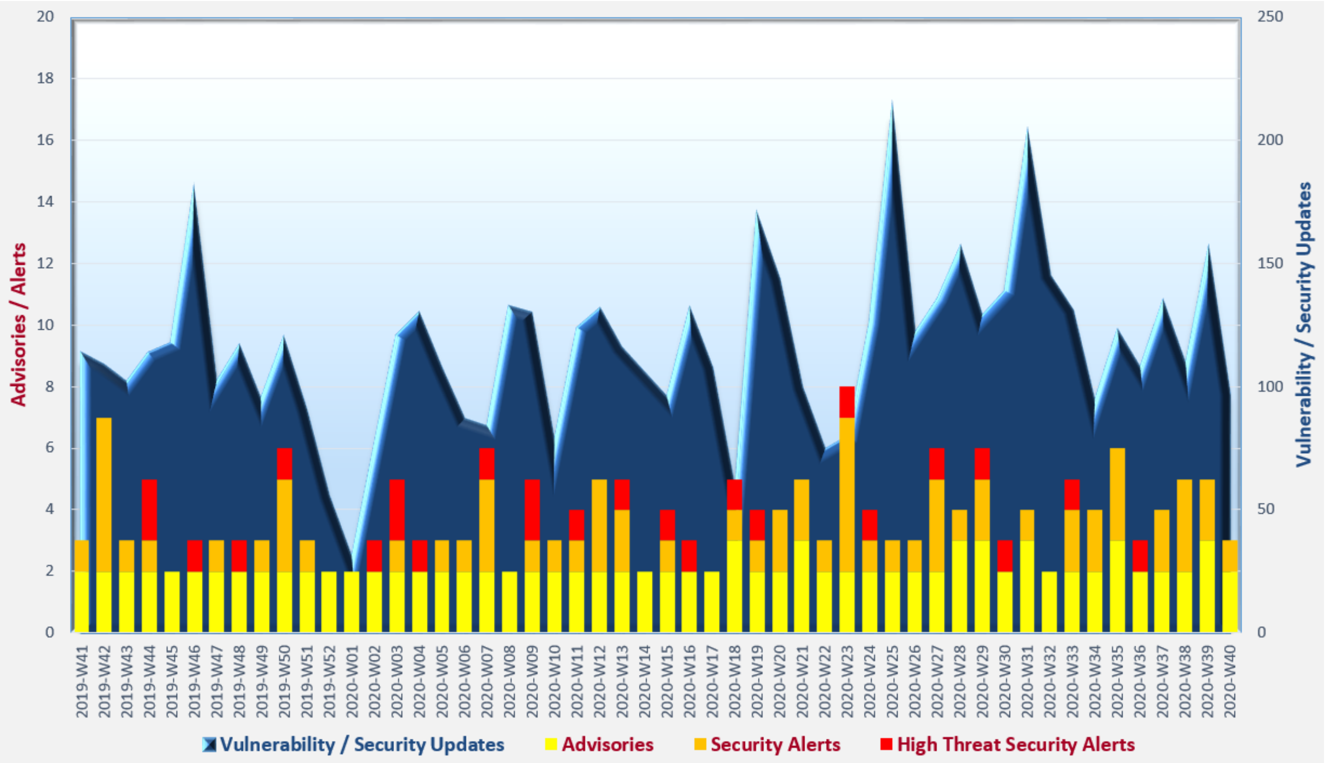
Cyber Security Threat Trends 2020-M09

September 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:

- ✧ **COVID-19 pandemic-themed threats** become the new norm. Users should raise their awareness on handling electronic messages and refrain from installing apps from untrusted sources.
- ✧ **Security software discovery** emerges as a prominent attack technique. System administrators should implement a multifaceted approach to monitor system processes as well as the usage of command-line arguments and utility tools that can capture system and network information.
- ✧ **Ransomware double extortion attack** continues causing serious threat. Organisations should endeavour to avoid ransomware infection by implementing measures such as timely software update, restrict network access and user account privileges, deploy updated endpoint security solution and educate their users in defence against attacks from malicious emails and websites.

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

CERT Advisories

Active exploitations against vulnerability in Microsoft Windows Netlogon Remote Protocol

SingCERT[2], CERT NZ[3], Australian Cyber Security Centre (ACSC)[4], Canadian Centre for Cyber Security[5], Cybersecurity and Infrastructure Security Agency (CISA)[6, 7, 8] issued alert regarding an elevation of privilege vulnerability (CVE-2020-1472) in Microsoft Windows Netlogon Remote Protocol that affected Windows Server 2008 R2 (or above) and Windows Server (version 1903 or above) with Domain Controller role. The vulnerability was exploited by attackers actively. Upon successful exploitation, the attacker could obtain domain administrator access and fully compromise the Domain Controller. System administrators should patch their affected Windows servers immediately.

Distributed Denial of Service (DDoS) and ransom DDoS campaigns worldwide

CISA[9] and SingCERT[10] issued alert/advisory to remind organisations to be cautious of DDoS attacks. Attack targets included finance, business, travel, and e-commerce industries worldwide. Attackers may send extortion email to the targeted organisations, threatening to launch an attack unless a ransom is paid. Organisations should secure their networks, minimise network exposure to the Internet, conduct vulnerability scanning regularly and fix any identified vulnerability timely. They could also consider adoption of anti-DDoS service and intrusion detection and prevention system to mitigate the risk.

Actionable reference for identifying and mitigating malicious activity

CISA[11] and cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom released a joint advisory that provided technical approaches to identify and mitigate malicious activity. The publication also covered some common mistakes in incident responding as well as other related security best practices.

[2] https://www.csa.gov.sg/singcert/alerts/al-2020-035

[3] https://www.cert.govt.nz/it-specialists/advisories/critical-windows-authentication-vulnerability-in-zerologon/

[4] https://www.cyber.gov.au/acsc/view-all-content/advisories/advisory-2020-016-zerologon-netlogon-elevation-privilege-vulnerability-cve-2020-1472

[5] https://www.cyber.gc.ca/en/alerts/microsoft-netlogon-elevation-privilege-vulnerability-cve-2020-1472

[6] https://us-cert.cisa.gov/ncas/current-activity/2020/09/14/exploit-netlogon-remote-protocol-vulnerability-cve-2020-1472

[7] https://us-cert.cisa.gov/ncas/current-activity/2020/09/18/cisa-releases-emergency-directive-microsoft-windows-netlogon

[8] https://us-cert.cisa.gov/ncas/current-activity/2020/09/24/unpatched-domain-controllers-remain-vulnerable-netlogon

[9] https://us-cert.cisa.gov/ncas/current-activity/2020/09/04/dos-and-ddos-attacks-against-multiple-sectors

[10] https://www.csa.gov.sg/singcert/alerts/al-2020-033

[11] https://us-cert.cisa.gov/ncas/alerts/aa20-245a

Industry Insight on Cyber Security Threat Trends

Ransomware attacks recorded a seven-fold increase in the first half of 2020

Bitdefender released the "Mid-Year Threat Landscape Report 2020”[12], which included their observations on threat trends in the first half of 2020. The major observations in the report were:

- **There was a 715 percent increase in ransomware attack detections during the first half of 2020 when compared to the same period in 2019.** Hackers intensified their ransomware campaigns by leveraging the COVID-19 pandemic, the increase in work-from-home workforce, and commodity ransomware provided via ransomware-as-a-service (RaaS). In addition to encrypting data for ransom, threat actors also threatened to expose the stolen data.

- **Banking Trojan attacks also increased seven-fold compared to the first half of 2019, with almost 65 percent of attacks were detected during Q2 2020.** On the other hand, the number of exploits increased by four times while the number of Potentially Unwanted Applications (PUA) and coin miners increased by 332.5 and 20.32 percent respectively.

- **Threats targeted Android increased since March 2020 as attackers spread malware via COVID-19 themed malicious Android apps**. These malicious apps counterfeited legitimate apps such as video conferencing apps and medical related apps and infected victims' devices with aggressive adware, banking Trojans, information stealers, ransomware, etc. Users should stay vigilant and refrain from downloading applications from untrusted sources, especially during the COVID-19 pandemic which was leveraged by threat actors for conducting malicious activities.

- **Attacks on Internet of Things (IoT) devices increased 46 percent from January 2020 to June 2020.** 55.73 percent of IoT network threats reported involved port-scanning attacks and 22.62 percent involved password stealing attempts. Typical issues related to IoT devices included users did not realise their IoT devices were vulnerable, weak or default passwords were used for IoT devices, lack of support from manufacturers on provision of patches for vulnerabilities, IoT devices were end of life, etc.

- **40 percent of emails related to COVID-19 were reported as spam during the first six months in 2020.** Malicious email was the top attack vector used by threat actors for cyberattack. During May and June 2020, 60 percent of the emails were found fraudulent. Threat actors continuously evolve their attack context to customise attacks targeting specific regions or people. For instance, fraudsters leveraged the gradual loosening of travel restrictions and started travel-related attack campaigns targeted travel enthusiasts.

Source: Bitdefender

[12] https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

Industry Insight on Cyber Security Threat Trends

Number of potential intrusions detected in the first half of 2020 surpassed the yearly total of 2019

CrowdStrike released the "2020 Threat Hunting Report: Insights from the CrowdStrike OverWatch Team"[13] to reveal the adversaries' tactics, techniques and procedures (TTPs) after analysing the threat data collected from millions of endpoints in the first half of 2020. The key findings were:

- **More than 41,000 potential intrusions were caught in the first six months of 2020, an upsurge of 17% compared to the total number for the whole year of 2019.** The increase in potential intrusions were resulted from the continuous growth of eCrime activities and the impact of the COVID-19 pandemic. Rapid adoption of remote workforces expanded the attack surfaces. Moreover, adversaries exploited the public fear through COVID-19 themed social engineering campaigns. Organisations should educate end users on security best practices in defending against the threat of phishing and social engineering. They should also adopt secure remote access solutions and formulate security policies for their remote workforces.

- **Dharma, Phobos, Medusa Locker, Revil (Sodinoki) and Makop were the top 5 ransomware detected in the first six months of 2020.** Availability of commodity malware through ransomware-as-a-service (RaaS) was one of the factors causing the growth in ransomware activities.

- **The "living off the land" tactic by using legitimate tools to launch attacks was the prevailing choice by threat actors for defence evasion.** Apart from those administrative tools native to the host operating systems, Process Hacker, ProcDump, Advanced IP Scanner, TeamViewer, and Advanced Port Scanner were the top 5 most common non-native tools used in interactive intrusions. Adversaries also abused penetration testing tools like Mimikatz, Cobalt Strike, PowerShell Empire, PowerSploit, Meterpreter, etc. System administrators should control over software allowed in their organisations, patch software and corresponding libraries timely, remove unused software and services, and utilise endpoint detection and response (EDR) solutions to mitigate the risks.

- **Among various attack techniques, the usage of discovery techniques became increasingly popular, especially security software discovery performed by eCrime adversaries, which was almost 3 times of the frequency for 2019**. Valid credentials were still the predominant way applied to initial access, persistence, privilege escalation and defence evasion attack stages. Organisations should enforce strong password policies, adopt multifactor authentication, as well as closely and periodically monitor authentication logs, account creation and changes in user privileges.

Source: CrowdStrike

[13] https://www.crowdstrike.com/resources/reports/threat-hunting-report-2020/

Industry Insight on Cyber Security Threat Trends

Over 50% of malware delivery attempts in the first half of 2020 were by spam email

F-Secure published the "Attack Landscape H1 2020"[14] on their study and analysis of cyber attacks in the first half of 2020. The major observations in the report were:

- **Spam email was the most prevalent method used by threat actors to distribute malware.** During the first six months of 2020, 51% of infection attempts were from spam email, increased from 43% for the same period in 2019.

- **Threat actors launched localised COVID-19 email spamming and phishing campaigns in different locations.** For instance, they impersonated public health authority in Japan to send email with malicious attachments to spread Emotet in Japan. Similar campaigns to distribute malware were found in other locations, such as spreading infostealer Lokibot in Vietnam and Remote Access Trojan (RAT) Remcos in Hong Kong. Two infostealers, Lokibot and Formbook, were found in 38% and 37% of email attachments in COVID-19 themed spam respectively. In most cases, the malicious attachments were in conventional formats like .doc, .zip, .pdf, etc. However, threat actors also used attachments with .iso, .img, .gz and .ace extensions to evade detection of email security solution.

- **Financial sector was the most commonly used by threat actors in phishing campaigns, accounted for 32% of phishing emails.** Nevertheless, 19% of phishing emails spoofed Facebook. There was an increase in phishing campaigns against cloud-based email services such as Microsoft Office 365, Google's Gmail and G-Suite. Threat actors also increasingly conducted spear phishing attacks targeted administrators of Microsoft Office 365 that aimed to control the organisations' Office 365 domain and accounts.

- **Threat actors targeted unpatched software vulnerabilities as well as insecure and exposed network connections to gain access to organisations' networks for subsequent ransomware infections.** For instance, exploitation of vulnerabilities of Pulse Secure VPN and Citrix server were observed in the first half of 2020. Double extortion tactics (i.e. in addition to encrypting the victims' data, threat actors also exfiltrated the data and threatened to expose the stolen data) were used by adversaries so as to increase the chance of receiving ransom from victims.

- **Port 23 (Telnet), 22 (Secure Shell, SSH) and 445 (Server Message Blocks, SMB) remained the top 3 targeted ports from July 2019 to June 2020.** However, peaks on attacks targeting UDP port 1900, default port for Universal Plug and Play (UPnP) and Simple Service Discovery Protocol (SSDP), were observed in March and June 2020. Both protocols were commonly used in home routers, printers and Internet of Things (IoT) devices.

Source: F-Secure

[14] https://blog-assets.f-secure.com/wp-content/uploads/2020/09/17142720/F-Secure-attack-landscape-h12020.pdf

Summary of Microsoft September 2020 Security Updates

14
Product Families with Patches

11
Critical

3
Important or below

Product Family	Impact[15]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4570333, KB4571756, KB4574727, KB4577015, KB4577032, KB4577041, KB4577049
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4570333, KB4571756, KB4574727, KB4577015, KB4577032
Windows 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4577038, KB4577048, KB4577066, KB4577071
Internet Explorer	Remote Code Execution	Critical ★★★★	KB4570333, KB4571756, KB4574727, KB4577010, KB4577015, KB4577032, KB4577038, KB4577041, KB4577049, KB4577051, KB4577066
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4570333, KB4571756, KB4574727, KB4577015, KB4577032, KB4577041, KB4577049, Release Notes
Microsoft Office-related software	Remote Code Execution	Critical ★★★★	KB4484466, KB4484469, KB4484513, KB4484517, KB4484530, KB4484532, KB4484533 Microsoft Excel: KB4484507, KB4484526, KB4486665 Microsoft Word: KB4484510, KB4484522, KB4486660 Microsoft Office 2019: Click to Run Microsoft Office Web Apps: KB4484481, KB4484518, KB4486661 Microsoft 365 Apps for Enterprise: Click to Run Microsoft Office Online Server: KB4484503

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

Product Family	Impact[15]	Severity	Associated KB and / or Support Webpages
			Microsoft Business Productivity Server: KB3101523 OneDrive: Release Notes
Microsoft SharePoint-related software	Remote Code Execution	Critical ★★★★	KB4484480, KB4484488, KB4484504, KB4484505, KB4484506, KB4484512, KB4484514, KB4484515, KB4484516, KB4484525, KB4484528, KB4486664, KB4486667
ChakraCore	Remote Code Execution	Critical ★★★★	Release Notes
Microsoft Dynamics	Remote Code Execution	Critical ★★★★	KB4574742, KB4577501, Release Notes
Microsoft Exchange Server	Remote Code Execution	Critical ★★★★	KB4577352
Microsoft Visual Studio	Remote Code Execution	Critical ★★★★	KB4571479, KB4571480, KB4571481, KB4576950 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, Release Notes Microsoft Visual Studio 2019 version 16.7: Release Notes Visual Studio Code: Release Notes
ASP.NET Core	Security Feature Bypass	Important ★★★	Release Notes
xamarin.forms	Spoofing	Important ★★★	Release Notes
SQL Server	Security Feature Bypass	Moderate ★★	Release Notes

Learn more:

Security Alert (A20-09-01): Multiple Vulnerabilities in Microsoft Products (September 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=508)

Sources:

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