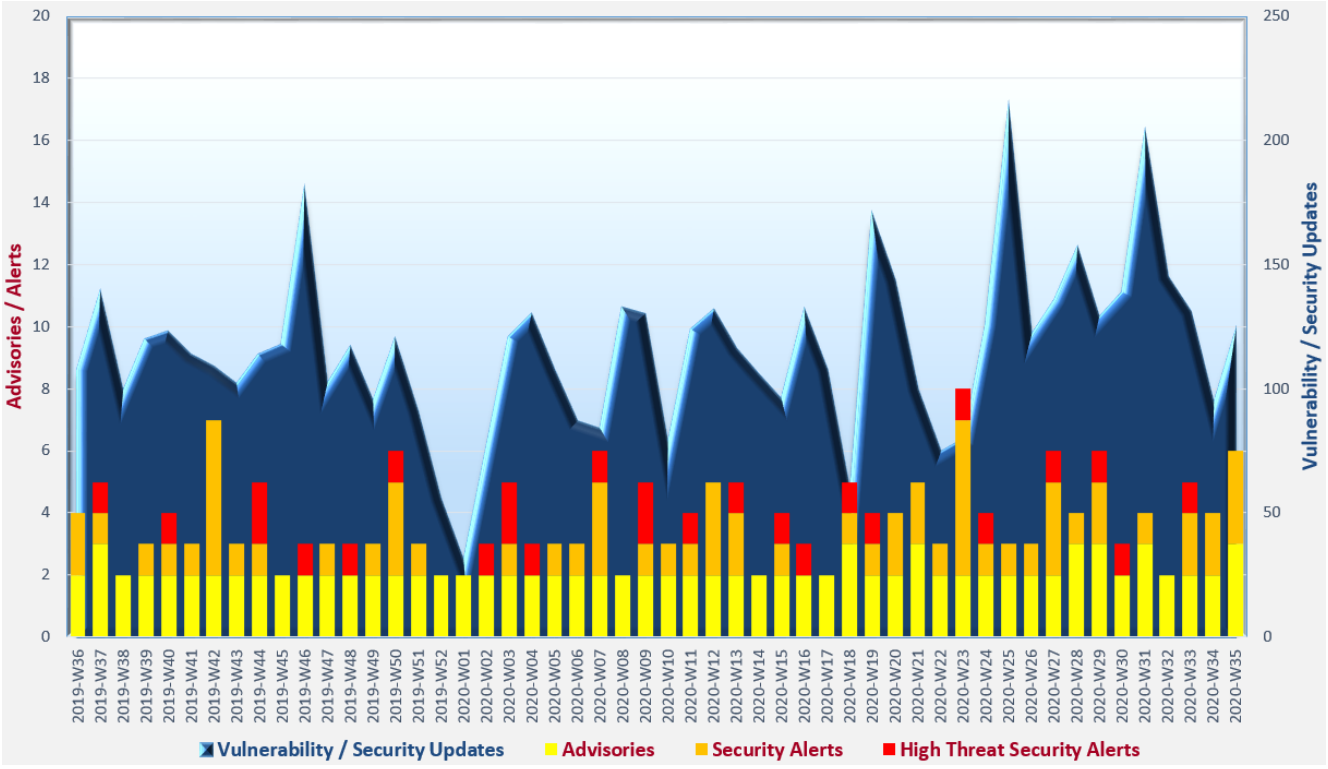
TLP:WHITE

Cyber Security Threat Trends 2020-M08

August 2020

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 breach** grows in both data volume and severity**.** Organisations should assure secure configurations, strong authentication and privileged access management are in place for their systems.
- **Defense evasion** by exploitation of vulnerabilities and abuse of legitimate administration tools remain prevalent attack tactics**.** System administrators should restrict the use of administration tools on need basis, apply strict audit policy and patch their systems timely.
- **Security and network misconfiguration** in cloud deployments are prevailing issues leading to breaches and data leakage. Organisations should adopt the security by design approach throughout the whole system development lifecycle. Least privilege principle should be adopted in system and network configuration.

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

CERT Advisories

Active exploitations against vulnerabilities in Microsoft Windows and Internet Explorer

GovCERT.HK [2] and Cybersecurity and Infrastructure Security Agency (CISA) [3] issued alerts regarding a spoofing vulnerability (CVE-2020-1464) that affected all supported Windows versions and a remote code execution vulnerability (CVE-2020-1380) which affected Internet Explorer 11. Both vulnerabilities were exploited actively. System administrators should install the latest security updates timely.

Phishing events in Hong Kong increased by 4 times in Q2 2020

HKCERT[4] released its Hong Kong Security Watch Report (Q2 2020). The number of security events declined from 14,433 in Q1 2020 to 13,365 in Q2 2020, contributed by the decrement of malware hosting events and botnet events. The number of malware hosting events decreased by 20% to 4,334, and the number of botnet events decreased by 25% to 5,952 in Q2 2020. However, the number of defacement events increased significantly by 85% to 1,062. Phishing events skyrocketed by 4 times to 2,017 in this quarter as threat actors leveraged the COVID-19 pandemic and created phishing sites using online entertainment as lures. Around 71% of phishing URLs spoofed an online gambling website.

Beware of Distributed Denial of Service (DDoS) extortion attacks

HKCERT[5] released an article to remind local organisations to be cautious to DDoS extortion attacks. Attackers targeted different industries and threatened to launch DDoS attack against the target unless a ransom was paid. The article also provided some advices to organisations for defence against the attacks, including preparedness on incident handling on DDoS, readiness of network monitoring and security detection, hardening of systems and networks, adoption of DDoS protection solution or service, etc.

Better understanding on Personal VPN Service

HKCERT[6] published an article to help computer users to understand the operation and limitation of personal VPN service. Security consideration of choosing personal VPN service and the proper configuration were also addressed in the article.

[2] https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=499
[3] https://us-cert.cisa.gov/ncas/current-activity/2020/08/11/microsoft-addresses-rce-and-spoofing-vulnerabilities-under-active
[4] https://www.hkcert.org/my_url/en/blog/20081201
[5] https://www.hkcert.org/my_url/en/blog/20083101
[6] https://www.hkcert.org/my_url/en/blog/20081801

CERT Advisories

Top 25 most dangerous software weaknesses released

CISA[7] issued an advisory to encourage IT practitioners and users to review the 2020 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses list and the recommended mitigation measures. The list revealed the most frequent and critical errors which could lead to breach path for threat actors to abuse and exploit.

[7] https://us-cert.cisa.gov/ncas/current-activity/2020/08/20/2020-cwe-top-25-most-dangerous-software-weaknesses

Industry Insight on Cyber Security Threat Trends

More than 27 billion records were exposed in the first half of 2020

Risk Based Security released the "2020 Mid Year Data Breach QuickView Report"[8], which included their observations on data breach trends in the first half of 2020. The major observations in the report were:

- **2,037 breaches were reported in the first six months of 2020, a decrease of 52% compared to the same period in 2019.** The researchers considered the decrease in breach events might be due to the delay in breach reporting in the pandemic. Despite the decrease in reported breaches, **the number of records exposed in the first half of 2020 (27.68 billion) was almost 6 times of the figure for the same period in 2019**. Three mega leaks were due to misconfigured databases and services accounted for 84% of the exposed records. Moreover, there was an increasing trend in the number of exposed records as well as the severity of the breach events.

- **In the first half of 2020, 1,334 reported breaches were primarily caused by unauthorised access to systems or services.** In terms of number of breached records, **online exposure was the top breach type, attributed to 26.5 billion exposed records**.

- **In the Q2 2020, over 350 million passwords along with email addresses or usernames were compromised by malicious actors.** Three data types (Email, passwords and names) remained the most exposed data types for three consecutive years. Most of the exposed passwords were found to be hashed with outdated algorithms and could be decrypted easily. The report also revealed that users used their office email addresses for personal use in a variety of web sites or services such as gaming sites, dating applications, etc. Organisations could consider adoption of usage policies on office email accounts for personal use to reduce the risk caused by third party data breaches.

- **The Information sector and Health Care sector reported the highest number of breaches with 215 and 211 breaches respectively.** The distribution of breach events in the two sectors, however, were quite different. Approximately 85% of the breaches in Information sector were from software publishers (including Software-as-a-Service), and other web-based services, while the breach events in Health Care sectors were fairly evenly distributed among hospitals, practitioners, and other facility or support service providers.

Source: Risk Based Security

[8] https://pages.riskbasedsecurity.com/en/2020-mid-year-data-breach-quickview-report

Industry Insight on Cyber Security Threat Trends

Attackers actively exploited vulnerabilities and legitimate administration tools

Kaspersky published the "Incident Response Analyst Report"[9] to reveal the adversaries' tactics and techniques used in cyber security incidents based on the analysis and statistics from the incident investigation services conducted in 2019. The key findings were:

- **In 2019, Industrial (29.5%), Finance (16.3%), Government (15.5%) and Telecoms (10.1%) were accounted for 71.4% of all reported cyberattacks.** Oil and gas organisations were the top target business and followed by bank. Ransomware and malware infection were the top two threats. Money theft incidents were specifically targeted to bank.
- **Threat actors increasingly abused legitimate tools in different phases of cyberattacks**. The tools were used in 30% of the security incidents investigated for stealing credentials from memory, evading security mechanisms by unloading security solutions and discovering services in the network. The administration tools like PowerShell (25%), PsExec (22%), SoftPerfect Network Scanner (14%) and ProcDump (8%), were most commonly used in the reported cyberattacks. PowerShell, PsExec, PsTools and Rexec were applied to the execution phase of almost 39% of the attacks. Administrators should restrict execution of PowerShell scripts or usage of administration tools on need basis only and consider enabling deep script block logging to facilitate the tracing of PowerShell activities.
- **Most cyberattacks were conducted by exploitation of vulnerabilities (0- and 1-day) with malicious emails and brute-force attacks.** Most incidents were caused by identified exploits of **remote code execution** in various software, such as **Microsoft Windows, Microsoft SharePoint, Drupal, Citrix Gateway, and Pulse Secure SSL VPN, etc.** Organisations should apply security patches timely and enforce strict password policies to mitigate the risks.
- **31.1% of attacks could be detected within a few hours and 13.3% were detected in days from the start of attack.** However, 22.2% of attacks were detected by months and 8.9% of attacks needed years to uncover, indicated that organisations needed to improve the detection time. Organisations were recommended to fine-tune their security tools in an on-going manner to reduce false positives, closely monitor the alerts generated by the security tools and conduct investigation timely.
- **Ransomware were found in 34% of reported incidents and mainly targeted the Government, Telecom and Information Technology (IT) sectors**. The median attack duration was one day but the adversary's activity might be started after a week from the initial compromise. User should perform regular data backup on offline and encrypted data storage.

Source: Kaspersky

[9] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/08/06094905/Kaspersky_Incident-Response-Analyst_2020.pdf

Majority of cloud deployments contained misconfigured services

Accurics analysed hundreds of cloud native infrastructure deployments, and published the study results in its "The State of DevSecOps Report - Summer 2020"[10]. The key findings were:

- **93% of cloud deployments had misconfigured cloud storage services** that led to the exposure of 845GB highly sensitive personal information from over 8 dating apps, and 409GB of financial and personally identifiable information leakage from a payment application. **91% had at least one network exposure to security group.** Over 30 billion records were exposed in more than 200 breaches in last two years due to these two problems.
- **72% of cloud deployments contained hardcoded private keys**, **and 41% had hardcoded keys with high privileges.** Half of the cloud deployments stored credentials in container configuration files without any protection. Leakage of these keys and credentials could lead to unauthorised access to the sensitive cloud resources.
- **Misconfigured routing rules were found in all studied cloud deployments which exposed the private subnet hosting sensitive resources, such as databases, to the Internet.** Moreover, Identity and Access Management (IAM) policies in 89% of cloud deployments were found to be overly permissive. Attackers could take advantage of these misconfigurations to compromise vulnerable cloud resources.
- The report revealed that cloud infrastructure changes during runtime were highly correlated with the risks of security breach. Nevertheless, **users in 90% of organisations could make changes to their cloud infrastructure during runtime.**
- **Only 6% of issues were addressed if risks were remediated manually.** On the contrary, the adoption of codifying remediation into development pipelines (Remediation as Code) could enable organisations to address 80% of risks.
- **Security should be integrated into the development lifecycle from the very beginning.** Security policy requirements such as database encryption, key rotation, multi-factor authentication, could be declared within codes (Policy as Code). Automated threat modelling using frameworks such as the MITRE ATT&CK Matrix for Enterprise and the Common Attack Pattern Enumeration and Classification (CAPEC) could be employed (Security as Code). Cloud deployments should be monitored continuously and risk assessments should be performed for any detected resource or configuration changes from a secure baseline (Drift as Code). Remediation as Code could also be adopted in order to handle the risk issues detected automatically.

Source: Accurics

[10] https://start.accurics.com/CT-2020-08-Research-Report_LP-Reg.html?utm_source=website&utm_campaign=report_summer_2020

Summary of Microsoft August 2020 Security Updates

13 Product Families with Patches

9 Critical

4 Important or below

Product Family	Impact[11]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB4565349, KB4565351, KB4566782, KB4571692, KB4571694, KB4571709, KB4571741
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4565349, KB4565351, KB4566782, KB4571694
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4571702, KB4571703, KB4571723, KB4571736, KB4578013
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4565349, KB4565351, KB4566782, KB4571692, KB4571694, KB4571709, KB4571741, Release Notes
Internet Explorer	Remote Code Execution	Critical ★★★★	KB4565349, KB4565351, KB4566782, KB4571687, KB4571692, KB4571694, KB4571703, KB4571709, KB4571729, KB4571736, KB4571741
Microsoft Office-related software	Remote Code Execution	Critical ★★★★	Microsoft Office: KB4484346, KB4484354, KB4484359, KB4484375, KB4484379, KB4484431, KB4484492, Click to Run Microsoft Access: KB4484340, KB4484366, KB4484385 Microsoft Excel: KB4484449, KB4484461, KB4484465 Microsoft Outlook: KB4484475, KB4484486, KB4484497 Microsoft Word: KB4484474, KB4484484, KB4484494 Microsoft Office 2013 C2R: Click to Run

[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 Office 2016 & 2019 for Mac: Release Notes Microsoft Office Web Apps: KB4484481, KB4484495 Microsoft 365 Apps for Enterprise: Click to Run Office Online Server: KB4484470
Microsoft .NET Framework	Remote Code Execution	Critical ★★★★	KB4569745, KB4569746, KB4569748, KB4569749, KB4569751, KB4570500, KB4570501, KB4570502, KB4570503, KB4570505, KB4570506, KB4570507, KB4570508, KB4570509, KB4571692, KB4571694, KB4571709, KB4571741
ChakraCore	Remote Code Execution	Critical ★★★★	Release Notes
Microsoft Dynamics 365	Remote Code Execution	Critical ★★★★	KB4541722, Release Notes
ASP.NET Core	Denial of Service	Important ★★★	Release Notes
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	KB4484183, KB4484191, KB4484462, KB4484471, KB4484472, KB4484473, KB4484476, KB4484478, KB4484479, KB4484487, KB4484490, KB4484498
Microsoft Visual Studio	Remote Code Execution	Important ★★★	Microsoft Visual Studio 2017 version 15.9: Release Notes Microsoft Visual Studio 2019 version 16.0: Release Notes Microsoft Visual Studio 2019 version 16.4: Release Notes Microsoft Visual Studio 2019 version 16.7: Release Notes Visual Studio Code: Release Notes
SQL Server Management Studio	Denial of Service	Important ★★★	Release Notes

Learn more:

Security Alert (A20-08-01): Multiple Vulnerabilities in Microsoft Products (August 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=499)

Sources:

- Microsoft August 2020 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Aug)