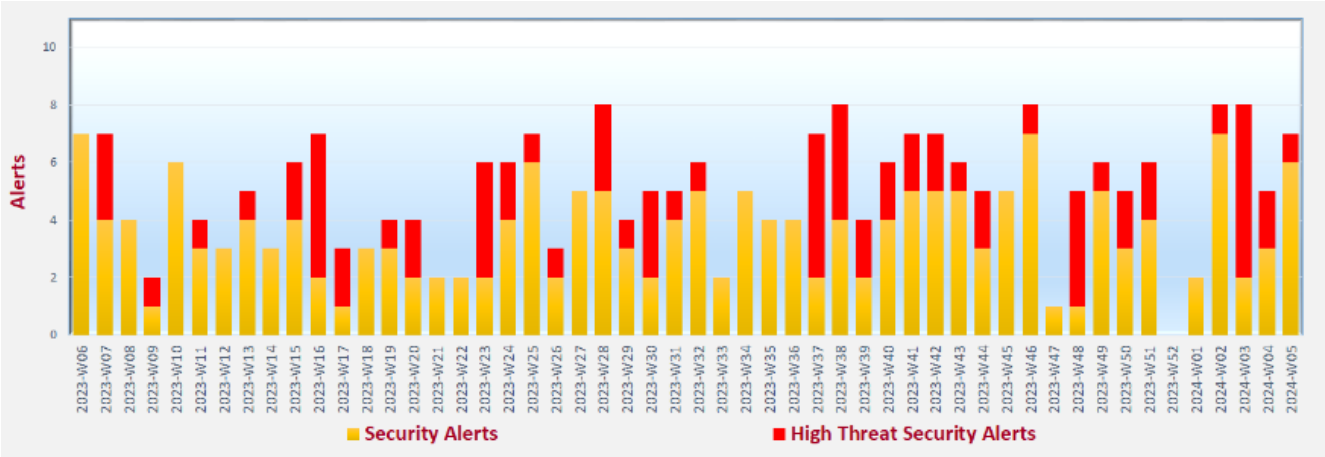
TLP:CLEAR

Cyber Security Threat Trends 2024-M01

January 2024

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:

Growing trend on **phishing attacks** continues and causes serious impacts to organisations and individuals. Users should stay alert to electronic messages received, and should not click any link, open any attachment or scan any QR code in the messages if they have doubt on the authenticity of the electronic messages.

[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], Cybersecurity and Infrastructure Security Agency (CISA)[4], Canadian Centre for Cyber Security[5], Australian Cyber Security Centre (ACSC)[6], SingCERT[7] and MyCERT[8] issued alerts regarding multiple vulnerabilities in Ivanti products. Security restriction bypass vulnerability (CVE-2023-46805), remote code execution vulnerability (CVE-2024-21887) and authentication bypass vulnerability (CVE-2023-35082) have been exploited in the wild.

- GovCERT.HK[9,10], HKCERT[11,12], Canadian Centre for Cyber Security[13] and SingCERT[14] issued alerts regarding multiple vulnerabilities in Google Chrome and Microsoft Edge. Vulnerability (CVE-2024-0519) has been exploited in the wild.

- GovCERT.HK[15], HKCERT[16], CISA[17], Canadian Centre for Cyber Security[18], SingCERT[19] and MyCERT[20] issued alerts regarding multiple vulnerabilities in Apple products. Vulnerabilities (CVE-2023-42916, CVE-2023-42917 and CVE-2024-23222) have been actively exploited.

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=1197
3 https://www.govcert.gov.hk/en/alerts_detail.php?id=1208
4 https://www.cisa.gov/news-events/alerts/2024/01/10/ivanti-releases-security-update-connect-secure-and-policy-secure-gateways
5 https://www.cyber.gc.ca/en/alerts-advisories/ivanti-security-advisory-av24-020
6 https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerabilities-ivanti-connect-secure-ics-and-ivanti-policy-secure-ips
7 https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-002
8 https://www.mycert.org.my/portal/advisory?id=MA-1011.012024
9 https://www.govcert.gov.hk/en/alerts_detail.php?id=1202
10 https://www.govcert.gov.hk/en/alerts_detail.php?id=1206
11 https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20240117
12 https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20240118
13 https://www.cyber.gc.ca/en/alerts-advisories/google-chrome-security-advisory-av24-034
14 https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-006
15 https://www.govcert.gov.hk/en/alerts_detail.php?id=1209
16 https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20240123
17 https://www.cisa.gov/news-events/alerts/2024/01/23/apple-releases-security-updates-multiple-products
18 https://www.cyber.gc.ca/en/alerts-advisories/apple-security-advisory-av24-044
19 https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-011
20 https://www.mycert.org.my/portal/advisory?id=MA-1014.012024

CERT Advisories

- GovCERT.HK[21], HKCERT[22], CISA[23], Canadian Centre for Cyber Security[24], ACSC[25], SingCERT[26] and MyCERT [27] issued alerts regarding multiple vulnerabilities in Citrix products. Vulnerabilities (CVE-2023-6548 and CVE-2023-6549) in Citrix NetScaler ADC and Citrix NetScaler Gateway have been actively exploited.

- HKCERT [28] issued an alert regarding multiple vulnerabilities in Samsung products. Vulnerabilities (CVE-2023-33063, CVE-2023-33106 and CVE-2023-33107) have been exploited in the wild.

- HKCERT[29] updated an alert regarding multiple vulnerabilities in VMware vCenter Server. Vulnerability (CVE-2023-34048) has been exploited in the wild.

Phishing attack cases handled by HKCERT in 2023 recorded a new high since 2019

HKCERT[30] released a summary on cyber security situation in Hong Kong in 2023 and the security outlook for 2024. A total of 7,752 security cases were handled in 2023, with nearly half (48%) of them were phishing attacks. Compared with 2022, the number of phishing cases increased 27% to 3,752, a record high since 2019. Detected phishing links increased 22% to over 19,000. More than half (55%) of phishing cases targeted banking, finance, e-payment and e-commerce industries. HKCERT also pointed out five key information security risks in 2024 and re-emphasised the importance of strengthening of information security awareness.

Security considerations for using Artificial Intelligence (AI) systems

ACSC[31], in collaboration with other international cybersecurity agencies, released a joint guidance for organisations on how to use AI systems securely. The guidance summarises security threats related to AI systems, and provides security considerations for organisations to reference when engaging with AI systems.

---

21 https://www.govcert.gov.hk/en/alerts_detail.php?id=1203
22 https://www.hkcert.org/security-bulletin/citrix-products-multiple-vulnerabilities_20240117
23 https://www.cisa.gov/news-events/alerts/2024/01/18/citrix-releases-security-updates-netscaler-adc-and-netscaler-gateway
24 https://www.cyber.gc.ca/en/alerts-advisories/citrix-security-advisory-av24-030
25 https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/vulnerabilities-citrix-netscaler-adc-and-netscaler-gateway-products
26 https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-007
27 https://www.mycert.org.my/portal/advisory?id=MA-1016.012024
28 https://www.hkcert.org/security-bulletin/samsung-products-multiple-vulnerabilities_20240105
29 https://www.hkcert.org/security-bulletin/vmware-vcenter-server-multiple-vulnerabilities_20231026
30 https://www.hkcert.org/press-centre/hkcert-releases-annual-information-security-outlook-and-forecast-next-level-phishing-attacks-difficult-to-distinguish-hackers-exploit-ai-for-crimes-could-become-a-new-normal
31 https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/engaging-with-artificial-intelligence

CERT Advisories

Impact of AI on cyber threats in the coming two years

National Cyber Security Centre (NCSC)[32] released an assessment report on how AI would affect cyber operations and cyber threats over the next two years. The assessment indicated that AI has already been and would increasingly be used by attackers. AI would also boost the capability of cyber attacks, particularly in reconnaissance and social engineering. Other assessments were also included in the report.

Guidance on using cloud services securely

NCSC[33] published a guidance to help small organisations for secure usage of cloud services. The guidance covers different areas including service provider selection, data backup, domain name security, account security, password security, etc.

[32] https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat
[33] https://www.ncsc.gov.uk/collection/using-online-services-safely

Industry Insight on Cyber Security Threat Trends

Discovered shadow APIs nearly equal to 31% of registered REST API endpoints

Cloudflare released the "2024 API Security & Management Report"[34], which highlighted the analysis on API security trends based on data collected from October 2022 to August 2023 and prediction on the upcoming trend in 2024. The key findings were:

- **Compared to REST API information provided by organisations, there were 30.7% more REST API endpoints discovered.** These shadow APIs, that were not managed or secured by the organisations, associated with over 15,000 accounts. This indicated that some organisations lacked full API inventory, resulting in uncovered attack surfaces and new security risks on data exposure, unpatched vulnerabilities, data compliance violations and lateral movement. Security administrator should keep an up-to-date API inventory to ensure the visibility.

- **51.6% of API traffic errors were due to HTTP Error 429 "Too Many Requests", followed by HTTP Error 400 "Bad Request" (13.8%) and HTTP Error 404 "Not Found" (10.8%).** Organisations were recommended to ensure the rate limiting has been properly set and adjusted according to business needs to limit the number of requests within a certain timeframe while prevent unintentional blocking of legitimate traffic.

- **HTTP anomaly was the most popular API threat and accounted for 60.7% of total attacks mitigated, followed by injection attack (26.3%) and file inclusion (5.5%).** Security administrator should adopt schema validation for allowing legitimate traffic to their organisations' APIs only, enforce authentication on publicly accessible APIs, properly grant permissions to APIs, and block API traffic with abnormal volume.

- **Higher API risks due to increase in API accessibility but lack of control over APIs, as well as uptrend in business logic-based fraud attacks would be anticipated in 2024.** Bot operators would more actively target against APIs behind business transaction workflows.

Source: Cloudflare

[34] https://www.cloudflare.com/lp/api-security-report/

Industry Insight on Cyber Security Threat Trends

Incidents involving suspicious logins rose in 2023

Expel released the "Annual Threat Report 2024"[35] based on analysis of incidents identified by their security operation center (SOC) in 2023. The key insights highlighted in the report were:

- **Identity-based incidents remained the dominant incident type for three consecutive years, and accounted for 64% of all incidents in 2023.** Number of identity incidents increased 144% compared with 2022. 60% of the incidents were unauthorised email logins, and 40% targeted authentications to identity and access management platforms. The top three industries targeted by identity incidents were non-profit organisations, technology and financial services. 69% of identity incidents involved malicious logins from suspicious infrastructure such as hosting providers or proxies.

- **Phishing incidents accounted for 6% of total incidents in 2023, increased from 2% in 2022.** An increase of QR code phishing (Qishing) aiming for better evasion from security controls was observed in 2023. Hospitality was the most targeted industry by phishing attacks (55%), followed by travel (12%) and technology (9%).

- **Upward trend on cloud infrastructure incidents continued in 2023.** Compared with 2022, there was a 72% increase in cloud infrastructure incidents. Near half of the cloud security incidents targeted technology industry. Exposed credentials were the major cause of cloud incidents, accounted for 42% of the incidents, followed by server-side request forgery (SSRF) attacks attempting to obtain sensitive information (28%) and use of default credentials (19%).

- **57% of malware incidents were identified as high-risk pre-ransomware seeking for initial access to target environments.** These malware were more frequently deployed via JavaScript (39%), EXE files (20%) and LNK files (12%). Top three high-risk malware targeted industries were financial services, hospitality and manufacturing. In 2023, there was a surge in infostealers downloaded from malicious advertisements and this trend was expected to continue in 2024.

Source: Expel

[35] https://expel.com/annual-threat-report/

Industry Insight on Cyber Security Threat Trends

Ransomware-associated vulnerabilities reached a new high since 2020

Securin issued the report "Ransomware 2023 Year in Review"[36], which summarised their findings on the trends of ransomware attack landscape in 2023. The key findings were:

- **The number of ransomware-associated vulnerabilities increased by 11%, growing from 344 in 2022 to 382 in 2023.** Among these vulnerabilities, 43.8% were classified as critical and 40.2% were rated as high severity by CVSS. However, organisations should not neglect those medium or low severity vulnerabilities, as they could also be exploited by attackers to perform ransomware attacks. The three most noteworthy exploited vulnerability were the Progress MOVEit Transfer Vulnerability (CVE-2023-34362), which was used to compromise over 1,000 organisations, the CitrixBleed Vulnerability (CVE-2023-4966) in NetScaler web application delivery control (ADC) and NetScaler Gateway appliances, as well as the Fortra GoAnywhere Managed File Transfer Vulnerability (CVE-2023-0669).
- **Education, healthcare and financial were the three most targeted sectors by ransomware attacks.** Cl0p, BlackCat, and LockBit were the most active ransomware groups in 2023.
- **Kill-chain vulnerabilities recorded a significant increase of 35.6% in 2023.** Attackers could infiltrate the target network, perform ransomware code execution and data exfiltration by exploiting one of these vulnerabilities.
- **113 ransomware-associated vulnerabilities impacted 1,042 open-source packages, with Linux being affected by 80% of these vulnerabilities.** Microsoft products were impacted by 125 ransomware-associated CVEs, with Microsoft Windows and Windows Server were the most affected products.
- To defend against ransomware attacks, organisations should arrange user education and security awareness training, patch their systems timely, use up-to-date anti-malware software, regularly monitor and reduce their attack surface, adopt proactive mitigation measures, conduct periodic penetration testing, properly implement network segmentation and access control, adopt the least privilege principle, and establish robust backup and recovery procedures.

Source: Securin

[36] https://www.securin.io/ransomware-report-2023-year-in-review-download/

Highlight of Microsoft January 2024 Security Updates

Product Family	Impact[37]	Severity	Associated KB and / or Support Webpages
Windows 10, 11	Remote Code Execution	Critical ★★★★	KB5034119, KB5034121, KB5034122, KB5034123, KB5034127, KB5034134
Windows Server 2016, 2019, 2022	Remote Code Execution	Critical ★★★★	KB5034119, KB5034127, KB5034129, KB5034130
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB5002539, KB5002540, KB5002541

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/2024-Jan.

Learn more:

Security Alert (A24-01-05): Multiple Vulnerabilities in Microsoft Products (January 2024) (https://www.govcert.gov.hk/en/alerts_detail.php?id=1194)

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