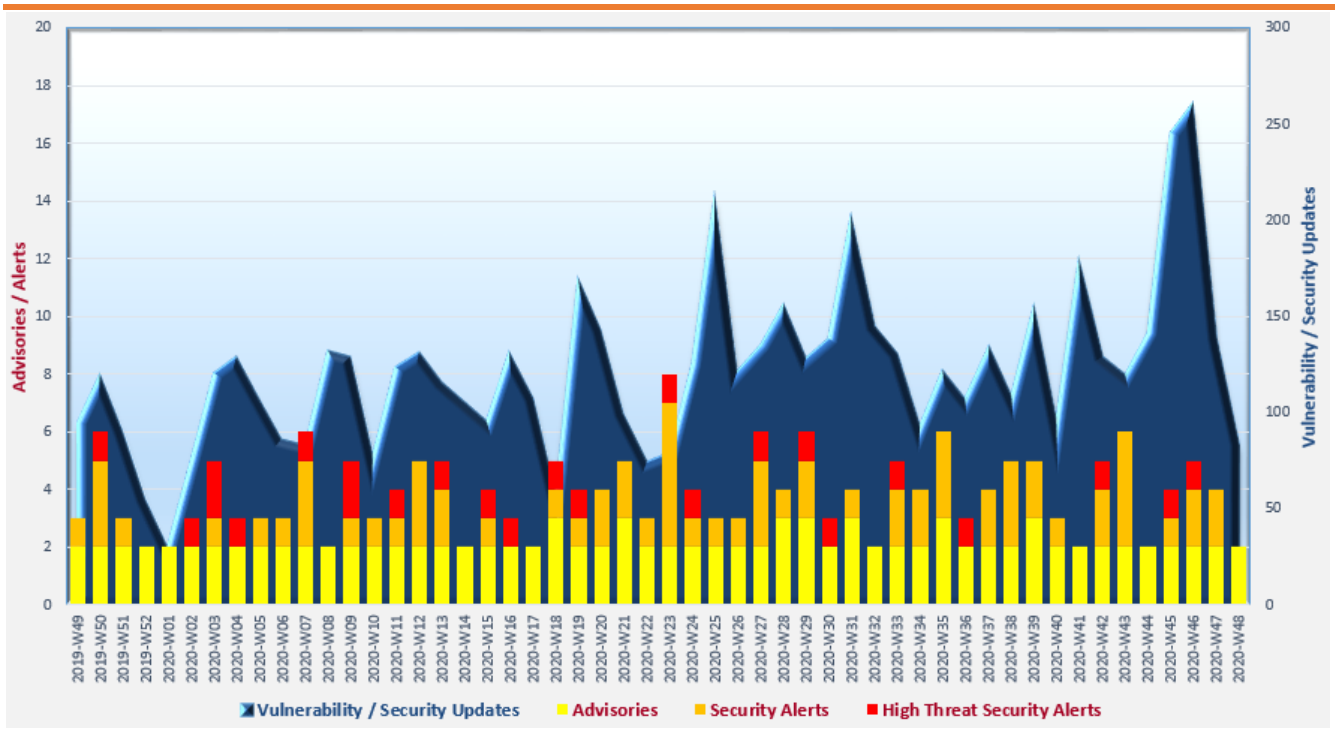
TLP:WHITE

Cyber Security Threat Trends 2020-M11

November 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:

- **Criminals** use encryption, legitimate penetration testing tools and common cloud services to hide their malicious activities. Organisations should adopt a multi-layered defense-in-depth strategy with full support of SSL/TLS inspection to protect from hidden malicious threats.
- **Windows Remote Desktop Protocol (RDP)** is heavily targeted by threat actors to launch cyber attacks. Organisations should ensure RDP service is not exposed to the Internet. Unnecessary services and network ports should be disabled to reduce attack surfaces.
- **Ransomware** continues to evolve with higher encryption speed and improved defense evasion mechanism, and induces more severe damages to victims. Organisations should patch their systems timely, adopt least privilege principle, and maintain offline backup to defend against the threat.

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

CERT Advisories

Active exploitations against vulnerabilities in iOS

GovCERT.HK[2], HKCERT[3], SingCERT[4], US-CERT[5] and Canadian Centre for Cyber Security[6] issued alerts regarding vulnerabilities in Apple iOS. Successful exploitation could lead to information disclosure, unauthorised access of files, privilege elevation, unexpected application termination and arbitrary code execution. Vulnerabilities (CVE-2020-27930, CVE-2020-27932, CVE-2020-27950) were being exploited actively. iOS users should install the latest patches immediately.

Security guideline for enterprise VPN usage

HKCERT[7] published security guidelines to help organisations to safeguard their enterprise VPN for minimising the associated cyber security risks. Actionable security measures covering security management and planning; security architecture, hardening and access control; and security monitoring and incident response aspects were recommended, such as implementing change management controls for enterprise VPN; adopting secure protocols and cryptographic algorithms; turning on the authentication log and reviewing the log on a regular basis, etc.

Beware of WhatsApp account hijacking

SingCERT[8] shared an advisory on WhatsApp account hijacking prevention. To take over a WhatsApp account, attackers would try to get access to a WhatsApp registration code. They might pretend as someone known by the victim or WhatsApp's support staff to cheat the victim to provide the registration code. Alternatively, attackers might also leverage the remote access function of voicemail and gain unauthorised access to the voice message with the victim's verification code for WhatsApp account. WhatsApp users were advised to switch on the "Two-Step Verification" feature, set up the backup email address, change default voicemail password and safeguard WhatsApp account verification codes and passwords.

[2] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=524
[3] https://www.hkcert.org/my_url/en/alert/20110602
[4] https://www.csa.gov.sg/singcert/alerts/al-2020-044
[5] https://us-cert.cisa.gov/ncas/current-activity/2020/11/06/apple-releases-security-updates-multiple-products
[6] https://www.cyber.gc.ca/en/alerts/apple-security-advisory-18
[7] https://www.hkcert.org/my_url/en/blog/20110901
[8] https://www.csa.gov.sg/singcert/advisories/ad-2020-007

Industry Insight on Cyber Security Threat Trends

Surge in ransomware distribution using encryption by five times since March 2020

Zscaler published the report "2020 State of Encrypted Attacks" [9], which included analysis results over 6.6 billion encrypted threats from January to September 2020 over encrypted channels. The major observations were:

- **Due to a sharp increase in cloud services adoption in the COVID-19 pandemic, there was about 260 percent spike in SSL-based threats blocked per month during the first nine months of 2020 when compared to the same period in 2019.** A record-breaking amount of 6.6 billion encrypted attacks, equivalent to an average of 733 million attacks per month were detected and blocked. Emotet and TrickBot occupied top two detected malware with each accounted for 40% of detections.

- **Ransomware attacks delivered over SSL/TLS channels soared five times since March 2020.** FileCrypt/FileCoder variants, Sodinokibi, Maze and Ryuk family variants were the most detected ransomware families. Telecommunication and technology sectors were mostly targeted, followed by healthcare sector, accounted for 40.5% and 26.5% of all ransomware attacks respectively. There was a noteworthy trend that ransomware increasingly coupled with data exfiltration feature to steal sensitive data from victims.

- **Over 193 million phishing attempts through encrypted channel were uncovered during the first nine months of 2020**. The top five targeted industries were manufacturing (38.6%), services (13.8%), healthcare (10.9%), education (9.3%) and technology (8.7%). Government sector also recorded almost 2.9 million phishing attempts. 36% of phishing spoofed Microsoft, followed by "Tech Support" scams and PayPal, accounted for 17% and 15% of phishing attacks respectively. During the pandemic, threat actors also increasingly conducted phishing attacks targeted streaming entertainment services.

- **Two billion SSL-based attacks from malicious contents hosted in cloud storage services were detected.** These attacks, accounted for over 30% of all SSL-based attacks, abused the wildcard SSL certificates and the popularity of cloud service providers such as Google Drive, OneDrive, AWS, or Dropbox, could evade the detection by URL filtering-based security solutions if the encrypted traffic was not inspected.

- **Organisations should inspect all SSL-based traffic as far as possible to ferret out hidden attacks.** A multi-layered defense-in-depth strategy should be adopted with capability on SSL/TLS inspection to enhance the protection against threats concealed in encrypted channels.

Source: Zscaler

[9] https://info.zscaler.com/resources-industry-reports-state-of-encrypted-attacks

Industry Insight on Cyber Security Threat Trends

Detection on threats related to COVID-19 increased six times in Q2 2020

McAfee published the report "McAfee Labs Threats Report"[10], which summarised their analysis on threats identified in the second quarter of 2020. The major observations were:

- **Six times increase in COVID-19 themed threats were detected in Q2 2020 compared with the first quarter.** On average, 419 threats were detected in every minute, accounting for a surge of around 12% as compared to Q1 2020. There was an increase of 117% and 103% in new PowerShell malware and Office malware respectively. Growth in new malicious signed binaries, Coin Miner malware, Linux malware, mobile malware and Internet of Things (IoT) malware were also detected. On the other hand, decrease in iOS malware, exploit malware, JavaScript malware and MacOS malware were observed.

- **Phishers targeted Microsoft OneDrive users in COVID-19 themed phishing attacks.** They impersonated government or other organisations related to the pandemic and sent phishing emails with links to malicious questionnaires, forms or other documents hosted in OneDrive, aiming to steal the OneDrive account credentials of their targets.

- **Hong Kong ranked the 9th in terms of number of cloud incidents with more than 150,000 incidents detected.** Attackers commonly targeted misconfigured cloud environments. They also abused the Instance Metadata of cloud instances for conducting data theft. To enhance cloud security, organisations should implement adequate security controls. Zero trust approach should be adopted in cloud implementation. Organisations should properly configure their cloud environments and ensure consistency in data protection and threat management strategy in their cloud platforms.

- **Attack surfaces continued to evolve and enlarged involving various devices and application stores.** For instance, threat actors expanded their malware distribution through ONE Store, a smartphone apps store in Korea. Vulnerabilities found in teleconference robots could be exploited by attackers to conduct eavesdropping, man-in-the-middle attack or remote take-over of control. System administrators should timely install patches to their systems and software libraries; adopt the principle of least privilege; implement network segregation and disconnect unnecessary network exposure to the Internet for risk mitigation.

Source: McAfee

[10] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf

Industry Insight on Cyber Security Threat Trends

Attackers employed Red Team's security tools to attack

Sophos published the "Sophos 2021 Threat Report"[11], which incorporated the analysis of malware and spam messages by professionals in area of incident response, cloud security and data science. The key findings were:

- **Cybercriminals continued to evolve ransomware to evade security solutions and spread at a faster pace.** Cybercriminals became working more cooperatively. Ransomware not only encrypted the data of victims at a higher speed, but also stole the data by sending the data to authentic cloud storage services, camouflaged the malicious activities to evade detection. It also searched for and destroyed data backups. Cybercriminals then threatened the victims for releasing sensitive data to public unless a ransom was paid. The average ransom in Q3 2020 was $233,817, a rise of more than 2.7 times compared to $84,116 in Q4 2019.

- **A steady increase in attacks on Windows servers and Linux servers were observed and this upward trend was expected to be continued.** Most of the attacks targeted servers were ransomware, cryptominer and data exfiltration. Attacks targeted Windows Remote Desktop Protocol (RDP) remained frequent. Around 4.3 million brute force RDP login attempts were detected in one month by honeypots setup in ten different geographical locations, with increasing frequency and ferocity throughout the period. Organisations should ensure RDP service was not exposed to the Internet. RDP-enabled Windows servers should be placed behind firewalls and protected by anti-malware software. Users should only be able to connect to the servers via secure VPN, and should avoid running desktop applications such as web browsers in servers. Stringent password policies should be adopted and if applicable, multi-factor authentication should be used.

- **Threat actors targeted vulnerable cloud environments.** During the recent rapid but unplanned expansion in the usage of cloud services, some cloud instances were found misconfigured with excessive access privileges and lack of visibility of cloud resources, making these cloud environments susceptible to cyber security threats.

- **The trend of threat actors using Red Team's tools, commonly used by penetration testers, to conduct malicious activities was expected to continue in 2021.** Some popular tools being misused were Metasploit, BloodHound, mimikatz, etc. Threat actors employed these tools since security solutions could not easily distinguish whether the tools were used for legitimate security assessment purpose or in performing malicious activities.

Source: Sophos

[11] https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf

Summary of Microsoft November 2020 Security Updates

12 Product Families with Patches

7 Critical

5 Important or below

Product Family	Impact[12]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4586781, KB4586785, KB4586786, KB4586787, KB4586793, KB4586830
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4586781, KB4586786, KB4586793, KB4586830
Windows 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4586808, KB4586823, KB4586834, KB4586845
Microsoft Internet Explorer	Remote Code Execution	Critical ★★★★	KB4586768, KB4586781, KB4586785, KB4586786, KB4586787, KB4586793, KB4586827, KB4586830, KB4586834, KB4586845
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4586781, KB4586785, KB4586786, KB4586787, KB4586793, KB4586830
Azure	Elevation of Privilege	Critical ★★★★	Release Notes
ChakraCore	Remote Code Execution	Critical ★★★★	Release Notes
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4484455, KB4484508, KB4484520, KB4484534, KB4486722, KB4486725, KB4486727, KB4486737, KB4486738 Microsoft Excel: KB4486718, KB4486734, KB4486743 Microsoft Word: KB4486719, KB4486730, KB4486740

[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 Office Online Server: KB4486713 Microsoft Office 2019: Click to Run Microsoft 365 Apps for Enterprise: Click to Run Microsoft Office 2019 for Mac: Release Notes
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	KB4486706, KB4486714, KB4486717, KB4486723, KB4486733, KB4486744
Microsoft Dynamics 365-related software	Spoofing	Important ★★★	KB4577009, KB4584611, KB4584612
Microsoft Exchange Server	Remote Code Execution	Important ★★★	KB4588741
Microsoft Visual Studio	Remote Code Execution	Important ★★★	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 16.7: Release Notes Microsoft Visual Studio 2019 version 16.8: Release Notes Visual Studio Code: Release Notes

Learn more:

High Threat Security Alert (A20-11-04): Multiple Vulnerabilities in Microsoft Products (November 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=526)

Sources:

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