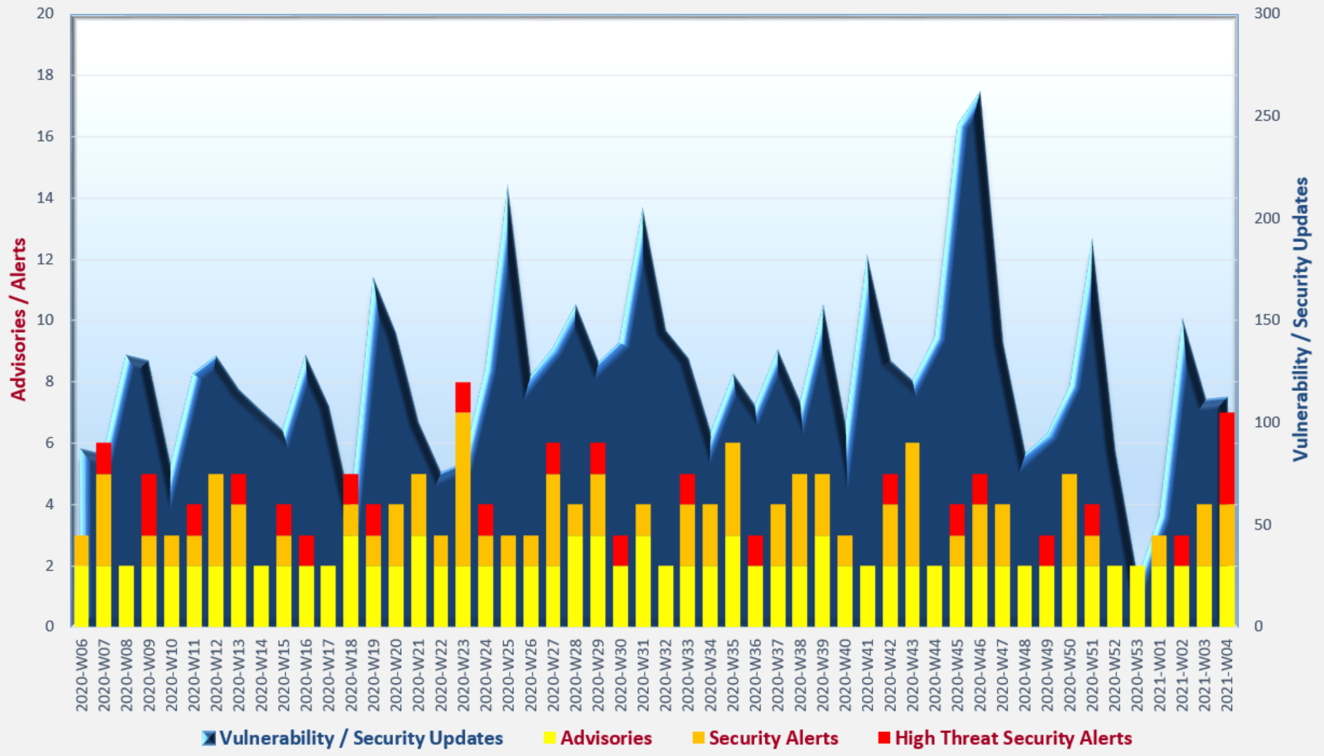
Cyber Security Threat Trends 2021-M01

January 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:

- **Vulnerabilities of virtual private network solution and remote desktop protocol** induce extreme risk of breach during pandemic. **New vulnerabilities on popular virtual meeting systems** are discovered and exploited. Organisations should prioritise patching based on associated risks such as risk severity, availability of Proof of Concept exploit and ease of exploitation.
- **Misconfigured databases or services** can lead to severe data breaches. Organisations should ensure their systems are properly configured with adoption of least privilege principle.
- **Web applications and application programming interfaces (APIs)** are targeted by threat actors to launch cyber attacks. Organisations should adopt secure by design approach, integrate security throughout application development lifecycle and adopt different protection measures such as web application firewall, API gateway, dedicated bot management tool, etc.

[1] https://www.first.org/tlp/

CERT Advisories

Apply patch to address vulnerabilities in Microsoft products

GovCERT.HK[2], HKCERT[3], SingCERT[4] and US-CERT[5] issued alerts reminding organisations and system administrators to patch Microsoft products. A remote code execution vulnerability (CVE-2021-1647) which could affect Windows Defender running on Windows and Windows Server platforms was under active exploitation. Moreover, Proof of Concept exploit for the privilege escalation vulnerability (CVE-2021-1648) in Windows splwow64 service was available. System administrators should patch the affected systems for risk mitigation as soon as possible.

Active exploitation against Apple iOS and iPadOS vulnerabilities

GovCERT.HK[6], CERT NZ[7] and Canadian Centre for Cyber Security[8] issued alerts reminding organisations and system administrators to patch Apple iOS and iPadOS for multiple vulnerabilities which could lead to arbitrary code execution or privilege escalation on affected device. Some of the vulnerabilities were under active exploitation. Users of the affected systems should promptly patch their devices.

Sudo vulnerability with Proof of Concept available

GovCERT.HK[9], HKCERT[10] and SingCERT[11] issued alerts reminding organisations and system administrators on a heap-based buffer overflow vulnerability in Sudo package with Proof of Concept available. By exploiting the vulnerability, attackers could run command with root privilege without authentication. Affected Sudo version included all legacy versions from 1.8.2 to 1.8.31p2 and all stable versions from 1.9.0 to 1.9.5p1. System administrators should patch the affected systems immediately.

[2] https://www.govcert.gov.hk/en/alerts_detail.php?id=538
[3] https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-jan-2021-_20210113
[4] https://www.csa.gov.sg/singcert/alerts/al-2021-001
[5] https://us-cert.cisa.gov/ncas/current-activity/2021/01/14/rce-vulnerability-affecting-microsoft-defender
[6] https://www.govcert.gov.hk/en/alerts_detail.php?id=543
[7] https://www.cert.govt.nz/it-specialists/advisories/vulnerability-in-apple-ios-reportedly-being-actively-exploited/
[8] https://www.cyber.gc.ca/en/alerts/apple-security-advisory-23
[9] https://www.govcert.gov.hk/en/alerts_detail.php?id=544
[10] https://www.hkcert.org/security-bulletin/linux-sudo-package-elevation-of-privilege-vulnerability_20210128
[11] https://www.csa.gov.sg/singcert/alerts/al-2021-007

CERT Advisories

🗎 Security tips for strengthening organisational cloud security

SingCERT[12] published an advisory on cloud services security and attack prevention. The advisory covered common causes of cloud attacks and recommendations on protective measures on various areas including account protection, network monitoring, log review, security policy enforcement, security awareness training, etc. Organisations were advised to implement appropriate security measures to reinforce the security of their cloud services.

🗎 Active exploitation against zero-day vulnerabilities in SonicWall SMA 100 Series products

GovCERT.HK[13], SingCERT[14] and CERT NZ[15] issued alerts advising organisations and system administrators to perform mitigation measures against actively exploited zero-day vulnerabilities in SonicWall SMA 100 Series products. Upon successful exploitation, a remote attacker could gain access to internal resources without authorisation. Updated firmware was released in early February 2021. System administrators should promptly apply the firmware update for risk mitigation.

[12] https://www.csa.gov.sg/singcert/advisories/ad-2021-001
[13] https://www.govcert.gov.hk/en/alerts_detail.php?id=545
[14] https://www.csa.gov.sg/singcert/alerts/al-2021-005
[15] https://www.cert.govt.nz/it-specialists/advisories/vulnerability-in-sonicwall-vpn-products-exploited/

Industry Insight on Cyber Security Threat Trends

Disclosed vulnerabilities nearly tripled in last five years

Tenable published its "2020 Threat Landscape Retrospective"[16] report which outlined notable vulnerabilities including zero-day, trends in ransomware and breaches, and the cybersecurity challenges related to the COVID-19 pandemic in 2020. The key findings were:

- **In 2020, 18,358 new Common Vulnerabilities and Exposures (CVEs) were reported, a 6% increase from 2019 and was the third consecutive year with yearly total more than 16,000.** When compared to 6,487 reported CVEs in 2015, there was a 183% increment in five years, an average annual growth rate of 36.6%. **29 zero-day vulnerabilities** were reported in 2020, with 35.7% related to web browsers, 28.6% related to Operating System and 14.3% related to font library.

- **Unpatched vulnerabilities in virtual private network (VPN) solutions posed the top cyber defence challenge facing by organisations.** Three of the top five vulnerabilities in 2020 were disclosed in 2018 and 2019. Unpatched vulnerabilities were targeted by threat actors. As the COVID-19 pandemic drove dramatic needs for remote workforce, securing VPN solutions became more critical and pressing to organisations. Obsolete solutions without security updates should be replaced or upgraded to supported versions.

- **Some organisations rushed for implementation of virtual meeting systems to meet business needs during the pandemic but neglected proper security protection.** Threat actors took advantage of the fragility and launched various attack campaigns targeted vulnerabilities of these systems.

- **Some critical vulnerabilities were not reported broadly by media headlines and might have been overlooked.** Analysis on high-profile vulnerabilities identified in 2020 revealed that factors such as availability of Proof of Concept exploits, exploitation complexity, business criticality of affected assets, etc. should also be assessed to determine the severity and priority of a vulnerability. Risk-based vulnerability management should be adopted.

- **More than 22 billion records were exposed from 730 breach events detected from January to October 2020.** Healthcare, Technology and Education were the top three affected industry sectors, accounted for 24.5%, 15.5% and 13% of analysed data breaches respectively. Ransomware caused over 35% of incidents and was the top cause of identified breaches. Other causes such as email compromises and misconfigured databases and servers contributed to 14.4% and 6% of breach events respectively. Attackers used new tactics to secure ransom demands by naming the victims in leak websites, inducing pressure to the victims to meet the ransom demands.

Source: Tenable

[16] https://www.tenable.com/cyber-exposure/2020-threat-landscape-retrospective

Industry Insight on Cyber Security Threat Trends

Number of records exposed in 2020 reached a record high since 2013

Risk Based Security published the "2020 Year End Data Breach QuickView Report"[17], which included the analysis result of 3,932 publicly reported breach events in 2020. The key findings were:

- **Publicly reported data breaches decreased by 48% to 3,932 events in 2020.** The report opined that the drop was due to factors such as less media coverage or slow reporting by the compromised organisations. However, the severity of breach events was found increasing gradually throughout 2020. 1,923 breaches (49%) did not disclose the number of records exposed. 676 breaches involved the usage of ransomware, nearly doubled the figures of 2019.

- **The total number of records exposed skyrocketed to over 37 billion, an increase by 141% compared to 2019 and record high since 2013.** Twenty-three breaches exposed more than 100 million records. 82% of the exposed records were contributed by the top 5 breaches, which were caused by misconfigured databases or services and with over one billion records were leaked in each breach event.

- **Hacking was the top breach type which caused 2,528 breach events in 2020.** On the other hand, 14 million records were breached due to improper disposal of computer equipment. Organisations and end users should ensure data were deleted from computer equipment securely and completely before disposal.

- **Name (46.5%) was the most exposed data type in reported breaches in 2020.** Breached email addresses and password dropped in Q4 2020 when compared with Q4 2019. Detail analysis on the breached data revealed that users were found using their professional or academic email address for public services registration and reused their passwords for different services, imposed further risk to spear phishing campaigns or other targeted attacks.

- **Health Care was the most compromised sector in 2020, followed by Information sector and Finance and Insurance sector.** Attackers leveraged the stress induced by COVID-19 to the Health Care sector and targeted hospitals, health care systems and pharmaceutical companies, making Health Care became the most breached sector.

Source: Risk Based Security

[17] https://pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report

Industry Insight on Cyber Security Threat Trends

Growing concern on protecting mobile applications and application programming interfaces (APIs) from cyber attacks

Radware surveyed more than 200 IT professionals from medium to large organisations in different industries and locations, and published the analysis on survey results in the "2020-2021 State of Web Application and API Protection Report"[18]. The highlights from the report included:

- **98% of respondents revealed that their applications and web servers encountered various attacks in 2020.** The top four attack vectors were Denial of Service (DoS) (89%), SQL or other injections (85%), application programming interface (API) manipulations (84%), and bot attacks (82%). About one-third of survey respondents expressed that their organisations encountered DoS attack targeted their web application weekly. HTTP flood (80%) and HTTPS flood (79%) were the most common type of DoS attacks that targeted application layer.

- **The top three types of API attack were DoS (87%), injections (80%) and access violations and brute force/credential stuffing (74%).** Web application firewall (WAF), API gateway and cloud services were the API protection technologies most commonly used by the survey respondents, accounted for 77%, 61% and 50% respectively. About 60% of organisations recognised the cyber risk associated with the increased use of APIs and would invest to improve API protection in 2021.

- **The top three types of bot attacks were DoS (86%), web scraping (84%), and account takeover (75%).** Only 39% of respondents were confident to address sophisticated bot attacks but 28% of respondents did not aware of any sophisticated bot attacks. 48% of organisations used WAF to distinguish real users and bots. Only 24% of organisations adopted dedicated anti-bot/anti-scraping solution.

- **63% of respondents considered security was fully integrated within the continuous delivery of web applications but only 36% had the same view for mobile applications development.** Moreover, 22% of respondents expressed that security was not integrated into their mobile applications development process.

- **More than 14% of respondent organisations expressed they were lack of visibility on the open source code used in their environment.** Nearly the same percentage of respondent organisations indicated they had no control over the third party services or apps processing their sensitive data.

Source: Radware

[18] https://www.radware.com/pleaseregister.aspx?returnurl=45ab42ce-03c0-443c-a44b-7c82b661858d

Summary of Microsoft January 2021 Security Updates

14
Product Families with Patches

6
Critical

8
Important or below

Product Family	Impact[19]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4598229, KB4598230, KB4598231, KB4598242, KB4598243, KB4598245
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4598229, KB4598230, KB4598242, KB4598243
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4598275, KB4598278, KB4598285, KB4598297
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4598229, KB4598230, KB4598231, KB4598242, KB4598243, KB4598245
Windows Defender, Microsoft System Center Endpoint Protection and Microsoft Security Essentials	Remote Code Execution	Critical ★★★★	CVE-2021-1647
HEVC Video Extensions	Remote Code Execution	Critical ★★★★	CVE-2021-1643, CVE-2021-1644
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4486755, KB4486759, KB4486762, KB4493142, KB4493143, KB4493168, KB4493181 Microsoft Excel: KB4486736, KB4493165, KB4493176, KB4493186 Microsoft Word: KB4486764, KB4493145, KB4493156 Microsoft Office Online Server: KB4493160

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

Product Family	Impact[19]	Severity	Associated KB and / or Support Webpages
			Microsoft Office Web Apps: KB4493171, KB4493183 Microsoft Office 2019: Click to Run Microsoft Office 2019 for Mac: Release Notes Microsoft 365 Apps for Enterprise: Click to Run
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	KB4486683, KB4486724, KB4493161, KB4493162, KB4493163, KB4493167, KB4493175, KB4493178, KB4493187
Microsoft Visual Studio	Remote Code Execution	Important ★★★	Microsoft Visual Studio 2015 Update 3: KB4584787 Microsoft Visual Studio 2017 version 15.9: Release Notes Microsoft Visual Studio 2019: version 16.0 - Release Notes version 16.4 - Release Notes version 16.7 - Release Notes version 16.8 - Release Notes
Microsoft SQL Server	Elevation of Privilege	Important ★★★	KB4583456, KB4583457, KB4583458, KB4583459, KB4583460, KB4583461, KB4583462, KB4583463, KB4583465
ASP.NET Core	Denial of Service	Important ★★★	Release Notes
Azure Kubernetes Service	Spoofing	Important ★★★	Release Notes
Bot Framework SDK	Information Disclosure	Important ★★★	Bot Framework SDK for Python: Security Update Bot Framework SDK for JavaScript: Security Update Bot Framework SDK for .NET Framework: Security Update
Microsoft Remote Desktop	Security Feature Bypass	Important ★★★	Microsoft Remote Desktop: Release Notes Remote Desktop client for Windows Desktop: Release Notes Microsoft Remote Desktop for Android: Release Notes

Learn more:
High Threat Security Alert (A21-01-02): Multiple Vulnerabilities in Microsoft Products (January 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=538)

Sources:

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