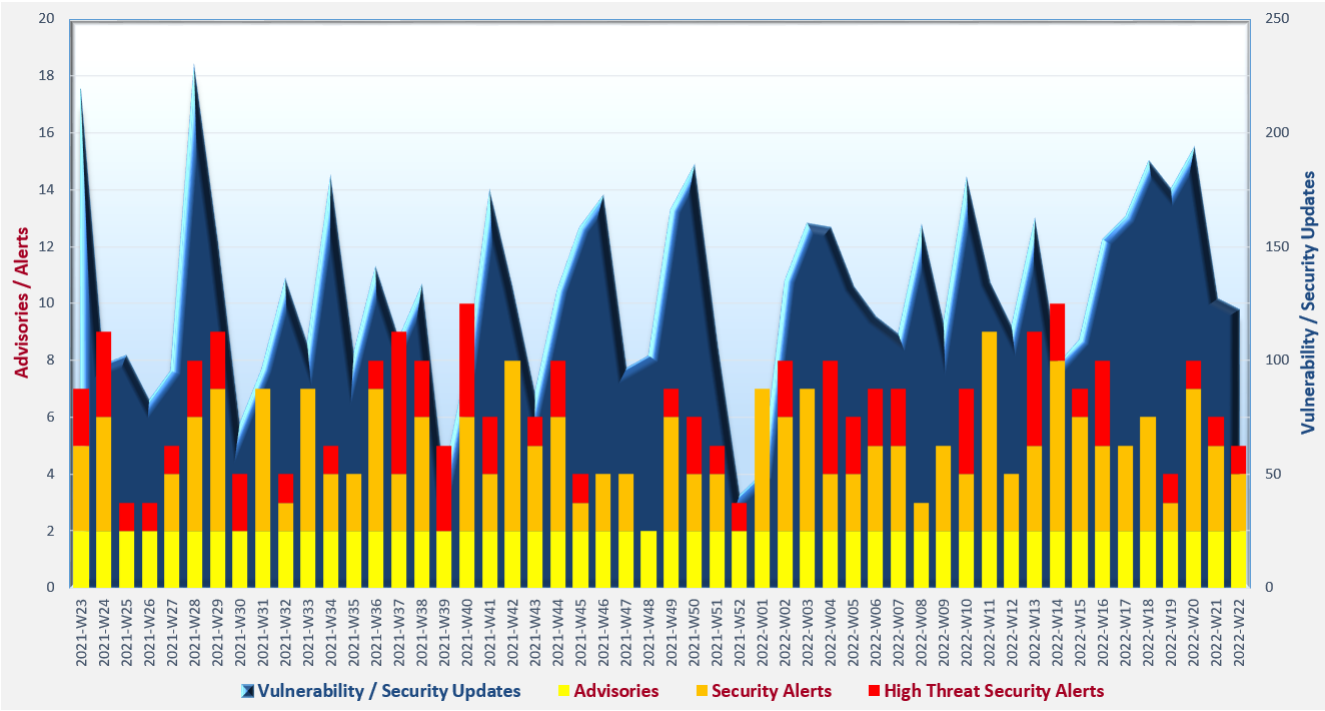
TLP:WHITE

Cyber Security Threat Trends 2022-M05

May 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:

Account takeover attacks, **vulnerability exploitations** and **malware activities** keep increasing. System administrators should timely apply security patches and disable unused services in their systems. Organisation should implement up-to-date security protection solutions at different layers including endpoint, network, application, etc.

[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)[6,7], Canadian Centre for Cyber Security[8,9], Australian Cyber Security Centre (ACSC)[10], MyCERT[11] and JPCERT[12] issued alerts regarding multiple vulnerabilities in Microsoft products. A remote code execution vulnerability (CVE-2022-30190) and a spoofing vulnerability (CVE-2022-26925) in Microsoft Windows and Server were being actively exploited. Technical details of a denial of service vulnerability (CVE-2022-22713) in Microsoft Windows and Server were publicly disclosed. System patch for CVE-2022-30190 was not yet available as at end of May 2022. System administrators should apply the workaround recommended by Microsoft for risk mitigation.

- GovCERT.HK[13], HKCERT[14], CISA[15,16], Canadian Centre for Cyber Security[17], ACSC[18] and SingCERT[19] issued alerts regarding a vulnerability in F5 BIG-IP. Vulnerability (CVE-2022-1388) was being exploited in the wild.

- GovCERT.HK[20] and HKCERT[21] issued alerts regarding a vulnerability in Cisco products. Vulnerability (CVE-2022-20821) in Cisco IOS XR software was being actively exploited.

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=801
3 https://www.govcert.gov.hk/en/alerts_detail.php?id=813
4 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-may-2022
5 https://www.hkcert.org/security-bulletin/microsoft-products-remote-code-execution-vulnerability_20220531
6 https://www.cisa.gov/uscert/ncas/current-activity/2022/05/11/microsoft-releases-may-2022-security-updates
7 https://www.cisa.gov/uscert/ncas/current-activity/2022/05/31/microsoft-releases-workaround-guidance-msdt-follina-vulnerability
8 https://www.cyber.gc.ca/en/alerts/microsoft-security-advisory-may-2022-monthly-rollup-av22-258
9 https://www.cyber.gc.ca/en/alerts/follina-vulnerability-impacting-microsoft-products
10 https://www.cyber.gov.au/acsc/view-all-content/alerts/exploitation-microsoft-office-vulnerability-follina
11 https://www.mycert.org.my/portal/advisory?id=MA-835.052022
12 https://www.jpcert.or.jp/english/at/2022/at220014.html
13 https://www.govcert.gov.hk/en/alerts_detail.php?id=800
14 https://www.hkcert.org/security-bulletin/f5-products-multiple-vulnerabilities_20220505
15 https://www.cisa.gov/uscert/ncas/current-activity/2022/05/04/f5-releases-security-advisories-addressing-multiple
16 https://www.cisa.gov/uscert/ncas/current-activity/2022/05/18/threat-actors-exploiting-f5-big-ip-cve-2022-1388
17 https://www.cyber.gc.ca/en/alerts/f5-security-advisory-av22-248
18 https://www.cyber.gov.au/acsc/view-all-content/alerts/multiple-vulnerabilities-present-f5-products
19 https://www.csa.gov.sg/singcert/Alerts/al-2022-020
20 https://www.govcert.gov.hk/en/alerts_detail.php?id=809
21 https://www.hkcert.org/security-bulletin/cisco-ios-xr-security-restriction-bypass-vulnerability_20220523

CERT Advisories

- HKCERT[22], CISA[23], Canadian Centre for Cyber Security[24] and SingCERT[25] issued alerts regarding multiple vulnerabilities related to Apple products. Vulnerability (CVE-2022-22675) was being exploited in the wild.

Data protection guideline

HKCERT[26] released a guideline on how to protect against data loss, data corruption and data leakage. Data protection measures covering areas on segregation of data storage, data backup, data encryption, secure data deletion, etc. were recommended.

Securing websites from cyber attacks

SingCERT[27] released a guidance for organisations' reference to protect websites from cyber attacks. The guidance provided actionable security measures on securing websites, protecting data, monitoring, housekeeping and incident handling.

[22] https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20220517
[23] https://www.cisa.gov/uscert/ncas/current-activity/2022/05/17/apple-releases-security-updates-multiple-products
[24] https://www.cyber.gc.ca/en/alerts/apple-security-advisory-av22-277
[25] https://www.csa.gov.sg/en/singcert/Alerts/al-2022-022
[26] https://www.hkcert.org/security-guideline/data-protection-guideline
[27] https://www.csa.gov.sg/singcert/Advisories/ad-2022-007

Industry Insight on Cyber Security Threat Trends

Detection of malware in 2021 increased 77%

Malwarebytes issued the "Malwarebytes 2022 Threat Review"[28], which summarised their findings on trends in malware and security threats in 2021. The highlights from the report included:

- **The number of malicious software detected in 2021 increased 77% compared to 2020.** Cryptomining malware detections increased by more than 300% as compared to 2020 which could be related to the soar of cryptocurrency values. Windows malware detection increased 65% for home computers and 143% for business computers. Malware detections on Macs also increased 200% from 2020.

- **There was a 38% decrease in ransomware detections in 2021**. The drop was related to the shift of attack targets of ransomware operators. They became more interested in compromising entire organisations than individuals.

- **Email threat detections in H2 2021 increased 56%, compared to H1 2021.** Nevertheless, detections in email threats in 2021 decreased from 2020. Detections of Emotet, TrickBot and Dridex in email threats dropped from 79% during 2018-2020 to 42% in 2021. Attackers shifted their tactics by sending fewer emails but in a more targeted approach.

- **Old and insecure third-party open source codebases, zero-day vulnerabilities of web browsers and other software such as ProxyLogon, PrintNightmare, Log4j, etc. caused significant cybersecurity threats to organisations in 2021.** Organisation should patch their systems in a timely manner, and adopt secure programming practices in software development.

Source: Malwarebytes

[28] https://www.malwarebytes.com/resources/malwarebytes-threat-review-2022/index.html

Industry Insight on Cyber Security Threat Trends

Events of malware, botnet and exploitation increased in Q1 2022

Nuspire released the "Q1 2022 Threat Landscape Report"[29], which included analysis results on over a trillion traffic logs from thousands of globally deployed devices. The key findings were:

- **There was an increase of 4.76% in malware activity compared to Q4 2021.** In the first quarter of 2022, the highest malware detection occurred in mid-March. Visual Basic for Applications (VBA) agents continued to be the top malware variant, although a downtrend was anticipated following Microsoft Office products' approach on blocking VBA macros by default in place.

- **Botnet activity increased 12.21% in Q1 2022 with a significant increase in STRRAT botnet activity.** There was a new STRRAT phishing campaign causing the detection on STRRAT botnet activity soared since February 2022. Peak Mirai botnet activity was detected in mid-February 2022. An increase in Mirai botnet activity was expected in Q2 2022 as the threat actors continued to exploit unpatched devices.

- **An increase of 3.87% of exploit detection was observed in Q1 2022.** The top three exploit attempts were SMB Brute Force (47.89%), SSH Brute Force (29.66%) and Apache Log4j (8.83%). Attackers consistently scanned for exposed and vulnerable services such as SMB and SSH, and attempted to gain access by brute-forcing or vulnerability exploitation.

- **Organisations should take proactive actions to detect active threats, combat malicious activities and mitigate security risks**. Actionable measures included organising training to enhance cyber security awareness of the staff, adopting a comprehensive "defence in depth" approach, implementing advanced malware detection and protection technology and network segregation. Besides, system administrators should apply security patches / mitigation measures to their systems timely, implement firewall with intrusion prevention system (IPS) and disable all unused services completely to defend against cyber attacks.

Source: Nuspire

[29] https://www.nuspire.com/resources/q1-2022-threat-report/

Industry Insight on Cyber Security Threat Trends

Record high bad bot traffic was detected in 2021

Imperva analysed the trends in bad bot activities from billions of bad bot requests in 2021 and incorporated their analysis results in the "2022 Imperva Bad Bot Report"[30]. The key findings were:

- **27.7% of internet traffic in 2021 was from bad bots, with an increase of 2.1% as compared to 2020.** Bad bot traffic showed an increasing trend throughout 2021 from 24.7% of internet traffic in January to the peak at 30% in December.
- **65.6% of total bad bot traffic detected were associated with evasive bad bots.** These bad bots increased their evasive capabilities by using randomised IPs, anonymous proxies, varying identifiable information, delaying requests, pretending human actions, etc.
- **Account takeover (ATO), scraping and scalping were the most frequently detected bot attacks in 2021.** ATO attacks surged by 148% throughout 2021, with over 64% of attacks were conducted by bad bots. An increase in ATO attacks was observed in H2 2021, with spikes in attacks targeted financial services, healthcare and gaming sectors in June, October and November-December respectively. Financial services (34.6%), travel (23.2%) and business services (11.4%) were the top 3 industries with the highest volume of ATO attacks.
- **Bad bots increasingly used mobile user agents and mobile Internet Service Providers (ISPs) and pretended to be legitimate users to avoid detection.** 35.6% of bad bots adopted mobile user agents, increased by 7.5% from 2020, and 27.2% used mobile ISPs, an increase of 12.1% from 2020.
- **Organisations should be proactive in identifying risks, reducing vulnerabilities and threats, as well as monitoring the traffic of their online services including web sites, APIs and mobile apps.** They could consider blacklisting browser versions which were no longer supported, denying traffic from malicious IPs, continuous monitoring for ATO attack attempts and traffic anomalies, as well as deploying bot protection solutions.

Source: Imperva

[30] https://www.imperva.com/resources/resource-library/reports/bad-bot-report/

Highlight of Microsoft May 2022 Security Updates

Product Family	Impact[31]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5013941, KB5013942, KB5013943, KB5013945, KB5013952, KB5013963
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5013941, KB5013942, KB5013944, KB5013952
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5014001, KB5014011, KB5014017, KB5014018, KB5014025
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4484347, KB4493152, KB5002184, KB5002187, KB5002196, KB5002199, KB5002204, KB5002205
Microsoft Exchange Server	Elevation of Privilege	Important ★★★	KB5014260, KB5014261

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/2022-May.

Learn more:

High Threat Security Alert (A22-05-05): Multiple Vulnerabilities in Microsoft Products (May 2022) (https://www.govcert.gov.hk/en/alerts_detail.php?id=801)

Data analytics powered by CRisP in collaboration with GovCERT.HK

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