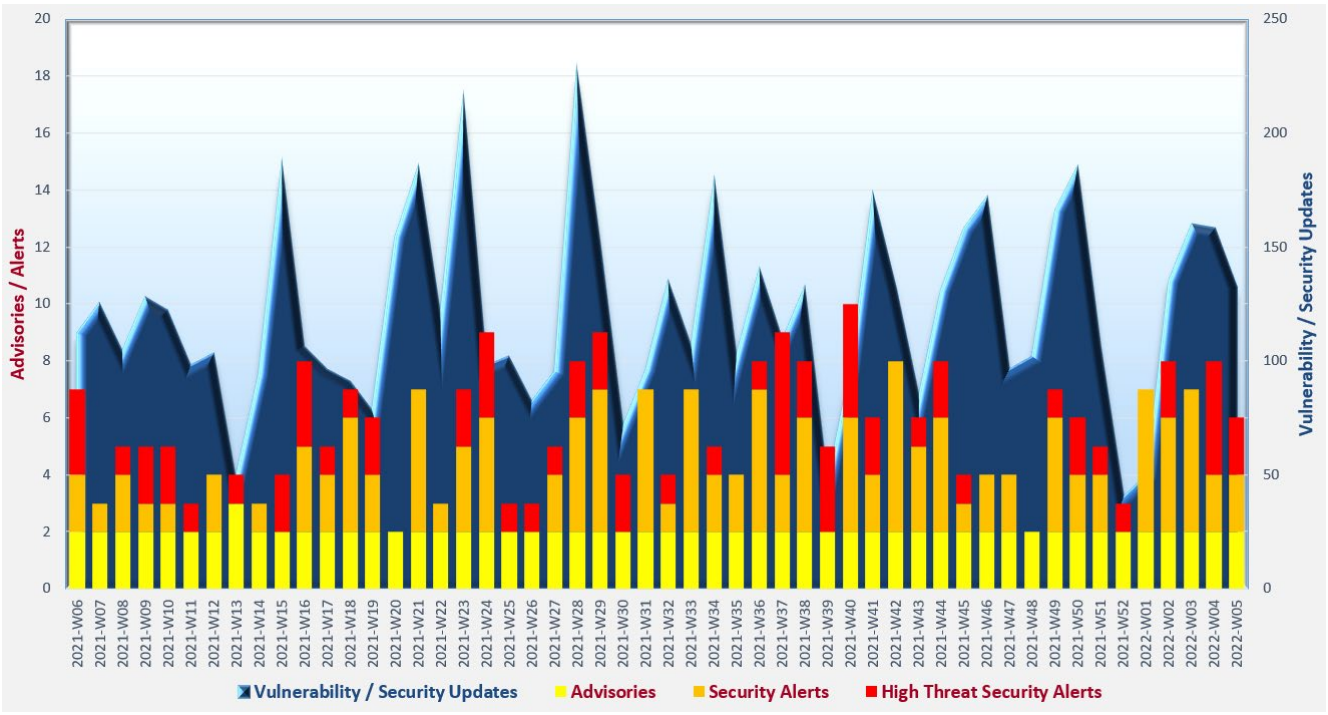
TLP:WHITE

Cyber Security Threat Trends 2022-M01

January 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:

Vulnerabilities and misconfigured cloud services are always the targets for the attackers. **Ransomware attacks** continue posing significant threats to organisations. Organisations should securely configure their cloud instances, apply patches on a timely basis, perform off-site backups regularly and encrypt their data properly.

[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], JPCERT[5], SingCERT[6], MyCERT[7] and Cybersecurity and Infrastructure Security Agency (CISA)[8] issued alerts and advisories regarding multiple vulnerabilities in Microsoft Products. A security feature bypass vulnerability in Microsoft Windows and Server (CVE-2013-3900) was being actively exploited. PoC code for exploitation of a remote code execution vulnerability in Microsoft Windows (CVE-2022-21907) was publicly available.

- GovCERT.HK[9] and HKCERT[10] issued alerts regarding vulnerability in Linux Operating Systems. PoC code for vulnerability (CVE-2021-4034) was publicly available. The vulnerability was being exploited in the wild.

- GovCERT.HK[11], HKCERT[12], CISA[13] and Canadian Centre for Cyber Security[14] issued alerts regarding multiple vulnerabilities in various Apple devices. A memory corruption vulnerability (CVE-2022-22587) was being actively exploited.

Safety tips of using QR code

QR codes became more popular and widely used in various areas such as mobile payment, website redirection, etc. To enhance the security awareness, HKCERT[15,16] and Canadian Centre for Cyber Security[17] published articles on secure use of QR code, QR code risks and protection measures.

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=715
3 https://www.govcert.gov.hk/en/alerts_detail.php?id=725
4 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-january-2022
5 https://www.jpcert.or.jp/english/at/2022/at220002.html
6 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-002
7 https://www.mycert.org.my/portal/advisory?id=MA-826.012022
8 https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/microsoft-releases-january-2022-security-updates
9 https://www.govcert.gov.hk/en/alerts_detail.php?id=728
10 https://www.hkcert.org/security-bulletin/linux-policy-kit-elevation-of-privilege-vulnerability_20220127
11 https://www.govcert.gov.hk/en/alerts_detail.php?id=729
12 https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20220127
13 https://www.cisa.gov/uscert/ncas/current-activity/2022/01/27/apple-releases-security-updates-multiple-products
14 https://www.cyber.gc.ca/en/alerts/apple-security-advisory-av22-041
15 https://www.hkcert.org/blog/introduction-of-qr-code-attacks-and-countermeasures
16 https://www.hkcert.org/blog/secure-use-of-qr-code
17 https://www.cyber.gc.ca/en/guidance/security-considerations-qr-codes-itsap00141

CERT Advisories

Security tips on "Work from Home"

During the pandemic, many organisations have work from home (WFH) arrangement with their staff to reduce the risk of spreading COVID-19 in the community. HKCERT[18] published an article that provided security tips on WFH for organisations and their employees.

Securing Signal and WhatsApp

Australian Cyber Security Centre (ACSC)[19,20] published guidance on how to secure Signal and WhatsApp with the use of multi-factor authentication (MFA), safety numbers and security codes. In addition, security guidance on Apple ID and other social media platforms were provided.

Actions to ensure the cyber hygiene controls

National Cyber Security Centre (NCSC)[21] released a guidance that help organisations to improve their cyber security. This guidance provided actionable security measures to organisations in reducing their vulnerability and impact on cyber attacks.

[18] https://www.hkcert.org/blog/business-as-usual-under-covid-19-with-sound-work-from-home-cyber-security
[19] https://www.cyber.gov.au/acsc/view-all-content/guidance/securing-signal
[20] https://www.cyber.gov.au/acsc/view-all-content/guidance/securing-whatsapp
[21] https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

Industry Insight on Cyber Security Threat Trends

Network attack volume dropped but endpoint malware detections increased in Q3 2021

WatchGuard collected the threat intelligence from perimeter appliances and endpoints and provided analysis on attack trends in its "Internet Security Report – Q3 2021"[22]. The highlights from the report included:

- **The region with most malware detection was Europe, the Middle East, and Africa (EMEA), followed by North, Central and South America (Americas) and Asia-Pacific (APAC).** These three regions accounted for 48.46%, 28.59% and 22.95% of malware detection respectively. The top 5 most-widespread malware were two Microsoft Office Equation Editor exploits on CVE-2018-0802 and CVE-2017-11882, Trojan.Cryxos, Zum.Androm and RTF-ObfsObjDat. Hong Kong was one of the top 3 locations with highest Zum.Androm detections and accounted for 15.96% of Zum.Androm detection. 69.8% of malware was transmitted over encrypted connections, in which 47% was zero-day malware, increased from 31.6% in Q2 2021.

- **Network attack volume dropped from almost 5.2 million in Q2 2021 to around 4.1 million in Q3 2021, which was slightly below Q1 2021 volume (around 4.2 million).** Most network attacks targeted the Americas (64.6%) in Q3, compared to APAC (19.9%) and EMEA (15.5%). Among the 4.1 million network attacks in Q3 2021, 81% were attributed to the top 10 signatures. The top signature was a web SQL injection attack which stayed at the leading position since Q2 2019. One new signature, "WEB Remote File Inclusion /etc/passwd", which attempted to access system password files and targeted older versions of Microsoft Internet Information Services (IIS) web servers, joined top 10 signatures in Q3 2021. 5.6 million visits to malicious domains were detected in Q3 2021, a 23% decrease from 7.3 million detections in Q2 2021.

- **Attackers trended to use scripts like PowerShell and JavaScript to start their malware attacks.** The volume of malware at endpoints that triggered from scripts in the first three quarters of 2021 was 10% more than the total of 2020. In terms of ransomware attacks, attack volume of the first three quarters in 2021 already reached 105% of volume of 2020.

Source: WatchGuard

[22] https://www.watchguard.com/wgrd-resource-center/security-report-q3-2021

Industry Insight on Cyber Security Threat Trends

More malware and data breaches linked to cloud storage

Netskope issued the "Cloud and Threat Report - January 2022"[23], which summarised their findings on trends in cloud attack activities and cloud data risks in 2021. The key findings were:

- **Cloud Storage was the primary malware download source in 2021, accounted for over 66% of the downloaded malware.** The trend was expected to persist in 2022. In 2021, 69% of cloud malware downloaded were from cloud storage applications, followed by collaboration applications (9%) and development tools (7%). The number of applications with malware downloads in 2021 was 2.5 times of the number in 2020.

- **Malicious Office documents were commonly used to deliver malware in 2021.** 37% of malware downloads were from Office documents in Q4 2021, up from 19% in Q1 2020. The Emotet malspam campaign in Q2 2020 contributed to a burst in abuse of Office documents (46%). Another surge was observed in the first half of 2021, with over 42% of malware downloads were from Office documents. The trend of more than one-third of malware downloads distributed by Office documents was expected to continue in 2022.

- **Attackers constantly attempted to use common passwords and compromised credentials to access sensitive information stored in cloud applications.** Over 50% of managed cloud applications instances experienced different kinds of credential attack. There were notable variations in attacking IP addresses in 2021, with only 2% of login attempts in 2021 came from IP addresses that also launched credential attacks in 2020.

- **Organisations should adopt multi-layered protection for all cloud and web traffic.** Multi-factor authentication and data protection solution with behavioural analysis should be used wherever applicable.

Source: Netskope

[23] https://resources.netskope.com/cloud-reports/cloud-and-threat-report-january-2022

Industry Insight on Cyber Security Threat Trends

More vulnerabilities and data breaches were reported in 2021

Tenable issued the "Tenable's 2021 Threat Landscape Retrospective"[24], which included analysis on more than 1,800 data breaches publicly disclosed from November 2020 to October 2021. The key findings were:

- **Number of data breaches reported in 2021 were 2.5 times of 2020**. From analysing the data breaches reported, in excess of 40 billion records were disclosed, above 260 terabytes of data were compromised, summing up to greater than 1.8 billion files, documents or email exposed. Over 24% of analysed data breaches were from the healthcare industry.
- **A total of 21,957 Common Vulnerabilities and Exposures (CVEs) were reported in 2021, 19.6% more than 2020.** 105 zero-day vulnerabilities were discovered in 2021, in which 30.5% were relevant to browser applications and 25.7% were about operating systems. 83% of tracked zero-day vulnerabilities were actively exploited, affected a wide range of products included Microsoft Exchange Server, Windows Print Spooler, Apache Log4j, various Virtual Private Network (VPN) solutions, web browsers, operating systems, web servers, etc.
- **Misconfigured cloud instances and Active Directory (AD) were targeted by attackers and posed high risks of data breach.** In addition, attackers targeted supply chain of various products, as well as open source libraries and repositories for distribution of malware including ransomware, backdoors, cryptominers, etc.
- **Ransomware attacks increased and became more sophisticated in 2021.** Ransomware-as-a-service (RaaS) model was increasingly adopted to launch attacks. Around 38% of analysed data breaches were caused by ransomware attacks, a 3% increase from 2020.
- Organisations should maintain perimeter security, ensure proper configurations, apply patches on a timely basis, conduct off-site / off-network data and system backups on a regular basis and plan for disaster recovery approaches.

Source: Tenable

[24] https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective

Highlight of Microsoft January 2022 Security Updates

Product Family	Impact[25]	Severity	Associated KB and / or Support Webpages
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5009543, KB5009545, KB5009546, KB5009557, KB5009566, KB5009585
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5009543, KB5009546, KB5009555, KB5009557
Windows 8.1 and Windows Server 2012, 2012 R2	Elevation of Privilege	Critical ★★★★	KB5009586, KB5009595, KB5009619, KB5009624
Microsoft Office-related software	Remote Code Execution	Critical ★★★★	KB4462205, KB5002052, KB5002057, KB5002060, KB5002064, KB5002107, KB5002114, KB5002115, KB5002116, KB5002119, KB5002122, KB5002124, KB5002128
Microsoft Exchange Server	Remote Code Execution	Critical ★★★★	KB5008631

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-Jan.

Learn more:

High Threat Security Alert (A22-01-07): Multiple Vulnerabilities in Microsoft Products (January 2022) (https://www.govcert.gov.hk/en/alerts_detail.php?id=715)

Data analytics powered by CRisP in collaboration with GovCERT.HK

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