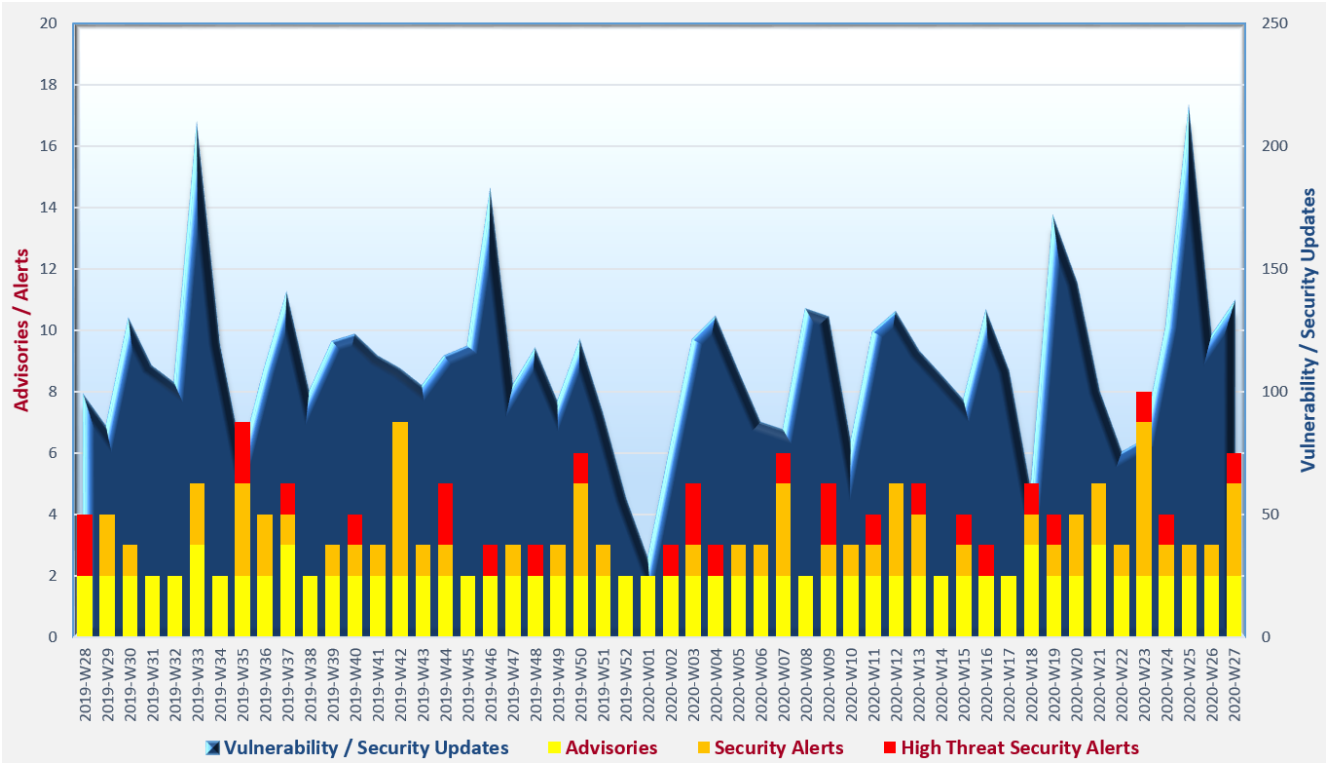
Cyber Security Threat Trends 2020-M06

June 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:

- ✧ **DNS-based attacks** stay frequent despite increased awareness of the threats by organisations. Organisations should take priority to maintain their DNS service availability and integrity to avoid their businesses being severely impacted.
- ✧ **Data theft, ransomware and cryptomining** are regarded as top threats to cloud environments. Cloud customers should work with their cloud service providers to conduct regular security risk assessments and reviews for assuring sufficient controls against prevalent threats.
- ✧ **Endpoint security** becomes increasingly important with decentralised workplaces amid the COVID-19 pandemic. Patching endpoint software timely, utilising endpoint detection and response (EDR) solutions, and educating end users of security best practices are key to secure the work-from-home model.

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

CERT Advisories

Cyber attacks targeted remote access systems

CERT NZ[2,3] reminded organisations that attacks targeting organisations' network leveraging remote access technologies such as Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) were observed. Once attackers gained access to remote access systems with unpatched software, weak authentication or lack of multi-factor authentication (MFA), they might perform further malicious actions such as stealing sensitive information, deploying ransomware, etc. System administrators should apply software patches timely, enforce strong password policy and adopt MFA for their remote access systems.

COVID-19 related cyber attacks continue

SingCERT[4,5] and MyCERT[6,7] issued several advisories to remind organisations and individuals to stay alert of COVID-19 related cyber attacks, including phishing campaigns and malicious mobile apps, which aimed to steal credentials, sensitive information and track users' activities. Users should verify the authenticity of the received emails. Smartphone users should download mobile apps from official and trusted sources and pay attention to the permission requested by their downloaded apps.

Microsoft Windows 10 version 1909 hardening

Australian Cyber Security Centre (ACSC)[8] released a guideline for system administrators to secure workstations running Microsoft Windows 10 version 1909. The guideline organised the hardening recommendations into high, medium and low priorities and covered wide range of areas including security features (e.g. attack surface reduction, controlled folder access), and Group Policy settings (e.g. exploit protection settings, disable credential caching).

[2] https://www.cert.govt.nz/it-specialists/advisories/active-ransomware-campaign-leveraging-remote-access-technologies/
[3] https://www.cert.govt.nz/individuals/alerts/businesses-compromised-through-remote-access-systems/
[4] https://www.csa.gov.sg/singcert/advisories/ad-2020-005
[5] https://www.csa.gov.sg/singcert/advisories/ad-2020-004
[6] https://www.mycert.org.my/portal/advisory?id=MA-788.062020
[7] https://www.mycert.org.my/portal/advisory?id=MA-789.062020
[8] https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-1909-workstations

Industry Insight on Cyber Security Threat Trends

DNS attacks become more sophisticated and increasingly targeting to cloud

EfficientIP and IDC released the "2020 Global DNS Threat Report"[9], which included the analysis results based on survey returns from 900 organisations across North America, Europe, and Asia Pacific. The major observations in the report were:

- **79% of the respondents suffered at least one DNS-based attack with an average 9.5 attacks in 2019.** 39% of DNS attacks were attributed by phishing, followed by malware-based attacks and traditional DDoS attacks, which accounted for 34% and 27% of DNS attacks respectively. The size of DDoS attacks also increased. 64% of DDoS attacks were greater than 5Gbit/s, a 4% increase compared with 60% in previous year. The average cost and mitigation time of DNS attack were US$ 924k and 5.25 hours respectively while more than one out of five of the respondents took over 7 hours to mitigate.

- **Application downtime was the most prevalent impact of DNS attacks as opined by 82% of the respondents.** Downtime for in-house application and cloud service were suffered by 62% and 50% of the respondents respectively. The increase in cloud service downtime was conspicuous, from 41% to 50%, due to the rise of number of business-critical applications hosted in hybrid-cloud environments. Compromised website (46%), brand damage (29%), loss of business (29%) and sensitive information stolen (16%) were other usual consequences of DNS attacks.

- **77% of the respondents recognised DNS security was critical, increased from 64% of previous year's results, showing that organisations' awareness on DNS security was improved.** DNS security was adopted in 98% of the respondents. However, 75% of DNS attacks could not be mitigated automatically and more than 50% of the respondents inevitably used some less favourable remediation measures such as shutting down processes and connections (58%) or disabling the applications (54%).

- **Government sector got the highest cloud instance misconfiguration abuse.** As more government services have adopted cloud services, their DNS attack surface have also expanded. System administrators should adopt the principle of least privileges in configuring their systems and third-party assessments should be carried out to assure secure settings.

- **A quarter of respondents reported no analytics on their DNS traffic while 35% of respondents did not use any internal DNS traffic for threat intelligence**. Organisation could consider leveraging advanced technologies such as user behavioural analytics and machine learning to analyse their DNS traffic and adopt a zero trust strategy.

Source: EfficientIP and IDC

[9] https://www.efficientip.com/resources/idc-dns-threat-report-2020/

Industry Insight on Cyber Security Threat Trends

Cloud computing security risks must be mitigated

IBM Security released their "2020 Cloud Security Landscape Report"[10]. The report was based on the survey data and case-study analysis of security incidents in 2019. The highlights from the report included:

- **Financially motivated threat actors were the most commonly observed in 2019.** They offered compromised cloud assets or cloud service accounts credentials in underground markets, which could then be acquired by attackers to perform other malicious activities, such as hosting phishing sites, launching DDoS attacks, etc. Moreover, variety of tools, scripts and learning resources for different kinds of attacks were also offered in the underground market. Nevertheless, nation state actors were also a persistent risk. With increasing volume of sensitive data to be stored in the cloud environment, espionage activity targeting cloud services were expected to continue. Organisations could consider to leverage threat intelligence for threat monitoring and cyber security defence.

- **Over 1 billion records were leaked in 2019 due to misconfiguration of cloud environments.** Personally identifiable information (PII), credit card numbers, client-related emails were some of the examples of the sensitive information leaked.

- **45% of cloud environment compromise events were by brute force attack and remote exploitation of cloud applications.** "Swimming upstream" was another technique used by attackers to gain access to cloud environments by compromising the underlying host and then accessed to other client environments. This approach blended the attackers' malicious activities with legitimate administration tasks, making them difficult to be discovered. Organisations should apply security best practices such as multi-factor authentication and privileged account management (PAM) to protect their cloud environment.

- **The top three malware types deployed in cloud environment were ransomware, cryptominers and botnets**, with number of incidents involving ransomware was three times of the cases for the other two. As Linux operating systems accounted for nearly 90% of cloud servers, the increasing trend of malware targeting Linux was expected to continue.

- **Threat actors used cloud environment to host malware or malicious sites, camouflaging malicious traffic with normal usage to evade from detection.** System administrators should monitor and log cloud events for detection of malware or malicious activity and forensic investigation.

Source: IBM Security

[10] https://www.ibm.com/account/reg/us-en/signup?formid=urx-44459

Industry Insight on Cyber Security Threat Trends

Attackers actively targeted vulnerabilities of internet facing systems

Rapid7 released the "2020: Q1 Threat Report"[11], which included their analysis results and observations for the first quarter of 2020. The key findings were:

- **Attackers actively scanned and exploited technologies such as remote access services, email systems, and virtualisation solutions.** Products from Citrix, Pulse Secure, Fortinet, Palo Alto, Microsoft, VMWare, Cisco, etc. were involved. System administrators should closely monitor the security notifications, alerts or advisories from the product vendors and CERT bodies for update cyber security information, and should closely monitor their systems, especially those internet-facing systems, and apply security patch timely.

- **More than 350,000 Microsoft Exchange servers exposed in the Internet were found vulnerable to a remote code execution vulnerability (CVE-2020-0688) during the reporting period.** However, only 7,000 systems were patched during the period between late March and end of April. The risk became more serious by the trend that threat actors were increasingly targeted user account credentials.

- **The top five targeted industries in Q1 2020 were Finance (17%), Professional Service (17%), Manufacturing (11%), Retail (11%) and Healthcare (9%).** 96% of attacks involved account credential compromise. Organisations should use multi-factor authentication (MFA) to improve user account security.

- **55% of malware was not detectable using traditional endpoint threat prevention software in the first quarter of 2020.** The monitoring of endpoint became more important than ever since the workplaces were decentralised due to work from home arrangement in many organisations during the COVID-19 pandemic. System administrators should ensure endpoint security agents could reach any endpoint for effective defence against threats. Organisations could use multiple cyber security solutions such as next-gen antivirus solutions, User Behaviour Analytics (UBA), Attacker Behaviour Analytics (ABA), and process behaviour analytics for threat detection. Organisations were also recommended to arrange security awareness training to end users. While working from home, end users should update their home routers with the latest firmware, change the default password and use strong encryption to secure their home Wi-Fi environments.

Source: Rapid7

[11] https://www.rapid7.com/research/report/2020Q1-threat-report

Summary of Microsoft June 2020 Security Updates

15 Product Families with Patches

7 Critical

8 Important or below

Product Family	Impact[12]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4549951, KB4556799, KB4557957, KB4560960, KB4561602, KB4561608, KB4561616, KB4561621, KB4561649
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4557957, KB4560960, KB4561608, KB4561616, KB4561621
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4561612, KB4561666, KB4561673, KB4561674
Internet Explorer	Remote Code Execution	Critical ★★★★	KB4557957, KB4560960, KB4561602, KB4561603, KB4561608, KB4561612, KB4561616, KB4561621, KB4561643, KB4561649, KB4561666
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4557957, KB4560960, KB4561602, KB4561603, KB4561608, KB4561612, KB4561616, KB4561621, KB4561643, KB4561649, KB4561666
Microsoft SharePoint-related software	Remote Code Execution	Critical ★★★★	KB4484391, KB4484400, KB4484402, KB4484405, KB4484409, KB4484414
ChakraCore	Remote Code Execution	Critical ★★★★	Release Notes
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office: KB4484342, KB4484351, KB4484373, KB4484378 Microsoft Excel: KB4484403, KB4484410, KB4484415 Microsoft Project: KB4484369, KB4484387, KB4484399

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

Product Family	Impact[12]	Severity	Associated KB and / or Support Webpages
			Microsoft Word: KB4484361, KB4484380, KB4484396 Microsoft Office 2019: Click to Run Microsoft Office 2016 & 2019 for Mac: CVE-2020-1225, CVE-2020-1226, CVE-2020-1229, CVE-2020-1321 Microsoft 365 Apps for Enterprise: Click to Run Microsoft Word for Android: Release Notes
Microsoft Dynamics	Spoofing	Important ★★★	KB4541722, KB4551998, KB4552002
Microsoft Visual Studio	Elevation of Privilege	Important ★★★	Microsoft Visual Studio 2015 Update 3: KB4562053 Microsoft Visual Studio 2017 version 15.9: Release Notes Microsoft Visual Studio 2019 version 16.0: Release Notes Microsoft Visual Studio 2019 version 16.4: Release Notes Microsoft Visual Studio 2019 version 16.6: Release Notes Visual Studio Code: Release Notes
Azure DevOps	Spoofing	Important ★★★	Azure DevOps Server 2019.0.1: Release Notes Azure DevOps Server 2019 Update 1: Release Notes Azure DevOps Server 2019 Update 1.1: Release Notes
Microsoft Forefront Endpoint Protection	Elevation of Privilege	Important ★★★	CVE-2020-1163, CVE-2020-1170
Microsoft Security Essentials	Elevation of Privilege	Important ★★★	CVE-2020-1163, CVE-2020-1170
Microsoft System Center Endpoint Protection	Elevation of Privilege	Important ★★★	CVE-2020-1163, CVE-2020-1170

Product Family	Impact[12]	Severity	Associated KB and / or Support Webpages
Windows Defender	Elevation of Privilege	Important ★★★	CVE-2020-1163, CVE-2020-1170

Learn more:

High Threat Security Alert (A20-06-07): Multiple Vulnerabilities in Microsoft Products (June 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=485)

Sources:

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