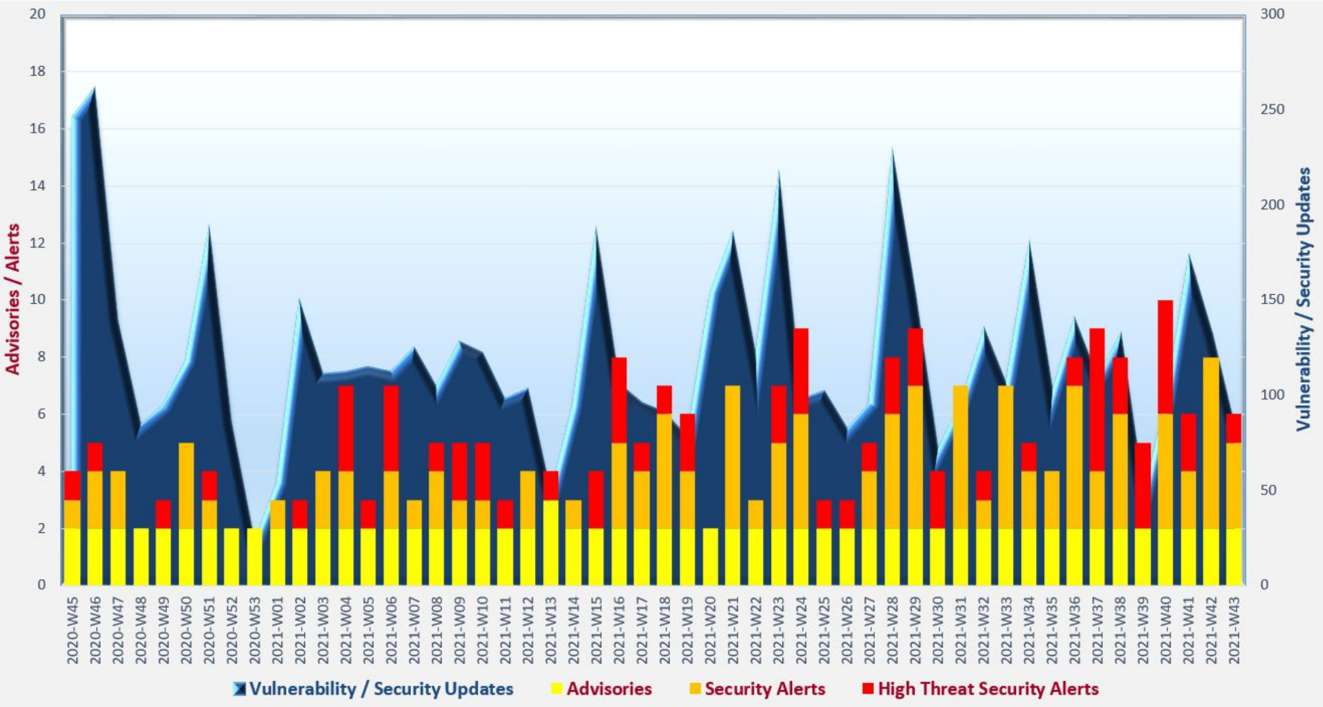
Cyber Security Threat Trends 2021-M10

October 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** attacks remain active and keep increasing their evasion capabilities. Users should always stay vigilant to suspicious electronic messages, and pay special attention in handling links or attachments.

[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], HKCERT [3], JPCERT [4] and SingCERT [5] issued alerts regarding multiple vulnerabilities in Microsoft products. An elevation of privilege vulnerability in Win32k (CVE-2021-40449), which affected all supported versions of Windows and Windows Server, including Windows 7 and Windows Server 2008, was being actively exploited.

- GovCERT.HK[6,7,8], HKCERT[9,10,11], Cybersecurity and Infrastructure Security Agency (CISA)[12] and Canadian Centre for Cyber Security[13,14,15] issued alerts regarding multiple vulnerabilities in Google Chrome and Microsoft Edge (Chromium-based). Vulnerabilities (CVE-2021-37975, CVE-2021-37976, CVE-2021-38000 and CVE-2021-38003) were being actively exploited.

- GovCERT.HK[16], HKCERT[17], CISA[18] and Canadian Centre for Cyber Security[19] issued alerts regarding an arbitrary code execution vulnerability (CVE-2021-30883) in various Apple devices. PoC code for exploitation of the vulnerability was publicly available.

- HKCERT[20] issued an alert regarding multiple vulnerabilities in McAfee ePolicy Orchestrator. PoC exploit code for the vulnerability CVE-2021-23840 was publicly available.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=672
[3] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-october-2021
[4] https://www.jpcert.or.jp/english/at/2021/at210045.html
[5] https://www.csa.gov.sg/en/singcert/Alerts/al-2021-061
[6] https://www.govcert.gov.hk/en/alerts_detail.php?id=662
[7] https://www.govcert.gov.hk/en/alerts_detail.php?id=663
[8] https://www.govcert.gov.hk/en/alerts_detail.php?id=682
[9] https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20211004
[10] https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20211004
[11] https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20211029
[12] https://us-cert.cisa.gov/ncas/current-activity/2021/10/29/google-releases-security-updates-chrome
[13] https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-68
[14] https://www.cyber.gc.ca/en/alerts/microsoft-edge-chromium-based-security-advisory-3
[15] https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-71
[16] https://www.govcert.gov.hk/en/alerts_detail.php?id=670
[17] https://www.hkcert.org/security-bulletin/apple-ios-remote-code-execution-vulnerability_20211012
[18] https://us-cert.cisa.gov/ncas/current-activity/2021/10/12/apple-releases-security-update-address-cve-2021-30883
[19] https://www.cyber.gc.ca/en/alerts/apple-security-advisory-43
[20] https://www.hkcert.org/security-bulletin/mcafee-epolicy-orchestrator-multiple-vulnerabilities_20211025

CERT Advisories

- GovCERT.HK[21, 22], HKCERT[23], JPCERT[24], SingCERT[25], CISA[26], Canadian Centre for Cyber Security[27] and Australian Cyber Security Centre (ACSC)[28] issued alerts regarding vulnerabilities in Apache HTTP Server 2.4.49 and 2.4.50. Vulnerabilities (CVE-2021-41773 and CVE-2021-42013) were being exploited in the wild.

🗎 Highlights of 2021 edition of Open Web Application Security Project Top Ten Web Application Security Risks (OWASP Top 10-2021)

HKCERT[29] published an article to summarise the changes and new categories in OWASP Top 10-2021. Organisations and web application developers are recommended to refer to the OWASP Top 10 as one of the resources on secure system development.

[21] https://www.govcert.gov.hk/en/alerts_detail.php?id=664
[22] https://www.govcert.gov.hk/en/alerts_detail.php?id=668
[23] https://www.hkcert.org/security-bulletin/apache-http-multiple-vulnerabilities_20210920
[24] https://www.jpcert.or.jp/english/at/2021/at210043.html
[25] https://www.csa.gov.sg/en/singcert/Alerts/al-2021-059
[26] https://us-cert.cisa.gov/ncas/current-activity/2021/10/07/apache-releases-http-server-version-2451-address-vulnerabilities
[27] https://www.cyber.gc.ca/en/alerts/apache-security-advisory-3
[28] https://www.cyber.gov.au/acsc/view-all-content/alerts/critical-vulnerability-certain-versions-apache-http-server
[29] https://www.hkcert.org/blog/owasp-top-10-2021-is-now-released

Industry Insight on Cyber Security Threat Trends

Bit-and-piece Distributed Denial of Service (DDoS) attacks rose in the first half of 2021

Nexusguard issued the "DDoS Threat Report FHY 2021"[30], which summarised their findings on DDoS attack trends in the first half of 2021. The key findings were:

- **Bit-and-piece DDoS attacks increased by 232.8% compared to H2 2020.** These bit-and-piece attacks aimed to evade from detection and exhaust network resources through high packet rate loads of small-sized traffic.
- **In H1 2021, over 99% of the DDoS attack size were less than 10 Gbps and around 95% of the attack size were less than 1 Gbps.** The largest attack size was over 300 Gbps, an increase of more than 230% from H2 2020. The average attack duration was 127.6 minutes and the duration of 84.6% of the attacks were shorter than 90 minutes. The longest attack lasted over 256 hours. Compared to H2 2020, the average and maximum attack duration decreased by 25.6% and 65.2% respectively.
- **Hong Kong ranked the 4th in application attack source region globally, accounted for 9.8% of application attacks in H1 2021.**
- **UDP Attack was the top attack vector in H1 2021 (43.7%), followed by DNS Amplification Attack (12.6%) and TCP SYN Attack (12.6%).** UDP Attacks increased by 83.9% compared to H2 2020. Over 81% of DDoS attacks in H1 2021 were from single attack vector.
- Organisation could consider adoption of behavioural DDoS detection and mitigation approach to defend against DDoS attacks with evolving evasion capabilities from threshold or signature based detection mechanism.

Source: Nexusguard

[30] https://blog.nexusguard.com/threat-report/ddos-threat-report-fhy-2021

Industry Insight on Cyber Security Threat Trends

More than half of survey respondents reused their passwords for different online accounts

Bitdefender published the "2021 Bitdefender Global Report: Cybersecurity and Online Behaviors"[31] based on results of a survey conducted in June 2021 with over 10,000 respondents from 11 economies in Europe, North America and Australia. The key findings on personal cyber security practices and level of exposure to cyber threats of consumer Internet users were:

- **22% of respondents used a single password for all online accounts.** 31% of respondents used a few passwords and reused them across multiple accounts. 27% of respondents indicated that they used simple passwords (e.g. Password, qwerty123, etc.) for online accounts.
- **30% of respondents did not use antivirus solution on their main mobile devices.** Among them, 30% considered they did not need antivirus solution for the mobile devices. Regarding using password to lock their mobile phones, 30% of respondents used simple passwords (e.g. same digit such as “0000”, consecutive digits such as “1234”, etc.). 11% of respondents did not lock their mobile phones.
- **61% of respondents experienced at least one cyber threat in the past year.** The top three cyber threats that they encountered were scam messages or call (36%), phishing (23%), and data breach (12%).
- **23% of respondents used at least one device at work to access their personal online accounts.**
- **Over one-third of respondents allowed their children having full access to their personal devices, including the right to install any apps.**

Source: Bitdefender

[31] https://www.bitdefender.com/files/News/CaseStudies/study/404/BD-Security-Behavior-Report-Final-at.pdf

Industry Insight on Cyber Security Threat Trends

Phishing attacks remained at high level in Q3 2021

Cofense released the "Q3 2021 Cofense Phishing Review"[32], which concluded the analysis results on phishing attacks detected in the third quarter of 2021 and predicted the upcoming trends in the fourth quarter. The key findings were:

- **More phishing activities were detected in Q3 2021 as compared to the same period in 2020.** Keylogger remained the most common type of malware delivered in phishing with Agent Tesla was the most frequently seen in the keylogger family. Information Stealer and Remote Access Trojan (RAT) were the second and third most common malware type respectively. New versions and increased activities of TrickBot were detected in Q3 2021.

- **Office documents were most widely used for delivering malware in Q3 2021, with increased activities exploiting CVE-2017-11882 detected.** The top three file extensions for attachments found in phishing email were .htm, .html and .pdf.

- **Based on the statistics collected in both Q2 and Q3 2021, over half of the Command and Control (C2) servers were located in the United States.** Percentage of C2 servers located in Hong Kong dropped in Q3 2021.

- **Threat actors made use of wide range of tactics in launching phishing attacks.** Usage of multi-layered links and redirection, multi-layered compression and multi-layered encoding increased. Services offered by trusted third-party were adopted by attackers for redirecting and hosting phishing websites.

- **New commodity malware downloader and increased TrickBot activity were anticipated in Q4 2021.** The general pattern of phishing trend for Q4 2021 would likely follow the pattern demonstrated in Q4 2020.

Source: Cofense

[32] https://get.cofense.com/Q3_2021_Phishing_Review.html

Highlight of Microsoft October 2021 Security Updates

Product Family	Impact[33]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5006667, KB5006669, KB5006670, KB5006672, KB5006674, KB5006675
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5006669, KB5006670, KB5006672, KB5006699
Microsoft Office-related software	Remote Code Execution	Critical ★★★★	KB4018332, KB4461476, KB5001960, KB5001982, KB5001985, KB5002004, KB5002027, KB5002030, KB5002036, KB5002043
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Important ★★★	KB5006671, KB5006714, KB5006729, KB5006732, KB5006739
Microsoft Exchange Server	Remote Code Execution	Important ★★★	KB5007011, KB5007012

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-Oct.

Learn more:
High Threat Security Alert (A21-10-11): Multiple Vulnerabilities in Microsoft Products (October 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=672)

Data analytics powered by CRisP in collaboration with GovCERT.HK

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