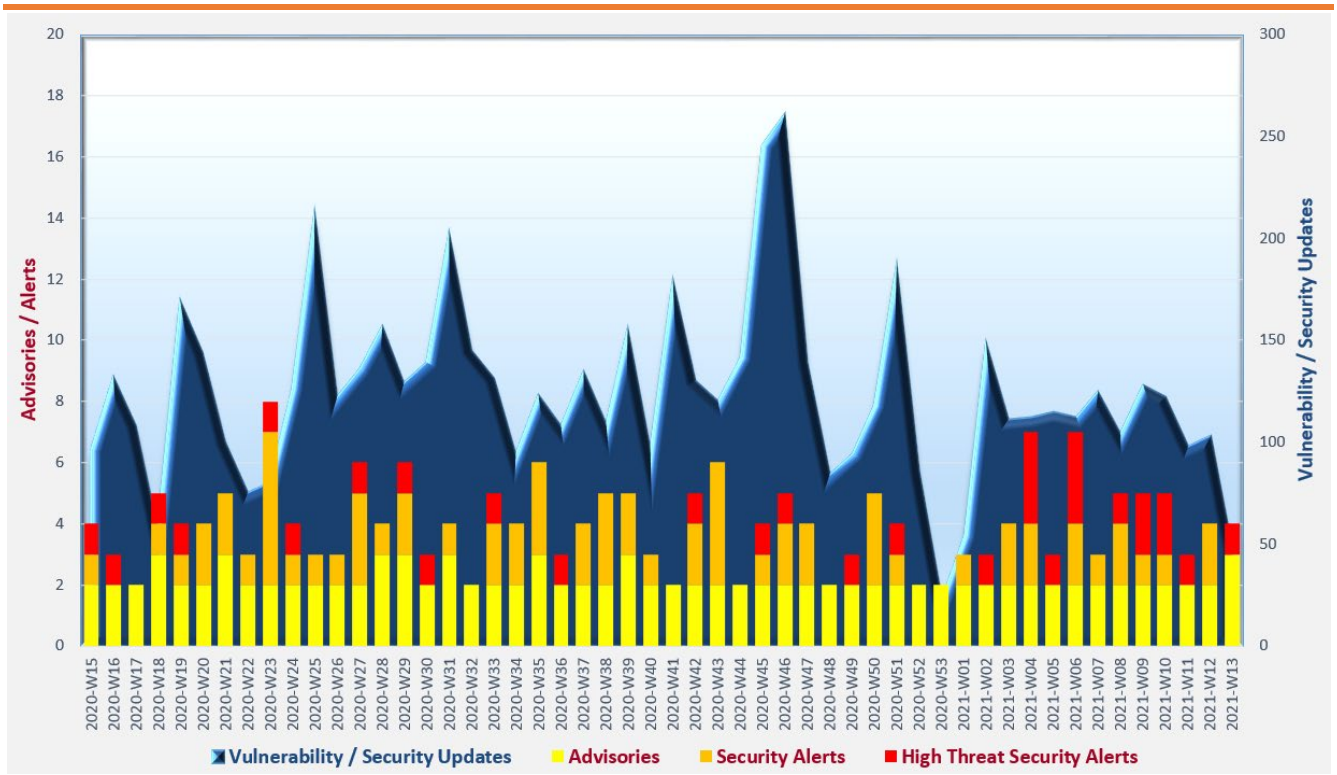
TLP:WHITE

Cyber Security Threat Trends 2021-M03

March 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:

- ✧ **Password reuse** and **weak passwords** increase the threat of user credential compromise. Adoption of multi-factor authentication is recommended. Organisations could check against blacklisted passwords regularly to screen out commonly used, weak or compromised passwords.
- ✧ **Distributed Denial of Service (DDoS) attacks** surge during COVID-19 pandemic. Attackers continue weaponising new attack vectors to launch attacks. Organisations should implement security controls such as subscription of DDoS mitigation service and reduce attack surface to defend against DDoS attacks.
- ✧ Attackers trend to employ **double-extortion ransomware attacks**. Backups should be stored offline as soon as possible. Sensitive data should be properly encrypted to deter attackers disclosing the information.

[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[2,3], HKCERT[4], Canadian Centre for Cyber Security[5], JPCERT[6] and National Cyber Security Centre (NCSC)[7] issued alerts regarding multiple vulnerabilities in Microsoft products, including out-of-band security updates regarding vulnerabilities in Microsoft Exchange Server. A number of vulnerabilities (CVE-2021-26411, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065) are being actively exploited.

- GovCERT.HK[8], HKCERT[9] and Canadian Centre for Cyber Security[10] issued alerts regarding multiple vulnerabilities in Google Chrome, which, upon exploitation, could lead to denial of service and remote code execution on the affected system. The vulnerability (CVE-2021-21193) is being exploited in the wild.

- GovCERT.HK[11], HKCERT[12], SingCERT[13] and Cybersecurity and Infrastructure Security Agency (CISA)[14] issued alerts regarding a cross-site scripting vulnerability (CVE-2021-1879) in Apple iOS and iPadOS. Active exploitation against the vulnerability was observed.

- GovCERT.HK[15], HKCERT[16], JPCERT[17] and Canadian Centre for Cyber Security[18] issued alerts regarding multiple vulnerabilities in F5 devices. Regarding the remote command execution vulnerability (CVE-2021-22986) in iControl REST interface, PoC codes for exploitation were publicly available and active scanning activities targeting this vulnerability were observed.

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=556
3 https://www.govcert.gov.hk/en/alerts_detail.php?id=560
4 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-march-2021-_20210310
5 https://www.cyber.gc.ca/en/alerts/microsoft-security-advisory-march-2021-monthly-rollup
6 https://www.jpcert.or.jp/english/at/2021/at210013.html
7 https://www.ncsc.gov.uk/news/advice-following-microsoft-vulnerabilities-exploitation
8 https://www.govcert.gov.hk/en/alerts_detail.php?id=562
9 https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20210315
10 https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-49
11 https://www.govcert.gov.hk/en/alerts_detail.php?id=565
12 https://www.hkcert.org/security-bulletin/apple-products-cross-site-scripting-vulnerability_20210329
13 https://www.csa.gov.sg/singcert/alerts/al-2021-020
14 https://us-cert.cisa.gov/ncas/current-activity/2021/03/26/apple-releases-security-updates
15 https://www.govcert.gov.hk/en/alerts_detail.php?id=561
16 https://www.hkcert.org/security-bulletin/f5-big-ip-multiple-vulnerabilities_20210311
17 https://www.jpcert.or.jp/english/at/2021/at210014.html
18 https://www.cyber.gc.ca/en/alerts/vulnerabilities-impacting-f5-big-ip-and-big-iq

Industry Insight on Cyber Security Threat Trends

Password reuse was still a prevailing problem in 2020

SpyCloud reviewed identified data breaches and collected logs in 2020 and published its "2021 Annual Credential Exposure Report"[19] which presented the analysis results and the trends on data breaches. The major observations in the report were:

- **In 2020, 854 data breach sources were identified and studied, a 33% year-over-year growth, and exposed around 1.5 billion credentials online.** Account takeover fraud attacks grew nearly 300% over the year. Analysis on the exposed credentials revealed that 60% Internet users reused or recycled same passwords or with little modification for multiple online services: 97.4% of reused passwords were exactly the same; 1.8% of reused password by adding numbers to the end, and less than 1% reused password by capitalising the first letter. The rampant password reuse issue induced a high risk of account takeover.
- **Among 465 data breaches included ".gov" email addresses, around 270,000 plaintext credentials associated with government email addresses were uncovered. The password reuse rate for government email addresses with at least two passwords exposed was 87%.** "Abcd1234", "password" and "aaron431" were the top three passwords for the exposed government email addresses. Users should use strong and unique password for every account.
- **Passwords were found hashed by outdated algorithms.** For instance, 32% of hashed passwords used MD5 and 22% used SHA-1. Only 17% of hashes were salted with a set of random numbers. Organisations were recommended to follow up-to-date guidelines such as Digital Identity Guidelines from the National Institute of Standards and Technology (NIST) for the best practices of storing authentication secrets.
- **4.6 billion personally identifiable information (PII) assets were discovered from data breaches in 2020.** Username (~1.29 billion), phone (~1.28 billion) and name (~1.14 billion) were the top three exposed PII. There was an increasing trend for username and phone breaches since 2017.
- **Among the passwords exposed in 2020, weak passwords such as "123456789" and "password" accounted for more than 3.6 million and 1.2 million occurrences respectively.** The brand name of breached companies were commonly found in compromised passwords. COVID-19 pandemic related buzzwords such as corona, virus, pandemic, etc. were found in the disclosed passwords and "2020" was found in more than 1.6 million exposed passwords. Organisations were recommended to check passwords against password blacklists regularly to screen out commonly used, weak or compromised passwords.

Source: SpyCloud

[19] https://spycloud.com/resource/2021-annual-credential-exposure-report/

Industry Insight on Cyber Security Threat Trends

Distributed Denial of Service (DDoS) Attacks soared during COVID-19 pandemic

Link11 published the "Distributed Denial of Service Report for the Year 2020"[20], which highlighted analysis on key trends of DDoS attacks in 2020. The major findings were:

- **The number of DDoS attack surged with an average growth of 98% and a peak increase of 197% during February to September 2020 comparing to the same period in last year.** The increase was due to greater reliance on digital service and IT infrastructure during coronavirus pandemic, resulting in increase of attack surface of DDoS attack. Moreover, attackers could easily acquire the tools to conduct DDoS attack or paid for readily available DDoS-for-hire service to launch attacks. There were about 137,000 attacks per day in 2020, mainly targeted electronic commerce, financial services, hosting providers, healthcare and educational sectors.
- **Number of high-volume DDoS attacks grew by 25% in 2020.** 48 attacks with peak bandwidth of over 100 Gbps and 175 attacks with largest bandwidth ranged from 50 to 100 Gbps were detected, although over 90% of attacks had a bandwidth of less than 10 Gbps. A record-breaking attack volume of 2.3 Tbps was reported in February 2020.
- **The longest DDoS attack detected in 2020 lasted for nearly 4 days and there were several hundred attacks with duration longer than 5 hours.** More than half of DDoS attacks ended within 5 minutes and 4% of attacks continued for more than 1 hour.
- **59% of DDoS attacks were multi-vector.** Among those multi-vector DDoS attacks, more than half of them were with 3 vectors (57%). The largest number of vectors of detected DDoS attacks was 14. Attackers targeted multiple vulnerabilities in the infrastructure, application and protocol level at the same time employed flood attacks and reflection amplification techniques, such complex multiple vector techniques increased the rate of successful attack.
- **More than 60% of DDoS attacks with attack bandwidths larger than 100 Gbps used reflection amplification technique.** About 26% amplification attacks in 2020 was DVR DHCPDiscovery, a new vector which exploited a vulnerability of digital video recorders, with an amplification factor between 20 to 30. Other new reflection amplification vectors in 2020 included attacks abused Plex Media Servers with an amplification factor of 4, and attacks exploited Citrix Netscaler which had an amplification factor of 35.
- **Growth of DDoS extortion started in H2 2020.** Attackers threatened their targets of impending DDoS attacks unless the ransom demands were met. Targeted organisations included infrastructure operators, financial service providers, hosting providers and e-commerce companies.

Source: Link11

[20] https://www.link11.com/en/downloads/request/109-ddos-report-for-the-full-year-2020/

Industry Insight on Cyber Security Threat Trends

Double-extortion ransomware attacks became more prevalent in 2020

F-Secure studied the security incidents and cyber threat of the second half of 2020 and released the "Attack landscape update: Ransomware 2.0, automated recon, supply chain attacks, and other trending threats"[21]. The highlights from the report included:

- **Infostealer and Remote Access Trojan (RAT) were the top two malware threats in H2 2020, accounted for 33% and 32% of malware detection respectively.** Four out of the top five malware families belonged to these two malware threats, including two infostealers, Lokibot (1st rank) and Formbook (2nd rank), and two RATs, Remcos (3rd rank) and Agent Tesla (5th rank).
- **Ransomware evolved with new technique: extortion by threatening to leak stolen information.** 21 out of 55 new ransomware families / variants identified in 2020 were capable to steal data. Existing ransomware families (around 20% of ransomware families / variants discovered since 2018) also added data-stealing ability. Example of ransomware family with data exfiltration ability included Maze, DoppelPaymer, LockBit, Sodinokibi, etc. Threat actors also used other approaches to mount further pressure on the victims to meet the ransom demand, such as "print bombing" – printing a large amount of ransom note via the printers in the victim organisation or launching Distributed Denial of Service (DDoS) attacks to the victim. Furthermore, ransomware also improved the lateral infection speed for 'rapid' domain-wide ransomware deployment, and the detection evasion capability by deployment of virtual machines to execute ransomware payload to avoid detection.
- **Threat actors more targeted on utility software and application software in supply chain attacks, which accounted for 32% and 24% of supply chain attacks in last ten years, respectively.** 12% of supply chain attacks were achieved by modifying code repositories, which could affect organisations using open-source code.
- **Email spam was the most common method of distributing malware in cyber attacks, accounted for 52% of malware distribution in H2 2020.** Nearly one out of three spam email included malicious attachment. PDF was the attacker's favourite file type which accounted for 32% of malicious attachments. PDFs contained in-document phishing links or URLs to malicious web pages became increasingly common. Attackers also adopted archive files such as ZIP, RAR, GZ and IMG which accounted for about 20% of malicious attachments.
- **Among the 11,950 security issues discovered in organisational networks in 2H 2020, 61% of vulnerabilities found were disclosed at least five years ago.** Organisations should patch their systems timely and should not neglect their legacy systems and infrastructure.

Source: F-Secure

[21] https://blog-assets.f-secure.com/wp-content/uploads/2021/03/30120359/attack-landscape-update-h1-2021.pdf

Summary of Microsoft March 2021 Security Updates

13 Product Families with Patches

9 Critical

4 Important or below

Product Family	Impact[22]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB5000802, KB5000803, KB5000807, KB5000808, KB5000809, KB5000822
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5000802, KB5000803, KB5000808, KB5000822
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB5000802, KB5000803, KB5000807, KB5000808, KB5000809, KB5000822
Microsoft Internet Explorer 11	Remote Code Execution	Critical ★★★★	KB5000800, KB5000802, KB5000803, KB5000807, KB5000808, KB5000809, KB5000822, KB5000841, KB5000847, KB5000848
Microsoft Exchange Server	Remote Code Execution	Critical ★★★★	KB5000871, KB5000978
Microsoft Visual Studio	Remote Code Execution	Critical ★★★★	Microsoft Visual Studio 2017 version 15.9: Release Notes Microsoft Visual Studio 2019 version 16.4: Release Notes Microsoft Visual Studio 2019 version 16.7: Release Notes Microsoft Visual Studio 2019 version 16.8: Release Notes Microsoft Visual Studio 2019 version 16.9: Release Notes Microsoft Visual Studio Code ESLint extension: Release Notes

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

Product Family	Impact[22]	Severity	Associated KB and / or Support Webpages
			Visual Studio Remote - Containers Extension: Release Notes Visual Studio Code - Java Extension Pack: Release Notes Visual Studio Code: Release Notes Microsoft Quantum Development Kit for Visual Studio Code: Release Notes
Azure	Remote Code Execution	Critical ★★★★	Azure Kubernetes Service: Release Notes Azure Container Instance, Azure Service Fabric, Azure Spring Cloud: CVE-2021-27075 Azure Sphere: CVE-2021-27074, CVE-2021-27080
HEVC Video Extensions	Remote Code Execution	Critical ★★★★	CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5000840, KB5000847, KB5000848, KB5000853
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4493200, KB4493203, KB4493214, KB4493225, KB4493228, KB4504703 Microsoft Excel: KB4493233, KB4493239, KB4504707 Microsoft PowerPoint: KB4493224, KB4493227, KB4504702 Microsoft Office Online Server: KB4493229 Microsoft Office Web Apps: KB4493234 Microsoft Office 2019: Click to Run Microsoft 365 Apps for Enterprise: Click to Run Microsoft Business Productivity Servers 2010: KB3101541 Microsoft Visio: KB4484376, KB4486673, KB4493151
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	KB4493177, KB4493199, KB4493230, KB4493231, KB4493232, KB4493238

Product Family	Impact[22]	Severity	Associated KB and / or Support Webpages
Power BI Report Server	Information Disclosure	Important ★★★	KB5001284, KB5001285
Windows Admin Center	Security Feature Bypass	Important ★★★	Release Notes

Learn more:

High Threat Security Alert (A21-03-05): Multiple Vulnerabilities in Microsoft Products (March 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=560)

Sources:

- Microsoft March 2021 Security Updates (https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Mar)