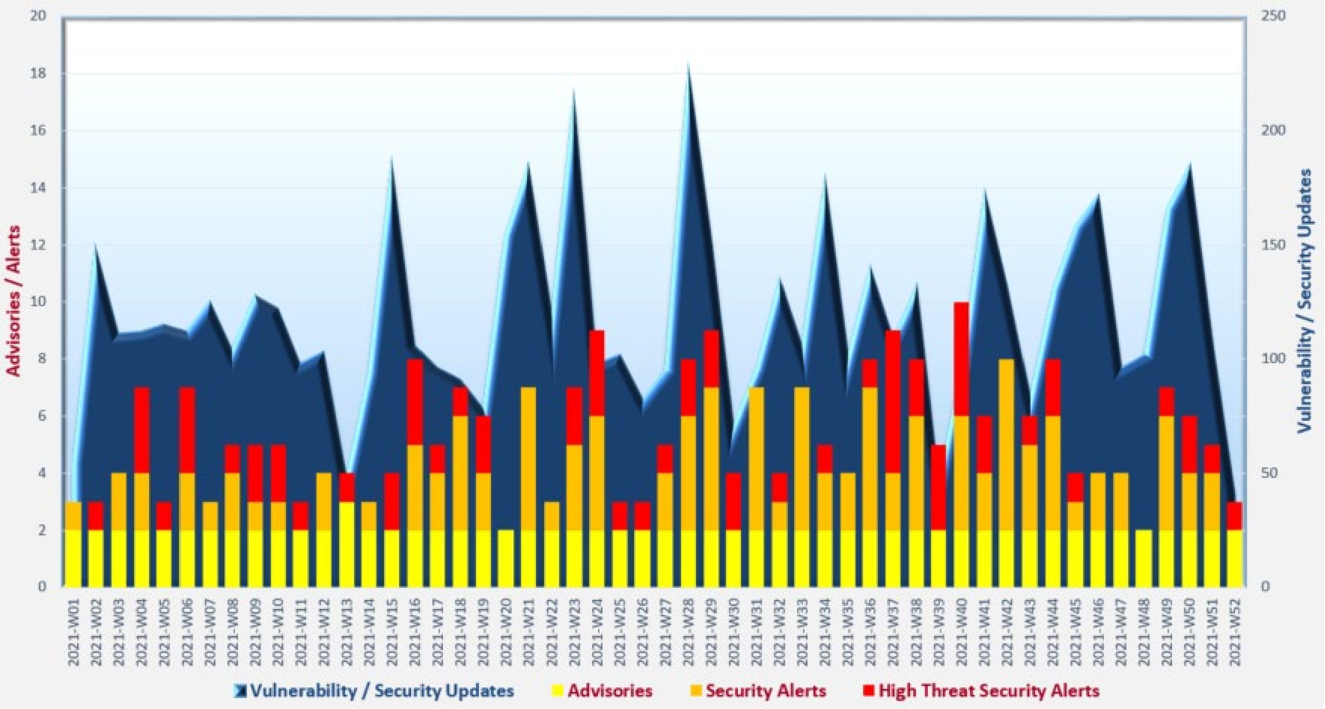
Cyber Security Threat Trends 2021-M12

December 2021

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:

- ✧ **Phishing** is a prevalent attack method for malware delivery and redirection to malicious web sites. All computer users should stay vigilant to suspicious links and attachments. Organisations should regularly conduct security awareness training and phishing simulation program to refresh their users on the knowledge of up-to-date cyber security threats along with the associated preventive measures.

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

CERT Advisories

Active exploitation of vulnerabilities in various products

CERT bodies issued alerts regarding active exploitation against vulnerabilities in various products. Proof of Concept (PoC) codes for exploitation of some vulnerabilities were publicly available. System administrators should refer to vendors' documentation, apply system patches and perform mitigation measures immediately.

- GovCERT.HK[2,3,4], HKCERT[5,6,7], SingCERT[8], MyCERT[9], CERT NZ[10], Australian Cyber Security Centre (ACSC)[11], National Cyber Security Centre (NCSC)[12], Canadian Centre for Cyber Security[13] and Cybersecurity and Infrastructure Security Agency (CISA)[14] issued alerts and advisories regarding multiple Apache Log4j (version 2.x) security vulnerabilities. A number of systems / technologies / products were affected. A critical remote code execution (RCE) vulnerability (CVE-2021-44228) dubbed Log4Shell was being actively exploited. PoC code for exploitation of related denial of service vulnerability (CVE-2021-45105) was publicly available. Other vulnerabilities such as CVE-2021-44832 and CVE-2021-45046 were also at high risk of exploitation. System administrators should keep a close surveillance on vendors' web sites for latest information and update their affected applications to the latest version of Apache Log4j or apply mitigation measures immediately.

- GovCERT.HK[15], HKCERT[16] and JPCERT[17] issued alerts regarding multiple vulnerabilities in Microsoft products. A remote code execution vulnerability (CVE-2021-4102) in Microsoft Edge (Chromium-based) and a spoofing vulnerability (CVE-2021-43890) in Windows AppX Installer were being actively exploited.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=700
[3] https://www.govcert.gov.hk/en/alerts_detail.php?id=705
[4] https://www.govcert.gov.hk/en/alerts_detail.php?id=708
[5] https://www.hkcert.org/security-bulletin/java-se-remote-code-execution-vulnerability_20211210
[6] https://www.hkcert.org/security-bulletin/apache-log4j-denial-of-service-vulnerability_20211220
[7] https://www.hkcert.org/blog/hkcert-urges-local-it-users-to-patch-apache-log4j-vulnerability-asap
[8] https://www.csa.gov.sg/en/singcert/Advisories/ad-2021-010
[9] https://www.mycert.org.my/portal/advisory?id=MA-825.122021
[10] https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/
[11] https://www.cyber.gov.au/acsc/view-all-content/advisories/2021-007-log4j-vulnerability-advice-and-mitigations
[12] https://www.ncsc.gov.uk/news/apache-log4j-vulnerability
[13] https://www.cyber.gc.ca/en/alerts/active-exploitation-apache-log4j-vulnerability
[14] https://www.cisa.gov/uscert/ncas/alerts/aa21-356a
[15] https://www.govcert.gov.hk/en/alerts_detail.php?id=704
[16] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-december-2021
[17] https://www.jpcert.or.jp/english/at/2021/at210051.html

CERT Advisories

- GovCERT.HK[18], HKCERT[19] and Canadian Centre for Cyber Security[20] issued alerts regarding multiple vulnerabilities in Google Chrome. Vulnerability (CVE-2021-4102) was being actively exploited.

- Canadian Centre for Cyber Security[21], ACSC[22] and CISA[23, 24, 25] issued alerts regarding vulnerabilities in Zoho ManageEngine Desktop Central, Zoho ManageEngine Desktop Central MSP and Zoho ManageEngine ServiceDesk Plus. An authentication bypass vulnerability (CVE-2021-44515) and an unauthenticated remote code execution vulnerability (CVE-2021-44077) were being exploited in the wild.

Security tips for online shopping and long holiday

HKCERT[26] published an article that provided security tips for individual to avoid online shopping fraud. In addition, actionable security measures were provided to organisations for improving their cyber security during long holidays.

Protect organisations' social media accounts

CISA[27] released a guidance that help organisations to protect their social media accounts and reduce the risk of unauthorised access to their accounts in the social media platforms. Protection measures such as credential management, adopting multi-factor authentication (MFA), vetting third-party vendors, establishing incident response plan, etc. were recommended to social media account administrators.

Ransomware protection guidelines

Ransomware is a prevalent cyber threat that can cause serious impact to organisations. MyCERT[28] and Canadian Centre for Cyber Security[29] published recommendations on protecting information systems, network and data against ransomware for organisations to reference.

[18] https://www.govcert.gov.hk/en/alerts_detail.php?id=702
[19] https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20211214
[20] https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-74
[21] https://www.cyber.gc.ca/en/alerts/zoho-security-advisory-0
[22] https://www.cyber.gov.au/acsc/view-all-content/alerts/zoho-manageengine-servicedesk-plus-remote-code-execution-vulnerability
[23] https://us-cert.cisa.gov/ncas/current-activity/2021/12/06/zoho-releases-security-advisory-manageengine-desktop-central-and
[24] https://www.cisa.gov/uscert/ncas/alerts/aa21-336a
[25] https://www.cisa.gov/uscert/ncas/current-activity/2021/12/02/cisa-and-fbi-release-alert-active-exploitation-cve-2021-44077-zoho
[26] https://www.hkcert.org/blog/beware-of-cyber-security-risks-from-online-shopping-and-long-holiday
[27] https://www.cisa.gov/uscert/ncas/current-activity/2021/12/09/cisa-releases-guidance-protecting-organization-run-social-media
[28] https://www.mycert.org.my/portal/advisory?id=MA-824.122021
[29] https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099

CERT Advisories

More phishing sites were observed in Q3 2021, although total security events dropped

HKCERT released its Hong Kong Security Watch Report (Q3 2021)[30]. The number of security events dropped 32% from 7,191 in Q2 2021 to 4,860 in Q3 2021. The number of Botnet (Bots) security events and defacement events declined 43% and 7% respectively, and there was no malware hosting, and Botnet Command and Control Centre (C&C) security event in Q3 2021. However, the number of phishing sites increased by 49% from 665 sites in Q2 2021 to 993 sites in Q3 2021. The top 3 top-level domain name of phishing sites were ".org" (30%), ".com" (29%), and ".cn" (10%). Other rarely used domains such as ".shop", ".cam", ".monster" and ".icu" were also observed in Q3 2021. Nginx continued to be the most targeted web server type (179 events) and "known vulnerability" and "file inclusion" were the major compromise causes. The top 5 botnet families were Mirai, Avalanche, Conficker, WannaCry and Virut, and they contributed 79% of all Botnet (Bots) events.

[30] https://www.hkcert.org/watch-report/hong-kong-security-watch-report-q3-2021

Industry Insight on Cyber Security Threat Trends

Ransomware attacks dropped from Q2 2021 but became more organised

Positive Technologies published the "Cybersecurity threatscape: Q3 2021"[31] report, which summarised the threat trends and investigation results observed in Q3 2021. The highlights from the report included:

- **The number of attacks decreased by 4.8% from Q2 2021.** Slight changes in the shares of attacks targeted organisation (from 77% in Q2 to 75% in Q3 2021) and attacks targeted individual (from 12% in Q2 to 14% in Q3 2021) were observed.

- **The top three targeted sectors were government, healthcare and manufacturing & industry which accounted for 21%, 12%, and 9% respectively.** Among different types of targeted attack, the attackers mostly aimed at compromising computers, servers and network equipment of organisations (75%). The consequence of attacks included leak of confidential information (45%), disruption of core activity (38%), direct financial loss (24%), etc. Attackers mostly targeted to steal personal data (33%), credentials (14%) and intellectual property data (14%) from affected organisations.

- **Attackers trended to use social engineering (83%) in attacks targeted individuals.** They commonly aimed at credentials, personal data and payment card information which accounted for 42%, 21% and 15% of stolen data respectively. The top three malware delivery channels to individuals were by websites (34%), email (19%) and compromising computers, servers and network equipment (16%). Remote access tool (RAT) was the most popular in malware attacks on individuals, accounted for 52% of all malware used and an increase of 2.5 times as compared to 21% in Q1 2021.

- **Number of ransomware attacks dropped but remained the most popular malware that targeted organisations (55%).** The top three targeted sectors in ransomware attacks in Q3 2021 were healthcare (23%), government (16%) and scientific / educational institutions (13%). The most common ransomware in Q3 2021 were REvil, LockBit 2.0, Conti, Hive and AvosLocker.

Source: Positive Technologies

[31] https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2021-q3/

Industry Insight on Cyber Security Threat Trends

Evolving ransomware attacks were observed in 2021

Darktrace analysed the latest trends in ransomware attacks and published its "2021 Ransomware Threat Report"[32]. The key findings were:

- **Evolving attack techniques were discovered with wider scale and faster speed.** In 2021, one ransomware attack was launched in 11 seconds on average, more frequent than one in every 40 seconds in 2016. Ransomware was perceived as an enormous threat to organisations. Organisations should adopt up-to-date and advanced anti-malware technologies to defend against the evolving attack techniques.

- **Shift to remote working induced new way of launching attacks.** Attackers increasingly targeted exploitation of Remote Desktop Protocol by using exposed credential or brute-forcing to compromise those systems that were not properly protected. More ransomware attacks were started in non-office hours to take advantage of slower human reaction time during the period.

- **Attackers utilised more tailor-made and targeted phishing campaigns to spread ransomware.** Latest news or topics were adopted as phishing themes in order to catch the attention of targets.

- **Attackers continued improving attack techniques for better evasion and lateral movement.** Increased adoption of Ransomware-as-a-Service (RaaS), which lowered the skills required for executing ransomware attacks, made the threat become more widespread. Attackers were expected to increasingly adopt AI-powered attacks with improved speed, scale, sophistication, personalisation and evasion capabilities.

- **Double extortion ransomware attacks remained in an uptrend.** Attackers threatened to publicise the stolen sensitive data, in addition to encrypting organisations' data.

Source: Darktrace

[32] https://www.darktrace.com/en/resources/wp-ransomware-threat-report.pdf

Industry Insight on Cyber Security Threat Trends

Simulated phishing attack results indicated end users' response to phishing was similar to last year

Terranova Security issued the "Phishing Benchmark Global Report 2021"[33], which summarised their findings on simulated phishing attacks in the 2021 Gone Phishing Tournament, a cyber security event with participating organisations from 12 different sectors and near 1 million phishing simulation emails in 20 different languages sent. The key findings were:

- **19.8% of recipients clicked on the phishing link in the simulated email and visited the phishing site, similar to the results in the 2020 event.** However, 14.4% of the recipients failed to identify the malevolent web site and downloaded malicious files from the web site, an increase when compared to the campaign in 2020.

- **Education was the sector with the highest click rate for phishing emails, with 27.6% of recipients clicked on the simulation emails' phishing links.** Other sector with click rates higher than average (19.8%) included finance & insurance (26.6%), information technology (25.6%), agriculture & food (21.2%) and service provider (20.2%). Among these 5 sectors, education (21.9%), information technology (21.6%), agriculture & food (16.8%) and finance & insurance (14.6%) also recorded above average (14.4%) malicious file download rate. Information technology sector had the highest click-to-download rate (84.4%).

- **Organisations with more than 3,000 employees had the highest click rate, download rate and click-to-download rate in the phishing simulation.** 18% of recipients clicked the phishing links and 12% of recipients downloaded the malicious files.

- **Asia Pacific was the region with the highest click rate, download rate and click-to-download rate.** 20.2% of recipients clicked the phishing links and 16% of recipients downloaded malicious files. Europe had the same click rate as Asia Pacific, but with a lower download rate and click-to-download rate.

- Organisations should offer more security awareness training with updated threat information from recent cyber attacks and security news to their employees. Repeat clickers should be identified and provided with sufficient support and training.

Source: Terranova Security

[33] https://terranovasecurity.com/gone-phishing-tournament/

Highlight of Microsoft December 2021 Security Updates

Product Family	Impact[18]	Severity	Associated KB
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5008206, KB5008207, KB5008210, KB5008212, KB5008215, KB5008218, KB5008230
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5008207, KB5008210, KB5008212, KB5008218, KB5008223
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5008255, KB5008263, KB5008277, KB5008285
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4486726, KB4504710, KB4504745, KB5002033, KB5002097, KB5002098, KB5002099, KB5002101, KB5002103, KB5002104, KB5002105

Note: Only widely-used Microsoft products are listed and it does not mean to be inclusive. For details, please refer to https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Dec.

Learn more:
High Threat Security Alert (A21-12-09): Multiple Vulnerabilities in Microsoft Products (December 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=704)