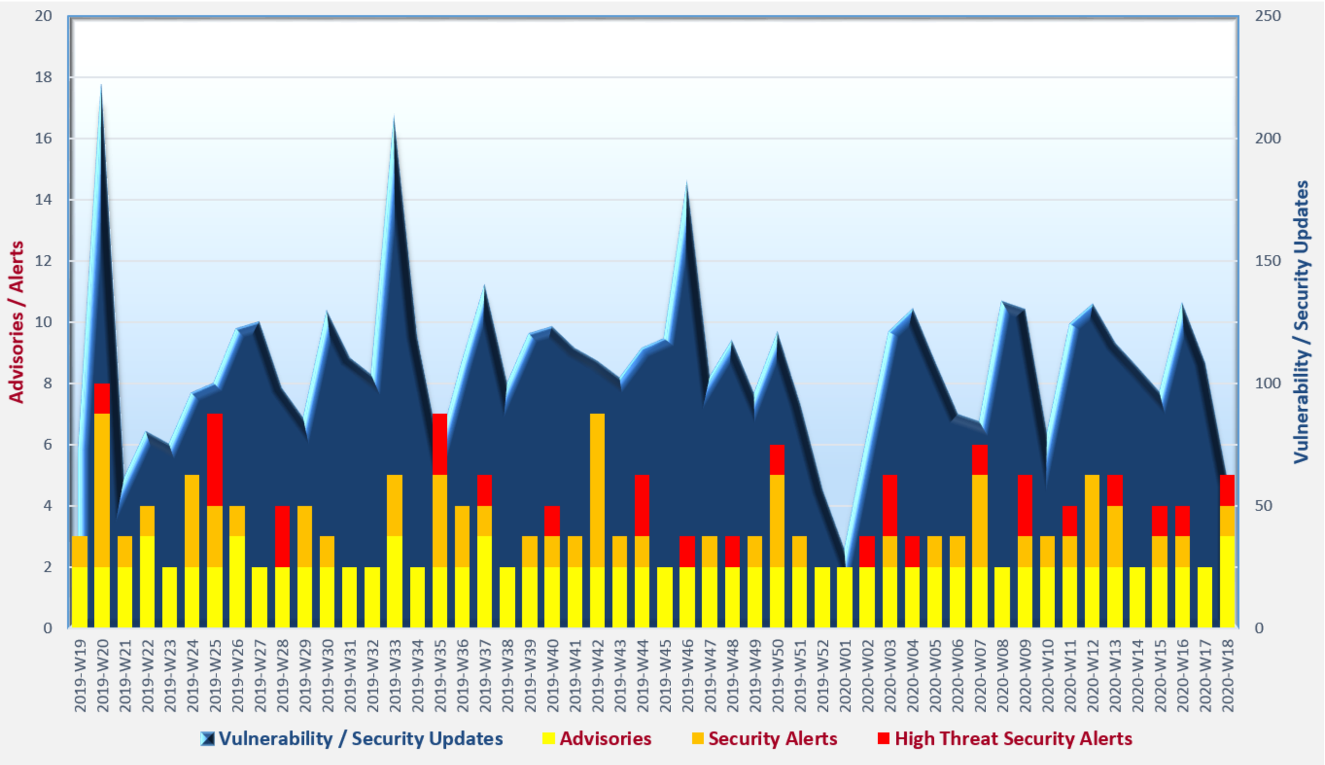
Cyber Security Threat Trends 2020-M04

April 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:

- ✧ **Threat actors** continue their attempts to exploit system vulnerabilities no matter the vulnerabilities are new or old. System administrators should timely patch known system vulnerabilities and conduct vulnerability scanning regularly to uncover any unfixed loopholes.
- ✧ **Cyber attacks related to the COVID-19 pandemic** evolve with the emergence of new phishing themes as lures. Users should always stay alert and be careful on handling any forms of electronic messages.
- ✧ **Macro-enabled documents** keep commonly used by attackers for malware delivery. Office macros should not be enabled by default when opening office documents. End users should exercise prudence in handling macro-embedded documents.

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

CERT Advisories

Stay vigilant while using video-teleconferencing (VTC) solution

HKCERT[2], MyCERT[3], Cybersecurity and Infrastructure Security Agency (CISA)[4], Canadian Centre for Cyber Security[5, 6], Australian Cyber Security Centre (ACSC)[7] and UK National Cyber Security Centre (NCSC)[8, 9, 10] issued respective advisories to remind the public potential security threats of using VTC solution. Some actionable security measures and tips were recommended, such as requiring password to join VTC meeting, adopting strong password and multifactor authentication to protect VTC account if applicable and not disclosing the VTC meeting link and password publicly. Moreover, VTC client software should be updated in a timely manner.

Remain alert to COVID-19 related cyber attacks

CISA[11], NSCS[12], SingCERT[13] and ACSC[14, 15] issued respective advisories to remind users to remain alert to cyber attacks related to COVID-19 and related themes, such as phishing attacks (via email, SMS, and other messaging channels), malware delivery (via malicious Excel documents, image files, etc.), malicious domains with name containing COVID-19 or coronavirus related wording, etc. Security measures on different areas were also suggested.

Defend against web shell malware

Threat actors were increasingly using web shell malware to establish remote access and execute arbitrary system commands on targeted web servers. Due to the difficulties to detect malicious web shells through passive web monitoring, ACSC[16] and CISA[17] jointly published a guidance to advise organisations and system administrators on the detection, prevention and mitigation of web shell malware.

[2] https://www.hkcert.org/my_url/en/blog/20040201

[3] https://www.mycert.org.my/portal/advisory?id=MA-782.042020

[4] https://www.us-cert.gov/ncas/current-activity/2020/04/02/fbi-releases-guidance-defending-against-vtc-hijacking-and-zoom

[5] https://www.cyber.gc.ca/en/alerts/considerations-when-using-video-teleconference-products-and-services

[6] https://www.cyber.gc.ca/en/staying-cyber-safe-while-teleworking

[7] https://www.cyber.gov.au/publications/web-conferencing-security

[8] https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations

[9] https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely

[10] https://www.ncsc.gov.uk/blog-post/video-conferencing-new-guidance-for-individuals-and-for-organisations

[11] https://www.us-cert.gov/ncas/alerts/aa20-099a

[12] https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

[13] https://www.csa.gov.sg/singcert/publications/capitalising-on-covid19-pandemic

[14] https://www.cyber.gov.au/advice/covid-19-protecting-your-small-business

[15] https://www.cyber.gov.au/advice/covid-19-cyber-security-tips-when-working-home

[16] https://www.cyber.gov.au/advice/detect-and-prevent-web-shell-malware

[17] https://www.us-cert.gov/ncas/current-activity/2020/04/22/nsa-asd-release-guidance-mitigating-web-shell-malware

Industry Insight on Cyber Security Threat Trends

Proper cybersecurity hygiene practices make organisations less vulnerable to cyber attacks

Lares released their "2019 Top 10 Penetration Test Findings Report”[18]. The report was based on the data collected from hundreds of engagements in 2019. The highlights from the report included:

- **The 10 most common penetration test findings were:**
  - **Brute Forcing Accounts With Weak and Guessable Passwords**
  - **Kerberoasting**
  - **Excessive File System Permissions**
  - **WannaCry/EternalBlue**
  - **Windows Management Instrumentation (WMI) Lateral Movement**
  - **Inadequate Network Segmentation**
  - **Inappropriate Access Control**
  - **Post-Exercise Defensive Control Tuning**
  - **Malicious Multifactor Enrolment or Multifactor Authentication (MFA) Bypass**
  - **Phish-in-the-Middle (PiTM)**

  All of them could be avoided by better cybersecurity hygiene practices such as properly configured security policies, password policies, network segmentation and account privileges, frequent review of audit logs, timely system patching and hardening, etc.

- **Organisations could implement multifactor authentication to mitigate the risk of brute force attacks on user accounts.** Nevertheless, organisations should adopt an appropriate enrolment process if self-enrolment was allowed. Enrolment period for self-enrolment of new accounts should be limited. Organisations could also consider to require a second authorisation factor in the enrolment process.

- **Least privilege principle should be adopted to user and system accounts.** This could help in avoiding security issues such as Excessive File System Permissions, Inappropriate Access Control and WMI Lateral Movement. In addition, routine review and audit on account privileges and file access permissions should be adopted.

- **Organisations should implement proper segmentation on their networks to reduce attack surface.** The internet accessible zone and other untrusted networks such as organisation’s guest wireless network should be isolated from the internal networks. Host-based firewalls on all servers and workstations should be deployed as far as practicable. Besides, system patching and hardening should be performed on a regular and timely basis to protect systems from system vulnerabilities.

Source: Lares

[18] https://www.lares.com/lares-top-10-penetration-test-findings-for-2019/

Industry Insight on Cyber Security Threat Trends

COVID-19 pandemic themed phishing campaigns surged in Q1 2020

Cofense released the "Q1 2020 Phishing Review"[19] on their analysis and observations of phishing campaigns and trends in the first quarter of 2020. The key findings were:

- **Information stealers were the top malware type identified in phishing campaigns in Q1 2020.** These malware families were largely used in phishing campaigns related to COVID-19 pandemic in which a large number of attackers adopted simple or open-sourced information stealer families.

- **Office macro-enabled documents remained the most commonly used malware delivery mechanism in phishing.** The second common delivery mechanism was the Equation Editor vulnerability (CVE-2017-11882), which was patched in 2017, showing that attackers still took chance to impact organisations which failed to patch their system completely. There was a rising trend in usage of GuLoader delivery mechanism. GuLoader typically downloaded DLL files from trusted source, used them to create malicious binaries and eventually executed the binaries in system memory of infected systems.

- **The COVID-19 themed phishing email campaigns skyrocketed.** Threat actors masqueraded various global and local organisations in different industries such as healthcare, education, logistics, etc. Nevertheless, the complexity of malware and delivery mechanisms in these campaigns diversified, ranging from simple email attachments with low evasion capability to more complex infection chains involving several different loaders in sequence. Multiple COVID-19 themed ransomware campaigns utilised tactics such as URL shortening, URL redirects, and password protected files and evaded detection by secure email gateways of organisations.

- **Some phishing campaigns leveraged trusted sources such as cloud service or customer surveys as part of the infection chain.** Organisations were suggested to adopt threat intelligence, network sandbox, content-filtering, harden network access control and organise security awareness training to educate staff in identification and reporting on phishing emails to mitigate the risk.

- **COVID-19 themed phishing email campaigns were expected to continue, with phishing campaigns related to US election were expected to grow.** Due to global pandemic and economic downturn, it was anticipated more novice threat actors would participate in phishing and ransomware attacks. Healthcare, education, small business and governments would continue to be main targets of ransomware attacks.

Source: Cofense

[19] https://go.cofense.com/q1-2020-phishing-review/

Industry Insight on Cyber Security Threat Trends

Organisations need to patch their systems faster

Automox released their "The 2020 Cyber Hygiene Report: What You Need to Know Now"[20]. The report included their analysis results based on survey returns from 560 IT operations and security professionals in more than 15 industries and government agencies. The key findings were:

- **81 percent of surveyed organisations suffered data breach in past two years.** The top 5 root causes opined by the respondents were phishing attack (36%), missing patch on OS (30%), missing patch on an app (28%), OS misconfiguration (27%) and insider threat (26%). Three of these top root causes could be addressed with better endpoint patching and hardening.

- **Organisations did not patch their systems fast enough.** Security experts recommended organisations to patch their vulnerable systems within 3 days for critical vulnerabilities. However, less than half of surveyed organisations were able to meet the recommended timeframe. About 15 percent of the respondents could not patch their systems within 30 days. The recommended time for organisations to patch and harden their systems to stop zero-day attacks was 24 hours after disclosure but only about 20 percent of survey respondents met the target. The time to patch remote desktop and laptop computers were even longer.

- **Surveyed organisations were more confident on cyber hygiene of on-premise systems and SaaS cloud applications.** On the contrary, they concerned about patching and hardening of Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) devices, application containers and Bring Your Own Devices (BYOD) mobile devices, as these systems were difficult to reach and their existing patching and hardening systems were designed for on-premises systems and did not cover remote and mobile devices, cloud-based systems and operational technology systems.

- **96 percent of surveyed organisations had some or full automation for system hardening.** 23 percent had fully automated system hardening, but 4 percent had no automation. 46 percent required certain amount of manual configuration changes for system hardening. 43 percent of surveyed organisations which hardened their systems daily or hourly adopted fully-automated hardening practices. There was a strong correlation between automation and the ability to harden the systems more frequently. Organisations should automate their patching and hardening processes as much as possible to better protect their computer systems.

Source: Automox

[20] https://www.automox.com/lp/2020-cyber-hygiene

Summary of Microsoft April 2020 Security Updates

13
Product Families with Patches

9
Critical

4
Important or below

Product Family	Impact[21]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4549949, KB4549951, KB4550922, KB4550927, KB4550929, KB4550930
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4549949, KB4549951, KB4550922, KB4550929
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4550917, KB4550951, KB4550957, KB4550961, KB4550964, KB4550965, KB4550970, KB4550971
Internet Explorer	Remote Code Execution	Critical ★★★★	KB4549949, KB4549951, KB4550905, KB4550917, KB4550922, KB4550927, KB4550929, KB4550930, KB4550951, KB4550961, KB4550964
Microsoft Edge (EdgeHTML-based)	Remote Code Execution	Critical ★★★★	KB4549949, KB4549951, KB4550922, KB4550927, KB4550929, KB4550930
Microsoft SharePoint-related software	Remote Code Execution	Critical ★★★★	KB4011581, KB4011584, KB4484291, KB4484292, KB4484293, KB4484297, KB4484298, KB4484299, KB4484301, KB4484307, KB4484308, KB4484321, KB4484322
Microsoft Dynamics-related software	Remote Code Execution	Critical ★★★★	KB4538593, KB4549673, KB4549674, KB4549675, KB4549676, KB4549677, KB4549678, KB4557699, KB4557700
ChakraCore	Remote Code Execution	Critical ★★★★	Release Notes

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

Product Family	Impact[21]	Severity	Associated KB and / or Support Webpages
Microsoft Business Productivity Server	Remote Code Execution	Critical ★★★★	KB2553306
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB3128012, KB3162033, KB3203462, KB4011097, KB4011104, KB4032216, KB4462153, KB4462210, KB4462225, KB4464527, KB4464544, KB4475609, KB4484117, KB4484125, KB4484126, KB4484132, KB4484167, KB4484214, KB4484226, KB4484229, KB4484235, KB4484238, KB4484244, KB4484246, KB4484258, KB4484260, KB4484266, KB4484269, KB4484273, KB4484274, KB4484281, KB4484283, KB4484284, KB4484285, KB4484287, KB4484290, KB4484294, KB4484295, KB4484296, KB4484300, KB4484319 Microsoft Office 2019: Click to Run Microsoft Office 365 ProPlus: Click to Run Microsoft Office 2016 & 2019 for Mac: Release Notes Microsoft AutoUpdate for Mac: Security Update OneDrive for Windows: Release Notes
Microsoft Apps-related software	Elevation of Privilege	Important ★★★	Microsoft Remote Desktop for Mac: Release Notes Microsoft RMS Sharing for Mac: Release Notes Microsoft Your Phone Companion App for Android: Release Notes
Microsoft Research JavaScript Cryptography Library	Security Feature Bypass	Important ★★★	Release Notes
Microsoft Visual Studio	Elevation of Privilege	Important ★★★	Microsoft Visual Studio 2019 v16.0: Release Notes Microsoft Visual Studio 2019 v16.4: Release Notes

Product Family	Impact[21]	Severity	Associated KB and / or Support Webpages
			Microsoft Visual Studio 2019 v16.5: Release Notes Microsoft Visual Studio 2017: Release Notes Microsoft Visual Studio 2015 Update 3: KB4540102

Learn more:
High Threat Security Alert (A20-04-03): Multiple Vulnerabilities in Microsoft Products (April 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=468)

Sources:

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