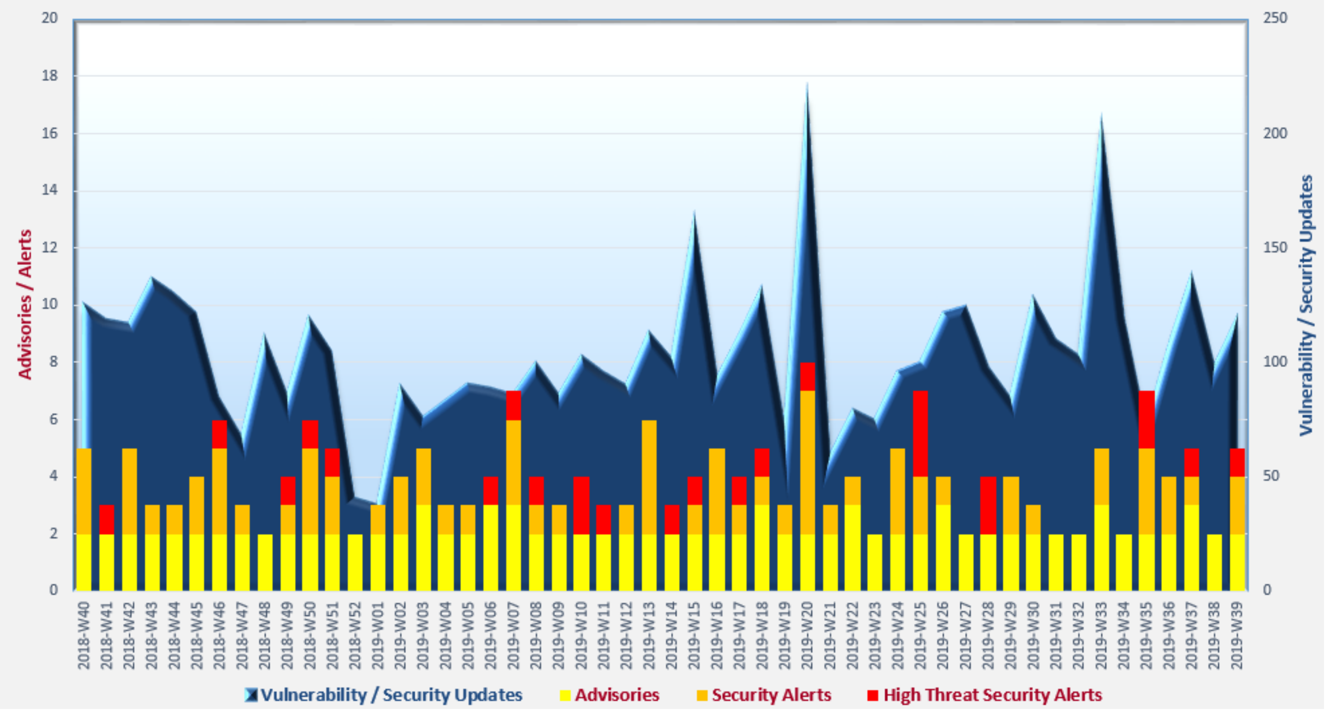
# Cyber Security Threat Trends 2019-M09

September 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:**

- ✧ **Domain Name System (DNS) amplification attacks** are on the rise. Attackers abuse the larger DNS Security Extensions (DNSSEC)-enabled response packets to generate more effective distributed denial-of-service (DDoS) traffic against target systems. Organisations should put in place applicable anti-DDoS measures to protect their critical services.
- ✧ **Phishing attacks** keep growing steadily. Business email compromise (BEC) scams against employees for financial gains is one of the major concerns. Staff should be educated to verify message authenticity before performing the requested financial transactions.
- ✧ **User credentials** are in high demand by attackers for compromising systems and identity theft. Users should use complex passwords and multi-factor authentication to protect themselves.

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

## CERT Advisories

### Be aware of Over-The-Air (OTA) phishing attacks on Android devices

SingCERT[2] issued an alert on the security flaw of OTA provisioning in Android-based devices, by which attackers could send OTA provisioning messages with rogue mobile data network settings to victims. Users were advised to stay vigilant of any OTA provisioning message prompt sent to them, enable automatic updates and install the latest security patch to their devices.

### Detect, respond to and resolve cyber incidents effectively

NCSC[3] issued guidelines on how to plan, build, develop and maintain an effective cyber incident response capability. The guidelines advised on the processes for cyber incident response, the formation of incident response team, and the technical capabilities required in the event of a cyber security incident.

### Protect the public domain names of your organisation

NCSC[4] issued guidelines on how to securely manage the public domain names owned by an organisation, including how to choose Domain Name System (DNS) registrar and DNS hosting, how to monitor DNS, the management of DNS records, and so on.

### Follow the best practices on prevention and response to data breach incident

MyCERT[5] issued an advisory on the security best practices to prevent and respond to data breach incident, including preventive measures such as security awareness training, regular patching and vulnerability assessment, etc., and the steps to be taken after a data breach incident.

### Apply latest patches to your VPN products

The Canadian Centre for Cyber Security[6] issued an alert on vulnerabilities found in various VPN products. Active exploitation against these vulnerabilities have been observed. System administrators should patch the affected systems immediately.

[2] https://www.csa.gov.sg/singcert/news/advisories-alerts/ota-provisioning-phishing-attacks-against-android-devices
[3] https://www.ncsc.gov.uk/collection/incident-management
[4] https://www.ncsc.gov.uk/guidance/managing-public-domain-names
[5] https://www.mycert.org.my/portal/advisory?id=MA-746.092019
[6] https://www.cyber.gc.ca/en/alerts/active-exploitation-vpn-vulnerabilities-0

## Industry Insight on Cyber Security Threat Trends

### Domain Name System (DNS) amplification attacks increased for more than 10 times compared with Q2 2018

Nexusguard collected and analysed information from attack data, research, publicly available information, honeypots, ISPs, and logs, and published the analysis results in its "DDoS Threat Report 2019 Q2"[7]. The key observations were:

- **DNS amplification was the top Distributed Denial of Service (DDoS) attack vector, with 8,382 cases detected and accounting for 65.95% of all DDoS attacks.** It increased for 1040.41% as compared with Q2 2018, and 31.01% as compared with Q1 2019.

- **Domain Name System Security Extensions (DNSSEC) was considered as the propeller for the large number of DNS amplification attacks.** DNSSEC was used to protect applications against malicious DNS data, e.g. those generated by DNS cache poisoning. The DNSSEC-enabled DNS responses were much larger than traditional DNS responses. Attackers took advantage of this property to conduct DNS amplification attacks by crafting malicious UDP packets with spoofed IP addresses of their targets to DNS servers. As a result, the target received a huge amount of responses and was victimised by the DDoS attack. The amplification factor of such attacks could be up to 54. As the adoption of DNSSEC continued to grow, it was expected that the rising trend of DNS amplification attack would persist.

- **HTTP Flood and HTTPS Flood were ranked as the second (7.14%) and the third (5.74%) leading attack vectors respectively.** Both of them recorded an increase for 281.51% and 363.33% respectively on a year-to-year comparison, although the number of attacks decreased by 12.78% and 36% respectively comparing to 2019 Q1.

- **74.18% of the attacks continued for less than 90 minutes.** The average attack duration in the quarter was 182.9 minutes, which was decreased by 65.57% on a quarter-to-quarter basis, and 42.50% on a year-to-year comparison.

- **91.58% of the attacks had attack size smaller than 1Gbps.** The average attack size was 0.969 Gbps, increased by 17.71% as compared with Q1 2019. The maximum attack size was 117.9 Gbps, decreased by 18.91% as compared with Q1 2019.

- **48.28% of DDoS attacks were generated from Windows-based computers and servers, and 20.48% were from iOS mobile device.** 4.38% attack were generated from Android based mobile device. 18.84% were from other device types, including IoT devices.

*Source: Nexusguard*

[7] https://www.nexusguard.com/threat-report-q2-2019

## Industry Insight on Cyber Security Threat Trends

### Bot attacks via creation of new accounts grew in the first half of 2019

LexisNexis analysed on a real-time basis the cyber-attacks it detected during the first half of 2019, and presented the observations and analysis in the "2019 Cybercrime Report"[8]. The highlights from the report included:

- **16.4 billion transactions were processed in January to June 2019, in which 62% were from mobile devices.** 277 million of the transactions were considered as human initiated/sophisticated attacks. This represented a growth of 13% for the 6-month period.

- **16.4% of new account creation transactions were considered as attacks, an increase of 24% comparing with the first half of 2018.** Fraudsters used credential information collected from data breaches to create fraudulent accounts to perform malicious activities.

- **A growing trend of bot attacks via new account creations, in particular targeting e-commerce and media was observed.** In the e-commerce fields such as online marketplaces, virtual gift card companies and ridesharing sites, the attack figures rose 171% on a year-to-year basis, and increased 305% if compared with the past 6 months. For media industry, the growth rate year-on-year and last 6 months were 123% and 65% respectively. There were considerable growth in bot attacks from India and South East Asia regions.

- **Attack rate on mobile platform (1.4%) was less than half of that on desktop platform (3.4%), mainly due to the build-in security feature of mobile devices such as the bundled biometric features.** Focusing on the mobile platform, attack rate on mobile app transactions (0.7%) were found to be 4 times lower than attack rate on mobile browser (2.9%). This was due to the pre-registration requirements or the additional layers of authentication in the mobile app. For instance, some mobile apps prevented registration from users of "jailbroken" or "rooted" phones. Nevertheless, a 144% increase from last 6 months on the attack rate of mobile app registration was detected, particularly on social media, gaming and gambling apps.

- **Geographically, most of the attacks were originated from the United States.** However, there was an apparent rise of attack sources from the growth economies such as Mexico and Brazil.

*Source: LexisNexis*

[8] https://risk.lexisnexis.com/insights-resources/research/2019-cybercrime-report

## Industry Insight on Cyber Security Threat Trends

**Software-as-a-Service (SaaS) and webmail services were the top industry sector targeted by phishing**

The Anti-Phishing Working Group (APWG) analysed the reported phishing attack cases, and complied the "Phishing Activity Trends Report, 2nd Quarter 2019"[9]. The findings in the report included the following:

- **Number of phishing sites detected slightly increased around 1% from 180,768 in Q1 2019 to 182,465 in Q2 2019.** However, the increases were remarkable when compared with the 138,328 cases in Q4 2018 and the 151,014 cases in Q3 2018. Within Q2 2019, the number of phishing sites were 59,756, 61,820 and 60,889 for April, May, and June respectively.

- **The top 3 sectors that were targeted by phishing were Software-as-a-Service (SaaS) and webmail service (36%), payment service (22%) and financial institution (18%).** There was a noticeable drop in phishing targeting cloud storage and file hosting sites, from 11.3% in Q1 2018 to 3% in Q2 2019. Phishing attacking cryptocurrency and gaming sectors, which was common in past years, diminished to insignificant levels.

- **65% of business e-mail compromise (BEC) attacks involved gift cards.** In this kind of attack, the attackers requested the victims to purchase and send the gift cards to them. This approach was increasingly adopted by the threat actors as it was less traceable and easier to cash out. Among these gift cards, those of Google Play were the most common (40.7%), followed by Steam Wallet (12.2%), Amazon (9%) and Apple iTunes (7.5%). 20% of BEC attacks requested payroll diversions and the remaining 15% of BEC attacks were about direct bank transfers. The report also indicated that there was no specific preference or inclination on BEC targets, meaning that both large and small organisations could be targeted by attackers.

- **55% of phishing sites were found to be hosted on HTTPS infrastructure.** The adoption of HTTPS by phishing sites gradually increased since 2016. Users should understand that HTTPS meant the data communication between the browser and the web site was encrypted and should not assume that a web site was safe simply because the web site adopted HTTPS.

*Source: APWG*

[9] https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf

## Industry Insight on Cyber Security Threat Trends

### 53.3% of social media logins were fraudulent

Arkose Labs analysed 1.2 billion user transactions conducted during April to June 2019 in various industries including financial services, e-commerce, travel, social media, gaming and entertainment, and prepared the "Fraud & Abuse Report Q3 2019"[10]. The following were highlights of the report:

- **Around 11% of all transactions were attacks.** The percentage of attacks on fraudulent logins, account registrations and payments were at 10.4%, 10.9% and 11.1% respectively. The report revealed that fraudulent payment and account registration attacks were more likely human driven while account takeover attacks were mostly automated attacks.

- **The United States, Russia, Philippines, Indonesia, and China were the top 5 regions from which the attacks were originated.** Except China, over 85% of the attacks from these countries were automated attacks, and the remaining were human driven attacks. For China, only 40.7% were automated attacks, and 59.3% were human driven. In terms of industries, more than half of the attacks encountered by the retail industry were human driven while more than 75% of the attacks on the gaming industry and social media were performed by automation.

- **69.1% of the transactions were originated from desktop and gaming consoles, and the remaining 30.9% were generated from mobile devices.** The attack rate for both mobile and desktop transactions were similar, with around 10.5% of the transactions were attacks.

- **Focusing on login attacks among various industries studied in the report, social media had the highest attack rate, with 53.3% of the logins found to be attacks.** The average figure across industries was 10.4%, and the individual attack rates for gaming industry, finance industry, retail and travel industry and technology industry were 10.3%, 9.1%, 5.7% and 4% respectively.

*Source:* Arkose Labs

[10] https://rsvp.arkoselabs.com/q3fraudreport/

## Summary of Microsoft September 2019 Security Updates

**17** Product Families with Patches

**8** Critical

**9** 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 ★★★★ | KB4512578, KB4515384, KB4516044, KB4516058, KB4516066, KB4516068, KB4516070 |
| **Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1903)** | Remote Code Execution | Critical ★★★★ | Windows Server 2016: KB4516044<br>Windows Server 2019: KB4512578<br>Windows Server v1803: KB4516058<br>Windows Server v1903: KB4515384 |
| **Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2** | Remote Code Execution | Critical ★★★★ | KB4516026, KB4516033, KB4516051, KB4516055, KB4516062, KB4516064, KB4516065, KB4516067 |
| **Microsoft Edge** | Remote Code Execution | Critical ★★★★ | KB4512578, KB4515384, KB4516044, KB4516058, KB4516066, KB4516068, KB4516070 |
| **Internet Explorer** | Remote Code Execution | Critical ★★★★ | IE 9: KB4516026, KB4516046, KB4520002, KB4519974<br>IE 10: KB4516046, KB4516055, KB4520007, KB4519974<br>IE 11: KB4512578, KB4515384, KB4516044, KB4516046, KB4516058, KB4516065, KB4516066, KB4516067, KB4516068, KB4516070, KB4517389, KB4519338, KB4519974, KB4519976, KB4519998, KB4520004, KB4520005, KB4520008, KB4520010, KB4520011 |
| **Microsoft SharePoint-related software** | Remote Code Execution | Critical ★★★★ | Microsoft SharePoint Foundation 2010 SP2: KB4475605<br>Microsoft SharePoint Foundation 2013 SP1: KB4484098, KB4484099 |

[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 |
|---|---|---|---|
| | | | Microsoft SharePoint Enterprise Server 2016: KB4475590, KB4475594<br>Microsoft SharePoint Server 2019: KB4464557, KB4475596 |
| **ChakraCore** | Remote Code Execution | Critical ★★★★ | ChakraCore: Security Update Guide |
| **Team Foundation Server and Azure DevOps Server** | Remote Code Execution | Critical ★★★★ | Team Foundation Server 2015 Update 4.2: Download<br>Team Foundation Server 2017 Update 3.1: Download<br>Team Foundation Server 2018 Update 1.2: Download<br>Team Foundation Server 2018 Update 3.2: Download<br>Azure DevOps Server 2019.0.1: Download<br>Azure DevOps Server 2019 Update 1: Download |
| **Microsoft Office-related software** | Remote Code Execution | Important ★★★ | Microsoft Office 2010 SP2: KB4464566, KB4475599<br>Microsoft Office 2013 and 2013 RT: KB4475607, KB4475611<br>Microsoft Office 2016: KB4475583, KB4475591<br>Microsoft Office 2019: Click to Run<br>Microsoft Office 2016 & 2019 for Mac: Release Notes<br>Microsoft Office 365 ProPlus: Click to Run<br>Microsoft Project 2010 SP2: KB4461631<br>Microsoft Project 2013 SP1: KB4464548<br>Microsoft Project 2016: KB4475589<br>Microsoft Excel 2010: KB4475574<br>Microsoft Excel 2013 SP1 & 2013 RT SP1: KB4475566<br>Microsoft Excel 2016: KB4475579 |
| **Microsoft Exchange Server 2016 (Cumulative Update 12&13) and** | Denial of Service | Important ★★★ | Microsoft Exchange Server 2019 Cumulative Update 1, 2 & 2016 Cumulative Update 12,13: KB4515832 |

| Product Family | Impact[11] | Severity | Associated KB and / or Support Webpages |
|---|---|---|---|
| **Microsoft Exchange Server 2019 (Cumulative Update 1&2)** | | | |
| **Microsoft Lync Server** | Information Disclosure | Important ★★★ | Microsoft Lync server 2013: KB4515509 |
| **Microsoft .NET Framework** | Elevation of Privilege | Important ★★★ | KB4514354, KB4514355, KB4514356, KB4514357, KB4514359, KB4514598, KB4514599, KB4514601, KB4514603, KB4514604, KB4516044, KB4516058, KB4516066, KB4516068, KB4516070 |
| **Microsoft Visual Studio** | Elevation of Privilege | Important ★★★ | Visual Studio 2015 Update 3: KB4513696<br>Visual Studio 2017 version 15.0: Release Notes<br>Visual Studio 2017 version 15.9: Release Notes<br>Visual Studio 2019 version 16.0: Release Notes<br>Visual Studio 2019 version 16.1: Release Notes |
| **ASP.NET Core** | Elevation of Privilege | Important ★★★ | .NET Core 2.1 & 2.2: Release Notes<br>ASP.NET Core 2.1, 2.2 and 3.0: Release Notes<br>ADAL.NET: Release Notes |
| **Rome SDK** | Information Disclosure | Important ★★★ | Rome SDK 1.4.1: Download |
| **Yammer for Android** | Security Feature Bypass | Important ★★★ | Yammer for Android: Security Update |
| **Nuget** | Elevation of Privilege | Important ★★★ | Nuget 5.2.0: Download |

Learn more:
High Threat Security Alert (A19-09-03): Multiple Vulnerabilities in Microsoft Products (September 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=419)

High Threat Security Alert (A19-09-05): Multiple Vulnerabilities in Microsoft Internet Explorer and Defender
(https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=421)

**Sources:**

- Microsoft September 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/24f46f0a-489c-e911-a994-000d3a33c573)