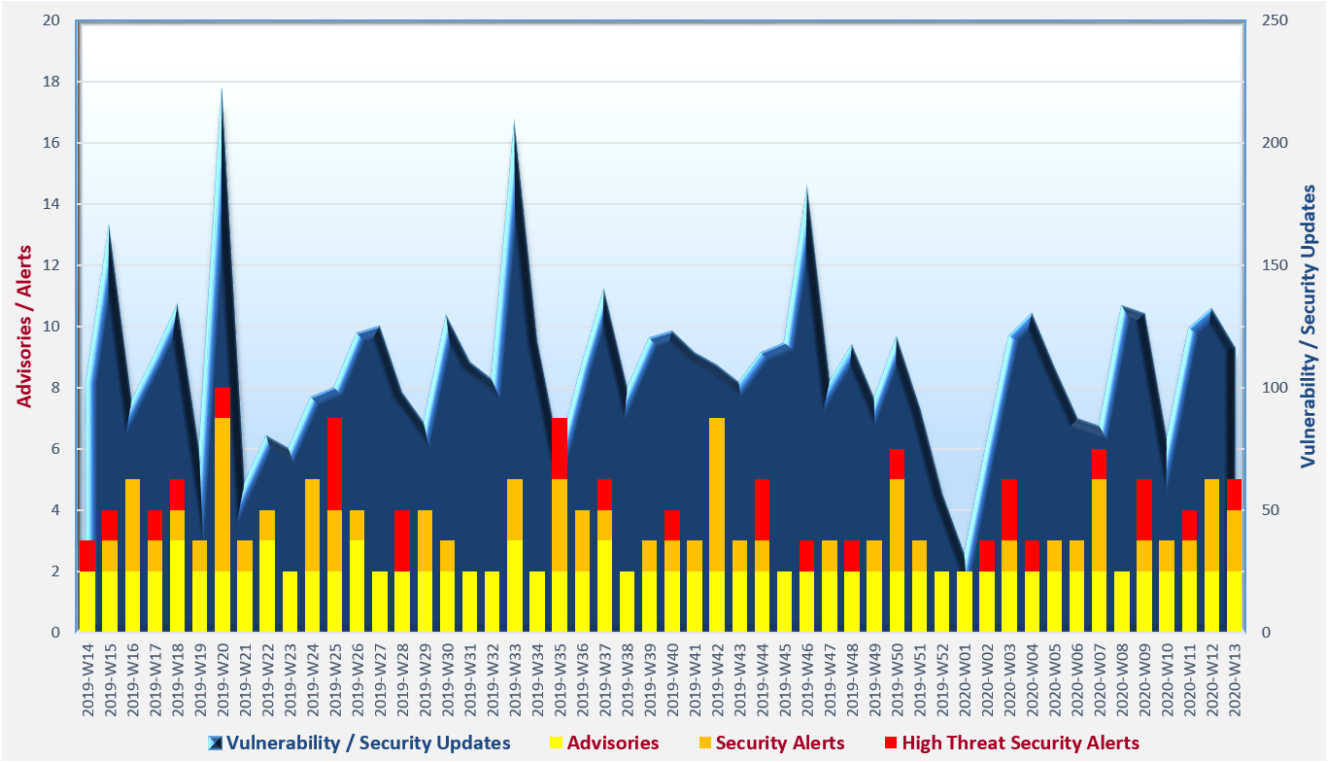
TLP:WHITE

# Cyber Security Threat Trends 2020-M03

March 2020

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:**

- ✧ **Hot topics, such as the recent Coronavirus pandemic,** are favourite lures used by culprits to launch scamming, phishing, smishing, pharming or similar attacks. Users should always remain vigilant when clicking links or opening attachments in electronic messages.
- ✧ **Use of unauthorised mobile apps** could lead to security breaches in organisations. Organisations should establish a policy to control the installation and use of mobile apps on corporate devices. A Mobile Device Management (MDM) system could be an effective solution to enforce the policy.
- ✧ **Malware** becomes increasingly evasive. Organisations could adopt and keep updating multi-layer defences at networks, servers and end-points to detect and stop the attacks.

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

## CERT Advisories

### Multiple Vulnerabilities in Microsoft Windows Adobe Type Manager Library

GovCERT.HK[2], HKCERT[3], JPCERT[4], MYCERT[5], CERT NZ[6], CISA[7], and Canadian Centre for Cyber Security[8] issued respective alert/advisory to remind organisations and computer users that multiple vulnerabilities in Microsoft Windows Adobe Type Manager Library were being exploited in the wild. These vulnerabilities affected not only all currently supported versions of Windows and Windows Servers, but also end-of-support Windows 7 and Windows Server 2008. If attackers exploited these vulnerabilities successfully, they could trigger remote code execution on the affected system. Patches for the affected products were not yet available as at end of March 2020. System administrators and users should refer to Microsoft's security advisory[9] and assess the impact of workarounds to mitigate the risks.

### Microsoft Exchange Server's flaw actively exploited

GovCERT.HK[10], CISA[11], CERT NZ[12] and Canadian Centre for Cyber Security[13] issued respective alert/advisory to remind organisations that an active exploitation against the vulnerability CVE-2020-0688 for remote code execution had been observed. This vulnerability was disclosed in February 2020 that affected Microsoft Exchange Server 2010 up to 2019. System administrators should apply the system patches immediately to mitigate the risks.

### Studies on security of Bluetooth Low Energy (BLE) devices and Wi-Fi devices

HKCERT released their "IoT Device (BLE) Security Study"[14,15] and "IoT Device (Wi-Fi) Security Study"[16,17] that aimed to raise the awareness of product developers and general users on the security of these Internet of Things (IoT) devices. Detail security analysis on different aspects, as well as recommendations on secure configuration of these devices were included in respective reports.

---

2 https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=463
3 https://www.hkcert.org/my_url/en/alert/20032402
4 https://www.jpcert.or.jp/english/at/2020/at200015.html
5 https://www.mycert.org.my/portal/advisory?id=MA-781.032020
6 https://www.cert.govt.nz/it-specialists/advisories/targeted-attacks-exploiting-vulnerabilities-in-microsoft-windows/
7 https://www.us-cert.gov/ncas/current-activity/2020/03/23/microsoft-rce-vulnerabilities-affecting-windows-windows-server
8 https://www.cyber.gc.ca/en/alerts/font-parsing-0-day-affecting-microsoft-windows
9 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200006
10 https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=458
11 https://www.us-cert.gov/ncas/current-activity/2020/03/10/unpatched-microsoft-exchange-servers-vulnerable-cve-2020-0688
12 https://www.cert.govt.nz/it-specialists/advisories/vulnerability-in-exchange-server-actively-exploited/
13 https://www.cyber.gc.ca/en/alerts/microsoft-exchange-validation-key-remote-code-execution-vulnerability
14 https://www.hkcert.org/my_url/en/blog/20030501
15 https://www.hkcert.org/c/document_library/get_file?uuid=d274b0a7-6272-4cc3-8f32-ab1e83d38500&groupId=16
16 https://www.hkcert.org/my_url/en/blog/20033101
17 https://www.hkcert.org/c/document_library/get_file?uuid=95140340-8c09-4c9a-8c32-cedb3eb26056&groupId=16

## CERT Advisories

### Beware of COVID-19 themed scams and campaigns

HKCERT[18], CERT NZ[19], CISA[20], and MyCERT[21] issued respective alert/advisory to remind computer users to remain vigilant for malicious campaigns related to COVID-19 such as fraudulent donation appeals, phishing emails or scam text messages with malicious attachments/links to trick users to download malicious contents/applications, etc. Users should obtain information from trusted sources, avoid clicking links and opening attachments from unsolicited emails, and verify the authenticity of the organisations which asked for sensitive information or donation.

### Security best practices for home office

ACSC[22], CERT NZ[23], and UK National Cyber Security Centre (NCSC)[24] provided cyber security best practices on working from home, such as to ensure the firewall and Virtual Private Network (VPN) solutions were up-to-date, adopt multi-factor authentication (MFA) for accessing IT resources (including cloud services), secure the mobile devices timely, encrypt removable media and good practices on other areas such as network security, physical security, etc.

### Protect Internet-connected cameras

UK NCSC [25] released guidance on securing Internet-connected cameras. This guidance suggested users to change the default password of camera, apply latest firmware or software to the camera, and disable remote access/viewing features if not needed. To further protect the device and home network, users could disable Universal Plug and Play (UPnP) and port forwarding on routers if possible.

[18] https://www.hkcert.org/my_url/en/blog/20032601
[19] https://www.cert.govt.nz/individuals/alerts/attackers-using-covid-19-themed-scams/
[20] https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams
[21] https://www.mycert.org.my/portal/advisory?id=MA-779.032020
[22] https://www.cyber.gov.au/news/cyber-security-essential-when-preparing-covid-19
[23] https://www.cert.govt.nz/about/news/covid-19-supporting-people-to-work-from-home
[24] https://www.ncsc.gov.uk/guidance/home-working
[25] https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home

## Industry Insight on Cyber Security Threat Trends

**43% of surveyed organisations sacrificed mobile security for various reasons**

Verizon surveyed 876 professionals, who were responsible for procuring, managing and securing mobile devices and IoT devices, from organisations of different sizes and industries. The survey results and data from other IT and security firms were analysed and the analysis results were compiled to the "Mobile Security Index 2020 Report"[26]. The key findings were:

- **39% of surveyed organisations suffered from security compromise or breach involving mobile devices or IoT devices in the reporting period, increasing in three consecutive years.** 66% of victims considered the security incidents led to major impact to their organisations such as system unavailability (59%), data loss (56%), further compromise of other devices (46%), etc. 36% of victims considered the backlash was lasting.

- **43% of surveyed organisations sacrificed mobile security.** The three most common factors causing organisations to take this risky approach were the need to meet deadlines (62%), convenience (52%) and profitability targets (46%). However, organisations should understand that attackers were undiscriminating and targeted organisations in all industries and of all sizes.

- **Changing default/vendor-supplied passwords, encrypting data transmitted over public networks, conducting security test regularly, and restricting data access on need-to-know basis were some basic protective measures on mobile security.** However, only 13% of surveyed organisations adopted all these basic measures to protect their mobile devices.

- **Malicious apps became more sophisticated and evasive, making them easily spread and difficult to be detected.** 21% of organisations encountered mobile compromise opined that unapproved mobile apps were the cause of the compromise. However, only 43% of surveyed organisations restricted the usage of approved and official apps.

- **In average, mobile devices connected to 2-3 insecure Wi-Fi hotspots daily**. 20% of those organisations victimised in mobile compromise found that insecure Wi-Fi hotspots were involved in the compromise. Nearly half (48%) of surveyed organisations forbidden their mobile devices to use public Wi-Fi.

- **Organisations were recommended to provide regular security training to their staff, establish formal acceptable use policy (AUP) on the permitted usage of networks and mobile apps, enforce password policy, adopt mobile device management (MDM) solution to enforce security policies and patch management, to improve their mobile security.**

*Source: Verizon*

[26] https://enterprise.verizon.com/resources/reports/2020/2020-msi-report.pdf

## Industry Insight on Cyber Security Threat Trends

**The attack traffic found in 2019 was four times more than 2018**

F-Secure released their "Attack Landscape H2 2019"[27]. The report was based on the data collected from their honeypots in the second half of 2019 and the malware seen in their customer endpoints in 2019. The highlights from the report included:

- **There was a huge increase in number of attacks in 2019**. Although the number of attacks in the second half of 2019 slightly decreased when compared to the first half of 2019, the total number in 2019 (5.7 billion attacks) was much higher than 2017 (792 million attacks) and 2018 (1,044 million attacks).

- **Hong Kong, with 65 million counts, was ranked as the eighth location with highest amount of attack source in the second half of 2019.** USA, China and Russia were the top three source locations in the second half of 2019, with 556 million, 430 million and 335 million counts respectively. During the same period, Ukraine, China and Austria were the top three attack destination locations with 357 million, 239 million and 230 million counts respectively.

- **Server Message Block (SMB) port 445 was the most targeted port with 526 million hits, followed by Telnet port 23 (523 million hits) and Secure Shell (SSH) port 22 (490 million hits) in the second half of 2019.** This indicated that SMB worms and exploits were still commonly used by attackers. Attackers also heavily targeted weakly secured IoT devices, brute forcing the administrative accounts with factory default credentials or weak passwords.

- **"admin" was the most common password used by attackers in brute force attacks.** "default", "12345", "password", "root" and factory default password of some devices such as digital video recorders (DVR), routers, etc., were also in the top ten list. Users should change the factory default password with strong password for their devices.

- **Email and spam were the most popular method to deliver malware, 43% malware were distributed by email and spam.** PDF (34%), Word and Excel macro documents (28%) and ZIP files (17%) were the top three malicious file types attached in spams. Moreover, a new trend of using ISO or disk image file (IMG) files with malicious contents was observed, although the volume (2%) was relatively low. Emotet (18.69%) was the top spam payload type, followed by lokibot (12.34%) and remcos (8.32%).

- **Ransomware attacks became more complicated and targeted.** Recent trend revealed that attackers threatened to publicly disclose the data stole from their victims if they could not get the demanded ransom.

*Source: F-Secure*

[27] https://blog-assets.f-secure.com/wp-content/uploads/2020/03/04101313/attack-landscape-h22019-final.pdf

## Industry Insight on Cyber Security Threat Trends

**Attackers continue to evolve their attack tactics**

VMware Carbon Black published the "2020 Cybersecurity Outlook Report"[28], which offered their analysis results on attackers' tactics based on the 2,000 samples collected from their own data, publicly available sources, and the dark web. The report also included the results of a survey with 624 IT/security managerial rank or above practitioners on the relationship between IT and security teams. The key findings were:

- **More than 90% of the malware samples and 95% of the ransomware samples attempted to evade detection.** They had the ability of altering the file signature in order to evade from signature-based detection solutions. They could also abuse system functions to hide their malicious activities from users' sight by hidden windows. Organisations could consider to use endpoint protection solution or application whitelisting to restrict program execution, and enable event logging and PowerShell logging to mitigate the risks. Malware also utilised common protocols such as HTTP, HTTPS, SMTP, DNS, etc. to communicate with the Command and Control servers, blending their malicious traffic with normal network traffic to avoid detection. In some occasions, they could be resilient by using secondary Command and Control servers when the communication channels with primary servers were blocked. Analysis and anomaly detection on network logs such as DNS logs, firewall logs, full packet captures, etc., as well as restriction on outbound network connections could be adopted by organisations for risk mitigation.

- **The top three targeted industries by ransomware in 2019 were Energy / Utilities (32%), Government (14.1%) and Manufacturing (13.8%).** Besides, healthcare providers and education were also victims of some notable ransomware attacks in 2019.

- **Wiper behaviours continued to increase in 2019.** To protect against data destruction, organisations should have their drilled disaster recovery plans readily available, equipped with resilient systems and supported with reliable and regular data backup mechanisms. Micro-network segmentation could also help to hinder the lateral movement of malware.

- **80% of survey respondents indicated that their organisations increased the funding on security in 2019, 77% of organisations invested on new security products and 69% hired more security staff.** Nevertheless, about half of the respondents indicated that their security team were still understaffed and more than 70% opined that it was very challenging to employ a right security talent for their organisations.

*Source: VMware Carbon Black*

[28] https://www.carbonblack.com/resources/threat-research/cybersecurity-outlook-report/

## Summary of Microsoft March 2020 Security Updates

**15** Product Families with Patches

**9** Critical

**6** Important or below

| Product Family | Impact[29] | Severity | Associated KB and / or Support Webpages |
|---|---|---|---|
| **Windows 10** | Remote Code Execution | Critical ★★★★ | KB4538461, KB4540670, KB4540673, KB4540681, KB4540689, KB4540693, KB4551762, ADV200006 |
| **Windows Server 2016, 2019 and Server Core installations** | Remote Code Execution | Critical ★★★★ | KB4538461, KB4540670, KB4540673, KB4540689, KB4551762, ADV200006 |
| **Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2** | Remote Code Execution | Critical ★★★★ | KB4540688, KB4540694, KB4541500, KB4541504, KB4541505, KB4541506, KB4541509, KB4541510, ADV200006 |
| **Internet Explorer** | Remote Code Execution | Critical ★★★★ | KB4538461, KB4540670, KB4540671, KB4540673, KB4540681, KB4540688, KB4540689, KB4540693, KB4541506, KB4541509, KB4541510 |
| **Microsoft Edge** | Remote Code Execution | Critical ★★★★ | KB4538461, KB4540670, KB4540673, KB4540681, KB4540689, KB4540693 |
| **Microsoft Office-related software** | Remote Code Execution | Critical ★★★★ | KB4475602, KB4484231, KB4484237, KB4484240, KB4484242, KB4484268, KB4484270<br>Microsoft Office 2019: Click to Run<br>Microsoft Office 2016, 2019 for Mac: Release Notes<br>Microsoft Office 365 ProPlus: Click to Run |
| **Microsoft SharePoint-related software** | Remote Code Execution | Critical ★★★★ | KB4475597, KB4475606, KB4484124, KB4484150, KB4484197, KB4484271, KB4484272, KB4484275, KB4484277, KB4484282 |

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

| Product Family | Impact[29] | Severity | Associated KB and / or Support Webpages |
|---|---|---|---|
| **ChakraCore** | Remote Code Execution | Critical ★★★★ | Release Notes |
| **Microsoft Dynamics** | Remote Code Execution | Critical ★★★★ | KB4538708, KB4538884, KB4538885, KB4538886, KB4538887, KB4538888, KB4551258, KB4551259 |
| **Microsoft Exchange Server** | Spoofing | Important ★★★ | KB4540123 |
| **Microsoft Visual Studio** | Elevation of Privilege | Important ★★★ | KB4538032<br>Microsoft Visual Studio 2019: Release Notes<br>Microsoft Visual Studio 2017: Release Notes |
| **Application Inspector** | Remote Code Execution | Important ★★★ | Release Notes |
| **Azure DevOps Server** | Elevation of Privilege | Important ★★★ | Azure DevOps Server 2019.0.1: Release Notes<br>Azure DevOps Server 2019 Update 1 & 1.1: Release Notes |
| **Azure Service Fabric** | Elevation of Privilege | Important ★★★ | Release Notes |
| **Team Foundation Server** | Elevation of Privilege | Important ★★★ | Team Foundation Server 2017 Update 3.1: Release Notes<br>Team Foundation Server 2018 Update 1.2: Release Notes<br>Team Foundation Server 2018 Update 3.2: Release Notes |

Learn more:

High Threat Security Alert (A20-03-02): Multiple Vulnerabilities in Microsoft Products (March 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=458)

**Sources:**

- Microsoft March 2020 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Mar)