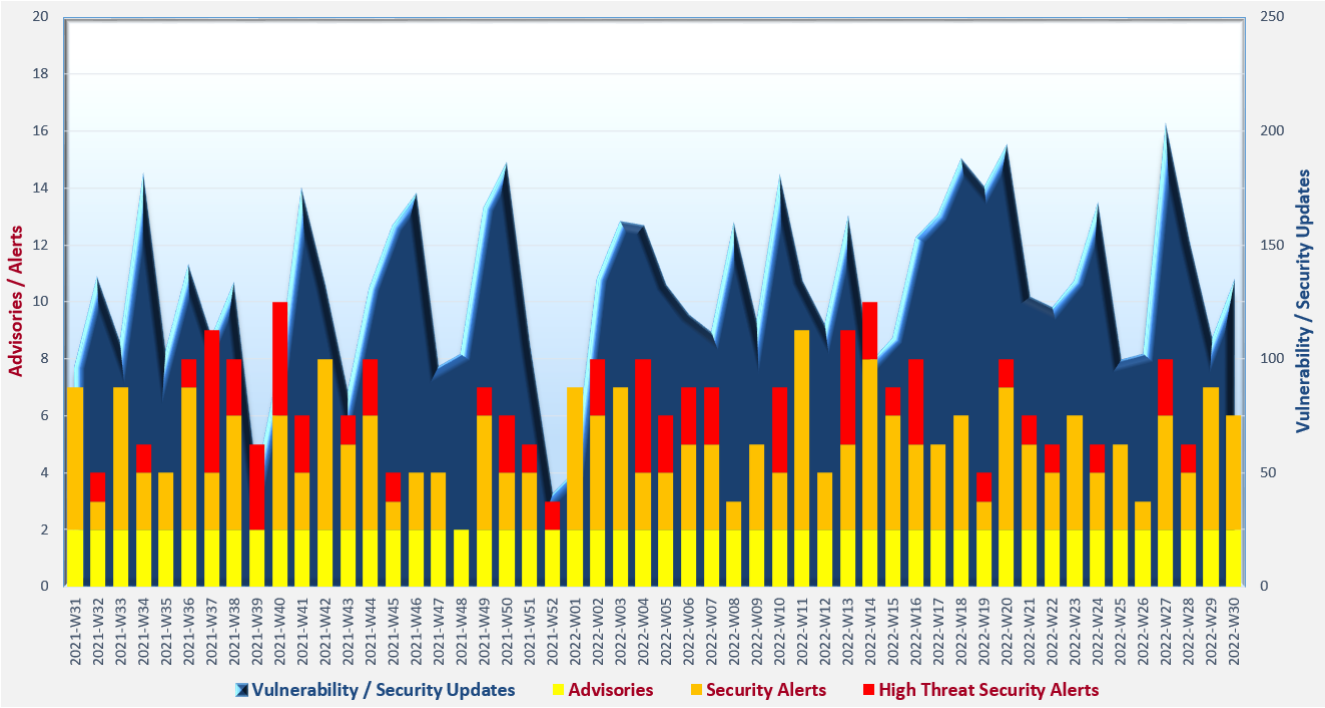
TLP:WHITE

Cyber Security Threat Trends 2022-M07

July 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 **ransomware** attacks remain significant threats affecting organisations' operation and data. Organisations should subscribe DDoS scrubbing service to detect and mitigate such attacks and regularly review and update their security protection measures in different aspects including patch management, backup arrangement, encryption of sensitive data, anti-malware solutions, attack surface management, user privilege management, 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], SingCERT[4], Canadian Centre for Cyber Security[5], Cybersecurity and Infrastructure Security Agency (CISA)[6], MyCERT[7] and JPCERT[8] issued alerts regarding multiple vulnerabilities in Microsoft Products. An elevation of privilege vulnerability (CVE-2022-22047) in Microsoft Windows Products, including both Client and Server, was being actively exploited in the wild. Multiple vulnerabilities (CVE-2022-22029, CVE-2022-22038, CVE-2022-22039, CVE-2022-30216 and CVE-2022-30221) were also at a high risk of exploitation.

- GovCERT.HK[9,10], HKCERT[11,12] and Canadian Centre for Cyber Security[13,14] issued alerts regarding multiple vulnerabilities in Google Chrome and Microsoft Edge (Chromium-based). Vulnerability (CVE-2022-2294) was being exploited in the wild.

Incident Response Guideline for SMEs

HKCERT[15] released its "Incident Response Guideline for SMEs" to help organisations strengthen their cyber defence and minimise the impact in cyber incidents. The guideline defined the tasks to develop a proper incident handling procedure and highlighted the steps in response to security incidents.

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=833
3 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-july-2022
4 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-029
5 https://www.cyber.gc.ca/en/alerts-advisories/microsoft-security-advisory-july-2022-monthly-rollup-av22-387
6 https://www.cisa.gov/uscert/ncas/current-activity/2022/07/12/microsoft-releases-july-2022-security-updates
7 https://www.mycert.org.my/portal/advisory?id=MA-844.072022
8 https://www.jpcert.or.jp/english/at/2022/at220018.html
9 https://www.govcert.gov.hk/en/alerts_detail.php?id=828
10 https://www.govcert.gov.hk/en/alerts_detail.php?id=829
11 https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20220705
12 https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20220707
13 https://www.cyber.gc.ca/en/alerts-advisories/google-chrome-scurity-advisory-av22-371
14 https://www.cyber.gc.ca/en/alerts-advisories/microsoft-edge-security-advisory-av22-380
15 https://www.hkcert.org/blog/incident-response-guideline-for-smes

CERT Advisories

Ramping up cyber security posture of organisations

Canadian Centre for Cyber Security[16,17,18] published a series of guidance for organisations to enhance their protection in cyber security. The guidance provided actionable security measures on protecting organisations and their Internet of Things (IoT) devices from various attacks such as malware infection.

Securing the use of online banking

Canadian Centre for Cyber Security[19] published a guidance to help individuals in securing the use of online banking. The guidance provided recommendations on security considerations and measures in protecting sensitive financial information when using online banking services.

[16] https://www.cyber.gc.ca/en/guidance/cyber-security-guidance-heightened-threat-levels-itsap10101
[17] https://www.cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057
[18] https://www.cyber.gc.ca/en/guidance/internet-things-iot-security-itsap00012
[19] https://www.cyber.gc.ca/en/guidance/how-use-online-banking-securely-itsap00080

Industry Insight on Cyber Security Threat Trends

Distributed Denial-of-Service (DDoS) attacks were on the rise

Cloudflare issued the "2022 Q2 DDoS report"[20], which summarised their analysis and observations on detected DDoS attacks and survey results from DDoS attacked organisations in the second quarter of 2022. The highlights from the report included:

- **Number of survey respondents encountered ransom DDoS attacks increased by 11% compared to Q1 2022.** June recorded the highest number of ransom DDoS attacks in 2022, with 20% of the respondents experienced ransom DDoS attacks.

- **Although the volume of application-layer DDoS attacks decreased by 16% compared to Q1 2022, there was an increase of 44% from Q2 2021.** Hong Kong was the third most targeted location by application-layer DDoS attacks. By industry, Aviation and Aerospace, the Internet as well as Banking, Financial Services and Insurance (BFSI) were the most targeted industry sectors.

- **Number of network-layer DDoS attacks increased by 15% and 109% compared to Q1 2022 and Q2 2021 respectively.** Hong Kong was the 10th most targeted location by network-layer DDoS attacks. Network-layer DDoS attacks targeted Telecommunications industry increased by 66% from Q1 2022. SYN floods was the top attack vector of network-layer DDoS Attacks in Q2 2022, accounted for 53% of all network-layer attacks, followed by DNS (17.6%) and RST floods (7.8%). Amplification DDoS attacks abusing the Character Generator Protocol (CHARGEN), exploiting the Ubiquiti Discovery Protocol and Memcached attacks were the top 3 attack vectors with the highest growth from Q1 2022, increased by more than 3.7, 3.2 and 2.8 times respectively.

- **92.8% of DDoS attacks were under 50k packets per second (kpps), increased by 3.6% compared to Q1 2022.** In terms of bitrate, over 96% of DDoS attacks were below 500 Mbps. However, attacks over 100 Gbps rose by around 8%. Over 92% of attacks lasted within 20 minutes. Attacks with short duration were difficult to detect and mitigate manually. Organisations should adopt DDoS scrubbing services to detect and mitigate such attacks in order to have better defence.

Source: Cloudflare

[20] https://radar.cloudflare.com/notebooks/ddos-2022-q2

Industry Insight on Cyber Security Threat Trends

Search Engine Optimisation (SEO) spam was found in more than half of detected website infections in Q2 2022

Sucuri released the "SiteCheck Malware Trends Report – Q2 2022"[21], which summarised their analysis on scanning result of almost 28 million websites in the second quarter of 2022. Findings and recommendations mentioned in the report were:

- **Nearly 1 out of every 100 scanned websites were found infected in Q2 2022.** SEO spam was the top detected malware family, with more than half of the total infected sites (55.4%) had SEO spam infection. Attackers injected malicious contents to targeted websites by different approaches such as HTML code injection, fake spam post injection or use of spam doorway pages, which adversely impacted the ranking and reputation of the affected websites. 44.82% of all SEO spam detections belonged to keyword spam. Hidden content and Japanese SEO spam occupied the second (23.14%) and third places (21.89%) of SEO spam respectively.

- **34.13% of infected websites were detected with injected malware, which was the second most common type of infections.** NDSW/NDSX malware injections were found in over 15,000 compromised sites, infected more than one million HTML pages or JavaScript files in Q2 2022. Among the most infected JavaScript files, jQuery related JavaScript files were found the most commonly affected. To evade detection, attackers used obfuscation techniques such as CharCode to hide the malicious contents. For the websites scanned in Q2 2022, blocklisted resources were found in 37,916 websites and 12,841 websites led to redirection to blocklisted domains.

- **Over 80% of scanned websites did not implement web application firewall (WAF), missed X-Frame-Options or no content security policy (CSP) adopted.** System administrators should install WAF, enable X-Frame-Options, CSP and strict transport security headers, enforce HTTPS protocol in their websites, as well as timely update and patch their website software and plugins for better defence against various attacks targeting websites and web applications.

Source: Sucuri

[21] https://blog.sucuri.net/2022/07/sitecheck-malware-trends-report-2022-q2.html

Industry Insight on Cyber Security Threat Trends

Ransomware continued to be favourable attack method targeted organisations

Positive Technologies published the "Cybersecurity threatscape: Q1 2022" [22] report, which summarised the threat trends observed in Q1 2022. The key findings were:

- **The number of attacks in Q1 2022 increased by 17.6% and 14.8% from Q1 and Q4 2021 respectively.** Government (16%), healthcare (11%), manufacturing and industry (8%) were the top 3 targeted sectors, with attacks targeted government institutions almost doubled from Q4 2021. 15% of attacks targeted individuals. There was a conspicuous growth for attacks targeted web resources of organisations from 13% in Q4 2021 to 22%. Credential compromise and brute force attacks targeted organisations' websites and social media accounts also increased. Attackers most commonly adopted malware, vulnerability exploitation and social engineering to launch attacks targeted organisations. However, social engineering was a dominant attack method for attacks targeted individuals.

- **55% of attacks targeted individuals and 45% of organisation-targeted attacks caused leakage of confidential data in Q1 2022.** Personal data and credentials were heavily targeted regardless of attack targets. Intellectual property information and medical data were also popular targets for attacks targeted organisations.

- **Ransomware was mostly adopted by attackers in malware attacks targeted organisations, although the share decreased from 53% in Q4 2021 to 44% in Q1 2022.** Healthcare (18%), government (13%), manufacturing and industry (13%) were the most targeted sectors in ransomware attacks. On the other hand, spyware and banking Trojans were the most common malware used in malware attacks targeted individuals.

- **Malicious email (52%) was the major malware distribution channel for attacks targeted organisations.** Compromised computers, servers and network equipment were also commonly used for malware distribution by attackers (36%). For attacks targeted individuals, compromised / counterfeited websites (34%), malicious email (20%) and instant messengers / SMS messages (17%) were the top 3 malware distribution channels.

Source: Positive Technologies

[22] https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2022-q1/

Highlight of Microsoft July 2022 Security Updates

Product Family	Impact[23]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5015807, KB5015808, KB5015811, KB5015814, KB5015832
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5015807, KB5015808, KB5015811, KB5015827
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5015863, KB5015874, KB5015875, KB5015877
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB5016714, KB5002112, KB5002121

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-Jul.

Learn more:

High Threat Security Alert (A22-07-07): Multiple Vulnerabilities in Microsoft Products (July 2022) (https://www.govcert.gov.hk/en/alerts_detail.php?id=833)

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