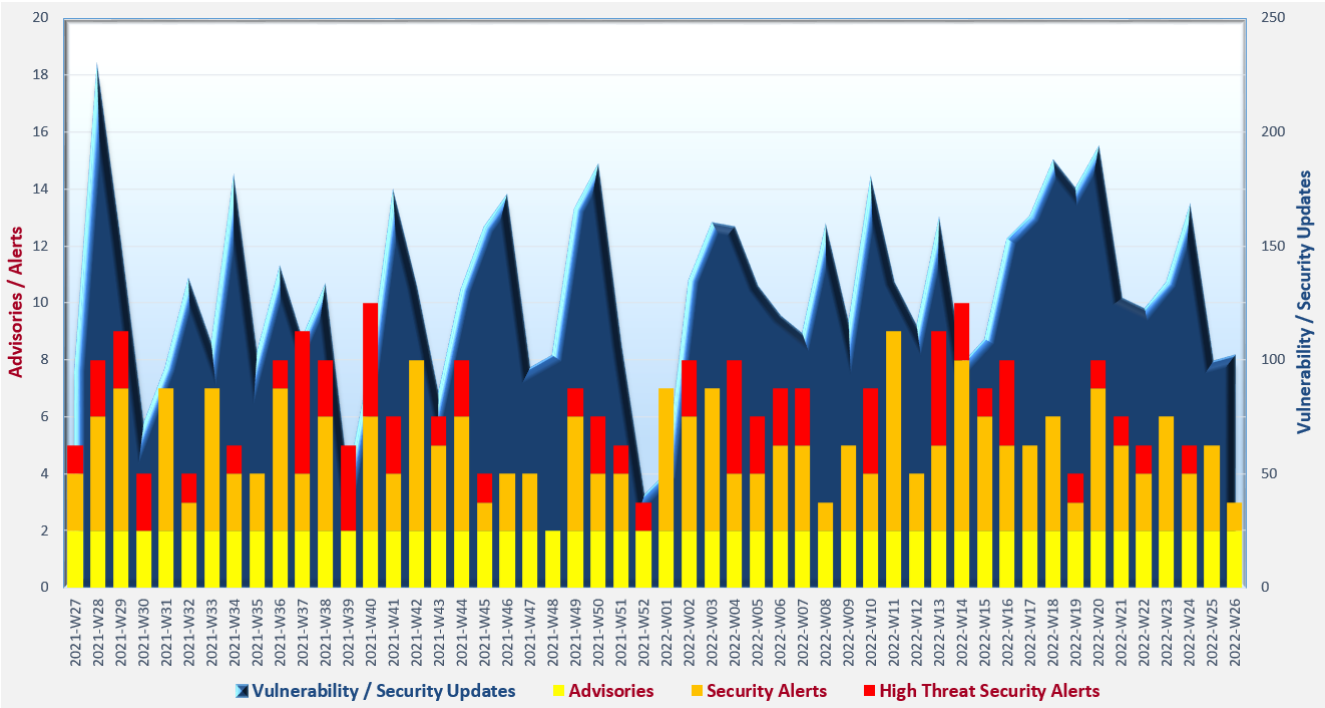
TLP:WHITE

Cyber Security Threat Trends 2022-M06

June 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:

Phishing attacks keep growing and posing serious threats to organisations and individuals. Users should check the authenticity of electronic messages and stay alert to doubtful links and attachments in electronic messages. Organisations should conduct security awareness training regularly to update their users on avoiding phishing attacks and upgrade their security protection solutions to improve their defence against evolving security threats.

[1] https://www.first.org/tlp/

CERT Advisories

Active exploitation of vulnerability in Microsoft products

GovCERT.HK[2], HKCERT[3], Canadian Centre for Cyber Security[4], JPCERT[5] and SingCERT[6] issued alerts regarding multiple vulnerabilities in Microsoft products. Vulnerabilities (CVE-2022-30136, CVE-2022-30139 and CVE-2022-30163) in Microsoft Windows and Server are at a high risk of exploitation. A remote code execution vulnerability (CVE-2022-30190) is being actively exploited. System administrators should refer to vendors' documentation, apply system patches and perform mitigation measures immediately.

Implementing Zero Trust architecture in organisations

HKCERT[7] released a guidance for organisations' reference to protect their networks by adopting a Zero Trust approach thereby to improve their security posture. The guidance provided actionable measures to implement Zero Trust approach in organisations.

Protect against Malicious Scan

HKCERT[8] published an article explaining what attackers could perform in Malicious Scans and other attacks such as brute force attacks and system vulnerabilities exploitation. Security advices were provided in the article for reference.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=821
[3] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-june-2022
[4] https://www.cyber.gc.ca/en/alerts-advisories/microsoft-security-advisory-june-2022-monthly-rollup-av22-325
[5] https://www.jpcert.or.jp/english/at/2022/at220016.html
[6] https://www.csa.gov.sg/en/singcert/Alerts/al-2022-026
[7] https://www.hkcert.org/blog/information-security-utopia-starts-with-zero-trust-architecture
[8] https://www.hkcert.org/blog/malicious-information-gathering-now-i-see-you

Industry Insight on Cyber Security Threat Trends

Threat detections increased more than 20% in the first four months in 2022

ESET released the "Threat Report T1 2022"[9], which summarised the analysis results of malware detection from January to April (T1) 2022. The key findings were:

- **Number of Remote Desktop Protocol (RDP) brute-force attacks fell by more than 40% from T3 2021 to T1 2022.** The number of brute-force attacks to exposed SQL and SMB services also shrank by 64% and 26% respectively. In spite of the drop in detections, password guessing remained the most popular external network intrusion vector (41%), followed by Log4J exploitations (13%).

- **Email threats increased 37% in T1 2022.** A number of massive Emotet email attacks, which sent malicious Microsoft Word documents through email, caused email threats to reach a peak in March 2022. Outlook, DHL and Microsoft were the most impersonated brands found in phishing emails.

- **Ransomware detections sank slightly (4.3%) in T1 2022.** A spike was observed in March 2022 caused by a ransomware variant MSIL/Filecoder.ACB. A slight drop (1.8%) was also observed in web threats detection, even though there was a 30% increase in number of blocked phishing URLs.

- **Detections of Android threats grew by 8% in T1 2022, in which spyware category recorded the largest rise in detection (170.2%).** HiddenApps detections reduced by 10.2% in T1 2022, nevertheless it remained the most popular Android threat. Other Android threats in downtrends included adware and stalkerware; both declined by around 11%.

- **Number of macOS threats detection dropped by 14.9% in T1 2022.** Nearly half (47%) of macOS threats detections belonged to the potentially unwanted applications (PUAs) category.

Source: ESET

[9] https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

Industry Insight on Cyber Security Threat Trends

Growth in adoption of ransomware-as-a-service (RaaS) was expected to continue

Zscaler released the "2022 ThreatLabz State of Ransomware Report"[10], which summarised their findings on ransomware attacks between February 2021 and March 2022 based on analysis on billions of blocked attacks. Findings, predictions and recommendations included:

- **There was a year over year increase of 80% for ransomware attacks, driven by the rise of RaaS.** In 2021, 8 of the top 11 ransomware families adopted RaaS. The increasing trend on adoption of RaaS was expected to continue in 2022-2023.
- **Double extortion ransomware attacks increased by 117%.** Manufacturing was the most targeted industry for the second year in a row, which made up nearly one in five (19.5%) of ransomware attacks. Double extortion ransomware attacks against healthcare sector increased by more than six-fold compared with last year. Conti and LockBit were the most active double extortion ransomware families in 2021.
- **Supply chain ransomware attacks increased.** Attackers breached the software suppliers or technology providers of organisations for gaining access and performing further malicious activities. The trend was expected to grow in 2022-2023.
- **Unpatched Microsoft Exchange servers, Microsoft Windows systems, network devices and Network Attached Storage (NAS) devices were being heavily targeted to conduct ransomware attacks.** System administrators should timely apply security patches and disable unused services in their systems.
- **Organisations should adopt defence-in-depth strategies, including reducing attack surface, enforcing least privilege access control, performing continuous monitoring and speedy anomaly detection, implementing zero trust network access architecture, etc.** It was expected that threat actors would continue improving their attack techniques and ransomware's evasion capability with shorter dwell time for performing attacks.

Source: Zscaler

[10] https://info.zscaler.com/resources-industry-report-2022-threatlabz-state-of-ransomware

Industry Insight on Cyber Security Threat Trends

Reported phishing attacks reached a record high in Q1 2022

Anti-Phishing Working Group (APWG) issued the "Phishing Activity Trends Report, 1st Quarter 2022"[11], which summarised their member organisations' analysis and observations on phishing attacks and other cyber security threats in the first quarter of 2022. The highlights from the report included:

- **Number of phishing attacks has increased by three-fold since early 2020.** In Q1 2022, number of reported phishing attacks increased to more than 300,000 per month, reaching a record high at over 380,000 in March 2022. Over 1,000,000 unique phishing sites were detected in Q1 2022.

- **The top three industries targeted by phishing attacks in Q1 2022 were financial institutions, Software as a Service (SaaS) / webmail providers and eCommerce or Retail web sites, which accounted for 23.6%, 20.5% and 14.6% of phishing attacks respectively.** Phishing attacks targeted social media service rose from 8.5% in Q4 2021 to 12.5% in Q1 2022.

- **The total number of ransomware attacks decreased by 25% in Q1 2022.** The top three targeted industries in ransomware attacks in Q1 2022 were manufacturing, business services and finance, which accounted for 25%, 12.2% and 10.2% of ransomware attacks respectively. Ransomware attacks targeted financial services increased 35% in Q1 2022.

- **63% of business email compromise (BEC) attacks used gift card requests as cash-out method.** Among wire transfer BEC attacks, there was an increase of 69% in the average requested amount and number of requests over US$100,000 was nearly tripled in Q1 2022. 82% of BEC messages were sent from free webmail accounts.

- **In Q1 2022, approximately 59% of malicious emails were credential theft phishing targeted enterprise users, represented a 7% increase.** Social media attacks against business continued their growing trend. Among the social media threats, impersonation attacks increased from 27% in Q4 2021 to 47% in Q1 2022.

Source: APWG

[11] https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf

Highlight of Microsoft June 2022 Security Updates

Product Family	Impact[12]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5013941, KB5013942, KB5013943, KB5013945, KB5013952, KB5013963, KB5014692, KB5014697, KB5014699, KB5014702, KB5014710
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5013941, KB5013942, KB5013944, KB5013952, KB5014677, KB5014678, KB5014692, KB5014699, KB5014702
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5014001, KB5014011, KB5014017, KB5014018, KB5014738, KB5014741, KB5014746, KB5014747
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB5002208, KB5002210, KB5002214, KB5002220

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-Jun.

Learn more:

High Threat Security Alert (A22-06-08): Multiple Vulnerabilities in Microsoft Products (June 2022) (https://www.govcert.gov.hk/en/alerts_detail.php?id=821)

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