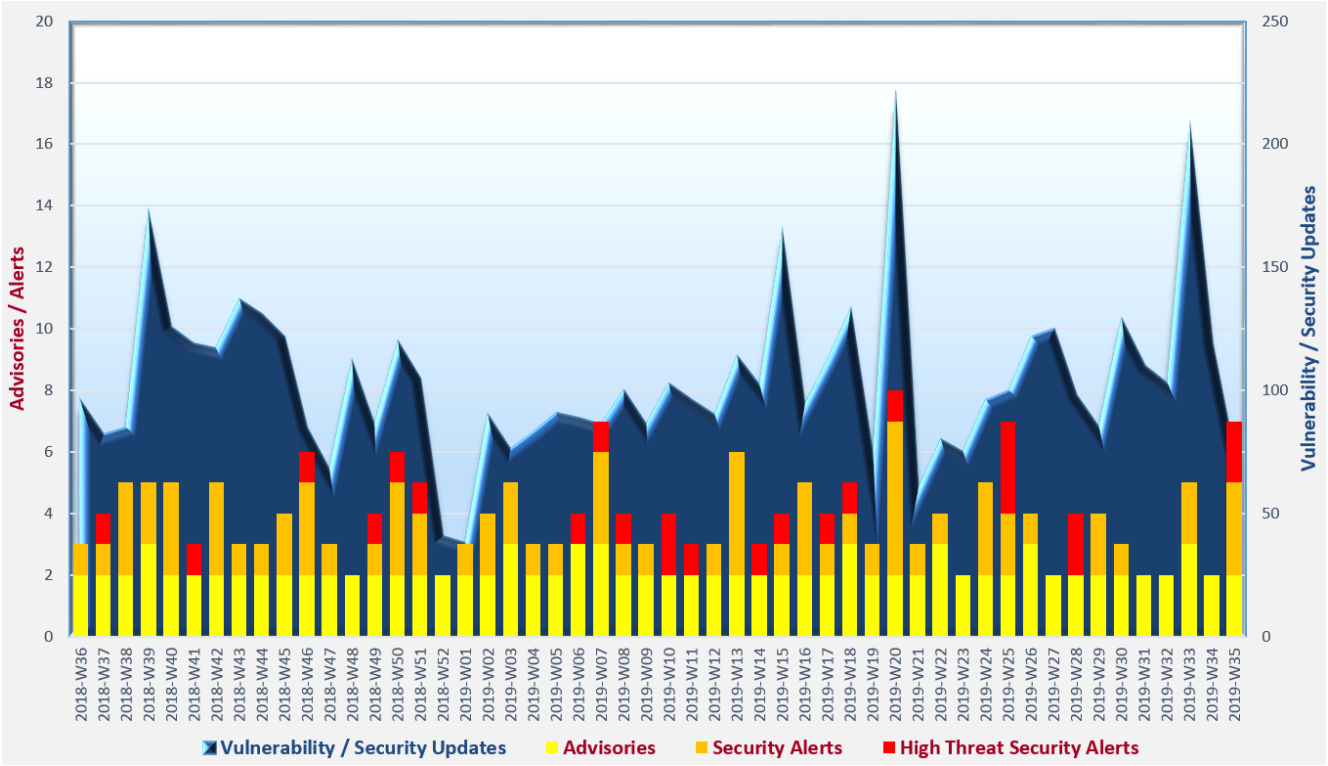
TLP:WHITE

# Cyber Security Threat Trends 2019-M08

August 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** attacks targeting organisations are on the rise. Organisations should secure their systems against remote exploitation and improve staff awareness against spear-phishing. Backup should be performed regularly and kept offline.
- ✧ **Vulnerable Remote Desktop Service (RDS)** is a frequent attack vector. System administrators should disable unnecessary RDS and timely patch their systems to minimise the risk exposure.
- ✧ **Evasion techniques** of malware continue to evolve and advance. Multi-layers of defense and detection mechanisms should be in place to protect the systems.

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

## CERT Advisories

### Patch your Microsoft Windows products for vulnerabilities in Remote Desktop Service (RDS)

GovCERT.HK [2], HKCERT [3] and US-CERT [4] issued alerts on the Remote Desktop Services vulnerabilities (CVE-2019-1181 and CVE-2019-1182) found in Microsoft products, which allowed for remote code execution. System administrators should patch the affected systems immediately.

### Patch your Fortinet and Pulse Secure products

GovCERT.HK[5] issued an alert on the SSL VPN services vulnerabilities (CVE-2018-13379 and CVE-2019-11510), which were being exploited in the wild. System administrators should patch the affected systems and change their passwords immediately.

### Protect against Password Spraying Attacks

The Australian Cyber Security Centre (ACSC)[6] issued a security advisory on how to protect against password spraying attacks. Password spraying attack was a brute-force attack in which attackers used one password to try to access a large amount of accounts, and then repeat the process with another password. The advisory set out the recommended detection and mitigations for the attack.

### Design secured virtualised systems

NCSC[7] issued the Virtualisation security design principles as a subset of its Cyber security design principles. The principles are organised into five sections including (1) Establish the context, (2) Make compromise difficult, (3) Make disruption difficult, (4) Make compromise detection easier, and (5) Reduce the impact of compromise.

### Protect backups stored in public cloud

NCSC[8] issued guidelines on protecting the backups stored in public cloud, including consideration on offline backup, restoration of backups, multiple backup copies, performing backup regularly, and so on.

---

[2] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=410
[3] https://www.hkcert.org/my_url/en/blog/19081501
[4] https://www.us-cert.gov/ncas/current-activity/2019/08/14/microsoft-releases-security-updates-address-remote-code-execution
[5] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=414
[6] https://www.cyber.gov.au/publications/advisory-2019-130-password-spray-attacks-detection-and-mitigation-strategies
[7] https://www.ncsc.gov.uk/blog-post/virtualisation-security-design-principles
[8] https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

## CERT Advisories

### Switch from Python 2 to Python 3

NCSC[9] issued a reminder to developers and organisations on switching from Python 2, which would be end of life on 1.1.2020, to Python 3. Tools and materials which could facilitate the switching were introduced.

### Number of malware hosting events dropped in Q2 2019, mentioned in the latest HKCERT quarterly report

HKCERT released its Hong Kong Security Watch Report (Q2 2019)[10]. The number of malware hosting events decreased from 72,201 in Q1 to 48,892 in Q2. However, the number of phishing events increased by more than 300%. 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.

[9] https://www.ncsc.gov.uk/blog-post/time-to-shed-python-2
[10] https://www.hkcert.org/my_url/en/blog/19080101

## Industry Insight on Cyber Security Threat Trends

**Modern malware increasingly equipped with improved evasion and anti-analysis capabilities**

Fortinet collected billions of threat events from their network sensors across the world, analysed the data from multiple perspectives of cyber-threat landscape, and published the analysis results in its "Threat Landscape Report for Q2 of 2019"[11]. The key observations were:

- **The Threat Landscape Index (TLI), an indicator for the malicious activity on the Internet,** increased 4% and reach its peak at the end of 2019 Q2. The main reason for the growth at the end of Q2 was due to the increase in exploits and malware activities.

- **Ransomware attacks in the quarter changed from the mass-volume and opportunistic approach to more targeting on organisations.** Attackers gained access to the networks of the victims first, collected information through pre-attack reconnaissance, before they actually deployed the ransomware on the selected systems. Some ransomware exploited system vulnerabilities. For instance, Sodinokibi exploited the critical vulnerability of Oracle's Weblogic Server which enabled it to execute malicious code remotely. System administrators should patch their systems timely to mitigate the risk.

- **More than 800,000 systems with vulnerable Remote Desktop Protocol (RDP) implementation (the "BlueKeep") were found on the Internet as at the end of 2019 Q2,** despite repeated warnings on this flaw from Microsoft, CERT community and other organisations. Organisations should disable unnecessary RDP on their systems, use strong passwords and account lockout to prevent brute-force attacks on RDP, timely apply available patches and updates to address known vulnerabilities, and enable network-level authentication.

- **The use of sophisticated anti-analysis and evasion techniques were growing.** Malware could detect if it runs in sandbox or emulator environments, disable security solutions of the systems, change the file names and hashes of the malware files in every user login, check for mouse movements, timers to delay execution, and so on. Organisations should deploy multi-layered defences including endpoint protection, network layer protection, application level protection, email protection, etc., instead of only using traditional signature and behaviour-based threat detection solutions.

- **Attacks via third parties, such as supply chain partners, imposed growing threats to organisations.** Attackers could compromise the network of an organisation by first indirectly hacking into the systems belonging to a third party (e.g. suppliers) as stepping stones.

*Source: Fortinet*

[11] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q2-2019.pdf

## Industry Insight on Cyber Security Threat Trends

**The number of detected ransomware cases targeted organisations increased 3.65 times in 2019 Q2 as compared with the same period in 2018**

Malwarebytes solicited telemetry data from their products, and prepared the "Cybercrime tactics and techniques: ransomware retrospective"[12] report. The observations of the report included:

- **In 2019 Q2, the detections of ransomware targeted organisations increased 365%, but those in consumer segment decreased 12%, comparing with 2018 Q2.** This was due to the attackers wanted to pursuit higher returns of investment, as the pay back they acquired from organisations were better than those from individuals and a higher chance of receiving payment from organisations.

- **Ransomware attacks targeted cities and municipalities became more frequent.** Industries such as healthcare and education, were also targets of ransomware attacks, probably due to the legacy infrastructure, obsolete software were used and insufficient funding for cyber security in these organisations.

- **GandCrab was the most popular ransomware in the period from June 2018 to June 2019.** It ran a ransomware-as-a-service (RaaS) model and evolved the distribution method continuously. In terms of trends on business ransomware detection, Ryuk and Phobos ransomware families increased 88% and 940% respectively from Q1 to Q2 2019. On consumer side, all the top five ransomware families recorded a decrease in detection in Q2 2019.

- **Around half of the ransomware detections were in the North America.** Europe, the Middle East, and Africa (EMEA) accounted for 35% of the ransomware detection, while there were only 10% cases found in the Latin America and 7% in the Asia Pacific. Among the countries affected by ransomware, the top 3 were the United States (53%), Canada (10%) and the United Kingdom (9%).

- **Exploits, blended attacks, and manual infection were used as infection vectors for ransomware.** In fact, attackers used a combination of these tactics to better target organisations and to increase their rate of successful attacks. Exploits targeting vulnerabilities in Server Message Block (SMB) and Remote Desktop Protocol (RDP) were typical examples of exploits used by attackers. Blended attacks allowed ransomware infect victims which were compromised by other Trojans or malware. Some ransomware were manually executed by the attackers, after the attackers compromised the target and disarmed the anti-malware software, in order to make the attack more effective.

*Source: Malwarebytes*

[12] https://resources.malwarebytes.com/files/2019/08/CTNT-2019-Ransomware_August_FINAL.pdf

## Industry Insight on Cyber Security Threat Trends

**Threat actors took only 5 days to weaponise new attack vectors for launching attacks**

Security vendor NETSCOUT used various measures such as automated malware analysis pipelines, sinkholes, scanners and honeypots to collect, analyse, and prioritise emerging threats data, and published their findings in the report "Threat Intelligence Report"[13]. Details of the report were:

- **Botmasters acted fast.** They made use of anything that were vulnerable and could be used in launching cyber attacks, such as smart home sensors, smartphones, routers, and software or services such as Apple Remote Management Services (ARMS) to make them as new attack vectors. It merely took 5 days for the attackers to weaponise the newly discovered attack vectors. Moreover, there were appropriately 7.7 million IoT devices connected to the Internet daily, with most of them had security issues, making them rich resources for the threat actors.

- **Mid-size DDoS attacks were more common in the first 6 months of 2019.** The overall number of DDoS attacks increased for 39% comparing to the first half of 2018. Attacks with size between 100 Gbps and 400 Gbps increased dramatically for 776%. On the contrary, attacks with size larger than 500 Gbps dropped 32%, and the maximum attack size dropped 63%, from 1.7 Tbps to 634 Gbps.

- **Proof-of-concept malware to attack IoT devices behind firewalls was available.** This could change the ecology of IoT attack, as the estimated ratio of IoT devices behind firewall to those connected to the Internet directly was 20:1.

- **Mirai was the top IoT malware in the first half of 2019.** More than 20,000 unique Mirai samples and variants were discovered. These variants evolved from the original version by using combinations of hard-coded administrative credentials and exploits as the means to compromise IoT devices.

- **Wireless and satellite communications were under attack.** The number of attacks targeting wireless and satellite communications increased for 193% and 255% respectively.

- **To cope with cyber attacks, organisations should deploy all devices and services with secure perimeters (such as secure VLANs with firewalls), block all unnecessary services, follow the best security practices, and conduct vulnerabilities scanning regularly.**

*Source: NETSCOUT*

[13] https://www.netscout.com/sites/default/files/2019-07/SECR_010_EN-1901 – NETSCOUT Threat Report 1H 2019 – Web.pdf

## Industry Insight on Cyber Security Threat Trends

**There were more than 4.1 billion records exposed in the first half of 2019**

Risk Based Security studied and analysed the data on potential data breaches collected from the Internet, news feeds, blogs, etc. The analysis results were published in the "2019 MidYear QuickView Data Breach Report"[14]. The highlights of the report were:

- **3,813 breaches were reported from January to June 2019, which leaked over 4.1 billion records.** The number of breach cases and the amount of leaked records increased by 54% and 52% respectively when compared with the same period in 2018.

- **Most of the reported breaches exposed less than 10,000 records.** However, there were eight breaches in the first half of 2019 exposed over 100 million records in each case. Totally more than 3.2 billion records (78% of total exposed records) were leaked by these eight breaches.

- **Data were exposed as systems were improperly configured or protected.** For instance, 149 out of the total 3,813 breach cases involved misconfigured databases and services, which leaked more than 3.2 billion records.

- **Based on the number of data leakage cases, hacking ranked as the top breach type, accounting for 3,128 case (82%).** Its popularity was related to the large number of vulnerabilities discovered and reported. In terms of the number of records leaked, exposure of data on the Internet ranked as the top, accounting for 3.3 billion records (about 80%). Hacking ranked as the second, causing leakage of 863 million records.

- **Email addresses were the top target of leakage cases,** with 70% of data breach exposed this type of information, increased from the 44% in 2018. Besides, 64% of breach cases leaked passwords, increased from the 39% in 2018. On the contrary, the percentage of leakage cases of some data types such as the date of birth, social security number, credit card number, etc. decreased from 2018.

*Source: Risk Based Security*

[14] https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

## Summary of Microsoft August 2019 Security Updates

**11** Product Families with Patches

**8** Critical

**3** 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 ★★★★ | KB4511553, KB4512497, KB4512501, KB4512507, KB4512508, KB4512516, KB4512517 |
| **Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1903)** | Remote Code Execution | Critical ★★★★ | Windows Server 2016: KB4512517<br>Windows Server 2019: KB4511553<br>Windows Server v1803: KB4512501<br>Windows Server v1903: KB4512508 |
| **Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2** | Remote Code Execution | Critical ★★★★ | KB4512476, KB4512482, KB4512486, KB4512488, KB4512489, KB4512491, KB4512506, KB4512518 |
| **Microsoft Edge** | Remote Code Execution | Critical ★★★★ | KB4511553, KB4512497, KB4512501, KB4512507, KB4512508, KB4512516, KB4512517 |
| **Internet Explorer** | Remote Code Execution | Critical ★★★★ | IE 9: KB4511872, KB4512476<br>IE 10: KB4511872, KB4512518<br>IE 11: KB4511553, KB4511872, KB4512488, KB4512497, KB4512501, KB4512506, KB4512507, KB4512508, KB4512516, KB4512517 |
| **Microsoft Office-related software** | Remote Code Execution | Critical ★★★★ | Microsoft Office 2010: KB4475506, KB4475531<br>Microsoft Office 2013 and 2013 RT: KB4464599<br>Microsoft Office 2016: KB4475538<br>Microsoft Office 2019 Security Update: Click to Run<br>Microsoft Office 2019 for Mac Security Update: Release Notes |

[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 365 ProPlus Security Update: Click to Run<br>Microsoft Office Online Server: KB4475528<br>Microsoft Office Web Apps 2010 Security Update: KB4475534<br>Microsoft Office Web Apps Server 2013 Security Update: KB4462216<br>Microsoft Outlook 2010: KB4475573<br>Microsoft Outlook 2013 & 2013 RT: KB4475563<br>Microsoft Outlook 2016: KB4475553<br>Outlook for iOS Security Update: Release Notes<br>Microsoft Word 2010: KB4475533<br>Microsoft Word 2013 & 2013 RT: KB4475547<br>Microsoft Word 2016: KB4475540 |
| **Microsoft SharePoint-related software** | Remote Code Execution | Critical ★★★★ | Microsoft SharePoint Foundation 2010 SP2: KB4475575<br>Microsoft SharePoint Foundation 2013 SP1: KB4475565<br>Microsoft SharePoint Enterprise Server 2013 SP1: KB4462137, KB4475557<br>Microsoft SharePoint Enterprise Server 2016: KB4475549<br>Microsoft SharePoint Server 2010 SP2: KB4475530<br>Microsoft SharePoint Server 2019: KB4475555 |
| **ChakraCore** | Remote Code Execution | Critical ★★★★ | ChakraCore: Security Update Guide |
| **Microsoft Visual Studio** | Elevation of Privilege | Important ★★★ | Visual Studio 2017: Security Update<br>Visual Studio 2017 version 15.9: Security Update |

| Product Family | Impact[15] | Severity | Associated KB and / or Support Webpages |
|---|---|---|---|
| | | | Visual Studio 2019 version 16.0: Security Update<br>Visual Studio 2019 version 16.2: Security Update |
| **Microsoft anti-malware software** | Elevation of Privilege | Important<br>★★★ | Windows Defender, Microsoft Forefront Endpoint Protection 2010, Microsoft Security Essentials, Microsoft System Center Endpoint Protection, Microsoft System Center 2012 R2 Endpoint Protection, Microsoft System Center 2012 Endpoint Protection: More Information |
| **Microsoft Dynamics 365** | Elevation of Privilege | Important<br>★★★ | Microsoft Dynamics 365 (on-premises) version 9.0: KB4508724 |

Learn more:

High Threat Security Alert (A19-08-01): Multiple Vulnerabilities in Microsoft Products (August 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=410)

**Sources:**

- Microsoft August 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/312890cc-3673-e911-a991-000d3a33a34d)