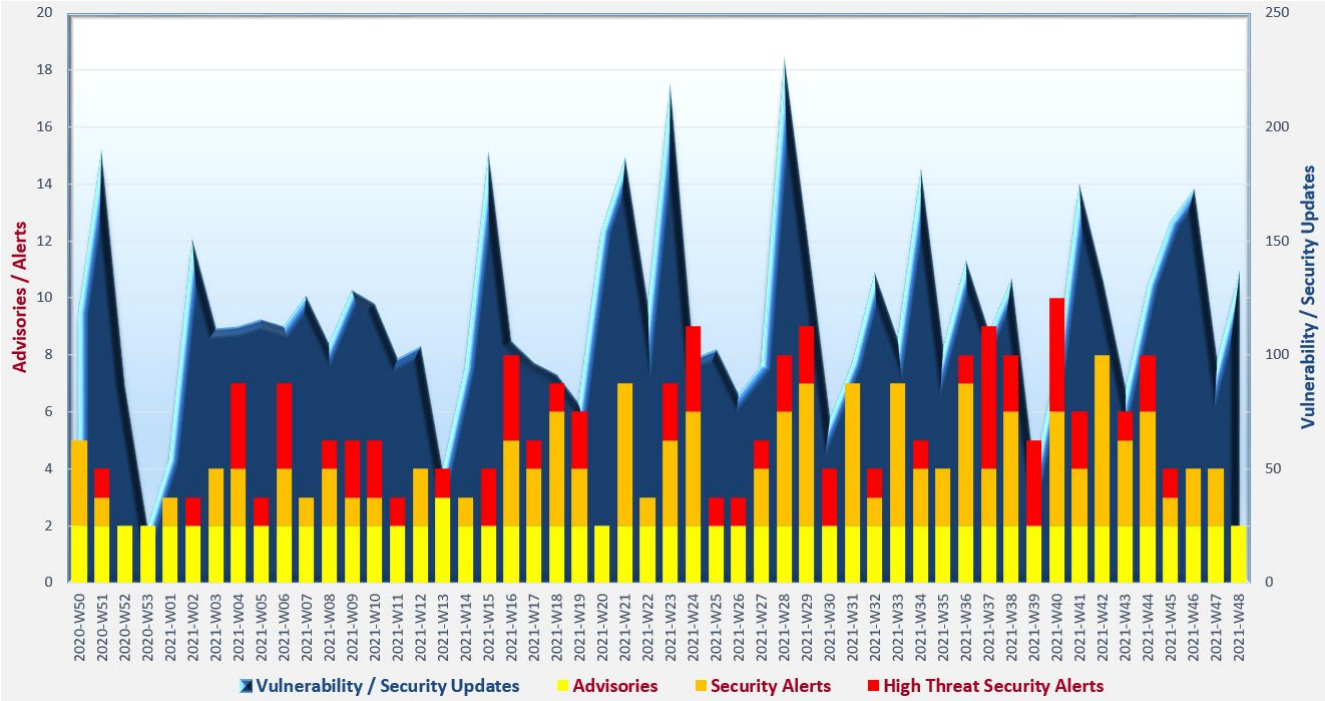
TLP:WHITE

Cyber Security Threat Trends 2021-M11

November 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:

Cyber security threats, attack tactics and malware evasion capabilities continue evolving. **Ransomware attacks** remain perilous threat to organisations and individuals. Organisations should continuously measure, monitor and improve their security protection tools and strategy to protect against the ever-changing 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], Australian Cyber Security Centre (ACSC)[5], Canadian Centre for Cyber Security[6] and CERT NZ[7] issued alerts regarding multiple vulnerabilities in Microsoft products. A remote code execution vulnerability in Microsoft Exchange Server (CVE-2021-42321) and security feature bypass vulnerability in Microsoft Excel (CVE-2021-42292) were being actively exploited. PoC codes for exploitation of vulnerabilities in Microsoft Windows' Kerberos protocols (CVE-2021-42282, CVE-2021-42278, CVE-2021-42291) and a Windows Installer elevation of privilege vulnerability (CVE-2021-41379) were publicly available.

- GovCERT.HK[8], HKCERT[9] and Canadian Centre for Cyber Security[10] issued alerts regarding multiple vulnerabilities in Microsoft Edge (Chromium-based). Vulnerabilities (CVE-2021-38000 and CVE-2021-38003) were being actively exploited.

- GovCERT.HK[11] and HKCERT[12] issued alerts regarding multiple vulnerabilities in GitLab. Vulnerability (CVE-2021-22205) was being exploited in the wild.

Enhance the security of mobile devices

Cybersecurity and Infrastructure Security Agency (CISA)[13] has released Capacity Enhancement Guides (CEGs), which provide actionable measures for users to improve cyber security of their mobile devices, and assist organisations to mitigate vulnerabilities of managed mobile devices and improve organisations' protection. Topics such as strong authentication, app security, network protection, etc. are covered in the CEGs.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=690
[3] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-november-2021
[4] https://www.jpcert.or.jp/english/at/2021/at210048.html
[5] https://www.cyber.gov.au/acsc/view-all-content/alerts/critical-vulnerability-present-certain-versions-microsoft-excel
[6] https://www.cyber.gc.ca/en/alerts/microsoft-security-advisory-november-2021-monthly-rollup
[7] https://www.cert.govt.nz/it-specialists/advisories/critical-vulnerability-in-windows-kerberos-protocol/
[8] https://www.govcert.gov.hk/en/alerts_detail.php?id=684
[9] https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20211103
[10] https://www.cyber.gc.ca/en/alerts/microsoft-edge-chromium-based-security-advisory-6
[11] https://www.govcert.gov.hk/en/alerts_detail.php?id=687
[12] https://www.hkcert.org/security-bulletin/gitlab-multiple-vulnerabilities_20210415
[13] https://us-cert.cisa.gov/ncas/current-activity/2021/11/24/cisa-releases-capacity-enhancement-guides-enhance-mobile-device

CERT Advisories

Beware of phishing scams

Phishing is a prevalent cyber attack that trick victims to visit malicious websites, download malware, disclose sensitive information, etc. JPCERT[14] issued an alert regarding recent growth of phishing scam aiming at stealing account information of webmail services. The alert explained the attack methods and impacts, and provided preventive and responsive measures on phishing attacks.

[14] https://www.jpcert.or.jp/english/at/2021/at210049.html

Industry Insight on Cyber Security Threat Trends

Near 80% of surveyed organisations could not effectively stop cyber attacks and identify, remediate and reduce the impact of security breaches

Accenture published the report "State of Cybersecurity Resilience 2021"[15] based on the results of a survey conducted in March to April 2021 with over 4,700 respondents from 18 economies and 23 industries in America, Europe and Asia Pacific. The key findings were:

- **2,761 out of 3,455 surveyed organisations (around 80%) were found weak in cybersecurity resilience.** These organisations encountered higher percentage of attacks that resulted in security breach (over 43%), could only found 15% or less security breaches within 1 day, only 30% of breaches could be fixed within 15 days, and over 75% of breaches caused impact.
- **Only 5% of 3,455 surveyed organisations were ranked as "Cyber Champions" which had strong cybersecurity resilience and aligned with business strategy of the organisations closely.** These organisations had a lower percentage of attacks that resulted in security breach (17%), could locate 55% of security breaches within 1 day and fix all breaches within 15 days, and 72% of breaches with no impact.
- **The average number of attacks (included unauthorised access to data, applications, services, networks or devices) per organisation was 270 in 2021, an increase of 31% compared to 206 in 2020.** Successful breaches through supply chain attacks increased from 44% in 2020 to 61% in 2021.
- **82% of respondents increased IT security budgets in last year.** 57% of respondents had an increase of 1-9% in IT security spending. IT security budgets accounted for 15% of total IT expenditure in 2021.
- **32% of respondents did not consider cloud security when they shifted their workloads to the cloud.** Cloud security should not be overlooked when organisations adopted cloud services. In addition, organisations should continuously measure, monitor and improve the maturity of their cybersecurity programs and balance the security and business aspects.

Source: Accenture

[15] https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

Number of ransomware continued growing steadily in Q3 2021

Ivanti issued the "Q3 2021 Ransomware Index Spotlight Report"[16], which summarised their findings on ransomware attack in Q3 2021. The key findings were:

- **12 vulnerabilities were newly found related to 7 ransomware strains in Q3 2021.** Five of these vulnerabilities were remote code execution (RCE) and four of them were related to exploitation on web applications. Ransomware strains of concern included Conti, LockFile, REvil/Sodinokibi, etc.

- **Attackers continued to exploit zero-day vulnerabilities.** CVE-2021-30116 was a zero-day vulnerability in the Kaseya Unitrends Service, which was exploited by the REvil group before Kaseya recognised it and published it on National Vulnerability Database (NVD). Ransomware groups also actively targeted some dangerous vulnerabilities such as PetitPotam (CVE-2021-36942), ProxyShell (CVE-2021-31207, CVE-2021-34473 and CVE-2021-34523) and PrintNightmare (CVE-2021-1675 and CVE-2021-34527).

- **Two over 10 years old vulnerabilities (CVE-2009-3960 and CVE-2010-2861) were found newly associated with Cring ransomware family in Q3 2021.** This indicated that attackers continued to seize opportunity to infect systems running obsolete software. Organisations should patch their systems promptly and refrain from using outdated software which security patch was no longer available.

- **Six vulnerabilities with publicly available exploits were newly identified and used in ransomware attacks in Q3 2021. Five new ransomware families were newly identified in Q3 2021.** Ransomware groups kept on evolving their attack techniques, such as adopting dropper-as-a-service and trojan-as-a-service models.

Source: Ivanti

[16] https://www.ivanti.com/lp/security/reports/2021-q3-ransomware-index-spotlight-report

Industry Insight on Cyber Security Threat Trends

Ransomware attack trends are expected to continue in 2022

Sophos released the "Sophos 2022 Threat Report"[17] which summarised trends on different types of threat in 2020-2021 and predictions on threat trends for 2022. The key findings were:

- **Ransomware-as-a-service (RaaS) attack model became increasingly popular in 2020-2021.** Usage of RaaS model increased the difficulty in analysis of ransomware attacks and identification of the attackers. Among the investigated ransomware attacks, Conti was the largest ransomware family involved, contributed to 16% of the attack cases. The RaaS model was expected to be remained prevalent in 2022.

- **There was an increasing trend on usage of Cobalt Strike Beacon by attackers, and the upward trend was expected to continue in 2022.** Attackers abused the penetration testing tool Cobalt Strike and utilised the Beacons as backdoor to target systems. Other common attack tools detected in 2020-2021 included mimikatz and Metasploit.

- **The trend of using broad-based attacks to lure large number of potential victims but only infecting targets fulfilling predefined criteria emerged in 2021 and was expected to be more widespread in the coming years.** The infection criteria could be particular languages, regions, device types, operating systems, IP address ranges, etc. Attackers adopted this kind of tactics to evade from detection and hinder the progress of analysis and investigation of the malware.

- **Dropper was the most prevailing Android malware types detected in 2021.** Flubot, one of the prevalent Android banking Trojans, was anticipated to be the top mobile malware affecting devices with Android platform in 2022. Moreover, more fraudulent applications exploiting loopholes in apps distribution in the iOS platform were expected in 2022.

Source: Sophos

[17] https://www.sophos.com/en-us/labs/security-threat-report.aspx

Highlight of Microsoft November 2021 Security Updates

Product Family	Impact[18]	Severity	Associated KB
Windows 10 and 11	Remote Code Execution	Critical ★★★★	KB5007186, KB5007189, KB5007192, KB5007206, KB5007207, KB5007215
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5007186, KB5007192, KB5007205, KB5007206
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5007245, KB5007247, KB5007255, KB5007260
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4486670, KB5002032, KB5002035, KB5002038, KB5002053, KB5002056, KB5002065, KB5002072
Microsoft Exchange Server	Remote Code Execution	Important ★★★	KB5007409
Microsoft Edge (Chromium-based) in IE Mode	Spoofing	Important ★★★	KB5007186, KB5007189, KB5007206, KB5007215

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/2021-Nov.

Learn more:
High Threat Security Alert (A21-11-07): Multiple Vulnerabilities in Microsoft Products (November 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=690)

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