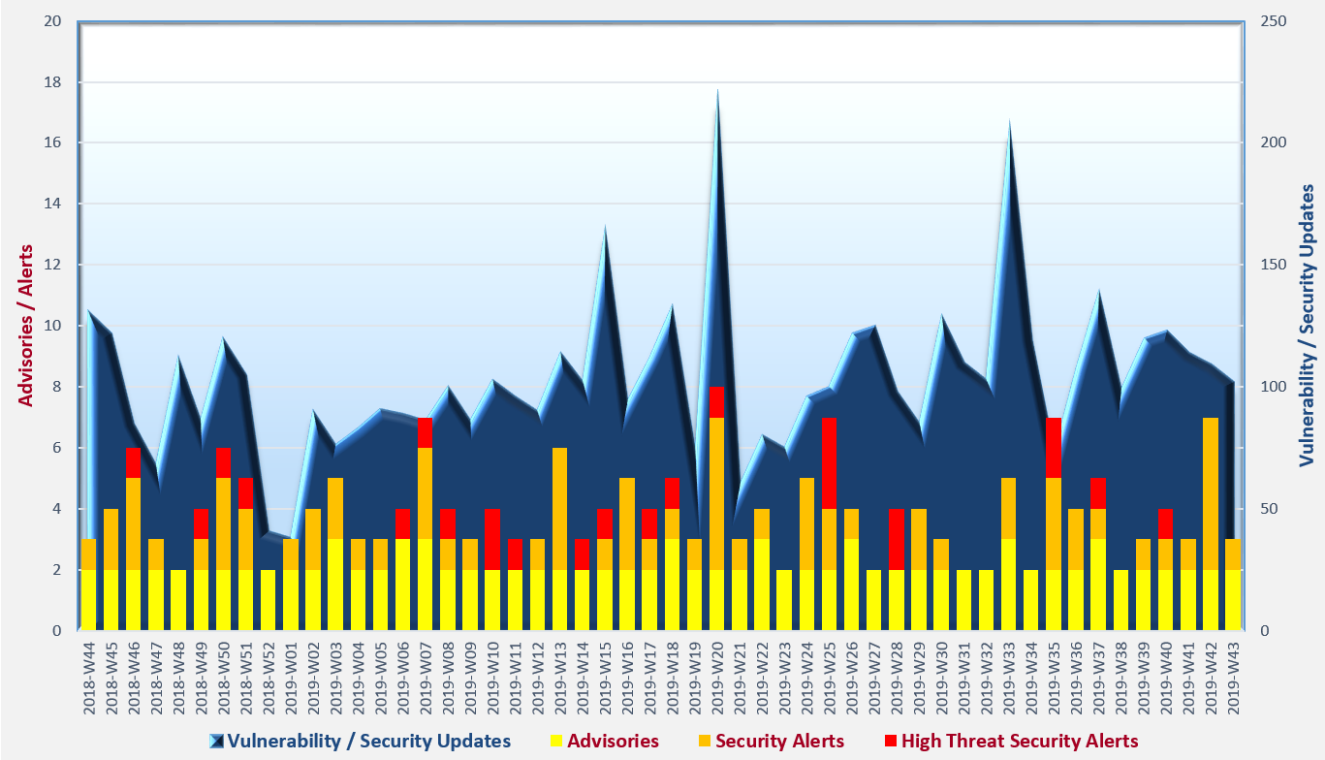
TLP:WHITE

Cyber Security Threat Trends 2019-M10

October 2019

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:

- ✧ **Phishing links** deployed from trusted domains and over Hyper Text Transfer Protocol Secure (HTTPS) sessions are widely adopted in attacks. End users should be trained to validate sources of emails and web links to defend phishing attacks.
- ✧ **Known software vulnerabilities** are often exploited by cyber criminals to compromise systems. Organisations should patch their systems timely and refrain from using de-supported software.
- ✧ **Web defacement** is frequently suffered by Internet-facing websites. Website owners should regularly review and strengthen the security functionalities and mechansims of their web applications and hosting platforms.

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

CERT Advisories

Reinforce website encryption and authentication by properly configuring Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS)

Australian Cyber Security Centre (ACSC)[2] issued guidelines on how to implement certificates, TLS and HTTPS. These included how to select cipher suites, encryptions methods, and certificates, the use of HTTP Strict Transport Security (HSTS) header, the transition to TLS 1.3, and so on.

Measures to protect against common cyber security incidents

ACSC[3] issued a guide on how to increase the security resilience of organisations against cyber security threats. Topics such as automatic update to operating systems and software applications, regular backup of business data, usage of Multi-Factor Authentication, access control, strong passphrases, security awareness training, and so on were covered.

Secure your email systems

The UK National Cyber Security Centre (NCSC)[4] issued guidelines about email security and anti-spoofing for IT managers and systems administrators. The first aspect was to implement anti-spoofing controls, such as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC). The second aspect was to implement Transport Layer Security (TLS) for incoming and outgoing emails.

Number of malware hosting and phishing events dropped in Q3 2019, but cases of defacement increased, mentioned in the latest HKCERT quarterly report

HKCERT released its Hong Kong Security Watch Report (Q3 2019)[5]. The number of malware hosting events decreased from 48,892 in Q2 to 17,273 in Q3, and number of phishing events also decreased from 1,306 in Q2 to 849 in Q3. However, the number of defacement events increased by more than 200%. Detail analysis results on the trend for defacement, phishing, malware hosting and botnet were presented in the report. Protection measures were suggested in the report, including patch the systems timely, follow best practices on user account and password management, disable unnecessary services, and so on.

[2] https://www.cyber.gov.au/publications/implementing-certificates-tls-and-https
[3] https://www.cyber.gov.au/publications/small-business-cyber-security-guide
[4] https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing
[5] https://www.hkcert.org/my_url/en/blog/19102101

Industry Insight on Cyber Security Threat Trends

Only 49% of organisations used encryption to protect their sensitive data in the cloud despite the usage of cloud increased continuously

Thales and Ponemon Institute analysed survey returns from 3,346 IT and IT security practitioners to understand the trends in cloud governance and security practices. The observations and insights derived from the analysis results were published in the "2019 Thales Cloud Security Study"[6]. The research results indicated that organisations have difficulties in applying security measures to their cloud environment. More details were presented below:

- **48% corporate data of the surveyed organisation were stored in the cloud,** increased from 43% in 2017. Regarding the type of corporate data stored in the cloud, 60% of the surveyed organisation stored customer information in the cloud, followed by business emails (48%) and consumer data (46%), although 46% and 33% of the respondents considered that storing customer information and consumer data in the cloud were risky. Only 49% of the organisations encrypted their data stored in the cloud.

- **32% of the surveyed organisation did not adopted any security-first approach for their data stored in the cloud.** Only 23% of the surveyed organisation considered security as a factor when choosing cloud provider.

- **72% of the surveyed organisation committed to protect their confidential or sensitive information in the cloud,** but only 50% of them established clearly defined roles and accountability for safeguarding such information in the cloud.

- **78% of respondents believed that it was important to own their encryption keys,** but only 53% of the surveyed organisation were in control of the encryption keys for the data encrypted in the cloud.

- **56% of respondents opined that it was more difficult to protect sensitive and confidential information when using cloud services, increased from 49% in last study.** They opined that it was difficult to apply the traditional information security practice in cloud environment, unable to inspect the cloud service providers directly and more difficult in user access control.

Source: Thales and Ponemon Institute

[6] https://www.thalesesecurity.com/2019/cloud-security-research

Industry Insight on Cyber Security Threat Trends

95% of detected malware was unique to a single PC, implying signature-based anti-malware technologies could not effectively detect such malware with polymorphic nature

Webroot captured and analysed the data and threat intelligence they collected and published the analysis results in its "2019 Threat Report Mid-Year Update"[7] report. The following were the highlights from the report:

- **Over 1.5 million unique phishing websites were detected in the first half of 2019. 29% of detected phishing sites used Hypertext Transfer Protocol Secure (HTTPS) protocol.** Attackers used this method to trick users into believing they were browsing trusted web sites. Users should understand that web site using HTTPS did not mean that the web site was "safe" and should be aware of the trick to avoid falling into the pitfall. The top 3 categories of phishing websites used HTTPS were education (77%), cryptocurrency (48%), and streaming (48%).

- **Malware targeting Windows 7 increased drastically by 71% when compared with 2018.** It was because attackers aimed at older operating systems, with a view to exploit unpatched vulnerabilities. In fact, the infection rate of Windows 7 base device was around 0.12 infections per device, around double of that of Windows 10 base device which was 0.05 infections per device.

- **24% of malicious URLs were found on trusted domains.** Attackers hijacked genuine websites to host malicious content, not only making them more difficult to be blocked by security measures, but also lowered the visitors' awareness on these malicious web pages hosted on recognisable domains.

- **1 out of every 50 URLs was found to be malicious.** The figure was worth to be aware of, given that over 85% of people clicked around 100 URLs everyday on average.

- **76% of malware on Windows system were found in three directories, viz, %temp%, %appdata%, and %cache%.** It was therefore suggested to enforce Windows policies to block file execution from %temp% and %cache%, so as to prevent infection on Windows based endpoint devices to a certain extent.

Source: Webroot

[7] https://mypage.webroot.com/2019-threat-report-update.html

Industry Insight on Cyber Security Threat Trends

Do not just focus on fixing newly discovered security issues but forget old vulnerabilities

Veracode assessed and analysed more than 85,000 applications, 1.4 million scans, and almost 10 million security findings from 1 April 2018 to 31 March 2019, and published the study results in its "State of Software Security report Volume 10"[8]. The major observations in the report were:

- **83% of applications were found to have at least 1 security flaw, and 20% of applications had high-severity flaws**. 68% of applications could not pass Open Web Application Security Project (OWASP) Top 10 vulnerabilities compliance testing, while 67% of applications failed in SANS 25 compliance testing.

- **Information Leakage (64%), cryptographic issues (62%), and CRLF (Carriage Return Line Feed) injection (61%) were the top 3 types of flaw.** Over the past 10 years, the three types of flaw that increased the most were CRLF injection (from 25% to 61%), insufficient input validation (from 7% to 48%), and Credentials Management (from 18% to 45%).

- **Organisations were only capable to fix 56% of the software security issues discovered.** The fix rate varied for different flaw categories. The fix rates for OWASP Top 10 vulnerabilities and SANS 25 software errors were 58.6% and 60.7% respectively.

- **The median time to fix flaws discovered in application was 59 days.** 30% of security flaws could be fixed in the first 2 weeks after they were discovered. However, there were some old security findings left unfixed for a long time, making the average time to remediate (TTR) became longer, at 171 days.

- **The prevalence of flaw for application developed by different programming languages varied.** 47% of applications developed in Python and 34% of JavaScript applications were found with no flaws. On the contrary, only 5% of Android applications and 8% of PHP applications did not have any security flaws discovered.

- **DevSecOps, which integrated software development, IT operations, and security, could be used to reduce security debt.** For applications that were scanned for 12 or fewer times a year (i.e. less than monthly), the median TTR was 68 days. When the scanning frequency increased to more than 260 scans a year, the median TTR reduced to 19 days, representing a 72% reduction.

Source: Veracode

[8] https://www.veracode.com/state-of-software-security-report

Industry Insight on Cyber Security Threat Trends

89% of the top 100 Distributed Denial of Service (DDoS) attack types were multi-vector attacks

CenturyLink monitored around 1.2 million unique active threats and correlated these threats with around 139 billion NetFlow sessions and 771 million Domain Name System (DNS) queries on a daily basis during the first half of 2019. The analysis results were published in its "2019 Threat Report"[9]. The observations in the report included:

- **Botnets continued to be a major security concern.** The continuous growth of Internet of Things (IoT) devices, such as home security cameras, smart appliances, etc., offered a rich resource of potential infection targets for botnets because they were easy to access and their security protection features were limited. In the first half of 2019, significant increases in unique Command and Control hosts for Mirai and Gafgyt were detected. In addition, some botnets continued to evolve to become more sophisticated and resilient. It was always a good practice to change the default password and disable unnecessary services of the devices.

- **DNS was a potential attack vector that was easily overlooked.** Cybercriminals could launch DNS related attacks such as DNS tunnelling for data exfiltration, DNS hijacking to manipulate DNS resolution, and the usage of Domain Generation Algorithms (DGA) to generate domains to change Command and Control infrastructure to evade detection, etc. System administrators were recommended to take defensive measures including monitor DNS traffic and looked for any malicious DNS activity.

- **In the first half of 2019, for the top 100 DDoS attack types, 89% of the attacks were multi-vector. The largest DDoS attack size was 430 Gbps, the longest DDoS attack duration was 9 days 4 hours and 40 minutes while the average attack size and duration was 25 Gbps and 1 hour and 51 minutes respectively.** DDoS was commonly used by cybercriminals to cause service delay or even service stoppage to their targets. On some occasions, culprits employed DDoS to try-out their targets' response to attack. An increasing trend of burst attacks that lasted for less than one minute was observed, indicating threat actors tried to evade detection by anti-DDoS solution.

- **The United States, China, India, Russia and Vietnam were the top five countries tracked with cumulative threats.** Hong Kong was ranked as the 8th and the 10th location with hosts containing phishing sites and hosts distributing malware respectively.

Source: CenturyLink

[9] https://www.centurylink.com/asset/business/enterprise/report/2019-threat-research-report.pdf

Summary of Microsoft October 2019 Security Updates

13 Product Families with Patches

7 Critical

6 Important or below

Product Family	Impact[10]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4517389, KB4519338, KB4519998, KB4520004, KB4520008, KB4520010, KB4520011
Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1903)	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4519998 Windows Server 2019: KB4519338 Windows Server v1803: KB4520008 Windows Server v1903: KB4517389
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4519976, KB4519985, KB4519990, KB4520002, KB4520003, KB4520005, KB4520007, KB4520009
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4517389, KB4519338, KB4519998, KB4520004, KB4520008, KB4520010, KB4520011
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4519974, KB4520002 IE 10: KB4519974, KB4520007 IE 11: KB4517389, KB4519338, KB4519974, KB4519976, KB4519998, KB4520004, KB4520005, KB4520008, KB4520010, KB4520011
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore: Security Update Guide
Azure App Service on Azure Stack	Remote Code Execution	Critical ★★★★	Azure App Service on Azure Stack: Security Update Guide
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010 SP2: KB4475569 Microsoft Office 2013 and 2013 RT: KB4475558

[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
			Microsoft Office 2016: KB4475554 Microsoft Office 2019 Security Update: Click to Run Microsoft Office 2016 & 2019 for Mac Security Update: Release Notes Microsoft Office 365 ProPlus Security Update: Click to Run Office Online Server: KB4475595 Microsoft Excel 2010: KB4484130 Microsoft Excel 2013 SP1 & 2013 RT SP1: KB4484123 Microsoft Excel 2016: KB4484112 Excel Services: KB4462176
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	Microsoft SharePoint Foundation 2010 SP2: KB4484131 Microsoft SharePoint Foundation 2013 SP1: KB4475608, KB4484122 Microsoft SharePoint Enterprise Server 2013: KB4462215 Microsoft SharePoint Enterprise Server 2016: KB4484111 Microsoft SharePoint Server 2019: KB4484110
Open Enclave SDK	Information Disclosure	Important ★★★	Open Enclave SDK: Security Update Guide
Microsoft Dynamics 365	Spoofing	Important ★★★	Microsoft Dynamics 365: KB4515519
SQL Server Management Studio	Information Disclosure	Important ★★★	SQL Server Management Studio 18.3 & 18.3.1: Security Update Guide
Windows Update Assistant	Elevation of Privilege	Important ★★★	Windows Update Assistant: Security Update Guide

Learn more:

High Threat Security Alert (A19-10-01): Multiple Vulnerabilities in Microsoft Products (October 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=424)

Sources:

- Microsoft October 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/28ef0a64-489c-e911-a994-000d3a33c573)