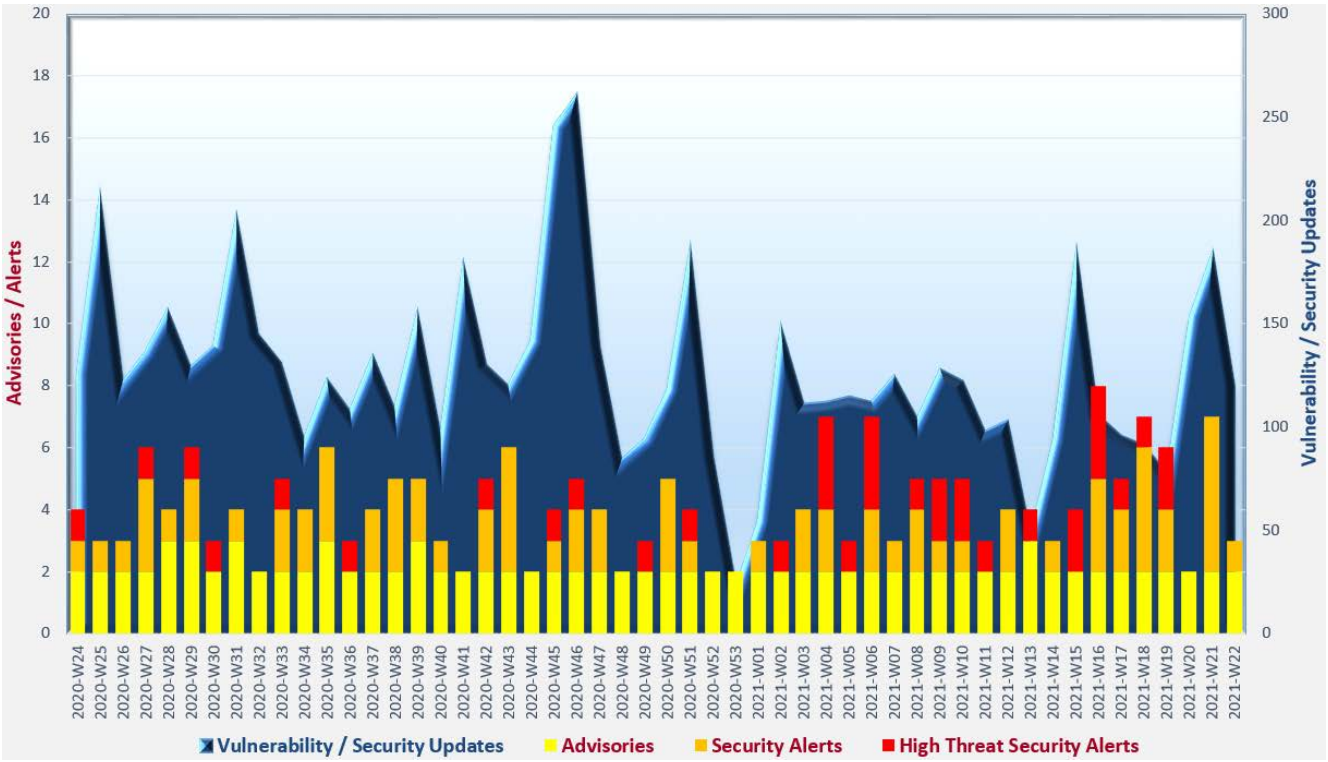
TLP:WHITE

Cyber Security Threat Trends 2021-M05

May 2021

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 keep on switching attack vectors and increasing attack volume in **Distributed Denial of Service (DDoS) attacks**. Organisations should implement and continuously review their DDoS protection measures.
- ✧ **Misconfigurations in cloud platforms** can lead to data leakage and security breach. Organisations should adopt least privilege principle, encryption, multi-factor authentication, network segmentation, etc. in their cloud environments.
- ✧ **Phishing** and **human negligence** are main causes of security breaches. Organisations should, in addition to conduct security awareness training and phishing simulation program customised to their environments, continuously review and upgrade their existing protection solutions to defend against evolving cyber security 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], JPCERT [4] and SingCERT [5] issued alerts regarding multiple vulnerabilities in Microsoft products. PoC codes for exploitation of a critical remote code execution vulnerability (CVE-2021-31166) were publicly available.

- GovCERT.HK[6], HKCERT[7], SingCERT[8,9], CERT NZ[10], Cybersecurity and Infrastructure Security Agency (CISA)[11], and Canadian Centre for Cyber Security[12] issued alerts regarding multiple vulnerabilities in various Apple devices. Vulnerabilities including CVE-2021-30663, CVE-2021-30665 and CVE-2021-30713 were being actively exploited.

- GovCERT.HK[13], HKCERT[14], JPCERT[15], CERT NZ[16], CISA[17], and Canadian Centre for Cyber Security[18] issued alerts regarding multiple vulnerabilities in Adobe Acrobat and Reader. The arbitrary code execution vulnerability (CVE-2021-28550) in Adobe Reader has been exploited in the wild for attacks targeting Windows users.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=584
[3] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-may
[4] https://www.jpcert.or.jp/english/at/2021/at210024.html
[5] https://www.csa.gov.sg/singcert/Alerts/al-2021-032
[6] https://www.govcert.gov.hk/en/alerts_detail.php?id=579
[7] https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20210525
[8] https://www.csa.gov.sg/singcert/alerts/al-2021-033
[9] https://www.csa.gov.sg/singcert/alerts/al-2021-030
[10] https://www.cert.govt.nz/it-specialists/advisories/vulnerabilities-in-apple-operating-systems-reportedly-being-actively-exploitednew-advisory-technical/
[11] https://us-cert.cisa.gov/ncas/current-activity/2021/05/25/apple-releases-security-updates
[12] https://www.cyber.gc.ca/en/alerts/apple-security-advisory-31
[13] https://www.govcert.gov.hk/en/alerts_detail.php?id=585
[14] https://www.hkcert.org/security-bulletin/adobe-monthly-security-update-may-2021
[15] https://www.jpcert.or.jp/english/at/2021/at210023.html
[16] https://www.cert.govt.nz/it-specialists/advisories/vulnerability-in-adobe-acrobat-and-reader-being-actively-exploited/
[17] https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/adobe-releases-security-updates-multiple-products
[18] https://www.cyber.gc.ca/en/alerts/adobe-security-advisory-40

CERT Advisories

Security events in Hong Kong slightly dropped in Q1 2021[19]

HKCERT released its Hong Kong Security Watch Report (Q1 2021). The number of security events declined from 5,074 in Q4 2020 to 5,017 in Q1 2021, contributed by the drop in malware hosting, defacement and botnet events. There were 295 defacement events and 4,227 botnet events in Q1 2021, both recorded a decrease of around 3% from Q4 2020. However, number of phishing events recorded an increase of around 25%. There was no Botnet Command and Control Centre (C&C) security event for six consecutive quarters. Mirai remained the largest botnet family though it dropped 19.2% in Q1 2021.

Comprehensive cyber security guidance for medium to large organisations

National Cyber Security Centre (NCSC)[20] published the "10 Steps to Cyber Security" guidance for medium to large organisations with dedicated personnel for cyber security management. Areas such as risk management, vulnerability management, supply chain security, architecture and configuration security, etc. were covered in the guidance. Organisations were advised to implement appropriate security measures to strengthen their cyber security protection.

[19] https://www.hkcert.org/watch-report/hong-kong-security-watch-report-q1-2021
[20] https://www.ncsc.gov.uk/collection/10-steps

Industry Insight on Cyber Security Threat Trends

Distributed Denial of Service (DDoS) attack volume increased in Q1 2021

Radware published the "Quarterly DDoS Attack Report, Q1 2021"[21], which summarised their analysis on DDoS attacks recorded in the first quarter of 2021. The highlights from the report included:

- **In Q1 2021, the total attack volume increased by 31% compared to Q4 2020 and the largest recorded attack volume was 295Gbps, up by more than 10% from 260Gbps in Q4 2020.** Nevertheless, the total number of attacks decreased by 2%. The average attack volume dropped to under 150Mbps from over 315Mbps in December 2020. Almost one in every 1,000 attacks had attack volume greater than 10Gbps.

- **Healthcare industry experienced high number of attacks in the first half of Q1 2021.** The public-facing assets of biotechnology and pharmaceutical organisations were mostly targeted during the period. Attackers shifted to launching smaller number of attacks targeting hospitals in the second half of Q1 2021.

- **High volume attacks targeted the government sector were recorded during February and March of 2021.** The attack pattern shifted from large amount of low-volume attacks recorded during Q4 2020. Government institutions in North America were the primary DDoS attack targets.

- **Majority of attacks targeted HTTPS and HTTP, accounted for 55.9% and 18% of attack volume, respectively.** Attacks targeted HTTPS increased significantly from around 7% in Q4 2020 due to high volume of UDP-based amplification attacks. On the other hand, attacks targeted DNS decreased from almost 45% in Q4 2020 to 11% in Q1 2021. UDP Fragment and UDP Floods were the most prominent attack vector and accounted for about 92% of attack volume in Q1 2021. UDP was the most abused protocol for DDoS attack and accounted for 99% of total attack volume in Q1 2021.

Source: Radware

[21] https://www.radware.com/quarterly-ddos-report//

Trends in cloud misconfigurations

Aqua Security issued the "Cloud Security Report – Cloud Configuration Risks Exposed" [22], summarising their analysis on cloud service configuration as well as trends and guidance on cloud security. The key findings were:

- **Over 80% of cloud storage were found exposed to public due to misconfigurations such as opening unnecessary network protocols and ports. More than half of them had all ports opened. Over-permissive storage policies and misconfigured access control lists were found in around 90% and 84% of cloud storage respectively.** Some organisations implemented one storage policy over multiple storage instances generically, which could lead to over-permissive user privileges. System administrators should configure their systems with adoption of the least privilege principles, and close unnecessary network protocols and ports from exposure to the Internet.

- **Almost 75% of cloud storage were not encrypted, and nearly 40% of traffic used unencrypted HTTP protocol.** Some organisations used obsolete TLS version. Sensitive data in cloud storage, no matter at rest, in transit and in processing, should be encrypted by up-to-date algorithms.

- **A number of misconfigurations were found in cloud identity access management service, including overuse of super-user account, multi-factor authentication not enabled, strong password policy not enforced, unused user accounts not removed, and so on.** Users should use multi-factor authentication and regularly change their passwords for better user credential protection.

- **More than one-third of organisations had issues in database configurations, exposing their databases vulnerable to unauthorised access.** Database access should be restricted to organisational private network or authorised IP addresses. Layered defence should be adopted for database access.

Source: Aqua Security

[22] https://info.aquasec.com/cspm-threat

Industry Insight on Cyber Security Threat Trends

Human risk played an important role in security breaches

Elevate Security and Cyentia Institute published its "Elevating Human Attack Service Management"[23] report, which presented the analysis results on human risk based on data collected from 2018 to 2020, including 4.5 million user actions of around 114,000 users in over 2,000 organisational departments. The highlights from the report included:

- **Generic phishing simulation programs, security awareness training and security controls might be less effective, as different types of employees had different level of human risks.** The report indicated that non-managerial employees had a higher phishing email click rate and malware infection events compared to managers. Organisation should adopt dynamic and adaptive security controls for different user types instead of using a one-size-fits-all generic approach.

- **The timing pattern of simulated phishing attacks were not realistic enough.** The report showed that there were timing pattern gaps between simulated phishing and real phishing in phishing emails delivery, clicked phish and reported phish. For instance, real phishing emails were delivered round the clock with a larger volume appeared near quitting time but simulated phishing showed a different pattern, with spikes at mid-night or near start of office hour. Organisations should improve the design of phishing simulation to make their phishing simulation programs more realistic.

- **The adoption of tools like password managers or multi-factor authentication (MFA) was low.** Only 21.5% of users used password managers and 6.1% of users used password managers with MFA. The report revealed that users with active password managers were less likely to download and execute malware. Organisations could consider the adoption of tools like password managers and MFA to improve their defence against security threats.

Source: Elevate Security & Cyentia Institute

[23] https://elevatesecurity.com/resource/cyentia-elevating-human-attack-surface-management/

Highlight of Microsoft May 2021 Security Updates

Product Family	Impact[24]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB5003169, KB5003171, KB5003172, KB5003173, KB5003174, KB5003197
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5003169, KB5003171, KB5003173, KB5003197
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5003203, KB5003208, KB5003209, KB5003220
Microsoft Internet Explorer 11	Remote Code Execution	Critical ★★★★	KB5003165, KB5003169, KB5003171, KB5003172, KB5003173, KB5003174, KB5003197, KB5003208, KB5003209, KB5003233
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4464542, KB4493197, KB4493206, KB5001914, KB5001918, KB5001919, KB5001920, KB5001923, KB5001925, KB5001927, KB5001928, KB5001931, KB5001936
Microsoft Exchange Server	Remote Code Execution	Important ★★★	KB5003435

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/2021-May.

Learn more:

High Threat Security Alert (A21-05-07): Multiple Vulnerabilities in Microsoft Products (May 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=584)

Data analytics powered by CRisP in collaboration with GovCERT.HK

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