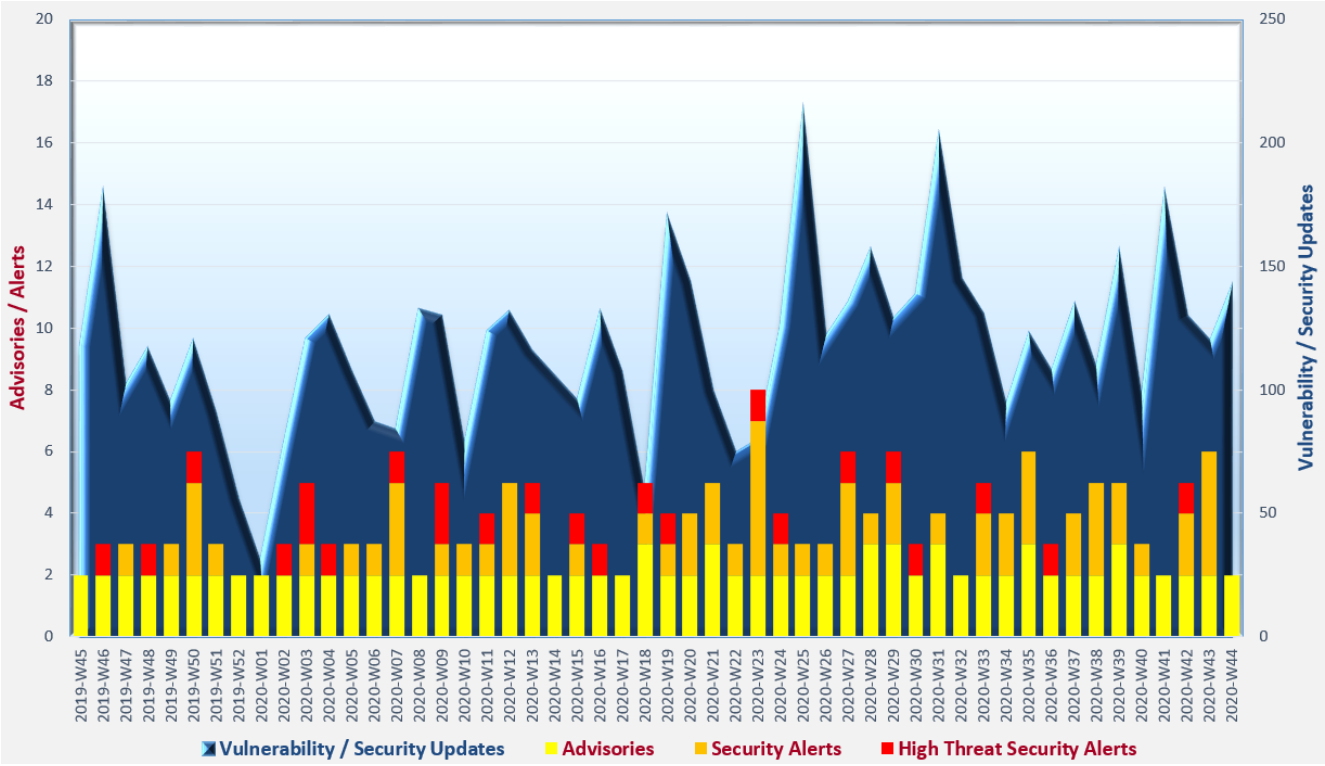
TLP:WHITE

Cyber Security Threat Trends 2020-M10

October 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:

- ✧ Result of a survey conducted by a web application security solution provider showed that **over one-third of organisations did not conduct security scan for all of their web applications**. Organisations should regularly conduct penetration test, security risk assessment and audit to detect and rectify security loopholes of their applications.
- ✧ **Rapid transition to remote workforce insecurely and usage of personal devices to access organisations' network** introduce security risk to organisations. Secure Virtual Private Network (VPN) and multi-factor authentication (MFA) should be adopted for work from home arrangement.
- ✧ **Phishing** continues to impose serious security threats to organisations and end users. Organisations should continuously educate staff in defence against phishing attacks. Users should always stay alert in handling links or attachments in electronic messages.

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

CERT Advisories

Active exploitations against vulnerability in Oracle WebLogic server

GovCERT.HK[2], SingCERT[3], and CERT NZ[4] issued alerts regarding vulnerabilities (CVE-2020-14750, CVE-2020-14882, CVE-2020-14883) in Oracle WebLogic server which were exploited actively. Proof-of-concept (PoC) code for exploiting these vulnerabilities was publicly available. The vulnerabilities, CVE-2020-14750 and CVE-2020-14882, were remotely exploitable without authentication. Successful exploitation could allow attacker to take over the affected system. System administrators should refer to product vendor's recommendations, and install the patches immediately.

Security tips for protecting social media and instant messaging accounts

HKCERT[5] published an article to help users to protect their social media and instant messaging accounts for minimising the risk of identity theft. Actionable security tips included using different passwords for different accounts; adopting 2-factor authentication or 2-step verification if available; using "private" mode of web browser, logout the accounts and close the web browser after use, etc.

The trend of double extortion ransomware attacks continued

HKCERT[6] consolidated recent threat intelligence and published an update on the latest trend of double extortion ransomware attacks. Ransomware attacks targeted a wide variety of industries including education, banks, hospitals, governments, utility companies, etc. The Maze ransomware and Netwalker ransomware were found using the double extortion approach actively. These ransomware exploited vulnerability that existed in VPN solutions. Organisations should patch their systems timely to mitigate the risks. Phishing email with malicious links or malicious attachments was the most prominent method to distribute ransomware. Computer users should stay vigilant to suspicious emails with links or attachments.

[2] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=521
[3] https://www.csa.gov.sg/singcert/alerts/al-2020-041
[4] https://www.cert.govt.nz/it-specialists/advisories/oracle-weblogic-server-vulnerability-being-exploited/
[5] https://www.hkcert.org/my_url/en/blog/20102801
[6] https://www.hkcert.org/my_url/en/blog/20101301

Industry Insight on Cyber Security Threat Trends

37% of surveyed organisations did not conduct security scans for all of their web applications

Netsparker published the report "New Vulnerability Found: Executive Overconfidence"[7], which concluded a survey performed in July 2020 on web application security. The major observations were:

- **Only 63% of surveyed organisations conducted security scans for all web applications regularly.** 25% of respondents indicated they intentionally skipped web applications which they considered as less important and 10% of respondents could not scan all web applications due to resources or technical limitations. This imposed the risk that vulnerability of unscanned applications could not be identified timely for rectification.

- **About half of the respondents indicated their organisations could not clear the backlog of vulnerabilities of their web applications timely.**

- **Executives' expectations on organisations' web application security were over-optimistic, comparing with the response on actual practices performed by security professionals and web application developers.** For instance, about 75% of surveyed executives expected that all web applications of their organisations were scanned but in practice, almost 45% of surveyed security professionals opined that their organisations did not regularly conduct security scans on all of their web applications. Another divergence existed on the views from executives and developers on clearance of vulnerability backlogs. Almost two-third of surveyed DevOps staff indicated vulnerabilities of their web applications could not be rectified timely, while only less than 42% of executives were aware of the situation.

- **Security and development personnel had different perceptions towards web application security.** Around 58% of security personnel opined that automatic escalation of unaddressed high threat security issues was in place whereas less than 40% of development personnel shared the same view. On the other hand, almost half of the security personnel respondents considered web application developers were reluctant to incorporate security in application development. Only 20% of surveyed developers concurred and had the same opinion.

- **Organisations were recommended to adopt security by design approach to incorporate security elements in the early stage of system design and throughout the application development lifecycle.** They were also recommended to conduct regular security scanning on all web applications to facilitate identification and rectification of security vulnerabilities.

Source: Netsparker

[7] https://www.netsparker.com/executive-overconfidence-web-application-security-survey-report/

Industry Insight on Cyber Security Threat Trends

Rapid changes of technology, process and workforce exposed weaknesses

Secureworks released the report "Pandemic-Driven Change: The Effect Of COVID-19 On Incident Response"[8], which included the analysis of incident response cases and the evolution of cyber threat during the COVID-19 pandemic. The major observations in the report were:

- **During pandemic, threat actors changed their tactics to use COVID-19 as lure to conduct phishing campaigns via email and SMS.** They also increased scanning activity to identify flaws in Virtual Private Network (VPN) and cloud applications and shifted their targets to healthcare, pharmaceutical and government organisations.

- **Cyber risk increased as organisation shifted to remote workforce rapidly without proper security control in place.** Organisations failed to deploy multi-factor authentication (MFA) in time to support the sudden increase of remote users. Many organisations could not patch their systems and remote access services timely. Due to limited VPN bandwidth or inadequate VPN solutions, some organisations allowed remote users to bypass the VPN and access SaaS applications directly, or used VPN Split Tunneling that allowed applications or devices to access the Internet directly. Some organisations also shifted to cloud-based collaboration services hurriedly without proper system hardening or enabling of security features.

- **Use of personal devices for remote work introduced security issues.** These personal devices were normally with less security control and monitoring, unencrypted, unpatched, without strong password, with USB ports enabled and operated with local admin rights. System administrators lacked of visibility on these un-administered devices, making monitoring, investigation or isolation on these devices highly difficult.

- **Organisations were recommended to adopt MFA for all services as far as possible.** They should also review and update their Bring Your Own Device (BYOD) policies, Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP) periodically and when necessary. Organisations could deploy Endpoint Detection and Response (EDR) tools for detection and protection against malicious activities and Mobile Device Management (MDM) solution for managing, monitoring and securing the mobile devices. Organisations should provide secure remote access channel for their employees. Furthermore, they should update employees on pandemic-related topics regularly; offer information security awareness training including topics on remote office security, proper use of VPN and mobile devices, prevention of social engineering attacks, etc.; and provide guidance to employees on work from home.

Source: Secureworks

[8] https://www.secureworks.com/resources/rp-effect-covid19-incident-response

Industry Insight on Cyber Security Threat Trends

Phishing attack was still at high level in Q3 2020

Cofense published the "Q3 2020 Phishing Review"[9] on their analysis and observations of phishing campaigns and trends in the third quarter of 2020. The major observations in the report were:

- **Keylogger was the top malware phenotypes by volume in Q3 2020, followed by Information Stealer and Remote Access Trojan (RAT).** There was an increase in ransomware related phishing attacks in Q3 2020. Some of the ransomware could steal victims' data and launched double extortion attacks.

- **Emotet resumed activity in Q3 2020 with new ability and adjusted tactics.** It improved its evasion capability by hash manipulation. It also broadened their targets by customising their phishing email with more different languages and sending phishing emails from more different domains. 337 unique sender top level domains were found in August 2020, surpassed the former high (259) in late 2019. The number of unique sender addresses observed in August 2020 increased dramatically to 120,500, nearly doubled the figure in 2019.

- **Office macros remained the most commonly used malware delivery mechanism in phishing.** There was a huge increase in usage of office macros in Q3 due to the growth of Emotet activity starting in July 2020. Equation Editor vulnerability (CVE-2017-11882) and GuLoader were the second and third top malware delivery mechanism respectively.

- **PDF files were the most common file types found in phishing email attachments, followed by HTML files and ZIP files.** Microsoft Office documents embedded with malicious macros were also common, occupied six out of the top ten most commonly found file extensions. Phishers employed improved tactics to evade the detection of Secure Email Gateways (SEG) to deliver the malicious files to end users' machines. For instance, some phishing emails included links to cloud services or cloud storage from which malicious files would be downloaded when the links were clicked. Users should stay vigilant to phishing electronic messages and be cautious before clicking any link or opening any attachment.

- **The COVID-19 themed phishing campaigns dropped slowly from the peak in April 2020.** However, these kind of campaigns were expected to continue, with healthcare organisations mostly targeted. Further outbreak of COVID-19 could lead to resurgence of pandemic themed campaigns. Mis-configured or vulnerable cloud services were expected to be increasingly targeted, as organisations accelerated the adoption of cloud service since COVID-19 pandemic but often misconfigured the security features of their new cloud services.

Source: Cofense

[9] https://go.cofense.com/q3-2020-phishing-review/

Summary of Microsoft October 2020 Security Updates

12 Product Families with Patches

6 Critical

6 Important or below

Product Family	Impact[10]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4577041, KB4577049, KB4577668, KB4577671, KB4579311, KB4580327, KB4580328, KB4580330, KB4580346
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4577668, KB4577671, KB4579311, KB4580346
Windows 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4580347, KB4580353, KB4580358, KB4580382
Microsoft Office-related software	Remote Code Execution	Critical ★★★★	KB4484417, KB4484435, KB4486682, KB4486688, KB4486700, KB4462175, KB4486689 Microsoft Excel: KB4486678, KB4486695, KB4486707, KB4462175 Microsoft Word: KB4486679, KB4486692, KB4486701, KB4486703 Microsoft Outlook: KB4484524, KB4486663, KB4486671 Microsoft Office 2013 Click-to-Run (C2R): Click to Run Microsoft Office 2019: Click to Run Microsoft 365 Apps for Enterprise: Click to Run Microsoft Office Online Server: KB4486674 Microsoft Office 2016/2019 for Mac: Release Notes
Microsoft SharePoint-related software	Remote Code Execution	Critical ★★★★	KB4484531, KB4486676, KB4486677, KB4486687, KB4486694, KB4486708

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

Product Family	Impact[10]	Severity	Associated KB and / or Support Webpages
3D Viewer	Remote Code Execution	Critical ★★★★	Release Notes
Microsoft Dynamics 365-related software	Spoofing	Important ★★★	KB4578105, KB4578106
Microsoft Exchange Server	Information Disclosure	Important ★★★	KB4581424
Microsoft .NET Framework	Information Disclosure	Important ★★★	KB4578968, KB4578969, KB4578971, KB4578972, KB4578974, KB4579976, KB4579977, KB4579978, KB4579979, KB4579980, KB4580327, KB4580328, KB4580330, KB4580346, KB4580467, KB4580468, KB4580469, KB4580470
Azure Network Watcher Agent virtual machine extension for Linux	Elevation of Privilege	Important ★★★	Release Notes
PowerShellGet	Security Feature Bypass	Important ★★★	Release Notes
Visual Studio Code	Remote Code Execution	Important ★★★	Release Notes

Learn more:

Security Alert (A20-10-01): Multiple Vulnerabilities in Microsoft Products (October 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=516)

Sources:

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