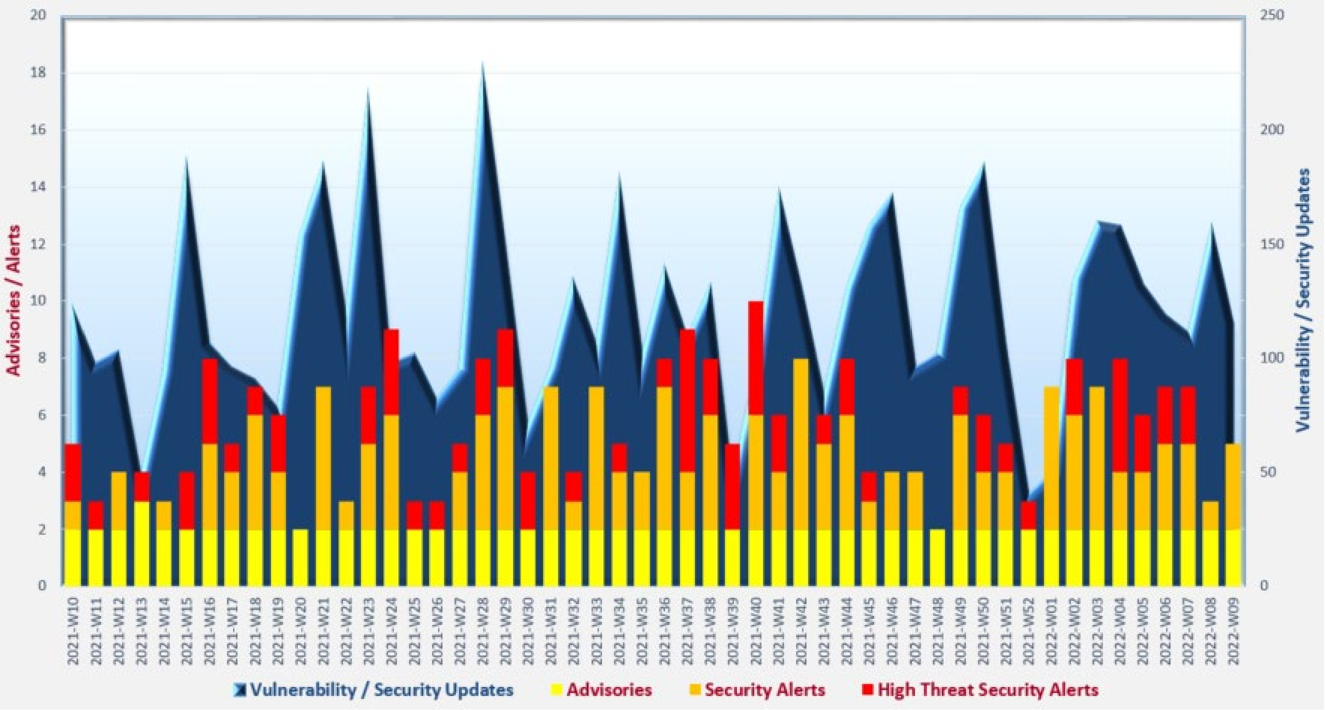
Cyber Security Threat Trends 2022-M02

February 2022

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:

Remote Desktop Protocol (RDP) is aggressively targeted by attackers. System administrators should disable internet-facing RDP, use strong passwords, avoid using default and blacklisted passwords and change the passwords regularly. Security patches should be applied timely. Unnecessary services and network ports should be disabled. Multi-factor authentication should be adopted whenever applicable.

[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], Cybersecurity and Infrastructure Security Agency (CISA)[6] and Canadian Centre for Cyber Security[7,8] issued alerts regarding multiple vulnerabilities in Google Chrome and Microsoft Edge (Chromium-based). Vulnerability (CVE-2022-0609) was being exploited in the wild.
- GovCERT.HK[9], HKCERT[10], SingCERT[11], CISA[12] and Canadian Centre for Cyber Security[13] issued alerts regarding an arbitrary code execution vulnerability (CVE-2022-22620) in various Apple devices. The vulnerability was being actively exploited.
- GovCERT.HK[14] issued alert regarding multiple vulnerabilities in Cisco products. PoC for exploitation of some vulnerabilities in Cisco Small Business RV Series Routers was publicly available.
- SingCERT[15] and CISA[16] issued alerts regarding a zero-day vulnerability (CVE-2022-24086) in Adobe Commerce and Magento Open Source Platforms. Successful exploitation could allow an attacker to take control of an affected system. The vulnerability was being exploited in the wild.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=740
[3] https://www.govcert.gov.hk/en/alerts_detail.php?id=742
[4] https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20220215
[5] https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20220217
[6] https://www.cisa.gov/uscert/ncas/current-activity/2022/02/15/google-releases-security-updates-chrome
[7] https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-av22-076
[8] https://www.cyber.gc.ca/en/alerts/microsoft-edge-security-advisory-av22-081
[9] https://www.govcert.gov.hk/en/alerts_detail.php?id=738
[10] https://www.hkcert.org/security-bulletin/apple-products-remote-code-execution-vulnerability_20220211
[11] https://www.csa.gov.sg/en/singcert/Alerts/al-2022-006
[12] https://www.cisa.gov/uscert/ncas/current-activity/2022/02/11/apple-releases-security-updates-multiple-products
[13] https://www.cyber.gc.ca/en/alerts/apple-security-advisory-av22-071
[14] https://www.govcert.gov.hk/en/alerts_detail.php?id=732
[15] https://www.csa.gov.sg/en/singcert/Alerts/al-2022-007
[16] https://www.cisa.gov/uscert/ncas/current-activity/2022/02/14/adobe-releases-security-updates-commerce-and-magento-open-source

- HKCERT[17], CERT NZ[18] and SingCERT[19] issued alerts regarding vulnerabilities in QNAP and Asustor Network Attached Storage (NAS) devices. The vulnerabilities were being actively exploited for ransomware purpose. System administrators should disable SSH and any remote access service of the NAS devices and should not expose the devices to the Internet.

Trend of ransomware threat

Cybersecurity authorities in the United States[20], Australia[21] and the United Kingdom[22] issued joint advisory highlighting globalised threat of ransomware. The advisory included information on attackers' behaviours, trends and mitigation recommendations.

Review and forecast of cyber security situation in Hong Kong

HKCERT[23] announced a review on the information security situation in Hong Kong in 2021 and the forecast for 2022. Among the 7,725 security incidents handled in 2021, 3,737 (48%) were phishing incidents. The number of phishing incidents increased 7% from 2020, continued the rising trend for four consecutive years and reached a new high. HKCERT reminded individuals and organisations the key information security risks in 2022 including security risks on Metaverse, Non-fungible token (NFT), cryptocurrency, emerging technologies, supply chain attacks, as well as targeted and organised cyber attacks.

[17] https://www.hkcert.org/security-bulletin/asustor-nas-vulnerability_20220225

[18] https://www.cert.govt.nz/it-specialists/advisories/qnap-and-asustor-nas-vulnerabilities-exploited-to-deploy-ransomware/

[19] https://www.csa.gov.sg/singcert/Alerts/al-2022-008

[20] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

[21] https://www.cyber.gov.au/acsc/view-all-content/advisories/2021-trends-show-increased-globalized-threat-ransomware

[22] https://www.ncsc.gov.uk/news/joint-advisory-highlights-increased-globalised-threat-of-ransomware

[23] https://www.hkcert.org/press-centre/cyber-attacks-become-more-complex-and-diversified-phishing-attacks-reach-new-high-hkcert-calls-on-public-to-raise-awareness-of-information-security

Industry Insight on Cyber Security Threat Trends

Attacks on login and registration increased in 2021

Arkose Labs issued the "2022 State of Fraud and Account Security Report"[24], which summarised their findings on trends in fraud attacks in 2021. The key findings were:

- **There was an 85% year-on-year increase in attacks targeting login and registration in 2021.** 20% of logins were Account Take Over (ATO) attempts. Credential stuffing, in which attackers used lists of compromised user credential to breach into a system, contributed to 80% of login attacks. Attackers made use of compromised accounts to steal sensitive information or resell the credentials. Fake account attacks increased by more than 300% in 2021, 25% of new account registrations were fake. Fake new accounts were used for content scraping, sending spam and phishing messages as well as free trial abuse.

- **Five out of the six industries covered in the report experienced increase in attack rate in 2021.** Attack rate of travel industry in 2021 increased 12.5 times compared to 2020 due to increased web scraping activities that crawled content from websites and inventory hoarding activities that caused inventory unavailable to legitimate customers. 45% of traffic on travel web sites were related to scraping attacks. Technology, media and entertainment, financial and retail industries also experienced increase of two to five times in attack rate. Attack rate for gaming industry in 2021 levelled off after experiencing a high attack rate in 2020.

- **Asia was the top attacking region and accounted for 40% of attacks in 2021.** Attack patterns varied in different regions. For instance, social media was the primary target for Europe, while technology and gaming industries were the main targets for Asia Pacific.

- **86% of all attacks in 2021 were automated by utilising bots.** Bots became more intelligent and sophisticated, yet easier and less expensive to deploy. They could mimic human online behaviour, perform different tasks such as IP spoofing and CAPTCHA solving during attacks.

- Organisations should improve their bot / spoofing detection and defence, deploy multi-layered user behaviour analysis and adopt more powerful challenge-response strategy for fraud prevention.

Source: Arkose Labs

[24] https://www.arkoselabs.com/resourceasset/2022-state-of-fraud-and-account-security-report/

Industry Insight on Cyber Security Threat Trends

77% of flaws found in third party libraries could not be fixed within three months after discovery

Veracode released the report "State of Software Security"[25], based on the application scanning results collected from over 1 million dynamic analysis scans, 5 million static analysis scans and 18 million software composition analysis scans. The key findings were:

- **On average, around 1 in 10 third party libraries had flaw in 2021, a notable decrease from around 35% in 2017.** Downward trends in percentage of libraries with known vulnerabilities were observed for libraries using Python (from 25% to around 10%), JavaScript (from 10% to under 4%) and Java (from 25% to around 12%).

- **Different software scanning methods yielded different results in weakness discovered.** For instance, the top 3 issues discovered by static analysis were CRLF injection, information leakage and cryptographic issues. Flaws in server configuration, insecure dependencies and information leakage were mostly found by dynamic analysis. Software composition analysis results indicated that insufficient input validation, information leakage and encapsulation were the top 3 discovered issues.

- **Issues found in dynamic analysis were resolved with the fastest pace.** More than 40% of issues were closed in the first 3 months after discovery and half of the issues could be resolved in 143 days. 32% of the issues discovered in static analysis were solved in the first 3 months and half of the issues were cleared in 290 days. Issues from software composition analysis took the longest time to remediate, with 77% of issues remain unfixed in the first 3 months and it took up 397 days for solving half of the issues, despite the duration already decreased significantly from over 3 years in 2017.

- **In 2021, 90% of applications conducted scanning more than once per week.** Moreover, there was a 31% rise in adoption of multiple scan types from 2018 to 2021.

Source: Veracode

[25] https://info.veracode.com/report-state-of-software-security-volume-12.html

Industry Insight on Cyber Security Threat Trends

Threat detections increased and Remote Desktop Protocol (RDP) attacks skyrocketed in the last four months of 2021

ESET released the "Threat Report T3 2021"[26], which summarised the threat trends observed from September 2021 to December 2021 (T3 2021) and the outlook in 2022. The key findings were:

- **Number of RDP brute-force attacks accelerated from 55 billion in T2 2021 to 206 billion in T3 2021, an increase of 274%.** Compared with 2020, number of RDP attacks in 2021 recorded an increase of almost 9 times from 29 billion to 288 billion. This external network intrusion vector was detected by almost half of the reporting clients (46%) in 2021. RDP attacks were expected to grow further in 2022.

- **Email threats increased 8.5% in T3 2021.** Increase in phishing attacks continued since May 2021. Detection on a publicly available exploit for CVE-2017-11882, a vulnerability in Microsoft Equation Editor, grew 60% in T3 2021. Hong Kong was one of the locations with most detections on phishing emails impersonating DHL during September to October 2021.

- **Ransomware detections grew slightly (0.6%) in T3 2021.** Several spikes were observed in September, October and December which were caused by activities of different ransomware families.

- **Detections of Android threats increased 2.8% in T3 2021, in which ScamApps (63%) and Ransomware (114%) recorded the largest increase in detections.** Although Android banking malware detections decreased by 20.6% in T3 2021, the total number of detections was more than five-folded in 2021 compared to 2020. More malicious apps exploiting the vulnerabilities of Android devices were expected in 2022.

- **Number of macOS threats detection declined 5.9% in T3 2021, with more than one-third of macOS threats detections were Trojans.** Hong Kong was targeted by a watering hole attack exploiting iOS and macOS zero-day or N-day vulnerabilities in 2021. In 2022, more targeted and evasive attacks would be expected and adware would continue to be the most common macOS threat.

Source: ESET

[26] https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf

Highlight of Microsoft February 2022 Security Updates

Product Family	Impact[27]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Important ★★★	KB5010342, KB5010345, KB5010351, KB5010358, KB5010359, KB5010386
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Important ★★★	KB5010342, KB5010351, KB5010354, KB5010359, KB5010456
Windows 8.1 and Windows Server 2012, 2012 R2	Elevation of Privilege	Important ★★★	KB5010392, KB5010395, KB5010403, KB5010412, KB5010419
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB3118335, KB3172514, KB5002133, KB5002137, KB5002140, KB5002146, KB5002149, KB5002156

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/2022-Feb.

Learn more:
High Threat Security Alert (A22-02-02): Multiple Vulnerabilities in Microsoft Products (February 2022) (https://www.govcert.gov.hk/en/alerts_detail.php?id=736)

Data analytics powered by CRisP in collaboration with GovCERT.HK

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