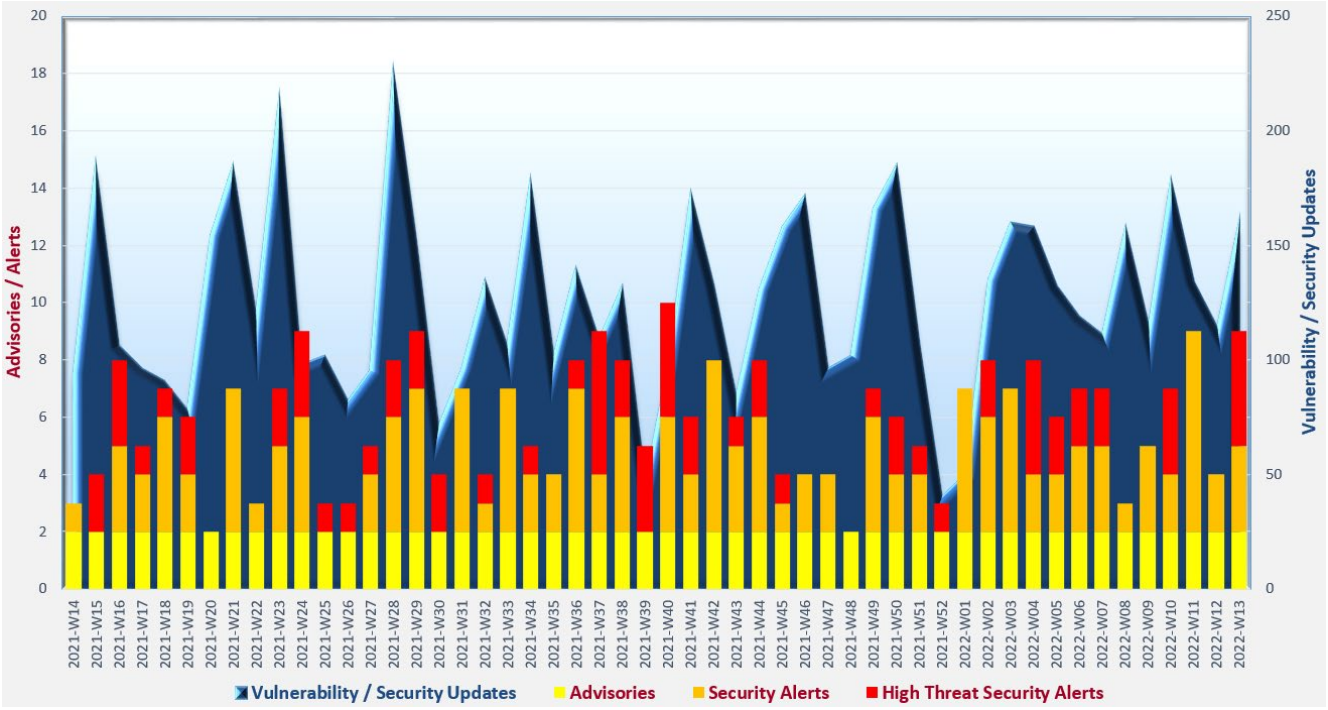
TLP:WHITE

Cyber Security Threat Trends 2022-M03

March 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:

Distributed Denial of Service (DDoS) and attacks targeted **web applications** and **mobile endpoints** continue increasing in quantity and sophistication. Organisations should strive to protect their critical services, applications and mobile endpoints such as deploying anti-DDoS measures, web application firewalls, mobile device protection solution, zero trust architecture, 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], HKCERT[3], Cybersecurity and Infrastructure Security Agency (CISA)[4], SingCERT[5] and JPCERT[6] issued alerts regarding multiple vulnerabilities in Microsoft products. Technical details of vulnerabilities CVE-2022-21990, CVE-2022-24459 and CVE-2022-24512 were publicly disclosed.

- GovCERT.HK[7], HKCERT[8], CISA[9], Canadian Centre for Cyber Security[10], Australian Cyber Security Centre (ACSC)[11], SingCERT[12] and CERT NZ[13] issued alerts regarding multiple vulnerabilities in Spring Framework. A remote code execution vulnerability (CVE-2022-22963) in Spring Cloud Function was being actively exploited. PoC exploit for another remote code execution vulnerability (CVE-2022-22965) in Spring Framework was publicly available.

- GovCERT.HK[14,15], HKCERT[16,17], CISA[18], Canadian Centre for Cyber Security[19,20] and SingCERT[21] issued alerts regarding an actively exploited vulnerability (CVE-2022-1096) in Google Chrome and Microsoft Edge (Chromium-based).

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=752
[3] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-march-2022
[4] https://www.cisa.gov/uscert/ncas/current-activity/2022/03/08/microsoft-releases-march-2022-security-updates
[5] https://www.csa.gov.sg/en/singcert/Alerts/al-2022-012
[6] https://www.jpcert.or.jp/english/at/2022/at220007.html
[7] https://www.govcert.gov.hk/en/alerts_detail.php?id=767
[8] https://www.hkcert.org/security-bulletin/spring-framework-remote-code-execution-vulnerability_20220401
[9] https://www.cisa.gov/uscert/ncas/current-activity/2022/04/01/spring-releases-security-updates-addressing-spring4shell-and
[10] https://www.cyber.gc.ca/en/alerts/spring-remote-code-execution-vulnerabilities
[11] https://www.cyber.gov.au/acsc/view-all-content/alerts/multiple-vulnerabilities-present-spring-framework-java
[12] https://www.csa.gov.sg/singcert/Alerts/al-2022-016
[13] https://www.cert.govt.nz/it-specialists/advisories/active-exploitation-of-rce-in-javas-spring-framework/
[14] https://www.govcert.gov.hk/en/alerts_detail.php?id=763
[15] https://www.govcert.gov.hk/en/alerts_detail.php?id=764
[16] https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerability_20220328
[17] https://www.hkcert.org/security-bulletin/microsoft-edge-remote-code-execution-vulnerability_20220328
[18] https://www.cisa.gov/uscert/ncas/current-activity/2022/03/28/google-releases-security-updates-chrome
[19] https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-av22-150
[20] https://www.cyber.gc.ca/en/alerts/microsoft-edge-security-advisory-av22-155
[21] https://www.csa.gov.sg/singcert/Alerts/al-2022-014

CERT Advisories

- GovCERT.HK[22], HKCERT[23], CISA[24], SingCERT[25] and Canadian Centre for Cyber Security[26] issued alerts regarding multiple vulnerabilities in Firefox. Vulnerabilities (CVE-2022-26485 and CVE-2022-26486) were being exploited in the wild.

- GovCERT.HK[27], HKCERT[28], CISA[29] and SingCERT[30] issued alerts regarding vulnerability in Linux operating systems. PoC code for the privilege escalation vulnerability (CVE-2022-0847) was publicly available.

- HKCERT[31], ACSC[32] and SingCERT[33] issued alerts regarding remote code execution vulnerability (CVE-2022-1040) in Sophos Firewall. The vulnerability was being exploited in the wild.

Securing online services

National Cyber Security Centre (NCSC)[34,35] released two guidance, namely "Building and Operating a Secure Online Service" and "Transaction Monitoring for Online Services", to help organisations in securing their online services. The guidance provided recommendations on security considerations and measures in building, monitoring and operating secure online services.

Protecting from Business Email Compromise (BEC)

SingCERT[36,37] published a playbook to make recommendations on how to prevent BEC and response to BEC incidents under different scenarios, including email domain spoofing, usage of lookalike email domain, compromise of email account, etc. to upkeep organisations' awareness and defence against BEC.

22 https://www.govcert.gov.hk/en/alerts_detail.php?id=749
23 https://www.hkcert.org/security-bulletin/mozilla-products-multiple-vulnerabilities_20220307
24 https://www.cisa.gov/uscert/ncas/current-activity/2022/03/08/mozilla-releases-security-updates
25 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-010
26 https://www.cyber.gc.ca/en/alerts/mozilla-security-advisory-av22-117
27 https://www.govcert.gov.hk/en/alerts_detail.php?id=750
28 https://www.hkcert.org/security-bulletin/linux-kernel-data-manipulation-vulnerability_20220309
29 https://www.cisa.gov/uscert/ncas/current-activity/2022/03/10/dirty-pipe-privilege-escalation-vulnerability-linux
30 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-011
31 https://www.hkcert.org/security-bulletin/sophos-firewall-remote-code-execution-vulnerability_20220328
32 https://www.cyber.gov.au/acsc/view-all-content/alerts/remote-code-execution-vulnerability-present-sophos-firewall-0
33 https://www.csa.gov.sg/singcert/Alerts/al-2022-015
34 https://www.ncsc.gov.uk/guidance/building-operating-secure-online-service
35 https://www.ncsc.gov.uk/guidance/transaction-monitoring-for-online-services
36 https://www.csa.gov.sg/singcert/Advisories/ad-2022-003
37 https://www.csa.gov.sg/singcert/-/media/Singcert/PDFs/Playbook-for-Business-Email-Compromise.pdf

Industry Insight on Cyber Security Threat Trends

Complexity and number of Distributed Denial of Service (DDoS) attacks increased in 2021

Link11 published the "DDoS Report Full Year 2021"[38], which highlighted and analysed the trends of DDoS attacks in 2021. The key findings were:

- **Number of DDoS attacks increased 41% in 2021.** Number of attacks in Q1 2021 doubled from Q1 2020 and amount for Q4 2021 was nearly 2.5 times of the same period in 2020. International hosting service providers, financial institutions, vaccination portals, learning platforms and public sectors were the targets of DDoS attacks.

- **Significant increase in high-volume attacks, with the highest bandwidth at 1.1 Tbps was detected in 2021.** The average attack bandwidth peak nearly tripled from 161 Gbps in 2020 to 437 Gbps in 2021, although the average total bandwidth slightly fell from 1.5 to 1.4 Gbps due to the increase in "carpet bombing" attacks, which were more evasive attacks on entire network blocks instead of targeting single IP address.

- **71% of DDoS attacks were multi-vector, rose from 59% in 2020, with almost half of them deployed 2 vectors (49%).** The largest number of vectors of detected DDoS attacks was 12. Attackers combined multiple techniques and targeted the vulnerabilities in the transport, application and protocol levels simultaneously to increase the rate of successful attack.

- **Ransom DDoS became a trend in 2021.** More attackers used DDoS attacks as extortion and demanded ransoms. Industries such as finance, e-commerce, media and logistics were the victims of ransom DDoS attacks.

- **Attackers continued to develop new attack vectors for reflection amplification attacks.** Datagram Transport Layer Security (DTLS) via Citrix Netscaler and Session Traversal Utilities for NAT (STUN) were abused to conduct reflection amplification attacks in the first half of 2021. The top 3 reflection amplification attack vectors were Simple Service Discovery Protocol (SSDP) (23%), DVR DHCP Discovery (20%) and Network Time Protocol (NTP) (19%).

- **Near 40% of DDoS attacks were from abused cloud resources.** Attackers compromised cloud servers hosted in various public cloud service providers and deployed the compromised instances to launch DDoS attacks.

Source: Link11

[38] https://www.link11.com/en/downloads/ddos-report-full-year-2021/

Industry Insight on Cyber Security Threat Trends

Web application attacks soared in 2021

Radware released the "2021-2022 Global Threat Analysis Report"[39], which studied the threat trends observed worldwide in 2021. The key findings were:

- **Blocked DDoS events and attack volume increased by 37% and 26% respectively as compared with 2020.** The top 3 most targeted industry in terms of attack volume were online commerce and gaming (22.3%), retail (21.5%) and government (13.3%). Retail, government and healthcare recorded most significant growth in attack volume from 2020 to 2021.

- **Total number of blocked malicious web application requests increased 88% compared to 2020.** The number of blocked attacks grew continuously during the first three quarters in 2021 and decreased from Q3 to Q4 but the amount was still higher than Q1. More than 75% of the web application attacks were broken access control and injection attacks. Attackers attempted to access hidden content and functionality of web applications such as obsolete configuration files or unpublished contents in more than 40% of web application attacks. Around 1 in 4 web application attacks targeted banking & finance industry and Software-as-a-Service providers.

- **Over 830,000 Log4Shell exploits were detected in December 2021.** Detection on scanning and exploit attempts started to appear only several hours after the vulnerability was announced. Peak volume was detected on 22 December 2021, with over 90,000 exploits were detected.

- **2.9 billion unsolicited or random attack events from more than 5.7 million unique IP addresses were detected by various sensors in 2021.** Half of the scanning and attacks on TCP services targeted SSH (port 22). Top 3 UDP services being targeted were SIP (port 5060) (29%), NTP (port 123) (20%) and Memcached (port 11211) (13%).

Source: Radware

[39] https://www.radware.com/pleaseregister.aspx/?returnurl=1d0f012c-ab3c-4277-a9e5-00566d3c63f3

Mobile threats were on the rise

Zimperium issued the "2022 Global Mobile Threat Report"[40], which summarised their findings on trends in mobile attacks based on the data collected from its security research team and survey results. The key findings were:

- **Mobile malware was the top threat encountered for mobile endpoints in 2021, 23% of the threats belonged to this category, followed by Man-in-the-middle attacks (13%), malicious websites (12%) and reconnaissance scans (12%).** Mobile malware was the top threat in all regions except Asia/Pacific (APAC) region, in which malicious website was identified as the top threat.

- **Compared to 2020, there was a 466% increase in the number of zero-day exploit targeted mobile endpoints in 2021.** Among all zero-day exploits in 2021, 31% of which were specific to mobile devices, in comparison to only 11% in 2020. In 2021, iOS vulnerabilities accounted for 64% of mobile-specific zero-day exploits.

- **In 2021, 75% of analysed phishing websites targeted mobile devices.** Links to phishing websites were delivered to mobile endpoints by SMS, social media or chat programs. In-app messages were abused to bypass external security controls to deliver phishing messages. The smaller screen size and lower security protection used in mobile devices, as well as attackers' adoption of adaptive and responsive techniques to target mobile devices, increased the phishing threat to mobile endpoints. Adaptive techniques allowed attackers to load different contents and website redirection depending on the access devices. Responsive websites could adjust the position and size of objects based on the screen size of the endpoint used and display the dialogue interface corresponding to the operating systems used to mislead users.

- **The increase in new mobile malware variants began in October 2021 and peaked in December 2021.** Moreover, detection of new Android malware variants also reached a high level in January 2021. Attackers took advantage of and abused discount promotion / advertisement campaigns for malware delivery.

Source: Zimperium

[40] https://get.zimperium.com/2022-global-mobile-threat-report/

Highlight of Microsoft March 2022 Security Updates

Product Family	Impact[41]	Severity	Associated KB and / or Support Webpages
Microsoft Exchange Server	Remote Code Execution	Critical ★★★★	KB5012698, KB5010324
Windows 10 and 11	Remote Code Execution	Important ★★★	KB5011485, KB5011487, KB5011491, KB5011493, KB5011495, KB5011503
Windows Server 2016, 2019, 2022 and Server Core Installation	Remote Code Execution	Important ★★★	KB5011487, KB5011495, KB5011497, KB5011503
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Important ★★★	KB5011486, KB5011527, KB5011535, KB5011560, KB5011564
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB5002068, KB5002139

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-Mar.

Learn more:

High Threat Security Alert (A22-03-07): Multiple Vulnerabilities in Microsoft Products (March 2022) (https://www.govcert.gov.hk/en/alerts_detail.php?id=752)

Data analytics powered by CRisP in collaboration with GovCERT.HK

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