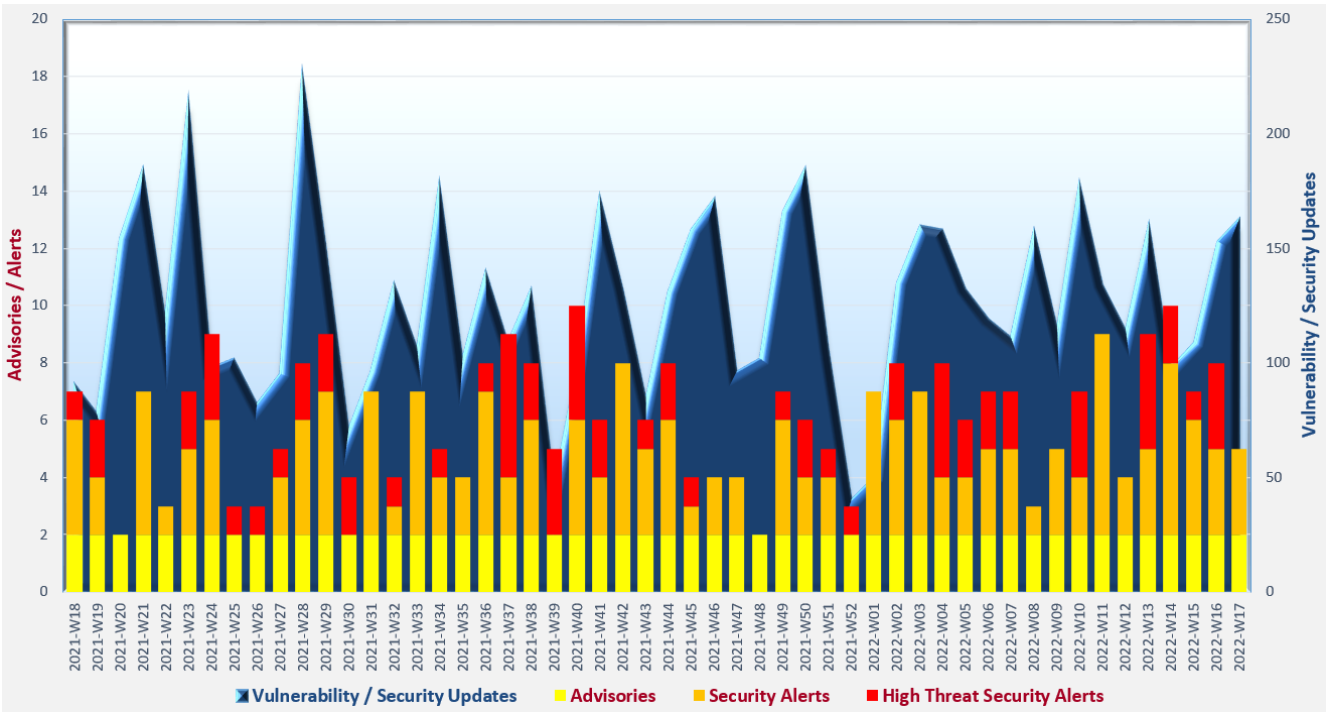
TLP:WHITE

Cyber Security Threat Trends 2022-M04

April 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:

Script-based attacks have been a major attack vector used by attackers for a long time. System administrator should restrict the execution of scripts on need basis only. Advanced malware protection solution with behaviour threat monitoring capability should be deployed if applicable. Least privilege principle and zero trust defence approach should be adopted.

[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], Cybersecurity and Infrastructure Security Agency (CISA)[4], Canadian Centre for Cyber Security[5], SingCERT[6], JPCERT[7] and MyCERT[8] issued alerts regarding multiple vulnerabilities in Microsoft products. An elevation of privilege vulnerability (CVE-2022-24521) was being actively exploited. Technical details of vulnerability CVE-2022-26904 were publicly disclosed.

- GovCERT.HK[9,10], HKCERT[11,12], CISA[13] and Canadian Centre for Cyber Security[14,15] issued alerts regarding an actively exploited vulnerability (CVE-2022-1364) in Google Chrome and Microsoft Edge (Chromium-based).

- GovCERT.HK[16,17], HKCERT[18], CISA[19], Canadian Centre for Cyber Security[20] and SingCERT[21] issued alerts regarding multiple vulnerabilities in VMware products. Vulnerabilities (CVE-2022-22954, CVE-2022-22960 and CVE-2022-22965) were being exploited in the wild.

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=784
3 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-april-2022
4 https://www.cisa.gov/uscert/ncas/current-activity/2022/04/12/microsoft-releases-april-2022-security-updates
5 https://www.cyber.gc.ca/en/alerts/microsoft-security-advisory-april-2022-monthly-rollup-av22-200
6 https://www.csa.gov.sg/singcert/Alerts/al-2022-019
7 https://www.jpcert.or.jp/english/at/2022/at220010.html
8 https://www.mycert.org.my/portal/advisory?id=MA-831.042022
9 https://www.govcert.gov.hk/en/alerts_detail.php?id=788
10 https://www.govcert.gov.hk/en/alerts_detail.php?id=789
11 https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerability_20220419
12 https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20220419
13 https://www.cisa.gov/uscert/ncas/current-activity/2022/04/15/google-releases-security-updates-chrome
14 https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-av22-211
15 https://www.cyber.gc.ca/en/alerts/microsoft-edge-security-advisory-av22-213
16 https://www.govcert.gov.hk/en/alerts_detail.php?id=775
17 https://www.govcert.gov.hk/en/alerts_detail.php?id=770
18 https://www.hkcert.org/security-bulletin/vmware-products-multiple-vulnerabilities_20220407
19 https://www.cisa.gov/uscert/ncas/current-activity/2022/04/07/vmware-releases-security-updates
20 https://www.cyber.gc.ca/en/alerts/vmware-security-advisory-av22-187
21 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-018

- GovCERT.HK[22], HKCERT[23] and CISA[24] issued alerts regarding multiple vulnerabilities in Apple iOS and iPadOS. An arbitrary code execution vulnerability (CVE-2022-22675) was being actively exploited in the wild.

GovCERT.HK Annual Report 2021

GovCERT.HK published the "GovCERT.HK Annual Report 2021"[25], highlighting the achievements and milestones made in 2021 on various areas including Cyber Security Information Sharing, Liaison and Collaboration, Awareness Building and Public Education, etc.

Security events related to Hong Kong decreased 4.8% in Q1 2022

HKCERT released its "Hong Kong Security Watch Report (Q1 2022)"[26]. The number of security events decreased from 4,753 in Q4 2021 to 4,527 in Q1 2022. The number of phishing events decreased 24% in Q1 2022. For botnets in Hong Kong network, the number of Sality soared 356% and became the second largest botnet family in Q1 2022. There were 718 defacement events in Q1 2022, 21% increase as compared with 595 events in Q4 2021. The report also provided security recommendations on prevention of Non-Fungible Token (NFT) cyber attacks and proper use of smart contract.

[22] https://www.govcert.gov.hk/en/alerts_detail.php?id=768
[23] https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20220401
[24] https://www.cisa.gov/uscert/ncas/current-activity/2022/04/01/apple-releases-security-updates-0
[25] https://www.govcert.gov.hk/en/annualreport.html
[26] https://www.hkcert.org/watch-report/hong-kong-security-watch-report-q1-2022

Industry Insight on Cyber Security Threat Trends

Almost 66% of newly discovered high risk URLs in 2021 involved phishing

BrightCloud released the "2022 BrightCloud Threat Report"[27] which included analysis on data collection from over 95 million sensors and other cyber threat information from different sources. The key findings were:

- **Malicious files detected at monitored Windows endpoints in 2021 decreased 58% as compared with 2020.** Around 86% of detected malware was unique to a single computer, similar to the figures in 2019 and 2020. The infection rate of business computers was around half of consumer computers. More than 45% of computers had multiple infections (i.e. infected more than once) in 2021, and over 12% were infected more than five times. Among the five regions with the highest infection rates, more than 14% of the computers were still using Windows 7, which was end of support in early 2020. Manufacturing, public administration and information were the top three industries with the highest infection rate.

- **In 2021, there was an increase in single-stage ransomware attacks.** Attackers directly distributed ransomware executables by phishing email for faster infection. Researchers anticipated the emergence of "stealth" ransomware attacks in 2022, in which attackers would threaten their targets to pay the ransom before launching the ransomware attacks, taking the advantage that some victims could opt for avoiding damage in organisations' image or compliance fines if actual attacks were conducted and disclosed, and resources to recover encrypted files for service resumption.

- **Almost 66% of 4 million new risky URLs detected in 2021 were related to phishing.** Hong Kong was one of the top five locations for malware site URLs and phishing URLs. There were two surges of phishing activities in May and November 2021, accounted for around 17% and 34% of detected phishing activities in 2021. Apple, Facebook, Microsoft and Google were among the top five most impersonated brands in phishing attacks for three consecutive years since 2019.

- **Regarding the top 50,000 malicious IP addresses in 2021, all of them performed multiple malicious behaviours, of which scanners, windows exploits, spam sources and botnets were the 4 major categories.** More than half of the top 50,000 malicious IPs were operative for three months or less.

Source: BrightCloud

[27] https://www.brightcloud.com/land/2022-brightcloud-threat-report

Industry Insight on Cyber Security Threat Trends

Over 85% of surveyed organisations encountered successful cyber attacks in 2021

CyberEdge Group issued its "2022 Cyberthreat Defense Report"[28], which highlighted the analysis results on replies from 1,200 IT security professionals across 19 industries in a survey conducted in November 2021. Major insights covered in the report included:

- **85.3% of surveyed organisations were impacted by successful cyber attacks in 2021, recorded a slight drop from 86.2% in 2020.** However, 40.7% of surveyed organisations encountered at least 6 cyber attacks, a record high since 2014. Organisations affected by successful ransomware attacks increased from 68.5% in last survey to a record high at 71%. 76.1% of respondents expected there would be at least one successful attack to their organisations in 2022, reached a new high.

- **Over 84% of surveyed organisations experienced lack of skilled IT security personnel, indicated in four consecutive years' survey results.** This contributed to a upward trend on outsourcing to managed security service providers (MSSPs). Monitoring and managing Security Information and Event Management (SIEM) platforms, detecting and responding to advanced cyberthreats / managed detection and response (MDR), as well as monitoring and managing web application firewalls (WAFs) were the top 3 functions outsourced to MSSPs.

- **Malware, account takeover (ATO) / credential abuse attacks and ransomware were the top three most concerning cyber threats as opined by the survey respondents.** For web and mobile application attacks, personally identifiable information (PII) harvesting and ATO / credential stuffing attacks were the most concerning attacks. Regarding cloud security, over 40% of survey respondents considered detecting unauthorised application usage, detecting and responding to cyberthreats, as well as accessing and inspecting multi-cloud traffic were the top 3 hybrid cloud security challenges.

- **41.9 % of surveyed organisations planned to implement next-generation firewall for network security.** Other technologies planned to implement included deception technology / honeypots (40.5%) for endpoint security, bot management (39.8%) for application and data security, advanced security analytics (39.7%) and threat intelligence platform or service (39.7%) for security management and operations, and biometrics (40.9%) for identity and access management.

Source: CyberEdge Group

[28] https://cyber-edge.com/cdr/

Industry Insight on Cyber Security Threat Trends

Malware detected and network attack volume increased around 40% in Q4 2021

WatchGuard issued the "Internet Security Report - Q4 2021"[29], which summarised their findings on trends in malware and network attack based on the data collected from various sources. The highlights from the report included:

- **Number of malware detected in Q4 2021 increased almost 40% as compared with Q3 2021,** even though zero-day malware which evaded from signature-based protection decreased around 2% to 65.6% in Q4 2021. 66.7% of malware was delivered over encrypted connections. Europe, the Middle East, and Africa (EMEA) recorded the highest malware detection (48%), followed by Asia-Pacific (APAC) (29%) and North, Central and South America (AMER) (23%).

- **Network attack volume reached a new high since Q4 2018 at around 5.7 million network exploits, increased around 40% from Q3 2021.** Web SQL injection attempt was the top network attack since Q2 2019, and was one of the most widespread network attacks in Q4 2021 as well. 61% of network attacks were detected in AMER, followed by APAC (29%) and EMEA (10%).

- **Among the top five most widespread malware, two of them had high detections in Hong Kong.** Almost 30% of Microsoft Office exploit CVE-2018-0802 and 16% of RTF document malware RTF-ObfsObjDat.Gen were detected in Hong Kong.

- **Script-based attacks remained the top source of malware infections throughout 2021, accounted for 86% of attack vectors in Q4 2021.** There was a downward trend for Java as attack vector in 2021, from several thousand detections in Q1 2021 to less than 10 detections in Q4 2021.

Source: WatchGuard

[29] https://www.watchguard.com/wgrd-resource-center/security-report-q4-2021

Highlight of Microsoft April 2022 Security Updates

Product Family	Impact[30]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5012591, KB5012592, KB5012596, KB5012599, KB5012647, KB5012653
Windows Server 2016, 2019, 2022 and Server Core installation	Remote Code Execution	Critical ★★★★	KB5012596, KB5012599, KB5012604, KB5012647
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5012639, KB5012650, KB5012666, KB5012670
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB5002143, KB5002148, KB5002162, KB5002169, KB5002175, KB5002177, KB5012681, KB5012686

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-Apr.

Learn more:

High Threat Security Alert (A22-04-13): Multiple Vulnerabilities in Microsoft Products (April 2022) (https://www.govcert.gov.hk/en/alerts_detail.php?id=784)

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