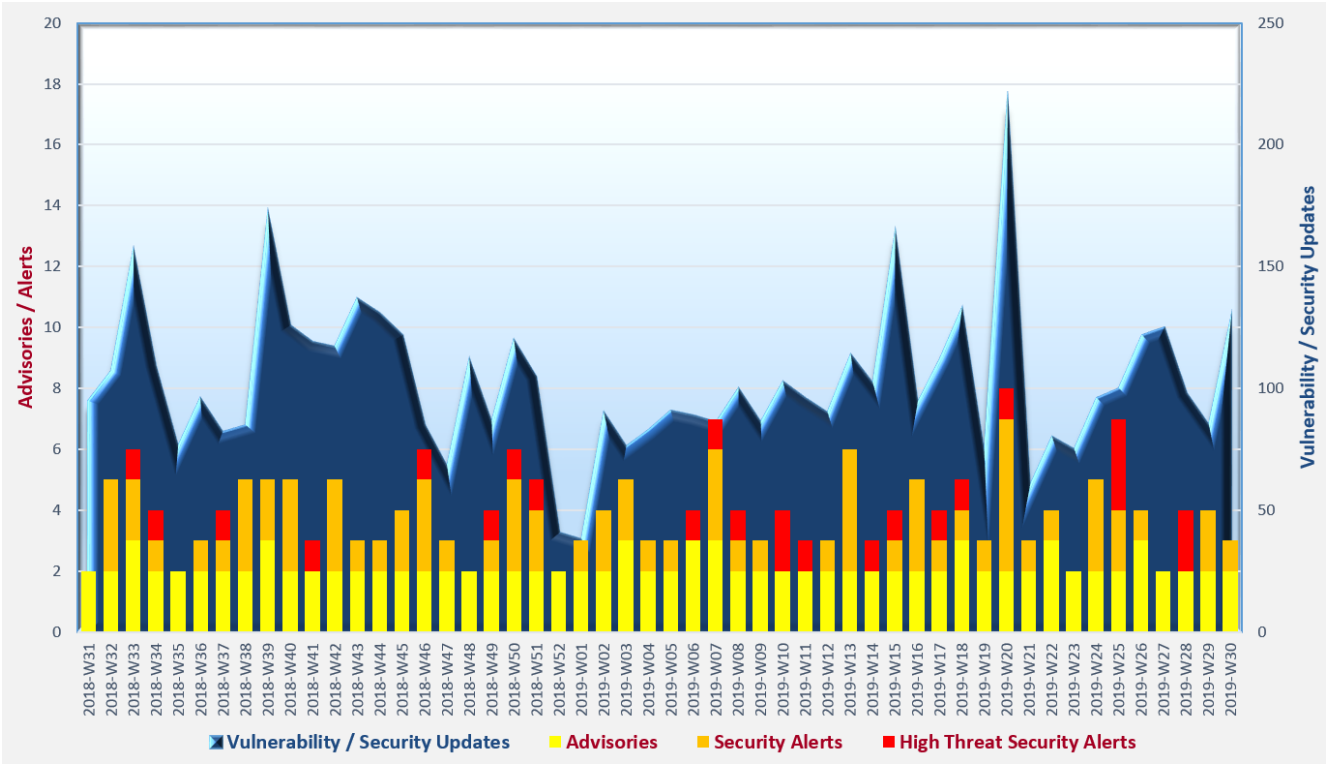
TLP:WHITE

Cyber Security Threat Trends 2019-M07

July 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:

- ✧ **Data loss and leakage** are the major cloud security concerns. Cloud resources should be properly configured and protected by strong authentication and authorisation.
- ✧ **PDF and Office documents** are common carriers of malicious scripts and macros. End users should not open attached documents from unsolicited emails or electronic messages. Execution of PowerShell scripts or Office macros should also be restricted on need basis.
- ✧ **Outdated technologies** pose risks to organisations because of lacking security updates or patches. Organisations should stop using de-supported technologies and plan for early upgrade of obsoleting technologies.

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

CERT Advisories

Protect your privacy when using mobile apps

US-CERT[2] issued a security tip on how to protect the personal information when using mobile apps, both before installing them and in their daily usage. Precautionary actions included avoiding potentially harmful apps (PHAs), reviewing the permissions each app requested, keeping the apps up to date and being cautious if social network accounts were used to sign in the apps.

Improve the quality and usability of your collected cyber security data

NCSC[3] issued a tip on the collection and analysis of cyber security related data, so as to address the most important cyber security challenges of organisations. Examples were given in the areas of data acquisition, visual exploration, automation and artificial intelligence (AI).

Safeguard your systems against ransomware attacks

US-CERT, together with other cyber security bodies in the US, released a Joint Ransomware Statement [4], which provided recommendations to protect against ransomware. The recommendations included regularly backing up all critical data and system configuration information remotely, providing cybersecurity awareness and education to staff, and revisiting and refining cyber incident response plans.

Mitigate the risk on DNS hijacking

NCSC[5] issued an advisory on the risk of DNS hijacking, such as creating malicious DNS records, obtaining SSL certificates, transparent proxying and domain hijack. Protective measures on different areas including registrar security, nameserver security and web application security were recommended.

Plan for a better patching strategy

NCSC[6] explained the importance of patching and explored the challenges and difficulties that might be encountered in patching the applications. Besides patching, some defensive measures were also suggested, including reducing attack surfaces, good IT assets management, operational risks management, effective backup mechanism on critical data, security monitoring, preparing and rehearsing incident response procedures and business continuity plans.

[2] https://www.us-cert.gov/ncas/tips/st19-003
[3] https://www.ncsc.gov.uk/blog-post/taking-a-data-driven-approach-to-cyber-security
[4] https://www.us-cert.gov/ncas/current-activity/2019/07/30/steps-safeguard-against-ransomware-attacks
[5] https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice
[6] https://www.ncsc.gov.uk/blog-post/the-problems-with-patching

Industry Insight on Cyber Security Threat Trends

Account Takeover (ATO) was a serious challenge in fraud prevention, and fraudsters participated in mobile account takeovers more vigorously

DataVisor studied 52 billion events, 1.1 billion users, 427 million IP addresses, 4.77 million /24 IP subnets, 1.46 million email domains, 5.84 million user-agent strings, 481K phone number prefixes and 263K device types during January to March 2019, and published the analysis results in its "Fraud Index Report: Q2 2019"[7]. Major observations in the report were:

- **ATO was an important cause for fraud losses.** In 2018, the fraud losses were amounted to $14.7 billion, in which $4 billion were due to ATO. 40% of fraud losses in the e-commerce sector in 2018 was caused by ATO, which almost doubled from 2017. For mobile accounts, there were around 700,000 ATO incidents in 2018, around 180% increase from 2017.

- **Password spraying, credential stuffing, social engineering, malicious software and phone hijacking were prevalent techniques to compromise accounts.** Password spraying were brute-force attacks on user credentials. User credentials with generic usernames and weak passwords were more vulnerable to this kind of attack. Users reusing the same password for multiple online services were more vulnerable to credential stuffing, as attackers attempted to login web sites or applications using leaked legitimate user credential data. Phishing remained a common social engineering attack technique. Malicious software such as keyloggers, spyware, banking Trojans, etc. were used in ATO. Many banking Trojans overlaid their malicious login page over legitimate login page of websites to steal user credentials. Phone hijacking allowed attackers to access to SMS messages that used for second-factor authentication.

- **Attackers acted stealthily and fast.** 65% of accounts compromised in ATO attacks were dormant accounts that had no login activity for more than 90 days. Detection on these attacks were difficult, as there was insufficient information to identify abnormal behaviour of these accounts. Attackers also avoided deviating significantly from the normal behaviour of the victim account owners. 20% of the compromised accounts were accessed within 300 miles of the account owners' geographic location. 72% of financial accounts were used by attackers to conduct fraudulent transactions within one hour after being compromised.

- **Proactive fraud management measures should be adopted**, such as using AI-powered unsupervised machine learning algorithms and behaviour analytics to identify potential attacks before damages were induced. Best practices for account security, such as enabling multi-factor authorisation should also be considered.

Source: DataVisor

[7] https://www.datavisor.com/intelligence-center/reports/datavisor-fraud-index-report-q2-2019/

Industry Insight on Cyber Security Threat Trends

More than 66% of devices used in small and midsize business (SMB) run on outdated or to-be-outdated Microsoft Operating System (OS) versions

Alert Logic analysed more than 1.3 petabytes of data, 10.2 trillion log messages, 2.8 billion intrusion detection system events, and 8.2 million verified security incidents and published their study results in the "Critical Watch Report SMB Threatscape 2019"[8]. The major observations in the report were:

- **More than 66% of devices were running Microsoft OS versions which were either expired or would be expired by January 2020.** The Windows OS of most of the studied device were released for more than 10 years. Outdated Linux kernels (around 50%) and email servers (more than 30%) were also found in the study. Organisations should upgrade their OS and other software to supported version with security updates.

- **42% of security issues were related to misconfigurations on encryption.** Remediation of these issues often required extended measures such as manual reviews, or a complete revamp of the system architecture. In the study, a total of 13 encryption-related misconfiguration issues were discovered, which accounted for 42% of all security issues identified.

- **66% of workload configuration issues were related to weak encryption.** Organisations often used the default encryption associated with the applications which could be outdated or insecure already. They should note that insecure encryption protocols such as MD5 (Message-Digest Algorithm), SHA-0 or SHA-1 (Secure Hash Algorithm) and DES (Data Encryption Standard) should not be used.

- **75% of the top 20 unpatched vulnerabilities were more than 1 years old,** despite there were automated patching implemented already. The use of open source software, in particular the open source software was embedded, made the patching of the vulnerabilities more difficult. Organisations could consider engaging third party validation on the software update process and conducting regular vulnerability scanning to handle this problem.

- **Secure Shell (SSH - 22/TCP), Hypertext Transfer Protocol Secure (HTTPS - 443/TCP) and HyperText Transfer Protocol (HTTP - 80/TCP) accounted for 65% of port vulnerabilities.** Organisations should close all unused ports and change the default settings and passwords. They should also conduct regular configuration checks, scans and penetration tests. Firewall should be installed on every host to monitor and filter port traffic. All devices, software or services connected to the ports should be patched and hardened.

Source: Alert Logic

[8] https://www.alertlogic.com/resources/industry-reports/critical-watch-report-smb-threatscape/

Industry Insight on Cyber Security Threat Trends

28% of organisations encountered public cloud related security incidents in the last 12 months

Security vendor Delta Risk surveyed technical executives and IT security practitioners to collect their opinions on the latest trends, key challenges and solutions for cloud security. Based on their responses, the "Cloud Security Report"[9] was prepared. The following were highlights from the report:

- **11%, 26% and 47% of the surveyed organisations opined that they were extremely confident, very confident, and moderately confident in their cloud security posture respectively.** However, the report reckoned that the findings revealed there was possibly an overconfidence in view of the security incidents and challenges identified in the report.
- **28% of organisations had security incidents related to public cloud in the last 12 months.** The types of incidents included data exposure (27%), malware infections (20%), account compromise (19%), and vulnerability exploited (17%).
- **Data loss and leakage (64%) was the top cloud security concern, slightly higher than the concern on data privacy and confidentiality (62%)**. Other concerns included legal and regulatory compliance and accidental exposure of credentials (both at 39%), data sovereignty, residency and control (35%) and incident response (29%).
- **Unauthorised access due to misuse of credentials and improper access controls, insecure interfaces and APIs (both at 42%) and misconfiguration of the cloud platform (40%) were the top three vulnerabilities of cloud security.**
- **54% of respondents believed that public cloud environments were more risky than traditional on-premises environments in terms of security breaches**, a 5% growth from last year. 22% believed that the public cloud environments were at a lower risk than on-premises environments, and 24% opined that the risk levels of the two environments were the same.
- **66% of respondents believed that their traditional security tools did not work or merely functional in cloud environments.** Organisations should adopt appropriate cloud security solutions to protect their data and resources in the cloud environments.
- **54% of organisations responded that they were hacked in the cloud.** However, 25% of the responded organisations did not know whether their cloud instances were hacked or not, which was alarming.

Source: Delta Risk

[9] https://go.deltarisk.com/2019-cloud-security-report

Industry Insight on Cyber Security Threat Trends

Rising trend on encrypted malware attacks and attacks targeted Internet of Things (IoT) continued

SonicWall investigated, analysed and explored new cybersecurity threat trends, tactics, strategies and attacks on data collected from over 1 million security sensors in nearly 215 countries and territories. It then published the findings in its report "Mid-Year Update: 2019 SonicWall Cyber Threat Report[10]". The details were:

- **Malware attacks decreased by 20%, with 4.78 billion detected cases in the first half of 2019 as compared with 5.99 billion for the same period in 2018.** Despite of a 17% decrease in malware attack cases, the United States (US) was the top victim in terms of malware attacks, with around 2.5 billion cases in the first half of 2019. This was almost 8 times of the number of detected cases of the second top victim, the United Kingdom (UK), which had 313.6 million cases.

- **2.4 million encrypted malware attacks were detected in the first half of 2019, a 76% increase over the same period in 2018.** The half-year figure was almost the same as the total amount in 2018, which was 2.8 million.

- **Ransomware attacks increased in the first half of 2019,** even though the overall figure for malware attacks decreased. There were 110.9 million cases and represented an increase of 15% over the same period in 2018, and in particular, the figure boosted up for 195% for the UK. More attackers used new tactics, such as ransomware-as-a-service (RaaS) and open-source malware kits in their attacks.

- **Attacks on IoT were on the rising trend.** The number of case were only 10.3 million in 2017, and raised substantially by 215% to 32.7 million in 2018. The figure reached 13.5 million in the first half of 2019, which was an increase of 55% over the same period in 2018.

- **Phishing attacks decreased by 19% in first half of 2019.** However, referred to figures in 2018, the attackers often chose high traffic months such as July, November and December to launch phishing campaigns.

- **Malicious PDFs and Office files such as Word documents, Excel spreadsheets, etc. continued causing damages to organisations.** About half of new or “never-before-seen” attacks were originated from malicious PDFs or Office files in February (51%) and March (47%) 2019. Macros in Office files were often exploited as attack channels to deploy malware. Users should always stay alert when opening PDFs and Office files, and should avoid opening those files from unknown and untrusted sources.

Source: SonicWall

[10] https://www.sonicwall.com/lp/2019-cyber-threat-report-lp/

Summary of Microsoft July 2019 Security Updates

19 Product Families with Patches

9 Critical

10 Important or below

Product Family	Impact[11]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4507435, KB4507450, KB4507453, KB4507455, KB4507458, KB4507460, KB4507469
Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1903)	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4507460 Windows Server 2019: KB4507469 Windows Server v1803: KB4507435 Windows Server v1903: KB4507435, KB4507453
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4507448, KB4507449, KB4507452, KB4507456, KB4507457, KB4507461, KB4507462, KB4507464
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4507435, KB4507450, KB4507453, KB4507455, KB4507458, KB4507460, KB4507469
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4507434, KB4507452 IE 10: KB4507434, KB4507462 IE 11: KB4507434, KB4507435, KB4507448, KB4507449, KB4507450, KB4507453, KB4507455, KB4507458, KB4507460, KB4507469
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore: Security Update Guide
Microsoft Visual Studio	Remote Code Execution	Critical ★★★★	Visual Studio 2010 SP1: KB4506161 Visual Studio 2012 Update 5: KB4506162 Visual Studio 2013 Update 5: KB4506163 Visual Studio 2015 Update 3: KB4506164

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

Product Family	Impact[11]	Severity	Associated KB and / or Support Webpages
			Visual Studio 2017: Download Visual Studio 2017 version 15.9: Download Visual Studio 2019 version 16.0: Download Visual Studio 2019 version 16.1: Download
Microsoft .NET Framework	Remote Code Execution	Critical ★★★★	KB4506986, KB4506987, KB4506988, KB4506989, KB4506991, KB4507411, KB4507412, KB4507413, KB4507414, KB4507419, KB4507420, KB4507421, KB4507422, KB4507423, KB4507435, KB4507450, KB4507455, KB4507458, KB4507460
Azure DevOps Server, Team Foundation Server	Remote Code Execution	Critical ★★★★	Azure DevOps Server 2019.0.1 and Team Foundation Server: Security Update Guide
Microsoft Office-related software	Remote Code Execution	Important ★★★	Microsoft Office 2010: KB4462224 Microsoft Office 2013 and 2013 RT: KB4018375, KB4464543, KB4464558 Microsoft Office 2016: KB4461539, KB4464534, KB4475514 Microsoft Office 2019 Security Update: Click to Run Microsoft Office 365 ProPlus Security Update: Click to Run Microsoft Excel 2010 SP2: KB4464572 Microsoft Excel 2013 SP1 & 2013 RT SP1: KB4464565 Microsoft Excel 2016: KB4475513
Azure IoT Edge, Microsoft Azure Kubernetes Service, Azure Automation	Elevation of Privilege	Important ★★★	Azure IoT Edge, Microsoft Azure Kubernetes Service, and Azure Automation: Security Update Guide
Microsoft SharePoint-related software	Elevation of Privilege	Important ★★★	Microsoft SharePoint Foundation 2010 SP2: KB4475510 Microsoft SharePoint Foundation 2013 SP1: KB4475527

Product Family	Impact[11]	Severity	Associated KB and / or Support Webpages
			Microsoft SharePoint Enterprise Server 2013 SP1: KB4475522 Microsoft SharePoint Enterprise Server 2016: KB4475520 Microsoft SharePoint Server 2019: KB4475529
Skype	Information Disclosure	Important ★★★	Skype for Business 2016: KB4475545
Microsoft Lync	Information Disclosure	Important ★★★	Microsoft Lync 2013: KB4475519
Microsoft Exchange	Elevation of Privilege	Important ★★★	Microsoft Exchange Server 2010 SP3: KB4509410 Microsoft Exchange Server 2013 & 2016: KB4509409 Microsoft Exchange Server 2019: KB4509408
Microsoft SQL Server	Remote Code Execution	Important ★★★	Microsoft SQL Server 2014 SP2 (GDR) : KB4505217 Microsoft SQL Server 2014 SP3 (GDR) : KB4505218 Microsoft SQL Server 2014 SP2 (CU+GDR) : KB4505419 Microsoft SQL Server 2014 SP3 (CU+GDR) : KB4505422 Microsoft SQL Server 2016 SP1 for x64-based Systems (GDR): KB4505219 Microsoft SQL Server 2016 SP2 for x64-based Systems (GDR): KB4505220 Microsoft SQL Server 2016 SP1 for x64-based Systems (CU+GDR): KB4505221 Microsoft SQL Server 2016 SP2 for x64-based Systems (CU+GDR): KB4505222 Microsoft SQL Server 2017 for x64-based Systems (GDR): KB4505224 Microsoft SQL Server 2017 for x64-based Systems (CU+GDR): KB4505225

Product Family	Impact[11]	Severity	Associated KB and / or Support Webpages
Mail and Calendar	Information Disclosure	Important ★★★	Mail and Calendar: Security Update Guide
Microsoft Identity Model	Elevation of Privilege	Important ★★★	Microsoft.IdentityModel 7.0.0: Security Update
ASP.NET Core	Spoofing	Moderate ★★	ASP.NET Core 2.1: Download ASP.NET Core 2.2: Download

Learn more:

High Threat Security Alert (A19-07-01): Multiple Vulnerabilities in Microsoft Products (July 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=405)

Sources:

- Microsoft July 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/48293f19-d662-e911-a98e-000d3a33c573)