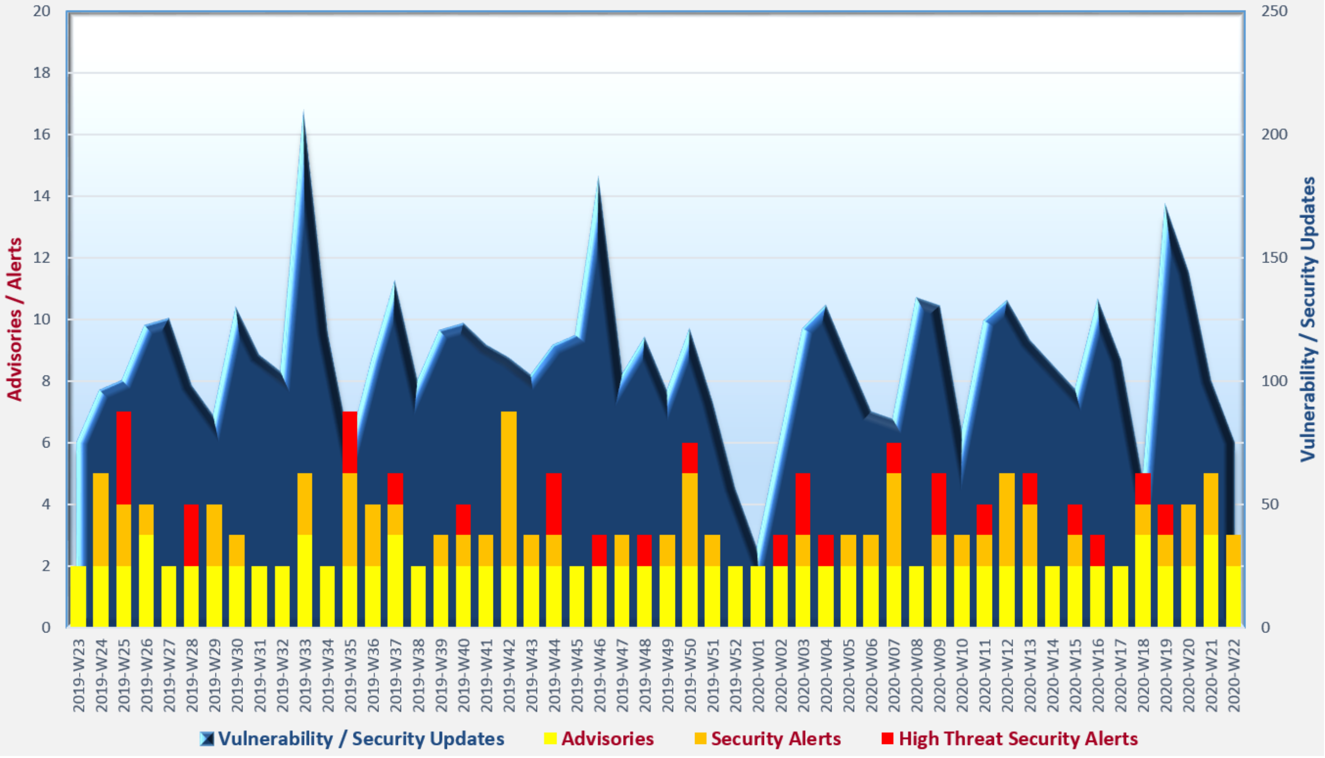
Cyber Security Threat Trends 2020-M05

May 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:

- ✧ **Vulnerable or outdated open source components** increase security risks to organisations yet they are easily neglected. Organisations should stocktake their software in use regularly to uncover any unpatched or obsolete components for security updates or product upgrades respectively.
- ✧ **Access credentials** are the common data type exposed in data breaches. Users should not use the same password for different systems / services, and multi-factor authentication should be adopted whenever applicable.
- ✧ **A local surge of malware hosting events in 2020 Q1 broke the downtrending throughout 2019.** System administrators should stay alert and follow security best practices including but not limited to keeping IT asset inventory up-to-date, patching system components timely, hardening server configuration, and reviewing logs regularly.

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

CERT Advisories

Malware hosting events in Hong Kong increased by 3.5 times in 3 months

HKCERT released its Hong Kong Security Watch Report (Q1 2020)[2]. Although the number of security events decreased for last three consecutive quarters, the trend stopped in Q1 2020. The total amount of security events raised to 14,433, an increase of 45.6% from Q4 2019. Among the events, the number of phishing events incremented significantly by more than 50% to 399, while the number of malware hosting events skyrocketed 3.5 times to 5,445. These two event types accounted for the growth of security events in this quarter. On the other hand, more threat actors had used file inclusion and SQL injection attack methods to compromise systems. In addition to normal patching on web applications and adopting secure coding practices, organisations were recommended to conduct web application security risk assessment at regular time intervals before system rollout.

Study result showed cyber defence readiness of organisations in Hong Kong dropped last year

The Hong Kong Productivity Council (HKPC) released the result of "SSH Hong Kong Enterprise Cyber Security Readiness Index Survey"[3]. The study was conducted independently by HKPC and supported by HKCERT. The result revealed that the Overall Index was 46.9, decreased by 2.4 from last survey. Most industry sectors such as Retail and Tourism, non-government organisations and schools attained Basic level while Financial Services sector reached a higher Managed level. Nevertheless, 56% of the respondents, a 15% increase from last survey, have encountered external cyber attacks. The top three types of external cyber attacks were phishing email (83%), ransomware (41%), and CEO Scam (26%). 30% of respondents would invest to improve cyber security measures in next 12 months.

Know more about security of ZigBee devices

HKCERT published the "IoT Device (ZigBee) Security Study"[4,5] that aimed to raise the awareness of product developers and general users on the security of ZigBee technology. In addition to introducing ZigBee technology, the report covered its configurations, security study, and security analysis. Recommendations to users and developers were also provided.

[2] https://www.hkcert.org/my_url/en/blog/20051401

[3] https://www.hkcert.org/my_url/en/blog/20051301

[4] https://www.hkcert.org/my_url/en/blog/20050801

[5] https://www.hkcert.org/c/document_library/get_file?uuid=3a1c8eed-012c-4b59-9d9e-971001d66c77&groupId=16

CERT Advisories

🗎 Cyber attacks targeted WordPress web sites

SingCERT[6] issued an alert stating that hackers leveraged Cross-Site Scripting (XSS) vulnerabilities in old WordPress plugins to attack WordPress web sites. System administrators or webmasters should regularly update WordPress and its plugins, or enable automatic update. Moreover, they should deactivate and remove any outdated plugins in the WordPress plugin repository.

[6] https://www.csa.gov.sg/singcert/alerts/al-2020-011

Industry Insight on Cyber Security Threat Trends

Organisations increasingly neglected their unpatched, outdated or abandoned open source libraries

Synopsys assessed and analysed more than 20,000 open-source codebases worldwide and anonymised audit findings from 1,253 applications in 17 industries, and published the study results in its "2020 Open Source Security and Risk Analysis Report"[7]. The major observations in the report were:

- **Open source adoption soared in 2019. 99% of the audited codebases contained at least one open source component and 70% of the audited codebases were open source.** On average, 445 open source components were found per codebase, a 50% increase from 298 in 2018. Organisations should maintain an up-to-date software Bill of Materials (BOM) for each application to have a complete visibility on the components used.

- **75% of assessed codebases were found with at least one known security vulnerability, increased from 60% in 2018. Percentage of assessed codebases with high-risk vulnerabilities also increased, from 40% in 2018 to 49% in 2019.** Almost 82 vulnerabilities per codebase were uncovered in average. Developers should incorporate security implementation into the software development process from the outset.

- **Timely patching was not in place. The average age of vulnerabilities identified was around 4.5 years.** Nearly one-fifth of the assessed codebases contained vulnerabilities over 10 years old. The oldest one was a 22 years old Linux kernel vulnerability (CVE-1999-0061). Organisations should set and regularly review the vulnerability patching priorities, with consideration on the business importance and the criticality of the asset, as well as the risk of exploitation. They should also note the patch delivery mechanism of the open source components they used, which could be different from the "push" mechanism commonly adopted in commercial software.

- **Usage of aging or abandoned open source components was alarming.** 82% of the assessed codebases contained components outdated for more than four years. Components with no development activity in the past two years were found in 88% of the audited codebases.

- **For the ten vulnerabilities most commonly found in the assessed codebases, five of them were related to the Bootstrap open source component and four of them affected jQuery.** Two high-risk Lodash prototype pollution vulnerabilities, CVE-2018-16487 and CVE-2019-10744, were most frequently found (around 500 occurrences) in the audited codebases.

Source: Synopsys

[7] https://www.synopsys.com/software-integrity/resources/analyst-reports/2020-open-source-security-risk-analysis.html

Industry Insight on Cyber Security Threat Trends

Number of records exposed skyrocketed in Q1 2020

Risk Based Security released the "2020 Q1 Data Breach QuickView Report"[8] on their analysis and observations of data breaches and records exposed in Q1 2020. The key findings were:

- **The total number of publicly reported breaches and the total number of records exposed in Q1 2020 were 1,196 and 8,451 million respectively.** The number of records exposed increased 273% compared to the same period in 2019 and also recorded a new high Q1 figure since 2013. Although the publicly reported breaches dropped by 58% compared to the peak in Q1 2019, researchers opined the drop could be due to disruption caused by the COVID-19 pandemic in reporting of breaches, and the breach activity did not decline actually.

- **Around 70% of breaches were caused by unauthorised access to systems or services, which on average exposed about 0.85 million records per breach.** In terms of data volume, disclosure of data on the Internet accountable for 90% of the records exposed, with about 106 million records exposed per breach on average. In the 1,196 reported breaches, 993 (around 83%) were caused by outsiders, while less than 13% (i.e. 154) were attributed to insiders. The most common exposed data types were access credentials (combinations of passwords and usernames / email addresses). Computer users should adopt different passwords in different systems or services.

- **Healthcare sector experienced the most breaches (15.4%), followed by Information (15.1%), Public Administration (12.2%) and Financial Services (10.5%) sectors.** These four sectors accounted for 53.2% of reported breaches in Q1 2020.

- **The COVID-19 pandemic created opportunities for threat actors to perform malicious activities.** COVID-19 themed phishing campaign was a growing threat to cyber security. Moreover, employees used unmonitored personal endpoints to work from home, could introduce new attack surfaces to threat actors and increased organisations' risk of systems being compromised.

- **Adverse economic condition could catalyse more cyber attacks.** The economy was expected to deteriorate due to the impact of the COVID-19 pandemic. Organisations could be forced to reduce the budget on IT and cyber security. With the growing cyber security threats but shrank in IT staffing and resources, attackers could seize the opportunities to compromise organisations' computer systems and exfiltrate organisations' data.

Source: Risk Based Security

[8] https://pages.riskbasedsecurity.com/en/2020-q1-data-breach-quickview-report

Industry Insight on Cyber Security Threat Trends

Visibility gap on computer and data assets in organisations are widening

Tanium released the "Visibility Gap Study”[9] report, which included the analysis results based on survey returns from 750 IT decision makers from the United States, United Kingdom, Australia, France, Germany, the Netherlands, Japan and Canada. The key findings were:

- **Only 26 percent of survey respondents felt they had complete visibility of the devices on their network.** 94 percent experienced discovery of endpoints, which were previously unaware of, in their organisations. 47 percent faced challenges in getting visibility for the devices connected to their network.

- **Survey respondents opined the problems of siloed IT, operations and security teams (39%), limited resources (31%), legacy systems (31%), Shadow IT (29%) and large variety of tools used (29%) further complicated the problem of visibility gaps.** On average, surveyed organisations used 43 different security and operations tools for the management of their IT environments.

- **Limited visibility could cause financial or reputational damages to organisations.** More than half of the survey respondents (53%) concerned that limited endpoints visibility could cause their organisations more vulnerable to cyber-attacks. Other concerns included damage to the company brand and customer loyalty, poor user experience, causing non-compliance fines, etc.

- **Organisations should have a comprehensive view on all computers and data assets in their entire IT environments.** With the knowledge of the patching status and the exact location of the IT assets, organisations could prioritise the vulnerability remediation more effectively. It could also facilitate organisations in incident response on security breach and meeting regulatory reporting requirements on security incidents.

Source: Tanium

[9] https://www.tanium.com/resources/mind-the-endpoint-visibility-gap

Summary of Microsoft May 2020 Security Updates

13
Product Families with Patches

8
Critical

5
Important or below

Product Family	Impact[10]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4551853, KB4556799, KB4556807, KB4556812, KB4556813, KB4556826
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4551853, KB4556799, KB4556807, KB4556813
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4556840, KB4556846, KB4556852, KB4556853
Internet Explorer	Remote Code Execution	Critical ★★★★	KB4551853, KB4556798, KB4556799, KB4556807, KB4556812, KB4556813, KB4556826, KB4556836, KB4556840, KB4556846
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4551853, KB4556799, KB4556807, KB4556812, KB4556813, KB4556826
Microsoft SharePoint-related software	Remote Code Execution	Critical ★★★★	KB4484332, KB4484336, KB4484352, KB4484364, KB4484383
Microsoft Visual Studio	Remote Code Execution	Critical ★★★★	Microsoft Visual Studio 2019 version 16.5: Release Notes Microsoft Visual Studio 2019 version 16.4: Release Notes Microsoft Visual Studio 2019 version 16.0: Release Notes Microsoft Visual Studio 2017: Release Notes Visual Studio Code: Release Notes

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

Product Family	Impact[10]	Severity	Associated KB and / or Support Webpages
ChakraCore	Remote Code Execution	Critical ★★★★	Release Notes
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Excel: KB4484338, KB4484365, KB4484384 Microsoft Office 2019: Click to Run Microsoft Office 2016 & 2019 for Mac: Release Notes Microsoft 365 Apps for Enterprise: Click to Run Microsoft Office 365 ProPlus for 32-bit Systems: Click to Run Microsoft Office 365 ProPlus for 64-bit Systems: Click to Run
Microsoft Dynamics	Spoofing	Important ★★★	KB4551998, KB4552002
Power BI Report Server	Spoofing	Important ★★★	Release Notes
Microsoft .NET Framework	Elevation of Privilege	Important ★★★	KB4552926, KB4552928, KB4552929, KB4552931, KB4556399, KB4556400, KB4556401, KB4556402, KB4556403, KB4556404, KB4556405, KB4556406, KB4556441, KB4556807, KB4556812, KB4556813, KB4556826
.NET Core and ASP.NET Core	Denial of Service	Important ★★★	ASP .NET Core 3.1: Release Notes .NET Core: Release Notes

Learn more:
Security Alert (A20-05-02): Multiple Vulnerabilities in Microsoft Products (May 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=473)

Sources:

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