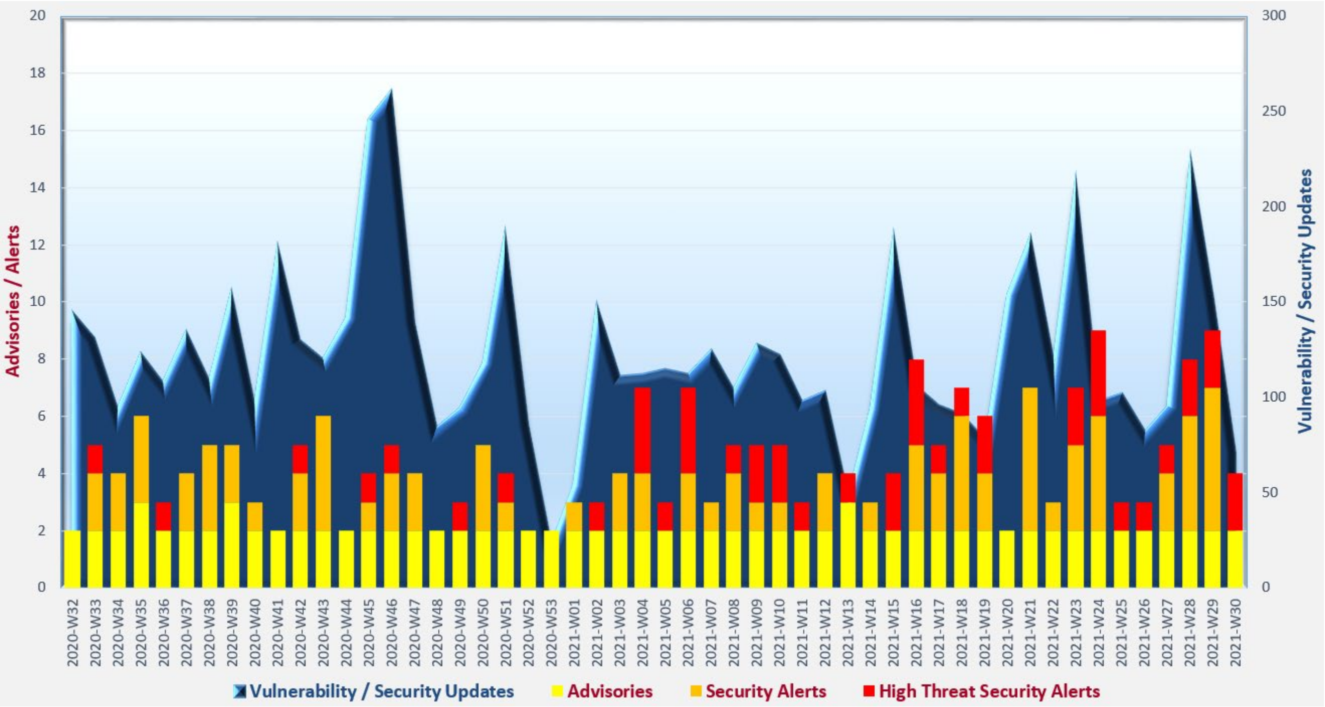
Cyber Security Threat Trends 2021-M07

July 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:

System vulnerabilities are being aggressively exploited by attackers. **Ransomware attacks** still pose serious threat to organisations. **Misconfigured and misused cloud services** cause leakage of sensitive data and security breach. Organisations should patch their systems and apply mitigation measures timely, disable unused services to reduce attack surfaces and adopt least privilege principle and zero trust defence approach.

[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], HKCERT[4,5], JPCERT[6,7], Cybersecurity and Infrastructure Security Agency (CISA)[8,9], and Canadian Centre for Cyber Security[10,11] issued alerts regarding multiple vulnerabilities in Microsoft products. PoC code for exploitation of a critical Windows Print Spooler vulnerability (CVE-2021-34527, also known as PrintNightmare) was publicly available. Vulnerabilities in Microsoft Windows and Server (CVE-2021-34527, CVE-2021-34448, CVE-2021-33771 and CVE-2021-31979) were being actively exploited. Successful exploitation could lead to remote code execution or elevation of privilege.

- GovCERT.HK[12,13], HKCERT[14], CISA[15], and Canadian Centre for Cyber Security[16,17] issued alerts regarding multiple vulnerabilities in Google Chrome and Microsoft Edge (Chromium-based). Vulnerability CVE-2021-30563 was being actively exploited.

- Australian Cyber Security Centre (ASCS)[18], CISA[19], and Canadian Centre for Cyber Security[20] issued alerts regarding a pre-authorisation remote code execution vulnerability (CVE-2021-35464) in ForgeRock Access Management. Successful exploitation could allow attackers to execute commands in the context of the current user. The vulnerability was being exploited actively.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=608
[3] https://www.govcert.gov.hk/en/alerts_detail.php?id=605
[4] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-july-2021
[5] https://www.hkcert.org/security-bulletin/microsoft-windows-remote-code-execution-vulnerability_20210702
[6] https://www.jpcert.or.jp/english/at/2021/at210031.html
[7] https://www.jpcert.or.jp/english/at/2021/at210029.html
[8] https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/microsoft-releases-july-2021-security-updates
[9] https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/cisa-issues-emergency-directive-microsoft-windows-print-spooler
[10] https://www.cyber.gc.ca/en/alerts/microsoft-security-advisory-july-2021-monthly-rollup
[11] https://www.cyber.gc.ca/en/alerts/windows-print-spooler-vulnerability-remains-unpatched
[12] https://www.govcert.gov.hk/en/alerts_detail.php?id=613
[13] https://www.govcert.gov.hk/en/alerts_detail.php?id=614
[14] https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20210716
[15] https://us-cert.cisa.gov/ncas/current-activity/2021/07/16/google-releases-security-updates-chrome
[16] https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-61
[17] https://www.cyber.gc.ca/en/alerts/microsoft-edge-chromium-based-security-advisory-0
[18] https://www.cyber.gov.au/acsc/view-all-content/alerts/forgerock-open-am-critical-vulnerability
[19] https://us-cert.cisa.gov/ncas/current-activity/2021/07/12/critical-forgerock-access-management-vulnerability
[20] https://www.cyber.gc.ca/en/alerts/forgerock-security-advisory

CERT Advisories

- HKCERT[21], SingCERT[22], CERT NZ[23], MyCERT[24], CISA[25,26], ACSC[27], and Canadian Centre for Cyber Security[28] issued alerts regarding attacks targeted Kaseya Virtual System Administrator (VSA). Threat actors exploited vulnerability of the affected product to deploy REvil (also known as Sodinokibi) ransomware via software update features. The vendor released the Kaseya VSA Detection Tool which checks a system for the presence of indicators of compromise (IoC). Security patch was released on 12 July 2021.

- HKCERT[29], CERT NZ[30], ASCS[31], CISA[32], and Canadian Centre for Cyber Security[33] issued alerts reminding system administrators that threat actors actively targeted end-of-life SonicWall Secure Mobile Access (SMA) 100 series and Secure Remote Access (SRA) products running 8.x firmware to launch ransomware attacks.

- GovCERT.HK[34] and HKCERT[35],[36] issued alerts regarding multiple vulnerabilities in major Linux distributions including Debian, RedHat, SUSE and Ubuntu. PoC code for exploitation of vulnerabilities CVE-2021-33909 and CVE-2021-33910 was publicly available.

- GovCERT.HK[37], HKCERT[38], SingCERT[39], CISA[40], and Canadian Centre for Cyber Security[41] issued alerts regarding an actively exploited vulnerability (CVE-2021-30807) in various Apple devices which upon exploitation could lead to remote code execution on the targeted system.

[21] https://www.hkcert.org/security-bulletin/kaseya-vsa-products-are-being-actively-attacked-by-revil-ransomware-supply-chain-attack

[22] https://www.csa.gov.sg/en/singcert/Alerts/al-2021-037

[23] https://www.cert.govt.nz/it-specialists/advisories/kaseya-management-software-being-used-to-deploy-ransomware/

[24] https://www.mycert.org.my/portal/advisory?id=MA-810.072021

[25] https://us-cert.cisa.gov/ncas/current-activity/2021/07/12/kaseya-provides-security-updates-vsa-premises-software

[26] https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

[27] https://www.cyber.gov.au/acsc/view-all-content/alerts/kaseya-vsa-supply-chain-ransomware-attack

[28] https://www.cyber.gc.ca/en/alerts/supply-chain-enabled-ransomware-activity-affecting-multiple-managed-service-providers

[29] https://www.hkcert.org/security-bulletin/sonicwall-products-zero-day-vulnerabilities_20210716

[30] https://www.cert.govt.nz/it-specialists/advisories/sonicwall-eol-equipment-targeted-by-ransomware/

[31] https://www.cyber.gov.au/acsc/view-all-content/alerts/sonicwall-devices-targeted-ransomware-utilising-stolen-credentials

[32] https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/ransomware-risk-unpatched-eol-sonicwall-sra-and-sma-8x-products

[33] https://www.cyber.gc.ca/en/alerts/sonicwall-releases-urgent-security-notice-eol-sra-and-sma-8x-devices-risk-ransomware

[34] https://www.govcert.gov.hk/en/alerts_detail.php?id=617

[35] https://www.hkcert.org/security-bulletin/linux-multiple-vulnerabilities_20210722

[36] https://www.hkcert.org/security-bulletin/linux-kernel-multiple-vulnerabilities_20210727

[37] https://www.govcert.gov.hk/en/alerts_detail.php?id=621

[38] https://www.hkcert.org/security-bulletin/apple-products-remote-code-execution-vulnerability_20210727

[39] https://www.csa.gov.sg/singcert/Alerts/al-2021-046

[40] https://us-cert.cisa.gov/ncas/current-activity/2021/07/27/apple-releases-security-updates

[41] https://www.cyber.gc.ca/en/alerts/apple-security-advisory-34

CERT Advisories

- GovCERT.HK[42], HKCERT[43], SingCERT[44] and CISA[45] issued alerts regarding a NT LAN Manager (NTLM) relay attack named PetitPotam which could potentially be used to attack Windows domain controllers or other Windows servers. PoC code for PetitPotam was publicly available. Security patches were not yet released as at end of July 2021, but Microsoft provided a security advisory with mitigation options.

🗎 Highly exploited vulnerabilities in 2020 and 2021

ASCS[46], National Cyber Security Centre (NCSC)[47], CISA[48] and Federal Bureau of Investigation (FBI) published a joint advisory that highlighted vulnerabilities highly exploited by attackers in 2020 and 2021. Among the most targeted vulnerabilities in 2020, four of them affected remote work solutions, Virtual Private Network (VPN) solutions, or cloud technologies. Vulnerabilities in Microsoft, Pulse Secure, Accellion, VMware, and Fortinet software were exploited highly in 2021. System administrators should patch their systems timely for risk mitigation.

[42] https://www.govcert.gov.hk/en/alerts_detail.php?id=622

[43] https://www.hkcert.org/security-bulletin/microsoft-ntlm-relay-attacks-on-active-directory-certificate-services_20210726

[44] https://www.csa.gov.sg/singcert/Alerts/al-2021-045

[45] https://us-cert.cisa.gov/ncas/current-activity/2021/07/27/microsoft-releases-guidance-mitigating-petitpotam-ntlm-relay

[46] https://www.cyber.gov.au/acsc/view-all-content/news/joint-advisory-top-cyber-vulnerabilities

[47] https://www.ncsc.gov.uk/news/global-cyber-vulnerabilities-advice

[48] https://us-cert.cisa.gov/ncas/alerts/aa21-209a

Industry Insight on Cyber Security Threat Trends

68% of malware were delivered through cloud in Q2 2021, continuously increased since Q1 2020

Netskope published the "Cloud and Threat Report: July 2021"[49], which summarised their analysis on cloud security in the first half of 2021. The key findings were:

- **The trend of adopting cloud applications to spread malware and avoid detection increased for six consecutive quarters since Q1 2020.** 68% of total malware downloaded in Q2 2021 were originated from cloud applications. Among the cloud-delivered malware, more than 66% were downloaded from cloud storage applications.

- **43% of malware downloaded in the second quarter of 2021 were in the form of Office documents**, increased from 34% in Q1 2021 and recorded a large increase as compared to 20% in the first quarter of 2020.

- **15% of staff being terminated uploaded data to their personal cloud applications either directly copied from organisations' managed application instances or data included personally identifiable information, healthcare information, intellectual property, source code, etc, before leaving the company.**

- **More than 35% of cloud instances of organisations in AWS, Azure and GCP were publicly accessible from the Internet**. Among these publicly exposed instances, 8.3% exposed the Remote Desktop Protocol (RDP) and 16% had all ports exposed. Virtual Private Network (VPN) or zero trust network access protection should be adopted for risk mitigation.

- **97% of cloud applications used in organisations with 500 to 2000 staff were shadow IT applications and almost half of these applications got poor risk rating.**

- **Organisations should apply strong authentication measures and access controls, conduct security risk assessments on a regular basis and enforce detection and mitigation controls to strengthen cloud security.**

Source: Netskope

[49] https://resources.netskope.com/cloud-reports/cloud-and-threat-report-july-2021

Industry Insight on Cyber Security Threat Trends

Ransomware attacks were prevalent in Q1 2021

Positive Technologies published the "Cybersecurity threatscape: Q1 2021"[50], which summarised information on cyber security threats in Q1 2021. The highlights from the report included:

- **Compared to Q4 2020, the number of attacks increased by 1.2% in Q1 2021, and an increase of 17% when compared to Q1 2020.** 88% of the attacks targeted organisations. Access to data, financial profit, and hacktivism were the top three motives for both attacks targeted organisations and individuals. Personal data and credentials were mostly stolen in both attacks targeted organisations and individuals, although intellectual property information was also highly targeted in attacks against organisations.

- **Ransomware was the most common malware in attacks targeted organisations which accounted for 63% of malware used in the attacks.** Attackers used email to deliver ransomware in 7 out of 10 ransomware attacks on organisations. Science and education (15%), manufacturing and industry (15%), government (14%), and healthcare (14%) sectors were most targeted by ransomware operators in Q1 2021. WannaCry ransomware resurged, with the number of organisations infected by WannaCry in March 2021 increased 40 times compared to October 2020.

- **Threat actors actively exploited vulnerabilities in Microsoft Exchange Server (ProxyLogon vulnerabilities) and the outdated Accellion FTA data transfer software in Q1 2021.** In addition, a zero-day vulnerability in SonicWall NetExtender and Secure Mobile Access VPN products was also exploited by attackers in Q1 2021.

- **Threat actors trended to attack virtualisation environments.** Remote code execution vulnerabilities (CVE-2021-21972, CVE-2019-5544 and CVE-2020-3992) in VMware products were targeted by multiple hacker groups. Multiple scanning activities probing for vulnerable systems were observed.

Source: Positive Technologies

[50] https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2021-q1/

Industry Insight on Cyber Security Threat Trends

Old vulnerabilities were still being exploited in the wild

Cognyte published the 'Vulnerability Threat Intelligence Report'[51], which summarised their analysis on latest common vulnerabilities and exposures (CVEs) on data collected from 15 different Deep and Dark Web forums from January 2020 to March 2021. The key findings were:

- **Among the 1,267 different CVEs mentioned in the 15 Dark Web forums studied, the 6 most popular CVEs were CVE-2020-1472 (aka ZeroLogon), CVE-2020-0796 (aka SMBGhost), CVE-2019-19781, CVE-2019-0708 (aka BlueKeep), CVE-2017-11882, and CVE-2017-0199.** Five of them were related to different Microsoft products such as Windows operating systems and Microsoft Office. Four CVEs, CVE-2020-0796 (52 posts in 11 forums), CVE-2019-19781 (49 posts in 10 forums), CVE-2019-0708 (38 posts in 9 forums) and CVE-2017-11882 (36 posts in 12 forums), were in the top five mentioned CVEs in terms of both number of posts and number of forums. All these CVEs were exploited by attackers in different campaigns.

- **The popularity of CVEs were different in forums of different languages.** For instance, CVE-2020-0796 was most mentioned in Chinese speaking forums, while the top mentioned CVE in Russian and English speaking forums included CVE-2019-19781. CVE-2020-0688 was also popular in English-speaking forums and CVE-2019-6340 was most mentioned in Turkish speaking forums.

- **Old CVEs were still interested and abused by threat actors**. More than 16% of CVEs mentioned in the forums were disclosed in 2018 or earlier. The oldest one was CVE-2005-1513, which was disclosed for over 15 years. Among the 6 most popular CVEs, two of them were disclosed in 2017. CVE-2012-0158, a CVE disclosed in 2012, was mentioned in only 16 posts in 9 different forums, was exploited by threat actors during the COVID-19 pandemic in 2020. Organisations should patch their systems on a timely basis to mitigate the risk.

Source: Cognyte

[51] https://www.cognyte.com/resources/cve-threat-research-report-2021/

Highlight of Microsoft July 2021 Security Updates

Product Family	Impact[52]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB5004235, KB5004237, KB5004238, KB5004244, KB5004245, KB5004249, KB5004945, KB5004946, KB5004947, KB5004948, KB5004950
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5004235, KB5004237, KB5004238, KB5004244, KB5004245, KB5004945, KB5004947, KB5004948
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5004233, KB5004285, KB5004294, KB5004298, KB5004302, KB5004954, KB5004956, KB5004958, KB5004960
Microsoft Exchange Server	Remote Code Execution	Critical ★★★★	KB5001779, KB5003611, KB5003612, KB5004778, KB5004779, KB5004780
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB5001949, KB5001973, KB5001977, KB5001979, KB5001983, KB5001986, KB5001993

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-Jul.

Learn more:
High Threat Security Alert (A21-07-04): Multiple Vulnerabilities in Microsoft Products (July 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=608)

Data analytics powered by CRisP in collaboration with GovCERT.HK

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