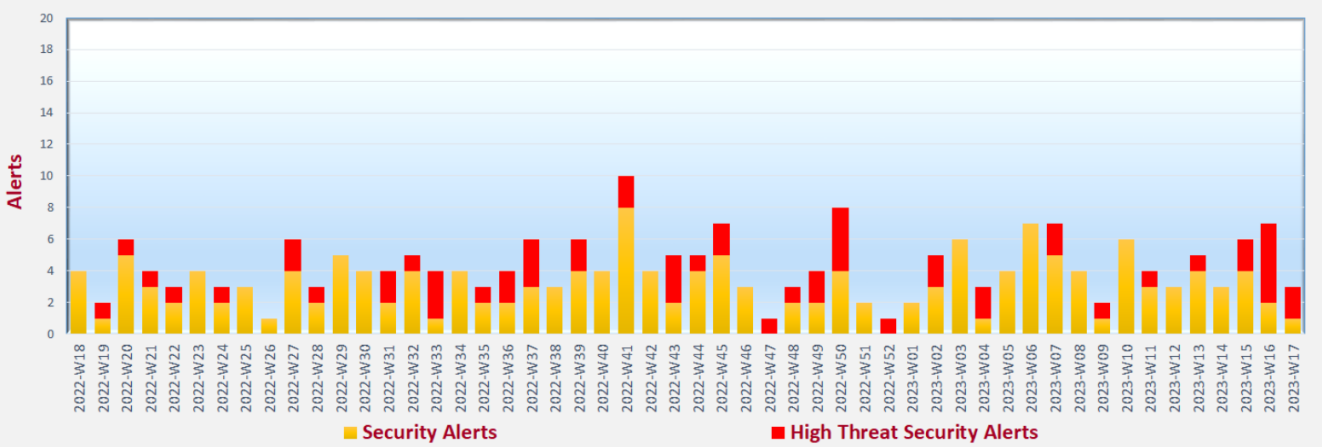
TLP:CLEAR

Cyber Security Threat Trends 2023-M04

April 2023

With reference to the FIRST Traffic Light Protocol (TLP) standard[1], this document is classified as TLP:CLEAR information. Recipients may share with peers and partner organisations without restriction.

Cyber Security Threat Landscape of the past 12 months (source: GovCERT.HK)



Trending:

Misconfigured, unsecured and unpatched systems and databases exposing to the Internet are prone to data breach and attackers' exploitation. System administrators should properly and securely configure their systems by adopting least privilege principle and disabling unused services and network ports. They should also apply security patches to their systems and upgrade outdated software timely.

[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], MyCERT[7] and JPCERT[8] issued alerts regarding multiple vulnerabilities in Microsoft products. An elevation of privilege vulnerability (CVE-2023-28252) in Microsoft Windows and Microsoft Windows Server has been exploited in the wild.

- GovCERT.HK[9], Canadian Centre for Cyber Security[10] and MyCERT[11] issued alerts regarding multiple vulnerabilities in Cisco products. PoC code for the privilege escalation vulnerability in Cisco ASR 5000 series routers and Cisco Virtualized Packet Core running StarOS software were available.

- GovCERT.HK[12], HKCERT[13], CISA[14], Canadian Centre for Cyber Security[15] and SingCERT[16] issued alerts regarding multiple vulnerabilities in Apple iOS and iPadOS. Vulnerabilities (CVE-2023-28205 and CVE-2023-28206) have been actively exploited.

- GovCERT.HK[17] and HKCERT[18] issued alerts regarding a remote code execution vulnerability (CVE-2023-1389) in TP-Link Archer AX21, which has been exploited in the wild.

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=1005
3 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-april-2023
4 https://www.cisa.gov/news-events/alerts/2023/04/11/microsoft-releases-april-2023-security-updates
5 https://www.cyber.gc.ca/en/alerts-advisories/microsoft-security-advisory-april-2023-monthly-rollup-av23-206
6 https://www.csa.gov.sg/alerts-advisories/alerts/2023/al-2023-047
7 https://www.mycert.org.my/portal/advisory?id=MA-926.042023
8 https://www.jpcert.or.jp/english/at/2023/at230007.html
9 https://www.govcert.gov.hk/en/alerts_detail.php?id=1013
10 https://www.cyber.gc.ca/en/alerts-advisories/cisco-security-advisory-av23-226
11 https://www.mycert.org.my/portal/advisory?id=MA-934.042023
12 https://www.govcert.gov.hk/en/alerts_detail.php?id=1003
13 https://www.hkcert.org/security-bulletin/apple-products-remote-code-execution-vulnerabilities_20230411
14 https://www.cisa.gov/news-events/alerts/2023/04/11/apple-releases-security-updates-multiple-products
15 https://www.cyber.gc.ca/en/alerts-advisories/apple-security-advisory-av23-197
16 https://www.csa.gov.sg/alerts-advisories/alerts/2023/al-2023-043
17 https://www.govcert.gov.hk/en/alerts_detail.php?id=1018
18 https://www.hkcert.org/security-bulletin/tp-link-router-remote-code-execution-vulnerability_20230426

CERT Advisories

- GovCERT.HK[19,20,21,22], HKCERT[23,24,25,26], Canadian Centre for Cyber Security[27,28,29], SingCERT[30,31] and MyCERT [32] issued alerts regarding multiple vulnerabilities in Google Chrome and Microsoft Edge. The vulnerabilities (CVE-2023-2033 and CVE-2023-2136) have been exploited in the wild.

Adopt data-driven cyber (DDC) to improve cyber security

National Cyber Security Centre[33] published an article to introduce DDC which making use of data and scientific methods to facilitate evidence-based decision making and actionable insights sharing about cyber security, so as to raise the cyber security resilience and posture of organisations. A DDC maturity model was provided in the article to facilitate organisations to assess their current and target level of DDC maturity in the adoption of DDC in cyber security.

[19] https://www.govcert.gov.hk/en/alerts_detail.php?id=1009
[20] https://www.govcert.gov.hk/en/alerts_detail.php?id=1011
[21] https://www.govcert.gov.hk/en/alerts_detail.php?id=1010
[22] https://www.govcert.gov.hk/en/alerts_detail.php?id=1016
[23] https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerability_20230417
[24] https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20230419
[25] https://www.hkcert.org/security-bulletin/microsoft-edge-remote-code-execution-vulnerability_20230417
[26] https://www.hkcert.org/security-bulletin/microsoft-edge-remote-code-execution-vulnerability_20230421
[27] https://www.cyber.gc.ca/en/alerts-advisories/av23-215-google-chrome-security-advisory
[28] https://www.cyber.gc.ca/en/alerts-advisories/google-chrome-security-advisory-av23-223
[29] https://www.cyber.gc.ca/en/alerts-advisories/microsoft-edge-security-advisory-av23-228
[30] https://www.csa.gov.sg/alerts-advisories/alerts/2023/al-2023-051
[31] https://www.csa.gov.sg/alerts-advisories/alerts/2023/al-2023-049
[32] https://www.mycert.org.my/portal/advisory?id=MA-930.042023
[33] https://www.ncsc.gov.uk/blog-post/data-driven-cyber-transforming-cyber-security-through-an-evidence-based-approach

Industry Insight on Cyber Security Threat Trends

Over 70 billion files were exposed in December 2022

CybelAngel released the "2023 State of the External Attack Surface: Annual Threat Trends Analysis"[34], which summarised the analysis of detected exposures based on collected data in 2022 and prediction of trends in 2023. The key findings were:

- **Almost 9% of scanned internet-facing systems and applications were not patched and vulnerable to attack in 2022.** Each of the top ten most common vulnerabilities had over 12 million detections and 987 vulnerabilities had over 1 million hits. System administrators should apply up-to-date security patches on a timely basis.
- **Over 70 billion files from near 500,000 distinct servers were accessible without proper protection in December 2022.** Among the exposed files, over 29 billion files and 15 billion files were exposed from rsync servers and ftp servers respectively. Around 116,000 ransomed servers, which were infected by ransomware of 198 unique categories, were found in December 2022.
- **Around 740,000 misconfigured or unauthenticated databases were found in 2022**, 71.8% of them were MongoDB databases and 17.4% were Elasticsearch databases. Moreover, 1.4 million misconfigured and exposed cloud services were detected in 2022. In 2022, over 6.8 million detections of leaked or stolen credentials and sensitive information were found from over 7,200 scanned marketplaces and forums on the deep web and the dark web.
- **Near 13% of 91 million web assets were found using invalid or expired SSL certificates in 2022.** Hackers could exploit the vulnerability to launch a variety of cyberattacks including man-in-the-middle attacks and phishing attacks. System administrators should regularly review the expiry dates of their SSL certificates and renew the SSL certificates before expiration.
- **Growth in credential theft targeting business accounts was anticipated in 2023.** Security risks related to cloud misconfigurations and unprotected shadow and unknown internet connected assets would also be trended upward in 2023.

Source: CybelAngel

[34] https://discover.cybelangel.com/2023-state-of-the-external-attack-surface

Industry Insight on Cyber Security Threat Trends

New generation of botnets abused Virtual Private Servers (VPS)

Cloudflare issued the "DDoS Threat Report for 2023 Q1"[35], which summarised their insights and analysis on the latest trends of DDoS attack landscape in the first quarter of 2023. The highlights from the report included:

- **16% of survey respondents reported ransom DDoS attacks in Q1 2023, same as Q4 2022 after experienced a four consecutive quarterly increase in 2022.** Compared with Q1 2022, there was a 60% increase.
- **Internet companies were most targeted by application layer DDoS attacks while Information Technology and Services industry was most targeted by network layer DDoS attacks.** In terms of targeted location, Israel, the United States and Canada were the top three most attacked location by application layer DDoS attacks. For network layer DDoS attacks, China, Singapore and the United States were the most targeted locations.
- **Most of network layer DDoS attacks were short-lasting and small volume.** In Q1 2023, 86% of network layer DDoS attacks lasted within 10 minutes and around 91% did not exceed 500 Mbps. However, attacks over 100 Gbps increased by 6%, and attacks with volume between 10 to 100 Gbps increased by over 89% as compared with Q4 2022. A 1.3 Tbps (terabits per second) DDoS attack, compromising of DNS and UDP attack traffic originated from a Mirai-variant botnet with around 20,000 bots from multiple locations including Hong Kong, was detected in Q1 2023.
- **DNS-based attack was the most common attack vector, accounted for around 30% of the attacks, followed by SYN floods (22%) and UDP-based attacks (21%).** Huge growths in Statistical Product and Service Solutions (SPSS)-based DDoS attacks, DNS amplification attacks and Generic Routing Encapsulation (GRE)-based DDoS attacks were observed in Q1 2023, increased by more than 15 times, 9 times and 8 times respectively.
- **Attackers compromised vulnerable and misconfigured virtual private servers to form VPS-based botnets to conduct large volume DDoS attacks.** As processing power of VPS was higher than Internet of Things (IoT) devices, VPS-based botnets could be 5,000 times more powerful than IoT-based botnets even though the amount of compromised devices was fewer.

Source: Cloudflare

[35] https://blog.cloudflare.com/ddos-threat-report-2023-q1/

Industry Insight on Cyber Security Threat Trends

Phishing attacks were on the rise

Zscaler released the "Zscaler ThreatLabz 2023 Phishing Report"[36], which summarised the threat landscape of phishing attacks in 2022. Major findings in the report were:

- **Phishing attacks in 2022 increased 47.2% when compared with 2021.** The United States remained the most targeted by phishing attacks. Over 65% of all phishing attempts observed targeted the US, increased from 60% in 2021. The number of phishing attempts observed targeted the United Kingdom in 2022 experienced a 269% increase.

- **Education was the industry most targeted by phishing attacks, followed by finance & insurance industry and government sector.** Over 300 million phishing attempts targeted the education sector, recorded a 576% increase in phishing attempts in 2022 compared with 2021. Finance and insurance industry recorded a 273% increase in phishing attempts and phishing attacks targeted the healthcare industry tripled from less than 31 million to above 114 million in 2022. The number of phishing attacks targeted retail and wholesale industry dropped 67%.

- **Microsoft was the most impersonated brand in 2022.** Together with brand name of other Microsoft products such as OneDrive, SharePoint and Microsoft 365, more than half of phishing attacks involving imitation of brand names impersonated Microsoft. Phishing attacks targeted a wide range of brand categories, included productivity tools, cryptocurrency sites, illegal streaming sites, social media platforms and messaging services, financial institutions, government sites and logistics services. COVID-themed phishing attacks involving imitation of brand names dropped from 7.2% in 2021 to 3.7% in 2022.

- **Phishing attack tactics and techniques became increasingly sophisticated.** The sophistication were observed in a variety of attacks including vishing attacks (i.e. voice calls phishing), adversary-in-the-middle (AiTM) phishing attacks, Browser-in-the-Browser (BiTB) phishing attacks, abusing legitimate hosting services and dynamic DNS services to host phishing sites, phishing attacks leveraging artificial intelligence, etc.

- Organisations should conduct regular security awareness training and implement security controls such as email scanning and encrypted traffic checking to mitigate the risk of phishing attacks.

Source: Zscaler

[36] https://info.zscaler.com/resources-industry-reports-threatlabz-phishing-report

Highlight of Microsoft April 2023 Security Updates

Product Family	Impact[37]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5022282, KB5022286, KB5022287, KB5022289, KB5022297, KB5022303, KB5025221, KB5025224, KB5025228, KB5025229, KB5025234, KB5025239
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5022286, KB5022289, KB5022291, KB5025228, KB5025229, KB5025230
Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5022343, KB5022346, KB5022348, KB5022352, KB5025272, KB5025285, KB5025287, KB5025288
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB5002213, KB5002221, KB5002373, KB5002375, KB5002381, KB5002383, KB5002385

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/2023-Apr.

Learn more:

High Threat Security Alert (A23-04-06): Multiple Vulnerabilities in Microsoft Products (April 2023) (https://www.govcert.gov.hk/en/alerts_detail.php?id=1005)

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