 18% in Q2 2020 to 29% in Q3 2020. The global share for Americas region (AMER) and Europe and Middle East region (EMEA) were 49% and 22% respectively. System administrators should keep the systems up-to-date with latest patches and adopt advanced network intrusion prevention service.

- **Network attacks targeted an authentication bypass vulnerability of a supervisory control and data acquisition (SCADA) control system (CVE-2016-4510) were detected in different networks worldwide, making this threat one of the most-widespread network attacks in Q3 2020.** Attackers targeted almost 46% of networks in AMER for this vulnerability. Other most-widespread network attacks in Q3 2020 included two SQL injection attacks and two cross-site scripting attacks.

- **High prevalence of COVID-19 scams was observed in Q3 2020.** Malicious web sites related to a COVID-19 adware campaign and a phishing attack abusing Microsoft SharePoint to host a pseudo-login page impersonating the United Nations debuted in the lists of top 10 compromised websites and top 10 phishing domains in Q3 2020. In average, 262 malware domains, 71 compromised websites, and 52 phishing campaigns were blocked per organisation. Organisation-wide awareness training on new phishing techniques should be prioritised to defend against attacks via phishing emails and malicious websites.

- **Over half of detected malware in Q3 2020 was zero day malware, a 64% decrease compared to Q2 2020.** Nevertheless, these malware samples changed frequently and were more likely to evade from detection by signature-based anti-malware solutions. Organisations could consider implementation of multi-layered anti-malware defence. Almost 54% of detected malware were distributed via encrypted communication channels (TLS/HTTPS). All encrypted traffic should be inspected as far as possible to ferret out hidden malware.

Source: WatchGuard

[23] https://www.watchguard.com/wgrd-resource-center/security-report-q3-2020

Summary of Microsoft December 2020 Security Updates

12 Product Families with Patches

7 Critical

5 Important or below

Product Family	Impact[24]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4592438, KB4592440, KB4592446, KB4592449, KB4592464, KB4593226
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4586781, KB4586786, KB4586793, KB4586830, KB4592438, KB4592440, KB4592449, KB4593226
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4592438, KB4592440, KB4592449
Microsoft Dynamics	Remote Code Execution	Critical ★★★★	KB4595459, KB4595462, KB4583556 Dynamics 365 for Finance and Operations: Release Notes
Microsoft Exchange Server	Remote Code Execution	Critical ★★★★	KB4593465, KB4593466, KB4593467
Microsoft SharePoint-related software	Remote Code Execution	Critical ★★★★	KB4486696, KB4486697, KB4486721, KB4486751, KB4486752, KB4486753, KB4493138, KB4493149
ChakraCore	Remote Code Execution	Critical ★★★★	Release Notes
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Important ★★★	KB4592468, KB4592484, KB4592495, KB4592497
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4486698, KB4486757, KB4493140 Microsoft Excel: KB4486754, KB4493139, KB4493148

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

Product Family	Impact[24]	Severity	Associated KB and / or Support Webpages
			Microsoft Outlook: KB4486732, KB4486742, KB4486748 Microsoft PowerPoint: KB4484372, KB4484393, KB4484468 Microsoft Office Online Server: KB4486750 Microsoft Office Web Apps: KB4486704, KB4486760 Microsoft Office 2019: Click to Run Microsoft 365 Apps for Enterprise: Click to Run
Microsoft Visual Studio	Remote Code Execution	Important ★★★	Microsoft Visual Studio 2017 version 15.9: Release Notes Microsoft Visual Studio 2019 version 16.0: Release Notes Microsoft Visual Studio 2019 version 16.4: Release Notes Microsoft Visual Studio 2019 version 16.7: Release Notes Microsoft Visual Studio 2019 version 16.8: Release Notes Visual Studio Code TS-Lint Extension: Release Notes Visual Studio Code Language Support for Java Extension: Release Notes Visual Studio Code Remote - SSH Extension: Release Notes
Azure	Security Feature Bypass	Important ★★★	Azure SDK for Java: Release Notes Azure DevOps Server 2019 Update 1.1: Release Notes, Release Notes Azure DevOps Server 2019 Update 0.1: Release Notes Azure DevOps Server 2020: Release Notes C SDK for Azure IoT: Release Notes
Team Foundation Server	Spoofing	Important ★★★	Team Foundation Server 2015 Update 4.2: Release Notes Team Foundation Server 2017 Update 3.1: Release Notes

Product Family	Impact[24]	Severity	Associated KB and / or Support Webpages
			Team Foundation Server 2018 Update 1.2: Release Notes Team Foundation Server 2018 Update 3.2: Release Notes

Learn more:

Security Alert (A20-12-01): Multiple Vulnerabilities in Microsoft Products (December 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=531)

Sources:

- Microsoft December 2020 Security Updates (https://msrc.microsoft.com/update-guide/releaseNote/2020-Dec)