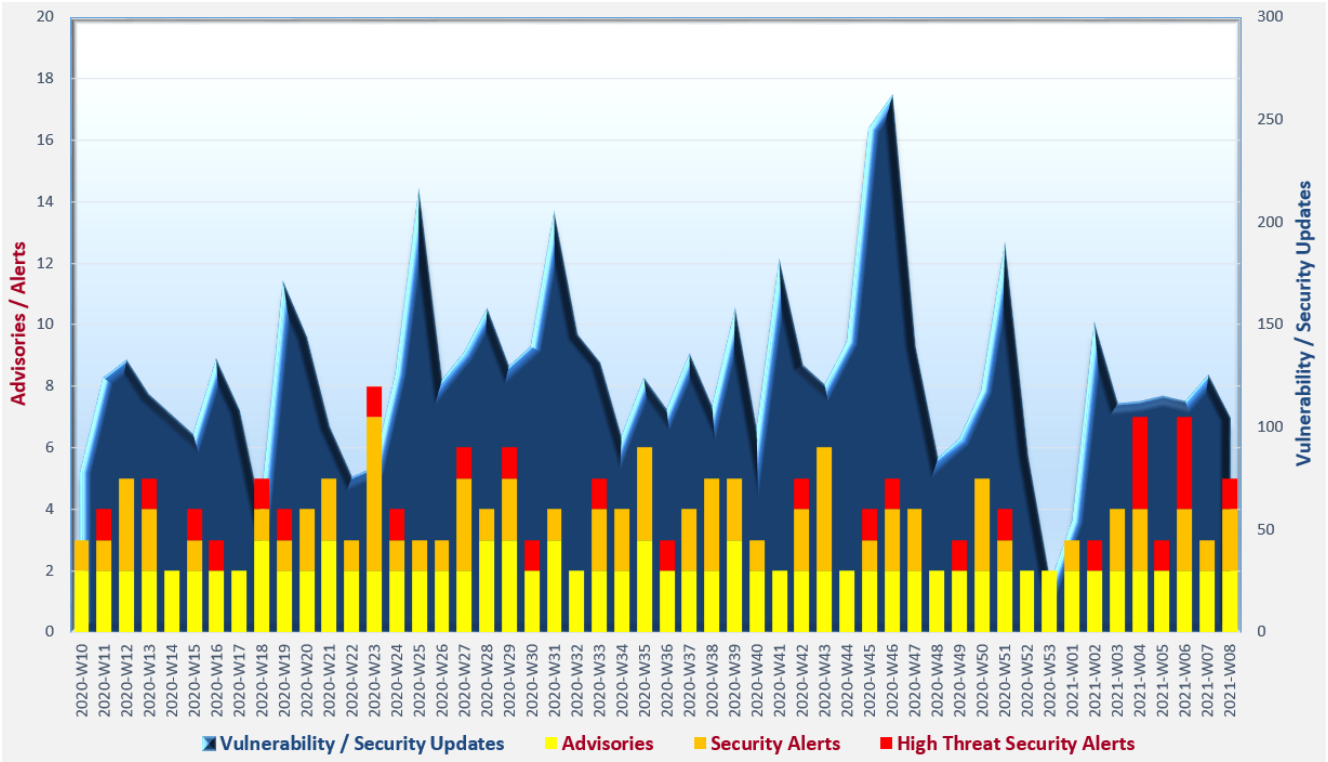
TLP:WHITE

Cyber Security Threat Trends 2021-M02

February 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:

- ✧ **Threat actors** actively and rapidly seize opportunities to exploit system vulnerabilities. System administrators should patch their systems timely to defend against potential exploitations.
- ✧ **Credential stuffing attacks** are widely used by attackers to compromise user accounts. Users should not use same password for different systems. Users should adopt strong passwords, change the passwords regularly, and enable multi-factor authentication wherever applicable.
- ✧ **Phishers and fraudsters** use common hot topics and shopping promotions as phishing themes to entice victims and use improved technologies to evade detection. Users should check the authenticity of electronic messages and websites, stay vigilant against suspicious links and attachments in electronic messages.

[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.

- SingCERT[2], Cybersecurity and Infrastructure Security Agency (CISA)[3], Australian Cyber Security Centre (ACSC)[4], National Cyber Security Centre (NCSC)[5] and cybersecurity authority of New Zealand released a joint advisory regarding four vulnerabilities (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104) in Accellion File Transfer Appliance which were exploited actively.

- GovCERT.HK[6], HKCERT[7], ACSC[8], CISA[9] and JPCERT[10] issued alerts regarding multiple vulnerabilities (CVE-2021-21972, CVE-2021-21973, CVE-2021-21974) in VMware products. PoC code for the remote code execution vulnerability (CVE-2021-21972) in VMware vCenter Server was publicly available. Active scanning for Internet-accessible vulnerable vCenter servers were observed.

- GovCERT.HK[11], HKCERT[12], JPCERT[13], CISA[14] and Canadian Centre for Cyber Security[15] issued alerts regarding multiple vulnerabilities in Adobe Reader/Acrobat. The arbitrary code execution vulnerability (CVE-2021-21017) was exploited in the wild.

- GovCERT.HK[16], HKCERT[17], CISA[18] and Canadian Centre for Cyber Security[19] issued alerts regarding a heap buffer overflow vulnerability in Google Chrome, which was actively exploited.

[2] https://www.csa.gov.sg/singcert/alerts/al-2021-009
[3] https://us-cert.cisa.gov/ncas/alerts/aa21-055a
[4] https://www.cyber.gov.au/acsc/view-all-content/alerts/potential-accellion-file-transfer-appliance-compromise
[5] https://www.ncsc.gov.uk/news/ncsc-advisory-on-accellion-file-transfer-appliance-customers
[6] https://www.govcert.gov.hk/en/alerts_detail.php?id=553
[7] https://www.hkcert.org/security-bulletin/vmware-products-multiple-vulnerabilities_20210225
[8] https://www.cyber.gov.au/acsc/view-all-content/alerts/vmware-vcenter-server-plugin-remote-code-execution-vulnerability-cve-2021-21972
[9] https://us-cert.cisa.gov/ncas/current-activity/2021/02/24/vmware-releases-multiple-security-updates
[10] https://www.jpcert.or.jp/english/at/2021/at210011.html
[11] https://www.govcert.gov.hk/en/alerts_detail.php?id=551
[12] https://www.hkcert.org/security-bulletin/adobe-monthly-security-update-feb-2021-_20210210
[13] https://www.jpcert.or.jp/english/at/2021/at210007.html
[14] https://us-cert.cisa.gov/ncas/current-activity/2021/02/09/adobe-releases-security-updates
[15] https://www.cyber.gc.ca/en/alerts/adobe-security-advisory-35
[16] https://www.govcert.gov.hk/en/alerts_detail.php?id=548
[17] https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerability_20210208
[18] https://us-cert.cisa.gov/ncas/current-activity/2021/02/05/google-releases-security-updates-chrome
[19] https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-45

CERT Advisories

- GovCERT.HK[20], HKCERT[21], JPCERT[22], CISA[23], Canadian Centre for Cyber Security[24] and SingCERT[25] issued alerts regarding multiple vulnerabilities in Microsoft products. The privilege escalation vulnerability (CVE-2021-1732) was actively exploited in the wild.

Second phase mitigation for Netlogon Remote Code Execution Vulnerability (CVE-2020-1472)

In September 2020, CERT bodies issued alerts regarding active exploitation against vulnerability in Microsoft Windows Netlogon Remote Protocol (CVE-2020-1472) that affected Domain Controllers. CISA[26] issued an advisory reminding system administrators the second phase mitigation to address this vulnerability. Beginning with the 9 February 2021 Security Update release, all supported Domain Controllers will be placed in enforcement mode. System administrators should refer to vendor's documentation, and install the latest security updates timely.

[20] https://www.govcert.gov.hk/en/alerts_detail.php?id=550
[21] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-feb-2021-_20210210
[22] https://www.jpcert.or.jp/english/at/2021/at210008.html
[23] https://us-cert.cisa.gov/ncas/current-activity/2021/02/09/microsoft-releases-february-2021-security-updates
[24] https://www.cyber.gc.ca/en/alerts/microsoft-security-advisory-february-2021-monthly-rollup
[25] https://www.csa.gov.sg/singcert/alerts/al-2021-008
[26] https://us-cert.cisa.gov/ncas/current-activity/2021/02/10/microsoft-launches-phase-2-mitigation-netlogon-remote-code

Industry Insight on Cyber Security Threat Trends

Significant increase in Adware, Bankbot, Potentially Unwanted Programs (PUPs) in Android, increase in Windows HackTool and Spyware despite decline in overall Windows malware detections in 2020

Malwarebytes issued the "2021 State of Malware Report"[27], which included analysis on key trends on malware detection and cyber threats in 2020. The major findings were:

- **Attackers customised their attack campaigns to take advantage of the COVID-19 pandemic in 2020.** Phishing messages on topics such as health advisories, donation requests, personal protective equipment, virtual conferencing applications, etc. were widely used. A notable increase in brute force attacks targeted Remote Desktop Protocol (RDP) was observed. Moreover, some threat actors adopted a malware distribution as a service approach to achieve higher specialisation and efficiency.

- **The total number of Windows malware detections, as compared to 2019, decreased by 12% in 2020.** Business detections and consumer detections decreased by 24% and 11% respectively. In spite of the overall decrease, malware categories HackTool, Rogue (e.g. tech support scammer materials) and Spyware recorded an increase in both business and consumer detections. HackTool.KMS was the top Windows malware detection in 2020, recorded an increase of over 20 times from 2019, probably due to an increase of cracked Microsoft applications users during the Work From Home era. Ransomware attacks have evolved in detection evasion and encryption speed. Attackers adopted a new tactic called "double extortion" by stealing data from victims in addition to encrypting their data, and threatened the victims the stolen data would be exposed unless ransom demands were met.

- **In 2020, the total number of Mac malware detections decreased by 38% compared to 2019.** Consumer detections aligned with the overall trend and shrank by 40%, while the number of business detections increased by 31%. PUPs and Adware accounted for over 98% of Mac malware detection. Nevertheless, the proportion of these two categories were different in consumer, small size businesses and medium to large businesses. PUPs detection in small size businesses was 94.3% but only 37.2% in medium to large businesses. On the contrary, Adware detection was the highest in medium to large businesses (60%) but with only 4.9% detections in small size businesses.

- **Android malware became increasingly prevalent in 2020.** Number of detection of HiddenAds, a malware which aggressively pushed advertisements to victim devices, recorded over 700,000 detections in 2020, an increase by over 420,000 from 2019. On the other hand, the detection of a banking Trojan, Bankbot, surged from around 5,000 detections in 2019 to over 198,000 in 2020.

Source: Malwarebytes

[27] https://resources.malwarebytes.com/resource/2021-state-of-malware-report/

Industry Insight on Cyber Security Threat Trends

Credential stuffing attacks soared in Q4 2020

Arkose Labs published the "2021 Q1 Fraud and Abuse Report"[28], which included the analysis result on fraud trends in 2020. The key findings were:

- **Credential stuffing attacks in Q4 2020 increased by nearly 90% compared to Q1 2020, and more than doubled compared to Q3.** The increase of newly created digital accounts as people turned to digital channels during COVID-19 pandemic-related lockdowns fuelled the increase of credential stuffing attacks.
- **Fraud attack volumes increased since Black Friday 2020 and remained at high level till the end of 2020. The attack rate mostly remained above 25% in Q4 2020.** Black Friday, and other holiday shopping periods, were commonly targeted by fraudsters. In 2020, industries not typically associated with Black Friday-related fraud attacks such as social media platforms, online dating companies and financial services also recorded significant increases in fraud attacks. The increase could be due to attackers used social media as disinformation distribution channels or they tried to blend their attacks in the increased traffic volumes of payment platforms during the affected period.
- **Number of bot attacks and human-driven attacks detected in 2020 were 3.9 billion and 0.47 billion respectively.** Although bots remained the preferred method, there was a rise in hybrid attacks. Bots were used to launch brute force attacks on large scale, supplemented by human-driven attacks when more nuance was required. Attacks targeted online dating apps had the highest rate of human-driven attacks (22.1%), followed by ecommerce with 20% of the attacks were human-driven attacks.
- **Taking into account on the attack volume in Q4 2020 only, nearly 50% of fraud attacks were originated from Asia, with Europe (24%) and South America (13.6%) ranked the second and third originating region respectively.** On the other hand, Europe accounted for 37% of fraud attacks in 2020 and was the top region overall, followed by Asia (31%) and North America (20%). The increased number of attack from Europe was due to financial distress related to COVID-19 and pandemic-related lockdowns.
- **Proportion of mobile attacks recorded a slight increase from 15% in Q3 2020 to 16.2% in Q4 2020 and varied for different industries.** For instance, 28% of attacks to the media industry were mobile attacks, while the proportion of mobile attacks in finance industry was only 0.7%.

Source: Arkose Labs

[28] https://www.arkoselabs.com/resource/2021-q1-fraud-and-abuse-report/

Industry Insight on Cyber Security Threat Trends

Upward trends in phishing attacks in Q4 2020

Anti-Phishing Working Group (APWG) published the "Phishing Activity Trends Report, 4th Quarter 2020"[29] on their analysis and observations of phishing attacks and other identity theft techniques in the fourth quarter of 2020. The major observations in the report were:

- **Increase in unique phishing sites and unique phishing email subjects started since March 2020.** The number of unique phishing sites was less than 100,000 in January 2020 and nearly doubled to 199,120 in December 2020. The number of unique phishing email subjects was slightly over 50,000 in January 2020 and skyrocketed to 133,038 in December 2020.

- **The top three targeted industries by phishing attack in Q4 2020 were financial institutions, Software as a Service (SaaS) or webmail-based organisations, and payment providers which accounted for 22.5%, 22.2% and 15.2% of phishing attack, respectively.** Social media services, as well as cryptocurrency exchanges and related sites, were targeted more frequently in Q4 2020.

- **Average amount requested in wire transfer business email compromise (BEC) attacks increased from $48,000 in Q3 2020 to $75,000 in Q4 2020.** BEC cases in which scammers requested direct bank transfers grew from 14% in Q3 2020 to 22% in Q4 2020. Payroll diversion request BEC cases increased from 6% in Q3 2020 to 13% in Q4 2020. Nevertheless, BEC cases in which scammers requested funds in the form of gift cards dropped from 71% in Q3 2020 to 60% in Q4 2020. There was an increase in BEC cases requested American Express, Visa and OneVanilla gift cards in Q4 2020, probably due to attackers shifted the way to redeem their profit. Scammers increasingly used free webmail to conduct BEC attacks, growing from 61% in Q1 2020 to 75% in Q4 2020. In addition, over 50% of malicious domains used in BEC attacks were registered under Namecheap (32%) and Public Domain Registry (23%).

- **In Q4 2020, majority of phishing domains were newly registered by threat actors instead of from compromised infrastructure.** ".com" was the most commonly used second-level domain for phishing domains.

- **The number of phishing sites using SSL/TLS incremented 3% in every quarter in 2020, and grew up to 84% in Q4 2020.** Domain Valid (DV) certificates contributed to 89% of certificates used in phishing sites in Q4 2020.

Source: APWG

[29] https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

Summary of Microsoft February 2021 Security Updates

16 Product Families with Patches

4 Critical

12 Important or below

Product Family	Impact[30]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4570333, KB4571756, KB4574727, KB4577015, KB4577032, KB4577049, KB4601315, KB4601318, KB4601319, KB4601331, KB4601345, KB4601354
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4570333, KB4571756, KB4574727, KB4577015, KB4601315, KB4601318, KB4601319, KB4601345
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4577038, KB4577048, KB4577066, KB4577071, KB4601348, KB4601349, KB4601357, KB4601384
.NET 5.0, .NET Core 2.1, .NET Core 3.1	Remote Code Execution	Critical ★★★★	Release Notes, Release Notes
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	KB4493194, KB4493195, KB4493210, KB4493223
Microsoft Visual Studio	Remote Code Execution	Important ★★★	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 Visual Studio Code and npm-script Extension: Release Notes
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4493192, Click to Run Microsoft Excel: KB4493196, KB4493211, KB4493222

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

Product Family	Impact[30]	Severity	Associated KB and / or Support Webpages
			Microsoft Office Web Apps Server: KB4493204 Microsoft 365 Apps for Enterprise: Click to Run
Microsoft Dynamics	Information Disclosure	Important ★★★	KB4595460, KB4595463, KB4602915
Microsoft Teams for iOS	Information Disclosure	Important ★★★	Release Notes
Microsoft Edge	Security Feature Bypass	Important ★★★	Release Notes
Microsoft Exchange Server	Spoofing	Important ★★★	KB4571787, KB4571788, KB4602269
Microsoft .NET Framework	Denial of Service	Important ★★★	KB4601050, KB4601051, KB4601054, KB4601056, KB4601318, KB4601354, KB4601887, KB4602958, KB4602959, KB4602960, KB4602961, KB4603002, KB4603003, KB4603004, KB4603005
Skype and Microsoft Lync	Denial of Service	Important ★★★	KB5000675, KB5000688
Azure	Elevation of Privilege	Important ★★★	Azure IOT CLI Extension: Pull Request
PsExec	Elevation of Privilege	Important ★★★	Release Notes
System Center	Elevation of Privilege	Important ★★★	KB4601269

Learn more:

High Threat Security Alert (A21-02-05): Multiple Vulnerabilities in Microsoft Products (February 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=550)

Sources:

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