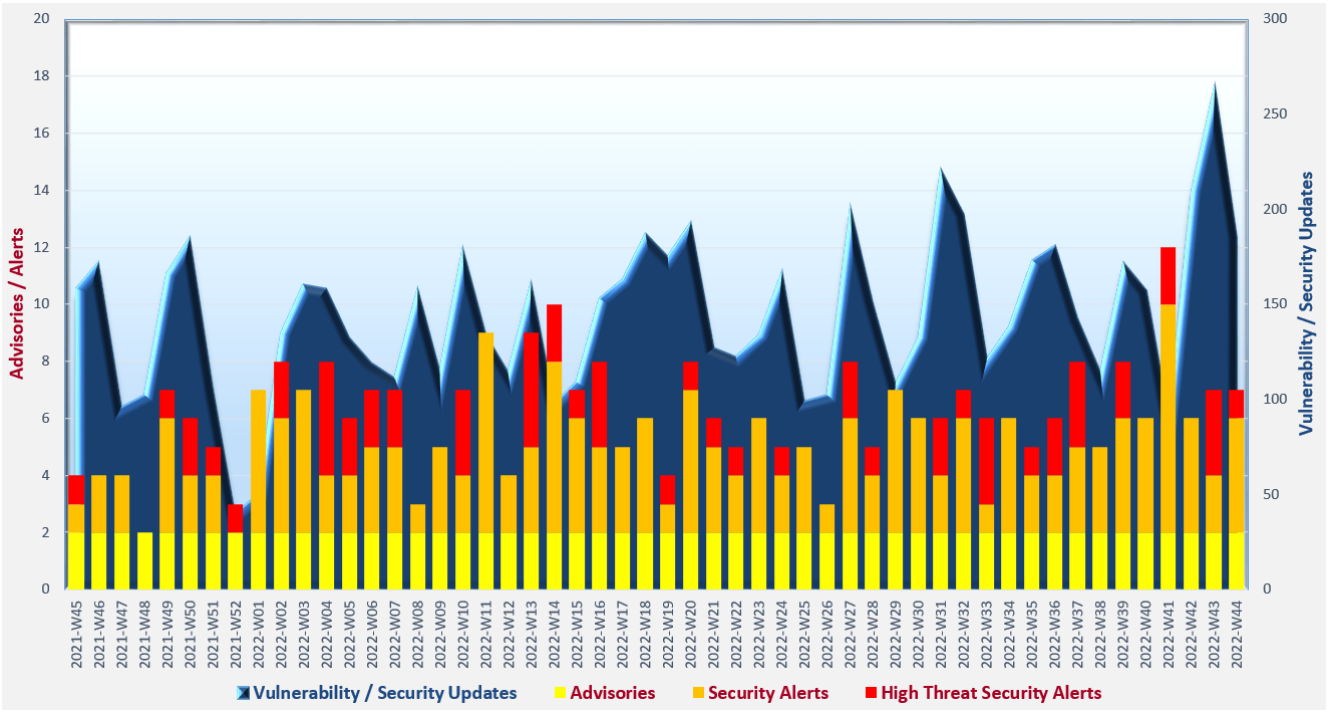
TLP:CLEAR

Cyber Security Threat Trends 2022-M10

October 2022

With reference to the FIRST Traffic Light Protocol (TLP) standard[1], this document is classified as TLP:CLEAR information. Recipients may share with peers and partner organisations without restriction.

Cyber Security Threat Landscape of the past 12 months (source: GovCERT.HK)



Trending:

Even though the number for phishing activities and other cyber threats may not be increasing, organisations should remain vigilant on the ever changing cyber threat landscape. Security awareness training should be conducted by the organisations to equip their staff with knowledge on up-to-date cyber security threats, phishing tactics and corresponding defensive measures. Organisations should also periodically review and upgrade their existing cyber security protection measures to defend against the advancing malware capability and other cyber threats.

[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], MyCERT[7] and JPCERT[8] issued alerts regarding multiple vulnerabilities in Microsoft Products. An elevation of privilege vulnerability (CVE-2022-41033) in Microsoft Windows and Server was being actively exploited. Technical detail of an information disclosure vulnerability (CVE-2022-41043) in Microsoft Office was publicly disclosed.

- GovCERT.HK[9], HKCERT[10], CISA[11], SingCERT[12] and MyCERT[13] issued alerts regarding multiple vulnerabilities in VMware Cloud Foundation. PoC code for exploitation of a remote code execution vulnerability (CVE-2021-39144) was publicly available.

- GovCERT.HK[14,15], HKCERT[16,17], Canadian Centre for Cyber Security[18,19] and SingCERT[20] issued alerts regarding a vulnerability (CVE-2022-3723) in Google Chrome and Microsoft Edge. This vulnerability was being exploited in the wild.

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=892
3 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-october-2022
4 https://www.cisa.gov/uscert/ncas/current-activity/2022/10/11/microsoft-releases-october-2022-security-updates
5 https://www.cyber.gc.ca/en/alerts-advisories/microsoft-security-advisory-october-2022-monthly-rollup-av22-570
6 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-061
7 https://www.mycert.org.my/portal/advisory?id=MA-873.102022
8 https://www.jpcert.or.jp/english/at/2022/at220028.html
9 https://www.govcert.gov.hk/en/alerts_detail.php?id=903
10 https://www.hkcert.org/security-bulletin/vmware-products-multiple-vulnerabilities_20221031
11 https://www.cisa.gov/uscert/ncas/current-activity/2022/10/28/vmware-releases-security-updates
12 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-066
13 https://www.mycert.org.my/portal/advisory?id=MA-881.102022
14 https://www.govcert.gov.hk/en/alerts_detail.php?id=905
15 https://www.govcert.gov.hk/en/alerts_detail.php?id=907
16 https://www.hkcert.org/security-bulletin/google-chrome-data-manipulation-vulnerability_20221028
17 https://www.hkcert.org/security-bulletin/microsoft-edge-data-manipulation-vulnerability_20221101
18 https://www.cyber.gc.ca/en/alerts-advisories/google-chrome-security-advisory-av22-612
19 https://www.cyber.gc.ca/en/alerts-advisories/microsoft-edge-security-advisory-av22-616
20 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-068

CERT Advisories

- GovCERT.HK[21], HKCERT[22], CISA[23], SingCERT[24] and MyCERT[25] issued alerts regarding multiple vulnerabilities in Apple iOS and iPadOS. Vulnerability (CVE-2022-42827) was being actively exploited.

- GovCERT.HK[26], HKCERT[27], Canadian Centre for Cyber Security[28], Australian Cyber Security Centre (ACSC)[29] and JPCERT[30] issued alerts regarding a vulnerability in FortiOS and FortiProxy. A remote authentication bypass vulnerability (CVE-2022-40684) was being exploited in the wild.

- HKCERT[31] issued an alert regarding a denial of service vulnerability (CVE-2022-35737) in SQLite. PoC code for exploitation of the vulnerability was publicly available.

- HKCERT[32] and SingCERT[33] issued alerts regarding a remote code execution vulnerability (CVE-2022-42889) in Apache Commons Text. PoC code for exploitation of the vulnerability was publicly available.

- HKCERT[34] and SingCERT[35] issued alerts regarding multiple vulnerabilities in Cisco products. Vulnerabilities (CVE-2020-3153 and CVE-2020-3433) were being exploited in the wild.

Assess supply chain cyber security

National Cyber Security Centre[36] has published a guidance helping organisations on assessing cyber security in their supply chains. The guidance proposes a five-stage approach with recommendations on practical steps at every stage for organisations' reference.

21 https://www.govcert.gov.hk/en/alerts_detail.php?id=902
22 https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20221025
23 https://www.cisa.gov/uscert/ncas/current-activity/2022/10/26/apple-releases-security-updates-multiple-products
24 https://www.csa.gov.sg/en/singcert/Alerts/AL-2022-065
25 https://www.mycert.org.my/portal/advisory?id=MA-878.102022
26 https://www.govcert.gov.hk/en/alerts_detail.php?id=888
27 https://www.hkcert.org/security-bulletin/fortinet-products-multiple-vulnerabilities_20221011
28 https://www.cyber.gc.ca/en/alerts-advisories/fortinet-security-advisory-av22-563
29 https://www.cyber.gov.au/acsc/view-all-content/alerts/remote-code-execution-vulnerability-present-fortinet-devices
30 https://www.jpcert.or.jp/english/at/2022/at220025.html
31 https://www.hkcert.org/security-bulletin/sqlite-denial-of-service-vulnerability_20221026
32 https://www.hkcert.org/security-bulletin/apache-commons-text-remote-code-execution-vulnerabilities_20221018
33 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-064
34 https://www.hkcert.org/security-bulletin/cisco-products-multiple-vulnerabilities_20221026
35 https://www.csa.gov.sg/singcert/Alerts/AL-2022-067
36 https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security

CERT Advisories

Implementing phishing-resistant multi-factor authentication (MFA)

CISA[37,38,39] has published guidance on implementation of phishing-resistant MFA and number matching in MFA applications to defend against cyber threats targeting MFA-protected systems such as phishing, push bombing, sim swap attacks or Signaling System 7 (SS7) protocol vulnerability exploitation.

[37] https://www.cisa.gov/uscert/ncas/current-activity/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching
[38] https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
[39] https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf

Industry Insight on Cyber Security Threat Trends

Number of Distributed Denial of Service (DDoS) attacks rose in the first half of 2022

Nexusguard issued the "DDoS Statistical Report 1HY 2022"[40], which summarised their findings on DDoS attack trends in the first half of 2022. The key statistics and trends were:

- **Total DDoS attack count in H1 2022 increased by 75.6% compared with H2 2021.** UDP Attack was the top attack vector in H1 2022 (39.58%), followed by HTTPS Flood (15.94%) and TCP ACK Attack (6.48%). UDP Attack and HTTPS Flood increased by 56.76% and 75.95% respectively. Attackers often used large amount of UDP attacks as cover for other malicious activities such as exfiltration of sensitive information or running of malware or remote code. Over 85% of DDoS attacks in H1 2022 were from single attack vector.

- **In terms of attack category, Direct Flood attack was the top attack category in H1 2022 (67.93%), followed by Application Attack (17.51%) and Amplification Attack (14.56%).** Compared with H2 2021, Direct Flood attack increased by 48%, while Application Attack and Amplification Attack increased by 330% and 106.65% respectively. Computers and servers such as Windows OS and MacOS devices were the most common source of application attacks (74.26%), while mobile devices such as Android OS and iOS devices accounted for 25.6% of application attacks.

- **In H1 2022, Hong Kong was one of the locations targeted by bit-and-piece attacks and ranked the 5th in top reflected attack destinations in APAC.** Moreover, in terms of attack source IP address, Hong Kong ranked the 8th in application attack source region globally, accounted for 3% of application attacks in H1 2022.

- **Average DDoS attack size decreased by 55.97% as compared with H2 2021.** In H1 2022, the attack size of over 99.8% of the DDoS attack was less than 10 Gbps and around 82% of the attacks with attack size less than 1 Gbps. The largest attack size was 232 Gbps, dropped by 66.82% compared with H2 2021. The average attack duration was around 90 minutes and around 70% of the DDoS attacks lasted shorter than 90 minutes. The longest attack lasted over 460 hours. Compared to H2 2021, the maximum attack duration increased by 113.98%, while the average duration decreased by 45.4%.

Source: Nexusguard

[40] https://blog.nexusguard.com/threat-report/ddos-statistical-report-for-1hy-2022

Industry Insight on Cyber Security Threat Trends

Overall threat detections declined 9.1% during May to August 2022

ESET released the "Threat Report T2 2022"[41], which summarised the cyber threat landscape and analysis results of threat detection from May to August (T2) 2022. The major observations were:

- **Number of Remote Desktop Protocol (RDP) attack detections decreased continuously from 123 billion in T1 2022 to 13 billion in T2 2022 with a decline of 89%.** Attack detections targeted public facing SQL services and SMB services also recorded decreases of 28.7% and 8.9% respectively. Password guessing (41%) remained the most popular external network intrusion vector, followed by the Log4j vulnerability (13%).

- **There was a significant decrease in ransomware detections by 24.1% in T2 2022.** The United States (7.5%), China (6%), and Israel (5.5%) were the top three economies most targeted by ransomware attacks in T2 2022.

- **Email threats dropped 10.2% in T2 2022.** While COVID-19 themed malicious email detections dropped nearly by half from T1 to T2 2022, detections on email threat with travel as mail subject were found increased by 70%. Windows executables (47%), script files (23%) and office documents (19%) were the top three malicious email attachment types in T2 2022.

- **Web threats, including scam URLs, phishing sites, malware-distributing web sites, etc. decreased by 6% in T2 2022.** However, detections of shipping-themed phishing web sites recorded an increase by six times. Attackers used phishing web sites impersonating shipping companies and tempted the victims to enter the web sites to verify shipping addresses. Finance (32.7%), social media (24.9%) and shipping (13.1%) were the top 3 phishing web site categories in T2 2022.

- **Android detections continuously increased by 9.5% in T2 2022 and Spyware was the fastest growing category (109%).** HiddenApps was the category recorded the highest Android detection number, with an increase of 32.4%. While overall detections for Adware slightly decreased by 4.2%, there was a spike in detections near end of T2.

Source: ESET

[41] https://www.welivesecurity.com/wp-content/uploads/2022/10/eset_threat_report_t22022.pdf

Industry Insight on Cyber Security Threat Trends

Phishing activities declined in Q3 2022

Cofense released the "Q3 2022 Cofense Phishing Intelligence Trends Review"[42], which included the analysis results on phishing attacks detected based on email and malware samples collected in the third quarter of 2022 and predicted the upcoming trends in the fourth quarter. The key findings were:

- **The number of phishing emails for malware delivery fell significantly in July 2022 and became stable till the end of Q3 2022.** The decrease in Emotet activities largely contributed to the drop of phishing email volume.
- **The top five most prevalent malware types in Q3 2022 remained unchanged as compared with Q2 2022.** Loader was the malware type found in most malicious email in both Q2 and Q3 2022. A surge in Keylogger was observed in Q3 and surpassed Information Stealer, which decreased in volume in Q3 2022, and became the second most prevalent malware type. The Remote Access Trojan malware recorded a faster growth and overtook Banker as the fourth most common malware type.
- **Office macro was most widely used for delivering malware in Q3 2022, with increased activities utilising malicious HTML detected.** The top three file extensions for attachments found in phishing email were .pdf, .htm and .html.
- **In both Q2 and Q3 2022, more than 2% of the IP address of Command and Control (C2) servers were in Hong Kong.** The percentage increased slightly from 2.31% in Q2 2022 to 2.6% in Q3 2022.
- **Uptrend in QakBot activity and advancement in its delivery mechanism and evasion ability were anticipated in Q4 2022.** Phishing campaigns using malicious html files for malware delivery were expected to be continued.

Source: Cofense

[42] https://go.cofense.com/q3-cofense-phishing-intelligence-trends-review/

Highlight of Microsoft October 2022 Security Updates

Product Family	Impact[43]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5016616, KB5016622, KB5016623, KB5016629, KB5016639, KB5018410, KB5018411, KB5018418, KB5018419, KB5018425, KB5018427
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5016622, KB5016623, KB5016627, KB5018411, KB5018419, KB5018421
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5016672, KB5016681, KB5016683, KB5016684, KB5018457, KB5018474, KB5018476, KB5018478
Microsoft Office-related software	Remote Code Execution	Critical ★★★★	KB5002026, KB5002279, KB5002288

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-Oct.

Learn more:

High Threat Security Alert (A22-10-09): Multiple Vulnerabilities in Microsoft Products (October 2022) (https://www.govcert.gov.hk/en/alerts_detail.php?id=892)

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