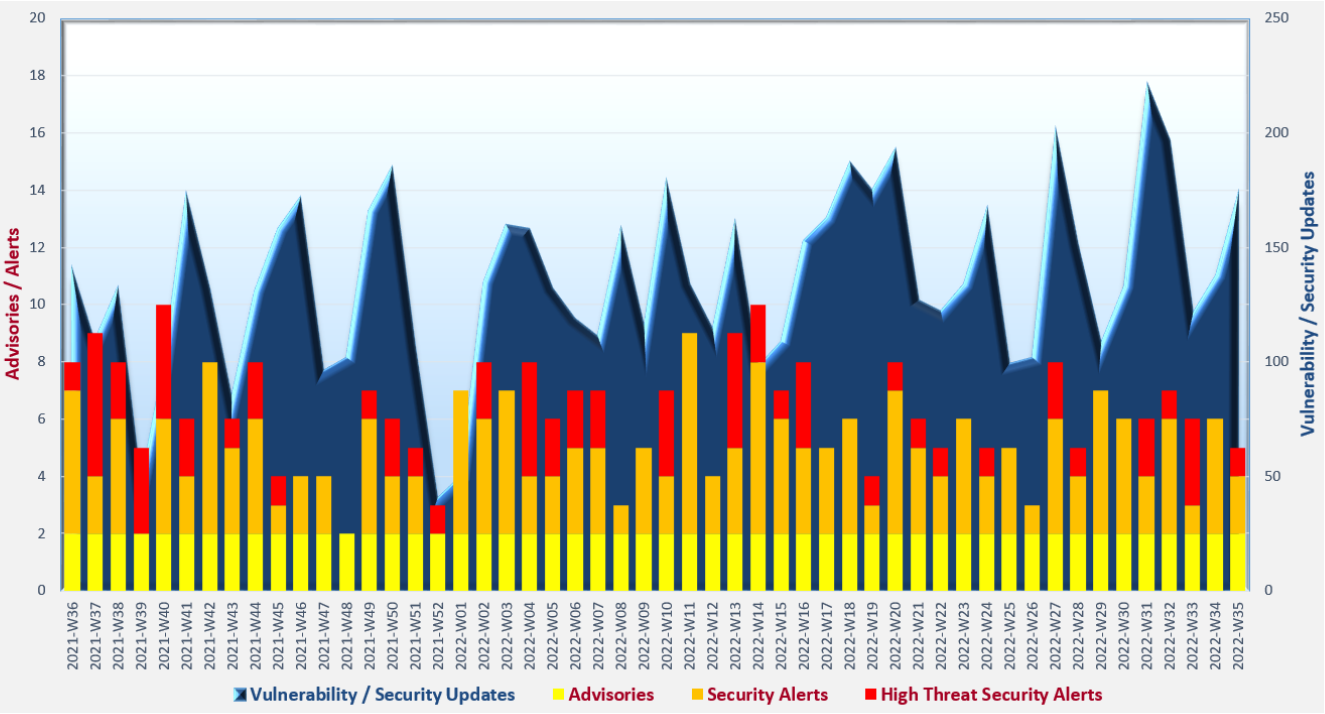
Cyber Security Threat Trends 2022-M08

August 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:

Attackers always attempt to exploit system vulnerabilities and compromise remote access services. System administrators should reduce unnecessary exposure of remote access services to the Internet and implement multi-factor authentication wherever applicable, as well as timely patch their systems.

[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], Canadian Centre for Cyber Security[5], SingCERT[6] and JPCERT[7] issued alerts regarding multiple vulnerabilities in Microsoft Products. A remote code execution vulnerability (CVE-2022-34713) in Microsoft Windows and Server was being actively exploited.

- GovCERT.HK[8,9], HKCERT[10,11], Canadian Centre for Cyber Security[12], SingCERT[13] and MyCERT[14] issued alerts regarding multiple vulnerabilities in Google Chrome and Microsoft Edge (Chromium-based). Vulnerability (CVE-2022-2856) was being 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 iOS and iPadOS. The vulnerabilities (CVE-2022-32893 and CVE-2022-32894) were being actively exploited.

- HKCERT[21], CISA[22] and Canadian Centre for Cyber Security[23] issued alerts regarding a denial of service vulnerability in Palo Alto PAN-OS. Vulnerability (CVE-2022-0028) was being exploited in the wild.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=850
[3] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-august-2022
[4] https://www.cisa.gov/uscert/ncas/current-activity/2022/08/09/microsoft-releases-august-2022-security-updates
[5] https://www.cyber.gc.ca/en/alerts-advisories/microsoft-security-advisory-august-2022-monthly-rollup-av22-448
[6] https://www.csa.gov.sg/singcert/Alerts/al-2022-036
[7] https://www.jpcert.or.jp/english/at/2022/at220021.html
[8] https://www.govcert.gov.hk/en/alerts_detail.php?id=854
[9] https://www.govcert.gov.hk/en/alerts_detail.php?id=856
[10] https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20220817
[11] https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20220818
[12] https://www.cyber.gc.ca/en/alerts-advisories/google-chrome-security-advisory-av22-462
[13] https://www.csa.gov.sg/en/singcert/Alerts/al-2022-041
[14] https://www.mycert.org.my/portal/advisory?id=MA-849.082022
[15] https://www.govcert.gov.hk/en/alerts_detail.php?id=855
[16] https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20220818
[17] https://www.cisa.gov/uscert/ncas/current-activity/2022/08/18/apple-releases-security-updates-multiple-products
[18] https://www.cyber.gc.ca/en/alerts-advisories/apple-security-advisory-av22-463
[19] https://www.csa.gov.sg/en/singcert/Alerts/al-2022-040
[20] https://www.mycert.org.my/portal/advisory?id=MA-850.082022
[21] https://www.hkcert.org/security-bulletin/palo-alto-pan-os-denial-of-service-vulnerability_20220811
[22] https://www.cisa.gov/uscert/ncas/current-activity/2022/08/10/palo-alto-networks-releases-security-update-pan-os
[23] https://www.cyber.gc.ca/en/alerts-advisories/palo-alto-networks-security-advisory-av22-452

CERT Advisories

Securing the cloud

National Cyber Security Centre[24] published an article related to cloud security, specifying the importance on choosing a "secure by design and by default" cloud service provider. It recommended the approach of adopting a "by default" robustly secured cloud service, and relax the restrictions with due diligence and only when needed.

Five-fold increase of unique phishing URLs in Q2 2022

HKCERT released its "Hong Kong Security Watch Report (Q2 2022)"[25]. The number of unique security events nearly doubled from 4,527 in Q1 2022 to 8,793 in Q2 2022. The number of detected phishing URLs increased more than five times compared with Q1 2022. For botnets in Hong Kong network, the number of Mirai and Avalanche increased 11.2% and 131.6% respectively and were the top two largest botnet families in Q2 2022. Number of defacement events dropped more than 80% from 718 in Q1 2022 to 118 in Q2 2022.

Strengthening security controls

Canadian Centre for Cyber Security[26,27] published guidance on strengthening security controls in organisations. The guidance provided actionable security measures on patching operating systems and applications as well as controlling permitted applications on organisations' systems.

[24] https://www.ncsc.gov.uk/blog-post/securing-the-cloud-by-design-and-by-default

[25] https://www.hkcert.org/watch-report/hong-kong-security-watch-report-q2-2022

[26] https://www.cyber.gc.ca/en/guidance/top-10-it-security-action-items-no2-patch-operating-systems-and-applications-itsm10096

[27] https://www.cyber.gc.ca/en/top-top-10-it-security-action-items-no-10-implement-application-allow-lists-itsm10095

Industry Insight on Cyber Security Threat Trends

Ransomware remained the top threat in Q2 2022

Kroll issued the "Q2 2022 Threat Landscape Report"[28], which summarised their analysis and observations on threat landscape in the second quarter of 2022. The highlights from the report included:

- **Ransomware remained the most popular threat incident type in Q2 2022.** 33% of the studied incidents were ransomware attacks, followed by email compromise (30%) and unauthorised access (26%).

- **Healthcare was the top targeted sector in Q2 2022.** 21% of attacks targeted healthcare sector, followed by professional services sector and financial services sector, with both were targeted by 12% of attacks in Q2 2022. Healthcare sector recorded a 90% increase in attacks during Q2 2022, with almost one-third of attacks were ransomware attacks, followed by unauthorised access and email compromise (both at 28%). Percentage of attacks targeted government or public sector were similar to the previous quarter.

- **Although phishing remained the most popular initial access method in Q2 2022, its percentage share dropped from 60% to 41%.** Meanwhile, abusing external remote services as initial access method recorded a 700% increase in Q2 2022, rose from 3% to 24% in Q2 2022 and became the second most popular method. The third most popular initial access method was CVEs or zero day exploitation, accounted for 19% of the total initial access method in Q2 2022, increased from 13% in Q1 2022. External remote services abuse was the most popular initial access method for deploying ransomware in Q2 2022, accounted for 67% of ransomware attacks. Organisations should reduce their remote services' exposure to the Internet, patch the vulnerabilities in a timely manner and implement multi-factor authentication for their remote services.

- **Conti was the most popular ransomware variants in Q2 2022 (18%), followed by Black Basta (13%) and BlackCat (10%).** Conti's share dropped slightly from 20% in Q1 2022, while significant surges were observed for Black Basta and BlackCat in Q2 2022.

Source: Kroll

[28] https://www.kroll.com/-/media/kroll-images/pdfs/q2-2022-threat-landscape-report.pdf

Industry Insight on Cyber Security Threat Trends

Increasing email attack volume with advanced attacks

Abnormal Security released the "H2 2022 Email Threat Report"[29], which included their analysis on email threat landscape and summarised the latest trend of email attacks in the first half of 2022 (H1 2022). The key findings were:

- **Overall email attack volume increased by 48% during the period from July 2021 to June 2022, from an average attack rate of 5.75 per 100 mailboxes to 8.51.** Credential phishing remained the most common attack type, accounted for 68.47% of advanced attacks. Credential phishing attacks became more complex and more convincing by impersonating well-known brands to spoof their targets to provide login credentials.

- **Over 425,000 credential phishing attacks involved brand impersonation in H1 2022.** More than half of these attacks impersonated social networks (32%) and Microsoft products (20%). Both shipping services and ecommerce platforms were the third most common categories in credential phishing attacks with brand impersonation (both at 8%). Over 60 brands in financial services industry were impersonated, accounted for nearly 25% of total number of impersonated brands. More than 35% of credential phishing attacks involved brand impersonation targeted education and religious organisations.

- **Business email compromise (BEC) attacks increased nearly 60% during July 2021 to June 2022, with peak detections in late May 2022.** Advertising / marketing was the industry with the highest chance of receiving BEC in H1 2022.

- **Financial supply chain compromise became a growing cyber threat.** Unlike BEC in which internal executives or employees were impersonated, attackers impersonated external parties such as vendors in financial supply chain compromise attacks, taking advantage of the trust relationships between the targets and the impersonated parties.

Source: Abnormal Security

[29] https://intelligence.abnormalsecurity.com/resources/h2-2022-report-brand-impersonation-phishing

Industry Insight on Cyber Security Threat Trends

Archive file formats were increasingly used by attackers to spread malware

HP published the "HP Wolf Security Threat Insights Report Q2 2022"[30], which summarised the security threats and trends observed in Q2 2022. The key findings were:

- **Number of malware delivered using archive file formats increased 11% while number of malicious scripts and executables decreased 15% in Q2 2022. Malicious spreadsheet remained the most popular file type adopted for spreading malware.** Macro-free code execution techniques, such as abuse of shortcut files, were increasingly adopted by attackers in Q2 2022.

- **Email was the most common attack vector for distributing malware which accounted for 69% of detected threats.** 14% of email-borne malware were found evaded from the scanners at email gateway. The top 5 file types of malware distributed through email were .xlsx, .xls, .rar, .zip and .doc. Web browser download was the second most popular threat vector, contributed 17% of detected threats. .exe, .msi, .rar, .zip and .pdf were the five most detected file format for malware distributed through web browser downloads. System administrators should block emails containing attachments with unsafe file types such as .exe files, and deploy update and advance endpoint protection solutions for better defence.

- **Active exploitations on a high severity remote code execution vulnerability in the Microsoft Support Diagnostic Tool (MSDT) URL protocol were detected in Q2 2022.** There was an increase in shipment-themed malware campaigns for spreading remote access Trojans (RATs) in Q2 2022. Attackers were found trying to hide malicious shellcode in the properties of Microsoft Office documents to distribute malware loader.

Source: HP

[30] https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-q2-2022/

Highlight of Microsoft August 2022 Security Updates

Product Family	Impact[31]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5012170, KB5016616, KB5016622, KB5016623, KB5016629, KB5016639
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5012170, KB5016616, KB5016622, KB5016623, KB5016627
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5012170, KB5016618, KB5016672, KB5016681, KB5016683, KB5016684
Microsoft Exchange Server	Elevation of Privilege	Critical ★★★★	KB5015321, KB5015322
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4462142, KB4462148, KB5001990, KB5002051, KB5002228, KB5002232, KB5002242

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-Aug.

Learn more:
High Threat Security Alert (A22-08-06): Multiple Vulnerabilities in Microsoft Products (August 2022)
(https://www.govcert.gov.hk/en/alerts_detail.php?id=850)

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.