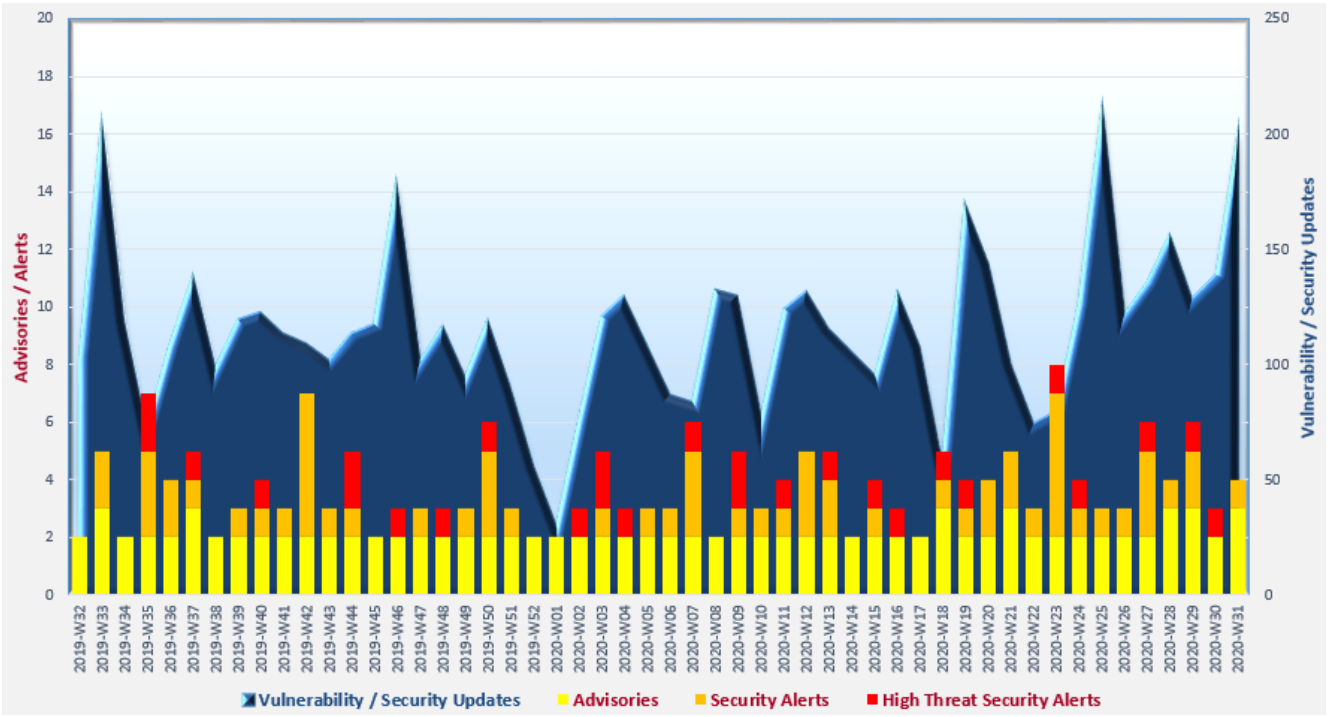
TLP:WHITE

Cyber Security Threat Trends 2020-M07

July 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:

- **Sophisticated distributed denial-of-service (DDoS) attack volume** reaches a new high. Organisations should subscribe DDoS mitigation service and plan for DDoS response actions to protect critical services. Users should install latest software patches and change default password to strong passwords for Internet of Things (IoT) devices such as digital video recorders, Wi-Fi routers, etc.
- **More new vulnerabilities in different platforms** are discovered. Organisations should adopt risk-based strategies to manage increasing vulnerabilities based on threat level and service impact, apply latest security patches to systems and devices timely.
- **Phishing** remains the top fraud attack type and new phishing campaigns keep emerging during COVID-19 pandemic. Organisations should educate staff and arouse their security awareness in defence against attacks via phishing emails and malicious websites.

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

CERT Advisories

COVID-19 themed phishing continues

SingCERT[2] and Australian Cyber Security Centre (ACSC)[3] reminded that COVID-19 themed phishing continued to broaden and evolve. Threat actors hosted fake online shopping and streaming service web sites. They also enhanced the appearance of phishing emails with official logos, font and layout which were the same as the emails from the genuine organisation. Users should pay extra caution when visiting websites and opening emails.

Active exploitation on critical vulnerability in F5 BIG-IP products

GovCERT.HK[4], SingCERT[5], JPCERT[6], Cybersecurity and Infrastructure Security Agency (CISA)[7], Canadian Centre for Cyber Security[8] issued alerts on multiple vulnerabilities existed in F5 BIG-IP products. In particular, CVE-2020-5902 was a critical vulnerability that was actively exploited by attackers. Successful exploitation could allow a remote, unauthenticated attacker to execute arbitrary commands. System administrators should refer to product vendor's recommendation and implement the mitigation measure immediately.

Wormable remote code execution vulnerability affects Windows DNS Server

GovCERT.HK[9], CERT NZ[10], and CISA[11] issued alert/advisory to remind organisations and system administrators to patch a remote code execution vulnerability that affected all versions of Windows Server with the Domain Name System (DNS) role, including Domain Controllers. A remote unauthenticated attacker could execute arbitrary code in the context of Local System Account on targeted servers. This vulnerability was rated as critical and also considered wormable. System administrators should apply the system patches immediately to mitigate the risks.

[2] https://www.csa.gov.sg/singcert/publications/phishing-in-the-time-of-covid-19
[3] https://www.cyber.gov.au/acsc/view-all-content/news/staying-hook-phishing-attacks
[4] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=492
[5] https://www.csa.gov.sg/singcert/alerts/al-2020-024
[6] https://www.jpcert.or.jp/english/at/2020/at200028.html
[7] https://us-cert.cisa.gov/ncas/current-activity/2020/07/04/f5-releases-security-advisory-big-ip-tmui-rce-vulnerability-cve
[8] https://www.cyber.gc.ca/en/alerts/active-exploitation-f5-big-ip-vulnerability
[9] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=494
[10] https://www.cert.govt.nz/it-specialists/advisories/critical-vulnerability-in-microsoft-windows-server/
[11] https://us-cert.cisa.gov/ncas/current-activity/2020/07/14/microsoft-addresses-wormable-rce-vulnerability-windows-dns-server

CERT Advisories

Double extortion ransomware and fake decryptor

HKCERT[12] released an article to reveal the latest tactics and evolution of ransomware. In order to have a higher chance of receiving ransom, cybercriminals adopted a new tactics known as double extortion. Cybercriminals stole sensitive information from the affected systems before encryption and threatened the victims that the stolen information would be published in the Internet if the ransom demands were ignored. The tactics used in ransomware campaigns, Maze and REvil (Sodinokibi), were analysed in the article. Another tactics used by cybercriminals was distribution of fake decryptor, which in fact was a ransomware attempting to infect the target system. The article also provided some security advices to organisations and normal users.

[12] https://www.hkcert.org/my_url/en/blog/20071301

UDP amplification attack weapons and Internet of Things (IoT) vulnerabilities aggravated large DDoS attacks

A10 Networks published the "Q2 2020: The State of DDoS Weapons Report"[13], which included the analysis results based on tracking almost 10 million unique source IP addresses. The major observations in the report were:

- **Portmap amplification** was the top Distributed Denial of Service (DDoS) attack vector, with over 1.8 million cases detected in Q2 2020. The **Simple Network Management Protocol (SNMP) and the Simple Service Discovery Protocol (SSDP)** were ranked as the second and third leading attack vectors with over 1.67 million cases detected each.

- Top countries and ASN hosting DDoS weapons were reported. Top 5 IoT binary detected were arm7, Cloud.x86, mmmmh.x86, Mozi.m and Mozi.a, of which 3 belonged to Gafgyt family, Cloud.x86 from Dark Nexus and mmmmh.x86 from Mirai family. The arm7 attack tootkit sample could be used for TCP floods, HTTP floods, UDP floods, DNS floods, etc.

- Malicious actors compromised unpatched IoT devices with Remote Code Execution (RCE) exploits, and the factory default user names and passwords, and weaponised them as DDoS botnets. Users should keep the firmware and operating systems of all of their IoT devices such as digital video recorders, Wi-Fi routers, wearable Internet connected devices, engineering sensors, etc. up-to-date with the latest patches and change the default device passwords with strong passwords to avoid attacks.

- **Amplified reflection attacks were the most common attack vectors used in volumetric DDoS attacks.** The attackers took advantage of the connectionless nature of the UDP protocol and sent forged network packets with the spoofed victim's IP address to exposed servers, causing these servers replied to the victim with large volume of amplified responses. In Q1 2020, Connection-less Lightweight Directory Access Protocol (CLDAP) reflection attacks were detected with record-breaking volume of 2.3 Tbps. This was almost 70% larger than the memcached-based DDoS attack in 2018. Organisations should subscribe DDoS mitigation service and work with their Internet service provider to plan in advance the response actions for DDoS attacks.

Source: A10 Networks

[13] https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

Industry Insight on Cyber Security Threat Trends

New vulnerabilities, as well as new ransomware and Trojan samples elevated in the first half of 2020

Skybox Security released the "2020 Vulnerability and Threat Trends Report Mid-Year Update"[14] on their observations of cyber threat landscape in the first half of 2020. The major observations in the report were:

- **9,799 new vulnerabilities were reported in the first half of 2020, a 34% increase compared to 7,318 new vulnerabilities in the same period of 2019, and also broke the last highest record, 8,485 vulnerabilities, in the first half of 2018.** The distribution of vulnerability severity in the first half of 2020 was similar to the same period of 2019. 15% of the new vulnerabilities were rated as critical. High-severity and medium-severity vulnerabilities were 42% and 40%, respectively. It was anticipated that over 20,000 vulnerabilities would be reported by the end of 2020. In prioritising the remediation of vulnerabilities, organisations were recommended not just based on the severity but should also take into account other factors such as exposure, exploitability, exploitation activity in the wild, etc.

- **The number of vulnerabilities of mobile OS increased by 50%, compared to the same period in 2019.** New Google Android vulnerabilities incremented significantly from 230 to 492. The need to mitigate the risk became more imminent, as during the pandemic, more users worked and accessed organisations' networks remotely using their mobile devices and home networks. Computer users should patch their devices timely to avoid attackers leveraging vulnerable domestic devices as stepping stone to gain access to organisations' IT assets. System administrators should improve their end-point visibility and control, apply secure configuration and up-to-date firmware and patches to their network devices, VPN solutions and firewalls, as well as closely monitor the ingress and egress network traffic.

- The number of **vulnerabilities of Microsoft Windows grew** from 250 to 449 and represented **an 80% increase. The risk became more serious as there were around 200 million machines still using obsoleted Windows versions for which free security update was no longer available.**

- **New samples of malware types increased in the first half of 2020, most significant were ransomware and Trojans. Threat actors tried to take benefit by leveraging the chaos of COVID-19 pandemic,** 78 ransomware campaigns were observed between March and June 2020, more than 60% happened in April during the lockdown period in a number of countries. Computer users should always be cautious to suspicious emails and instant messages, and should regularly backup their data and keep the backups offline.

Source: Skybox Security

[14] https://lp.skyboxsecurity.com/WICD-2020-07-WW-VT-Trends_Reg.html

Industry Insight on Cyber Security Threat Trends

Phishing remains the top fraud attack type

RSA released the "RSA Quarterly Fraud Report: Q1 2020"[15], which included the analysis results based on fraud attacks identified by RSA across the globe in the first quarter of 2020. The major observations in the report were:

- **Phishing was the top fraud attack type in the first quarter of 2020, accounted for over 27,000 attacks.** 54% of fraud attacks were phishing attacks, followed by brand abuse attacks (22%) and rogue mobile apps (15%). The amount of brand abuse attacks recorded an increase of 12% over the previous quarter, and a 5% increase (from 17% to 22%) in terms of their share in overall fraud attacks. Fraudsters used social media content, website and fake domain registrations to mislead users.

- **Canada was most targeted by phishing attacks for 5 consecutive quarters, with 66% phishing attacks.** The second mostly targeted was the United States with around 7% of phishing attack, and Spain came the third with 5% phishing attacks. The United States, China and Germany were the top three locations for phishing hosting.

- **The percentage of fraud transactions originated from mobile applications doubled from 13% to 26% compared to 2019 Q4.** On the other hand, the percentage of fraud transactions originated from mobile browsers decreased by 13%. With the overall percentage of fraud transactions originated from mobile channels remain unchanged, it showed the fraudsters shifted their way of attacks from mobile browsers to mobile applications.

- **In Q1 2020, 58% of e-commerce fraud transaction value originated from trusted accounts on new devices, indicating account takeover remained commonly used by threat actors.**

- **COVID-19 related fraud soared.** Fraudsters exploited the fear and uncertainty caused by COVID-19 and developed different COVID-19 scams such as sending scam emails and text messages. Besides general public, medical testing facilities and other health organisations were also targeted by ransomware attacks and information thefts. Organisations should educate users to be aware of phishing attacks and common pitfalls, review fraud prevention strategy, using strong spam filters to protect their email systems, patching the hardware and software timely, and backup the critical information regularly and storing the backups in different locations to mitigate the risk. Individual users should stay vigilant to phishing and scam emails and text messages.

Source: RSA

[15] https://www.rsa.com/en-us/offers/rsa-fraud-report-q1-2020

Summary of Microsoft July 2020 Security Updates

18 Product Families with Patches

11 Critical

7 Important or below

Product Family	Impact[16]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4558997, KB4558998, KB4565483, KB4565489, KB4565503, KB4565508, KB4565511, KB4565513, KB4565552, KB4565553, KB4565554, KB4565911, KB4565912, KB4566785
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4558997, KB4558998, KB4565483, KB4565503, KB4565511, KB4565554, KB4565912, KB4566785
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4565524, KB4565535, KB4565537, KB4565540, KB4565541, KB4566425, KB4566426
Internet Explorer	Remote Code Execution	Critical ★★★★	KB4558998, KB4565479, KB4565483, KB4565489, KB4565503, KB4565508, KB4565511, KB4565513, KB4565524, KB4565537, KB4565541
Microsoft Office-related software	Remote Code Execution	Critical ★★★★	Microsoft Office: KB4484451, KB4484456 Microsoft Project: KB4484441, KB4484450, KB4484463 Microsoft Outlook: KB4484363, KB4484382, KB4484433 Microsoft Word: KB4484438, KB4484446, KB4484458 Microsoft Office 2019: Click to Run Microsoft Office 2016 & 2019 for Mac: CVE-2020-1342, CVE-2020-1409, CVE-2020-1445, CVE-2020-1446, CVE-2020-1447 Microsoft Office Web Apps: KB4484357, KB4484381

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

Product Family	Impact[16]	Severity	Associated KB and / or Support Webpages
			Microsoft 365 Apps for Enterprise: Click to Run OneDrive for Windows: Release Notes
Microsoft SharePoint-related software	Remote Code Execution	Critical ★★★★	KB4484348, KB4484353, KB4484370, KB4484374, KB4484411, KB4484436, KB4484440, KB4484443, KB4484448, KB4484451, KB4484452, KB4484453, KB4484460
Microsoft Visual Studio	Remote Code Execution	Critical ★★★★	Microsoft Visual Studio 2015 Update 3: KB4567703 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 Visual Studio Code ESLint extension: Release Notes
Microsoft .NET Framework	Remote Code Execution	Critical ★★★★	KB4565489, KB4565508, KB4565511, KB4565513, KB4565627, KB4565628, KB4565630, KB4565631, KB4565633, KB4566466, KB4566467, KB4566468, KB4566469, KB4566516, KB4566517, KB4566518, KB4566519, KB4566520
.NET Core	Remote Code Execution	Critical ★★★★	Release Notes
Microsoft Lync Server	Elevation of Privilege	Critical ★★★★	Microsoft Lync Server: KB4571334
Skype for Business Server	Elevation of Privilege	Critical ★★★★	Skype for Business Server: KB4571332, KB4571333

Product Family	Impact[16]	Severity	Associated KB and / or Support Webpages
Azure DevOps Server	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 Edge	Information Disclosure	Important ★★★	KB4558998, KB4565483, KB4565489, KB4565503, KB4565508, KB4565511, KB4565513
Azure Storage Explorer	Elevation of Privilege	Important ★★★	Release Notes
Microsoft Forefront Endpoint Protection	Elevation of Privilege	Important ★★★	CVE-2020-1461
Microsoft Security Essentials	Elevation of Privilege	Important ★★★	CVE-2020-1461
Microsoft System Center Endpoint Protection	Elevation of Privilege	Important ★★★	CVE-2020-1461
Windows Defender	Elevation of Privilege	Important ★★★	CVE-2020-1461

Learn more:

High Threat Security Alert (A20-07-05): Multiple Vulnerabilities in Microsoft Products (July 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=494)

Sources:

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