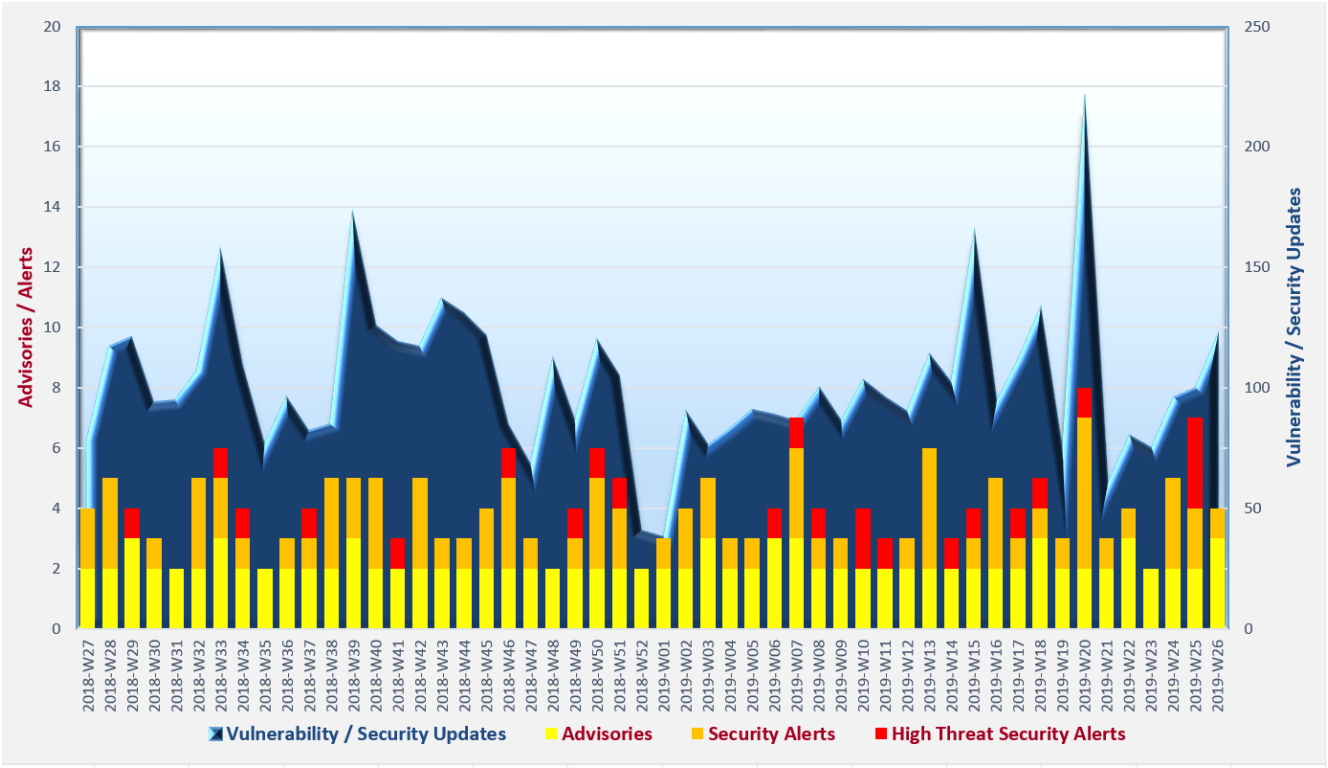
TLP:WHITE

Cyber Security Threat Trends 2019-M06

June 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:

- ✧ **Ransomware** is still a serious threat to organisations and users. Regular and offline backup should be performed. Organisations could consider implementing automated backup solutions.
- ✧ Culprits always target to **compromise user credentials**. Users should use complex passwords, change their passwords regularly and use multi-factor authentication wherever applicable. They should not reuse the same password for multiple online services.
- ✧ Increase in **cloud platform** adoption is inclined to lead to more cloud-based security incidents. Cloud governance mechanism and usage policy should be established when deploying the technologies to mitigate the risks.

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

CERT Advisories

Be aware of new trends of Ransom email attacks

HKCERT[2] issued an alert on ransom email attacks, in which the email pretended to be sent from the email accounts of the recipients themselves. The content of the email varied, such as claiming the attackers had "hacked" the recipients' computers, and asked the recipients to pay a ransom. In fact, the claimed hacking activity never happened. The ransom emails were sent randomly. Users were advised to regularly update their computing devices, install security software, change password periodically, use multi-factor authentication and perform regular offline backup.

Patch your Firefox

GovCERT.HK[3,4], HKCERT[5,6] and US-CERT[7,8] issued alerts on vulnerabilities (CVE-2019-11707 and CVE-2019-11708) found in Firefox, which were being exploited in the wild. Remote attackers could tempt users using vulnerable browser to visit malicious web pages to exploit the vulnerabilities. System administrators should patch the affected systems immediately.

Non-email sending (parked) domains should be protected

NCSC[9] issued an advice to protect non-email sending (parked) domains against being used to send spam email. Suggested actions included creating a Sender Policy Framework (SPF) record with no permitted senders, including a DMARC Policy of Reject, creating a null Mail Exchange (MX) record and applying a wildcard Domain Keys Identified Mail (DKIM) key.

Be aware of the Ryuk ransomware

NCSC[10] issued an advisory on Ryuk ransomware campaigns which targeted organisations globally. System administrators could reference the advisory for mitigation and protection against the malware.

[2] https://www.hkcert.org/my_url/en/blog/19060601
[3] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=399
[4] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=401
[5] https://www.hkcert.org/my_url/en/alert/19061901
[6] https://www.hkcert.org/my_url/en/alert/19062102
[7] https://www.us-cert.gov/ncas/current-activity/2019/06/18/Mozilla-Releases-Security-Updates-Firefox-and-Firefox-ESR
[8] https://www.us-cert.gov/ncas/current-activity/2019/06/20/Mozilla-Releases-Security-Updates-Firefox-and-Firefox-ESR
[9] https://www.ncsc.gov.uk/blog-post/protecting-parked-domains
[10] https://www.ncsc.gov.uk/news/ryuk-advisory

Industry Insight on Cyber Security Threat Trends

Don't just rely on automated detection technologies in defence against phishing; human intelligence also plays an important role

Cofense analysed millions of emails and malware samples every day, and presented the observations and analysis on phishing and malware threats in the "Phishing Threat and Malware Review 2019"[11]. The highlights from the report included:

- **90% of verified phishing emails, which were reported by users, were found in environments using secure email gateways (SEG).** These phishing emails evaded detection by those SEG and layers of defence controls and reached the inbox of users, who found and reported these suspicious emails. Organisations should understand that although technical solutions could contribute a lot in phishing defence, they could not offer 100% immunity against phishing. Continuous education to users with latest anti-phishing knowledge still needed.

- **Threat actors improved their evasion and infection techniques.** In some phishing campaigns, the payloads performed differently in different geolocations, trying to impede analysis by security solution providers. An increase in using legitimate link shorteners to hide malicious payload locations was observed. There was another observation that threat actors used .ISO files and .NET executables trying to bypass security controls. Some phishers used CAPTCHA on their phishing sites to prevent content analysis.

- **Cloud file sharing platforms were abused to host and spread malicious content.** Since more and more organisations adopted these cloud file sharing platforms, it was less likely the links to these platforms were blocked. Users became more accustomed to download contents from these file sharing platforms. Moreover, automated URL analysis tools had difficulties to determine whether the link to the cloud file sharing platform was malicious, especially if user credentials were required.

- **These was a change in attack tactics regarding Business Email Compromise (BEC).** Instead of targeting the senior executives of organisations, attackers now impersonated ordinary employees to request payroll administrators to change their payroll bank information.

- **Various courses of action could be adopted to protect against phishing and malware,** including educating users, in particular on new tactics, techniques, and procedures (TTPs) of threat actors, enabling multifactor authentication and apply patch to the systems timely.

Source: Cofense

[11] https://cofense.com/phishing-threat-malware-review-2019/

Industry Insight on Cyber Security Threat Trends

More than 90% of surveyed organisations invested in machine learning (ML) and/or artificial intelligence (AI) to tackle advanced cyber security threats

CyberEdge surveyed 1,200 IT security decision makers and practitioners of organisations with more than 500 employees in 19 industries of 17 countries in North America, Europe, Asia Pacific, the Middle East, Latin America and Africa. Their responses were studied, analysed and summarised in the "2019 Cyberthreat Defense Report"[12]. The highlights from the report included:

- **Security analytics was the most-wanted security management and operations technology for 2019,** with 46.9% of organisations planned to acquire such technologies. This echoed the survey respondents' replies that the top inhibitor to establish effective cyberthreat defences was there were too much data needed to be analysed. User and entity behaviour analytics (UEBA) and Full-packet capture and analysis were ranked at the second (36.5%) and third (35.0%) places respectively.

- **Application development and testing was rated as the most deficient functional security capabilities for three consecutive years.** Application containers were considered as the IT component which was the most difficult to secure. IT security vendors continued to innovate tools to improve and automate the application development and testing process including Static application security testing (SAST), Software composition analysis (SCA), Dynamic application security testing (DAST), and Mobile application security testing (MAST).

- **56.1% of surveyed organisations infected with ransomware, up from 55.1% last year.** 45% of victims decided to pay for the ransom, increased from 38.7% last year. Organisations should implement automated backup solutions to mitigate the damage caused by ransomware.

- **In this year's survey, 78% of organisations had their global network been successfully compromised by a cyberattack within the past 12 months.** However, referring to last year's survey results, only 62.3% of respondents thought that their organisations' network were likely of being successfully attacked in the same 12 months period.

- **94.4% of surveyed IT security organisations acquired solutions using ML / AI technologies.** 81.1% of respondents agreed that the ML / AI technologies could help their organisations to detect advanced cyber threats.

- **84.2% of organisations were experiencing a shortage of qualified IT security employee,** as compared with the 80.9% last year. Recruiting high calibre security talent was one of the most serious challenges facing by many organisations.

Source: CyberEdge

[12] https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

Industry Insight on Cyber Security Threat Trends

SQL Injection (SQLi) was the most popular attack vector for web application, accounting for 65.1% of the attacks

Akamai analysed web application firewall alerts collected in the 17 months period between November 2017 and March 2019, and published their findings in the report "Web Attacks and Gaming Abuse Report"[13]. Details of the report were:

- **SQL Injection (SQLi) and the Local File Inclusion (LFI) attacks were the two major attacks against web application,** accounting for 65.1% and 24.7% of the attacks respectively. Cross-site scripting (XSS), PHP Injection (PHPi), and Remote File Inclusion (RFI) were relatively small in numbers and accounted for 8.4% of total number of attacks.

- **SQLi attacks grew much faster than other types of attack,** from 44% of web application layer attacks in the first quarter of 2017, to 65.1% in the reporting period.

- **The United States was the top source as well as the top target country in terms of web application attacks.** The second and third source countries of attack were Russia and Netherlands, while the second and third target countries were the United Kingdom and Germany. The term source countries only meant the location where the attack traffic originated from. The actual attackers might not present in the source countries to launch the attacks.

- **There were 55 billion credential stuffing attacks detected during the report period, in which 12 billion attacks targeted gaming sites.** Attackers tried to access and takeover accounts in the attacks. Many of the attacks were initiated from botnets, or All-in-One (AIO) attack applications. These attacks targeted login forms, APIs, etc. using combination lists of usernames and passwords.

- **Some organisations have already applied expanded authentication options such as multifactor authentication (MFA), open authorisation (OAuth), and hardware-based authenticator tokens to protect against credential stuffing attacks.** However, some of them allowed their users to opt to use these authentication options, leaving the accounts of those users opted not to use the options remain more vulnerable to credential stuffing attacks. Users should also avoid re-using password in multiple web sites.

Source: Akamai

[13] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-report-2019.pdf

Industry Insight on Cyber Security Threat Trends

Research results indicated that organisations lacking visibility on usage of cloud applications by their employees

Symantec surveyed 1,250 cloud and IT security decision makers in 11 countries worldwide, including the US, the UK, Australia, Japan, Singapore, etc. By analysing and correlating the survey responses and the data from the vendor's own products and services, the research result was published in the "Cloud Security Threat Report"[14]. Findings of the report included:

- **Actual number of cloud apps used in organisations was nearly 4 times larger than the amount organisations perceived.** This indicated organisations could not have a complete visibility on cloud apps being used in the organisations, which could lead to higher chance of data loss or leakage, as 39% of these "Shadow IT apps" were considered as unsuitable for business use.

- **73% of respondents experienced at least one cloud security incident due to immature security practices.** These included use of personal accounts, lack of multi-factor authentication (MFA) or data loss prevention (DLP) services, etc. The research found that 65% of organisations did not use MFA on Infrastructure-as-a-Service (IaaS) and 80% did not use encryption. Besides, 54% of respondents believed that the cloud security maturity of their organisation was unable to keep up with the rapid expansion of cloud apps deployed.

- **53% of the organisations migrated their computing workloads to the cloud, but 49% believed their cloud security manpower was inadequate.** 92% of them would like to enhance cloud security skills in their organisations.

- **93% of respondents opined that sensitive and compliance-related data were over-shared.** They estimated that 35% of files should not be shared in the cloud environment. **68% of respondents confirmed or believed with strong evidence that their company data were available for sale on the Dark Web.** Only 31% believed that their data were safe.

- **Organisation could adopt a number of best practices for building cloud security strategy.** These included developing a cloud governance strategy to establish and enforce security policies on cloud usage, embracing a Zero-Trust model, promoting shared responsibility, using automation and artificial intelligence wherever possible, and adopting DevSecOps to integrate security practices within the software development processes and information technology operations. Organisations could also consider adopting Cloud Access Security Brokers (CASB).

Source: Symantec

[14] https://resource.elq.symantec.com/LP=7326?inid=symc_en-post_blog_to_leadgen_form_LP-7326_cstr&CID=70138000001FmXKAA0

Summary of Microsoft June 2019 Security Updates

11 Product Families with Patches

6 Critical

5 Important or below

Product Family	Impact[15]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4503267, KB4503279, KB4503284, KB4503286, KB4503291, KB4503293, KB4503327
Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1903)	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4503267 Windows Server 2019: KB4503327 Windows Server v1803: KB4503286 Windows Server v1903: KB4503293
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4503263, KB4503269, KB4503273, KB4503276, KB4503285, KB4503287, KB4503290, KB4503292
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4503267, KB4503279, KB4503284, KB4503286, KB4503291, KB4503293, KB4503327
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4503273, KB4503287, KB4503259 IE 10: KB4503259, KB4503285 IE 11: KB4503259, KB4503267, KB4503276, KB4503279, KB4503286, KB4503290, KB4503291, KB4503292, KB4503293, KB4503327, KB4503284
ChakraCore	Remote Code Execution	Critical ★★★★	Security Update
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010 SP2: KB4462178 Microsoft Office 2019 Security Update: Click to Run Microsoft Office Online Server: KB4475511

[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 Office Web Apps 2010 SP2: KB4461621 Microsoft Office 2016 & 2019 for Mac Security Update: Release Notes Microsoft Office 365 ProPlus Security Update: Click to Run Microsoft Word 2010 SP2: KB4461619 Microsoft Word 2013 & RT SP1: KB4464590 Microsoft Word 2016: KB4464596
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	Microsoft SharePoint Foundation 2013 SP1: KB4464597, KB4464602 Microsoft SharePoint Foundation 2010 SP2: KB4464571 Microsoft SharePoint Server 2019: KB4475512 Microsoft SharePoint Server 2010 SP2: KB4461611 Microsoft SharePoint Enterprise Server 2016: KB4464594 Microsoft SharePoint Enterprise Server 2013 SP1: KB4464602
Microsoft Lync Server	Denial of Service	Important ★★★	Microsoft Lync Server 2010 & 2013: KB4506009
Microsoft Project Server	Spoofing	Important ★★★	Microsoft Project Server 2010 SP2: KB4092442
Azure DevOps Server	Spoofing	Important ★★★	Azure DevOps Server 2019: Security Update Guide

Learn more:

Security Alert (A19-06-01): Multiple Vulnerabilities in Microsoft Products (June 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=396)

Sources:

- Microsoft June 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/253dc509-9a5b-e911-a98e-000d3a33c573)