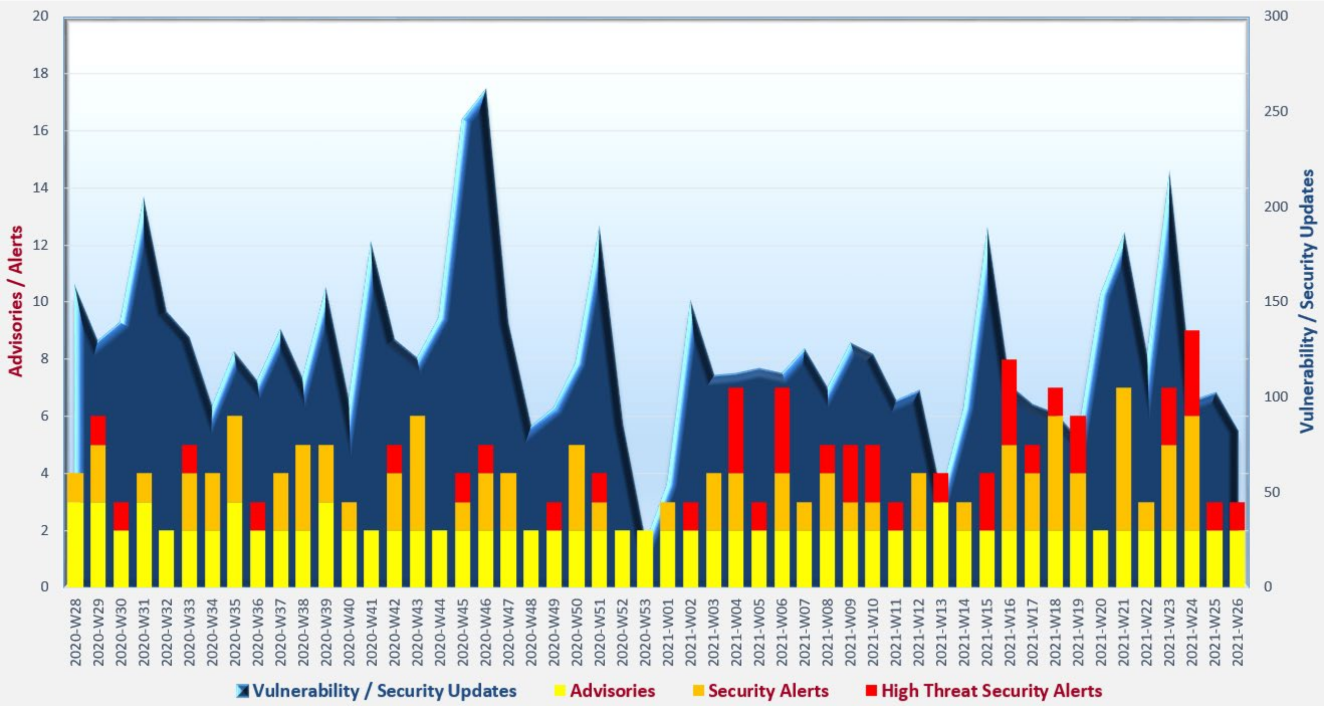
Cyber Security Threat Trends 2021-M06

June 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:

- ✧ Attackers continue to seize opportunities to compromise **Virtual Private Network (VPN)** of organisations. Organisations should prioritise and promptly patch or perform mitigation measures to their VPN solutions, and keep abreast of up-to-date cyber security news and vendors' security bulletins.
- ✧ **Exposed vulnerabilities, servers and cloud instances** are always targeted by attackers. System administrators should patch their systems timely, disable unneeded network ports and services, and keep an up-to-date IT asset inventory including servers and public cloud instances.
- ✧ **Ransomware attacks** resurge with new attack and extortion tactics, causing serious damage to the victims. Organisations should strictly follow the least privilege principle, implement updated endpoint protection solutions, regularly backup their data, keep offline backup, and properly encrypt their sensitive data.

[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 Canadian Centre for Cyber Security[5] issued alerts regarding multiple vulnerabilities in Microsoft products. Vulnerabilities in Microsoft Windows and Server (CVE-2021-31199, CVE-2021-31201, CVE-2021-31955, CVE-2021-31956, CVE-2021-33739 and CVE-2021-33742) were being actively exploited. Successful exploitation could lead to remote code execution, elevation of privilege, or information disclosure.

- GovCERT.HK[6, 7, 8], HKCERT[9, 10, 11], Australian Cyber Security Centre (ACSC)[12], Canadian Centre for Cyber Security[13], and Cybersecurity and Infrastructure Security Agency (CISA)[14, 15] issued alerts regarding multiple vulnerabilities in Google Chrome and Microsoft Edge (Chromium-based). Vulnerabilities CVE-2021-30551 and CVE-2021-30554 were being actively exploited.

- GovCERT.HK[16], HKCERT[17], JPCERT[18], MyCERT[19] and CISA[20] updated alerts regarding multiple vulnerabilities in VMware vCenter Server and VMware Cloud Foundation. PoC codes for exploitation of a critical remote code execution (RCE) vulnerability (CVE-2021-21985) were publicly available and active exploitation on the vulnerability were detected.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=593

[3] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-jun-2021

[4] https://www.jpcert.or.jp/english/at/2021/at210027.html

[5] https://www.cyber.gc.ca/en/alerts/microsoft-security-advisory-june-2021-monthly-rollup

[6] https://www.govcert.gov.hk/en/alerts_detail.php?id=596

[7] https://www.govcert.gov.hk/en/alerts_detail.php?id=603

[8] https://www.govcert.gov.hk/en/alerts_detail.php?id=604

[9] https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20210610

[10] https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20210615

[11] https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20210618

[12] https://www.cyber.gov.au/acsc/view-all-content/alerts/google-releases-security-updates-chrome-browser

[13] https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-59

[14] https://us-cert.cisa.gov/ncas/current-activity/2021/06/10/google-releases-security-updates-chrome

[15] https://us-cert.cisa.gov/ncas/current-activity/2021/06/18/google-releases-security-updates-chrome

[16] https://www.govcert.gov.hk/en/alerts_detail.php?id=591

[17] https://www.hkcert.org/security-bulletin/vmware-products-multiple-vulnerabilities_20210526

[18] https://www.jpcert.or.jp/english/at/2021/at210025.html

[19] https://www.mycert.org.my/portal/advisory?id=MA-807.062021

[20] https://us-cert.cisa.gov/ncas/current-activity/2021/06/04/unpatched-vmware-vcenter-software

CERT Advisories

- GovCERT.HK[21], HKCERT[22], CISA[23], and Canadian Centre for Cyber Security[24] issued alerts regarding multiple vulnerabilities in various Apple devices. Vulnerabilities CVE-2021-30761 and CVE-2021-30762 were being actively exploited.

Growth and evolution of ransomware attacks

Ransomware became key cyber threat nowadays and high-profile ransomware incidents happened recently. In view of that, CERT bodies issued advisories reminding individuals and organisations to stay vigilant to ransomware. HKCERT[25] revealed the multiple extortion tactics used in ransomware attacks, including Distributed Denial of Service (DDoS) extortion, contacting victims' customers and partners, short selling victims' stock, and disruption of critical infrastructure systems operated by victims. SingCERT[26,27] and CISA[28] also published advisories on recent ransomware incidents and recommended preventive measures against ransomware attacks. Moreover, CISA[29] has released the Ransomware Readiness Assessment (RRA) in the Cyber Security Evaluation Tool (CSET), which is a self-assessment tool to help organisations assess their readiness on defence against ransomware attacks and recovery from ransomware incidents.

Best and bad cyber security practices

Canadian Centre for Cyber Security[30] published a guidance that summarised security measures in thirteen security control categories, which aimed to help organisations in reducing cyber risk and improving the ability to respond to security incidents. In order to remind organisations to avoid bad practices in cyber security, CISA[31],[32] introduced a catalogue of bad cyber security practices which adversely affect the cyber security of organisations and critical infrastructure.

[21] https://www.govcert.gov.hk/en/alerts_detail.php?id=599

[22] https://www.hkcert.org/security-bulletin/apple-ios-multiple-vulnerabilities_20210615

[23] https://us-cert.cisa.gov/ncas/current-activity/2021/06/15/apple-releases-security-updates-ios-1254

[24] https://www.cyber.gc.ca/en/alerts/apple-security-advisory-32

[25] https://www.hkcert.org/blog/ransomware-keep-evolving-multiple-extortion

[26] https://www.csa.gov.sg/en/singcert/Advisories/ad-2021-006

[27] https://www.csa.gov.sg/en/singcert/Publications/the-ransomware-menace-continues

[28] https://us-cert.cisa.gov/ncas/current-activity/2021/06/09/cisa-addresses-rise-ransomware-targeting-operational-technology

[29] https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat

[30] https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035

[31] https://us-cert.cisa.gov/ncas/current-activity/2021/06/29/cisa-begins-cataloging-bad-practices-increase-cyber-risk

[32] https://www.cisa.gov/BadPractices

Industry Insight on Cyber Security Threat Trends

Organisations should strive to minimise their attack surface and areas of exposure

Zscaler published the '2021 "Exposed" Report'[33], which summarised their analysis on attack surface based on data collected from around 1,500 organisations during February 2020 to April 2021. The key findings were:

- **Organisations had an average of 135 known vulnerabilities exposed.** Among the 202,316 potential CVE vulnerabilities found in the report period, 49 percent were classified as Critical or High severity. The top five most common CVEs found were all related to Apache HTTP Server.

- **95,742 web servers were found supported outdated SSL/TLS protocols, including SSLv2, SSLv3, TLSv1 and TLSv1.1.** According to the data analysed, Hong Kong organisations had an average of 107 servers with SSL/TLS vulnerabilities. System administrators should configure their servers to support current protocols such as TLSv1.2 and TLSv1.3 to avoid man-in-the-middle attacks and cease using outdated protocols.

- **Organisations had an average of 40 public cloud instances exposed.** This could be due to misconfiguration, instances setup by personnel without IT knowledge, or forgotten / abandoned instances. Due to the increased adoption of cloud platform, organisations should have a full picture of their cloud assets for a complete visibility on the attack surfaces.

- **Telecommunication industry had the highest possible CVE exposure and outdated SSL/TLS issues, with an average of 319 CVEs and 106 servers with outdated SSL/TLS.** Restaurants, bars & food services had the most server and public cloud exposure, with an average of 403 exposed servers and 129 public cloud instances exposed. Number of CVE vulnerability (111), SSL/TLS vulnerability (44), exposed servers (149) and exposed public cloud instances (28) in Government sector were all below the average values. Nevertheless, government agencies should endeavour to eliminate any unnecessary attack surface as government organisations were frequent targets of cyberattack.

Source: Zscaler

[33] https://info.zscaler.com/resources-ebooks-global-corporate-network-attack-surface-report

Industry Insight on Cyber Security Threat Trends

Downward trend in Malware and Botnet activities, but attack against remote access grew in Q1 2021

Nuspire issued the "Quarterly Threat Landscape Report, Q1 2021"[34], which included analysis on 90 billion traffic logs collected from thousands of devices around the world. The key findings were:

- **A drop of more than 50% was observed in malware activity comparing with Q4 2020, due to the shrinkage of activity from Visual Basic for Applications (VBA) and agent variants, as well as from Emotet**. VBA agents were still the top malware variants although their activities dropped by nearly 65% compared to Q4 2020. Emotet activity diminished for about 40% compared to the last quarter in 2020, owing to the decommissioning of command-and-control infrastructure worldwide.

- **Botnet activity decreased by around 10% as compared to Q4 2020**. The main cause of the decrease was the nearly complete closure of Emotet botnet. In Week 11, ZeroAccess botnets recorded a huge surge of 6,194 times in activity as compared to the start of Q1 2021.

- **Server Message Block (SMB) brute force attempts skyrocketed with a rise of more than 15,000,000 attempts near the end of Q1 2021.** Organisations should deploy system patches in a timely manner, adopt firewalls and Intrusion Prevention Systems (IPS), and disable unused services and network ports.

- **Increase in attacks aimed at exploiting Virtual Private Network (VPN) solutions vulnerabilities were observed in Q1 2021.** For instance, attacks targeted CVE-2018-13379 in Fortinet's FortiGuard SSL VPN web portal and CVE-2019-11510 in Pulse Connect Secure VPN recorded increase of over 19 times and 15 times respectively.

- **Organisations should adopt a layered approach in security defence.** Endpoint protection and next-generation anti-malware solution should be deployed. Network segregation and least privilege principle should be adopted. Organisations should also conduct regular security awareness training to educate their staff with up-to-date defence knowledge against emerging cyber attack tactics.

Source: Nuspire

[34] https://www.nuspire.com/resources/q1-2021-threat-report

Industry Insight on Cyber Security Threat Trends

Attack volume and sophistication level increased in 2020

VMware surveyed more than 3,500 C-level officers from organisations in various sectors across 14 locations and compiled the "VMware Global Security Insights Report 2021"[35], which summarised the analysis of respondents' view on the landscape and trend of cyber security in 2020. The highlights from the report included:

- **81% of respondents' organisations suffered security breach in 2020.** The top five causes of security breach were third-party applications, ransomware, outdated security technology, process weaknesses and Operating System vulnerability.
- **Ransomware resurged with more sophisticated attack campaigns and double extortion attack tactics.** It was the most prevalent attack type in the US, Japan, and some European regions such as Germany, France, the Nordics region and the UK.
- **Over 70% of respondents indicated that attacks became more sophisticated and both the number and volume of attacks increased in 2020.** Among these respondents, 78% of them opined the growth of cyber attack was due to the increased remote workforces during the COVID-19 pandemic. To address the challenge on the expansion of attack surface, organisations should improve their visibility on applications, data and endpoints to provide secure remote work environments.
- **Respondents opined that their organisations experienced cloud-based attacks most frequently in 2020.** The sudden transformation to highly distributed working practices during the COVID-19 pandemic led to surge in cloud usage. 98% of respondents have already used or planned to adopt a cloud-first security approach to protect their cloud workloads.

Source: VMware

[35] https://www.carbonblack.com/resources/global-security-insights-report-2021/

Highlight of Microsoft June 2021 Security Updates

Product Family	Impact[36]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB5003635, KB5003637, KB5003638, KB5003646, KB5003687
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5003637, KB5003638, KB5003646
Windows 8.1, Windows Server 2012, 2012 R2 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5003636, KB5003671, KB5003681, KB5003696, KB5003697
Microsoft Outlook	Remote Code Execution	Important ★★★	KB5001934, KB5001942
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB5001943, KB5001947, KB5001950, KB5001951, KB5001953, KB5001955, KB5001956, KB5001963

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/releaseNote/2021-Jun.

Learn more:
High Threat Security Alert (A21-06-02): Multiple Vulnerabilities in Microsoft Products (June 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=593)

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