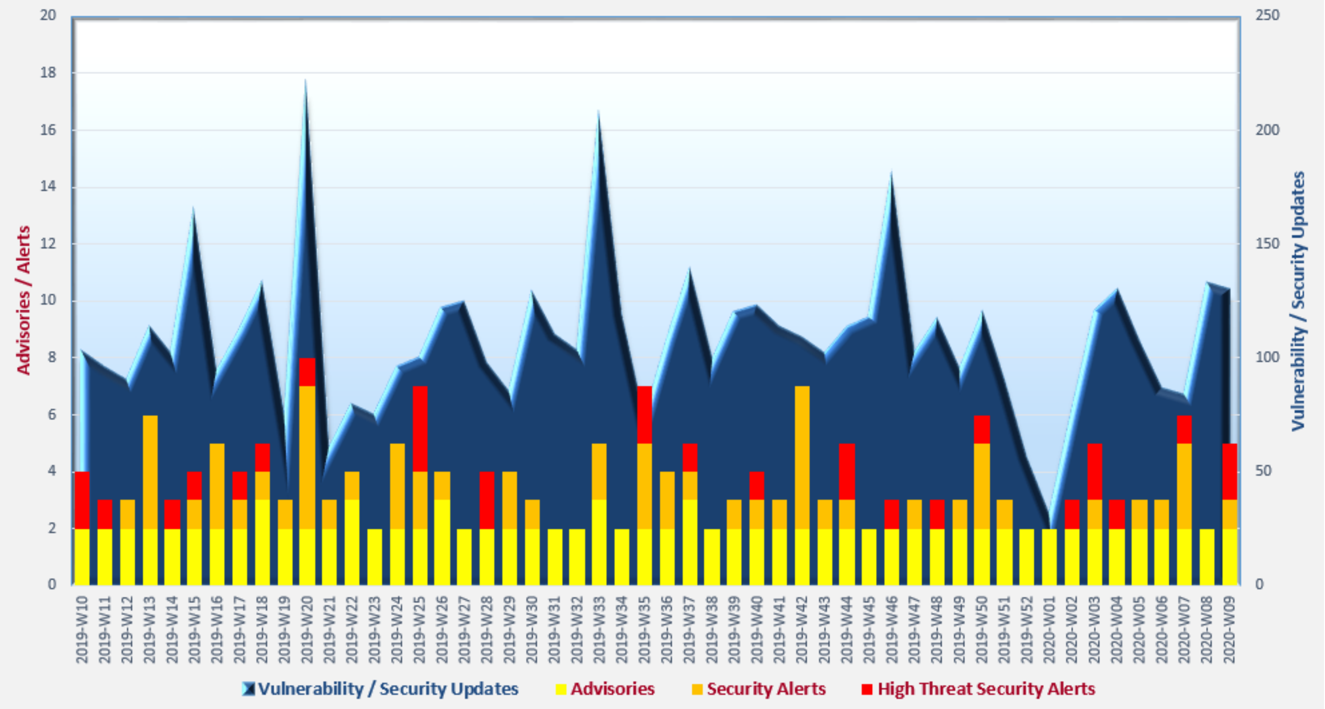
Cyber Security Threat Trends 2020-M02

Feburary 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:

- **Default credentials and security weaknesses** in IoT devices are targeted by attackers for taking control of the devices to form botnets. General users and organisations should change the default credentials for the devices, adopt strong administrator passwords, and disable unnecessary features (e.g. remote management).
- **Multi-vector attacks** are increasingly popular among threat actors to conduct attacks at both network and application levels. Organisations are advised to adopt multi-layer anomaly detection solutions to defend against complex attacks.
- **Use of weak passwords** has been a common problem for a long time. Users could consider using long passwords made up of multiple phrases. Organisations should enforce strict password policies for important systems.

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

CERT Advisories

Comprehensive resource for upgrading Transport Layer Security (TLS) to secure versions

In view of the end of support for TLS 1.0 and TLS 1.1 in March 2020, HKCERT[2] published its "TLS Upgrade Guideline" for IT practitioners to analyse, plan, implement and verify the upgrade of TLS to TLS 1.2 and TLS 1.3. In order to help the IT administrators to stock-take the IT assets that require TLS support, a ready-to-use "Inventory Table Template" was also shared. Two implementation profiles were recommended: 1) adopting TLS 1.3 only for maximising the security; or 2) adopting both TLS 1.2 and TLS 1.3 to strike the balance between compatibility and security.

Stay vigilant while using charging facilities in public areas

Charging facilities are available in many public areas. Nevertheless, hackers may abuse these charging facilities and load malware to infect connected mobile devices. HKCERT issued security tips[3] to general users on how to use these public charging stations securely.

Guideline and security tips for remote access services

Employees may occasionally need to work from home or elsewhere. HKCERT released a guideline[4] for organisations to list out three different approaches when choosing remote access services. In addition, HKCERT also issued six actionable security tips[5] related to working from home for both organisations and their employees.

Beware of coronavirus-themed phishing attacks

HKCERT published advisories[6,7] to remind users to stay alert to any kind of phishing messages via emails, instant messaging and social media. Users should not open any attachments, or click any URL links from un-trusted sources or suspicious emails, and beware of any email requesting financial assistance. Organisations could also refer the advice from the UK National Cyber Security Centre (NCSC)[8,9] on prevention against phishing attacks.

Malware and ransomware mitigation guidance for organisations

NCSC[10] published a "Mitigating malware and ransomware attacks" guideline. It provided steps and measures to be taken before and after malware and ransomware infection.

[2] https://www.hkcert.org/my_url/en/blog/20022802

[3] https://www.hkcert.org/my_url/en/blog/20022801

[4] https://www.hkcert.org/my_url/en/blog/20022001

[5] https://www.hkcert.org/my_url/en/blog/20022002

[6] https://www.hkcert.org/my_url/en/blog/20020401

[7] https://www.hkcert.org/my_url/en/blog/20022501

[8] https://www.ncsc.gov.uk/blog-post/phishing-still-a-problem-despite-the-work

[9] https://www.ncsc.gov.uk/information/phishing-webinar

[10] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Industry Insight on Cyber Security Threat Trends

Data breaches and attacks targeting IoT devices and Operational Technology (OT) are expected to continue their growth trend in 2020

IBM Security released the "IBM X-Force Threat Intelligence Index 2020"[11] on their analysis and observations of security events and trends in 2019. The key findings were:

- **The number of breached records was more than 8.5 billion, three times greater than the amount in 2018.** 86% of the breached records were caused by misconfiguration even though the number of misconfiguration incidents decreased 14% in 2019.

- **In 2019, cybercriminals returned to ransomware business.** Ransomware accounted for 19% of attacks in first half of 2019, increased from 10% in the second half of 2018. Ransomware attacks became more targeted. Infected organisations included schools, public institutions, government agencies, healthcare providers, and so on. 80% of observed ransomware attacks attempted to exploit the vulnerabilities in the Window Server Message Block (SMB) protocol, which were abused in WannaCry campaigns. Attackers also used multi-stage infection in order to have better control and higher evasive ability.

- **For multiple Mirai campaigns targeting IoT devices in 2019, attackers shifted their targets from consumer electronic products to enterprise-grade devices.** The most common attack technique was command injection (CMDi) attack, which was highly facilitated by the use of default credentials or weak password in IoT devices.

- **The top three initial attack vectors were phishing, scanning and exploiting vulnerabilities, and use of stolen credentials, accounted for 31%, 30%, and 29% respectively.** Although phishing was the top initial attack vector in 2019, it was dropped from 44% in 2018. Scanning and exploiting vulnerabilities, however, were increasingly used by attackers, rising from 8% in 2018. 90% of the vulnerabilities targeted by spam campaigns were two Microsoft Office vulnerabilities, CVE-2017-11882 and CVE-2017-0199. Organisations should apply up-to-date security patches to their software promptly to mitigate the risks.

- **A dramatic 2000% growth in OT attack since 2018 was observed and the growing trend will continue in 2020.** Attackers used password-spraying attacks and targeted known vulnerabilities of SCADA and Industrial Control Systems (ICS) hardware to compromise the systems. The increasingly merged IT and OT infrastructures also posed risks to organisations in the way that system breaches in IT systems laterally moved to infect the OT infrastructure.

Source: IBM Security

[11] https://ibm.biz/downloadxforcethreatindex

Industry Insight on Cyber Security Threat Trends

Cloud resource abuses, multi-vectors and new tactics ramped up DDoS attack complexity and volume

Link11 published the "Distributed Denial of service Report for the Year 2019"[12]. The report was based on the data collected from 25,000 repulsed attacks on the web pages and servers. It revealed the following security trends in Distributed Denial of Service (DDoS) attacks in 2019:

- **The number of multi-vector DDoS attacks increased by almost 19% in Q4 as compared to Q1 2019.** Attacks using ten vectors were uncovered in more than 40 multi-vector attacks. Nearly half of multi-vector attacks utilised three vectors in 2019. The increasing complexity in the attack patterns facilitates simultaneous attack on the network and application layers. Organisations should consider to enhance the network security solutions to detect the anomalies on multiple protocols and applications.

- **There were 42 attacks recorded with an attack volume of more than 100 Gbps, of which nearly 90% happened in first half of 2019.** The greatest attack volume was almost double compared with 2018, amounted to 724 Gbps from 371 Gbps, due to the growth of malicious usage of cloud resources and the numerous IoT devices. Moreover, the average attack bandwidth rose to 5 Gbps from 2 Gbps in 2016. The longest recorded attack in 2019 lasted over 100 hours.

- **Domain Name System (DNS) (34%) was the most prevalent amplification attack vector, followed by Connection-less Lightweight Directory Access Protocol (CLDAP) and Simple Network Management Protocol (SNMP) with 16%.** There were over 2.7 million insecurely configured DNS servers worldwide in 2019. Besides the rise of TCP amplification attacks, the UDP-based protocols such as Web Services Dynamic Discovery (WS-Discovery) and Apple Remote Management Service were also abused for amplification attacks.

- **Almost one out of two identified DDoS attacks leveraged the corrupted cloud servers in 2019**, **increased by almost 16% compared with 2018.** With the growth of multi-cloud deployment, organisations would face the challenges of siloed security mechanisms, inconsistent security policies, and segregated reporting.

- **'Carpet bombing' attacks surged in the second half of 2019 to bypass the DDoS mitigations.** A flood of individual attacks targeted a large number of IP addresses was used to simultaneously attack an entire subnet or Classless Inter-Domain Routing (CIDR) block with thousands of hosts. The volume of each individual attacks was small so as to evade detection.

Source: Link11

[12] https://www.link11.com/en/downloads/ddos-report-for-the-full-year-2019/

Industry Insight on Cyber Security Threat Trends

Weak password and password reuse problems are still serious

SpyCloud studied 640 data breaches in 2019 involving 9 billion breach records and published its "2020 Annual Credential Exposure Report"[13] which presented the analysis results and the trends on data breaches. The highlights from the report included:

- **From the 9 billion breach credentials, it was discovered that 28% internet users reused their password.** 94% of these users reused the same password, 4% reused the password with a little modification by adding numbers to the end, and 2% reused by capitalizing the first letter or other minor changes. These kinds of usage could make passwords easily compromised by crimeware, which could test for both exact matches and slight variations, and evade detection by limiting the number of login attempts.

- **The amount of breach credentials increased from 3.5 billion in 2018 to 9 billion in 2019.** Number of breach related to vulnerable servers also increased. One of the possible cause could be due to increased adoption of cloud infrastructure by organisations. Some of the cloud servers were setup by personnel with limited cloud security experience and knowledge for server hardening. Once a breach occurred, the threat actors normally shared the breach records within limited groups of accomplices to take profit, and disclosed the breach records to public 18 months or longer after the breach.

- **Organisations used weak or obsolete hashing algorithms to hash user passwords.** However, passwords hashed by these problematic hashing algorithms could be easily cracked by cracking tools. Organisations were recommended to follow NIST's Digital Identity Guidelines for the best practices of storing authentication secrets.

- **"123456", "123456789", "qwerty", "12345" and "password" were the top 5 reused passwords.** Many passwords in the top 100 reused passwords were variations of the top five or dictionary words. Moreover, for breaches related to specific companies, the brand names of the breached companies were commonly found in the compromised passwords. Organisations were recommended to check user passwords against those had been exposed or compromised in previous breach incidents, as well as commonly used or easy-to-guess passwords.

Source: SpyCloud

[13] https://spycloud.com/2020-annual-credential-exposure-report/

Summary of Microsoft February 2020 Security Updates

12
Product Families with Patches

6
Critical

6
Important or below

Product Family	Impact[14]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems	Remote Code Execution	Critical ★★★★	KB4502496, KB4524244, KB4532691, KB4532693, KB4537762, KB4537764, KB4537776, KB4537789
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4524244, KB4532691, KB4532693, KB4537762, KB4537764
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4502496, KB4537794, KB4537803, KB4537810, KB4537813, KB4537814, KB4537820, KB4537821, KB4537822
Internet Explorer	Remote Code Execution	Critical ★★★★	KB4532691, KB4532693, KB4537762, KB4537764, KB4537767, KB4537776, KB4537789, KB4537810, KB4537814, KB4537820, KB4537821
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4532691, KB4532693, KB4537762, KB4537764, KB4537776, KB4537789 Microsoft Edge (Chromium-based): Release Notes
ChakraCore	Remote Code Execution	Critical ★★★★	Release Notes
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4484156, KB4484163, KB4484250, KB4484254, KB4484256, KB4484265, KB4484267 Microsoft Office 2019: Click to Run Microsoft Office 2016, 2019 for Mac: Release Notes Microsoft Office 365 ProPlus: Click to Run

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

Product Family	Impact[14]	Severity	Associated KB and / or Support Webpages
Microsoft SharePoint-related software	Spoofing	Important ★★★	KB4484255, KB4484259, KB4484264
Microsoft Exchange Server	Remote Code Execution	Important ★★★	KB4536987, KB4536988, KB4536989
Microsoft SQL Server	Remote Code Execution	Important ★★★	KB4532095, KB4532097, KB4532098, KB4535288, KB4535706
Microsoft Surface Hub	Security Feature Bypass	Important ★★★	KB4537765
Windows Malicious Software Removal Tool	Elevation of Privilege	Important ★★★	KB891716

Learn more:
High Threat Security Alert (A20-02-03): Multiple Vulnerabilities in Microsoft Products (February 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=451)

Sources:

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