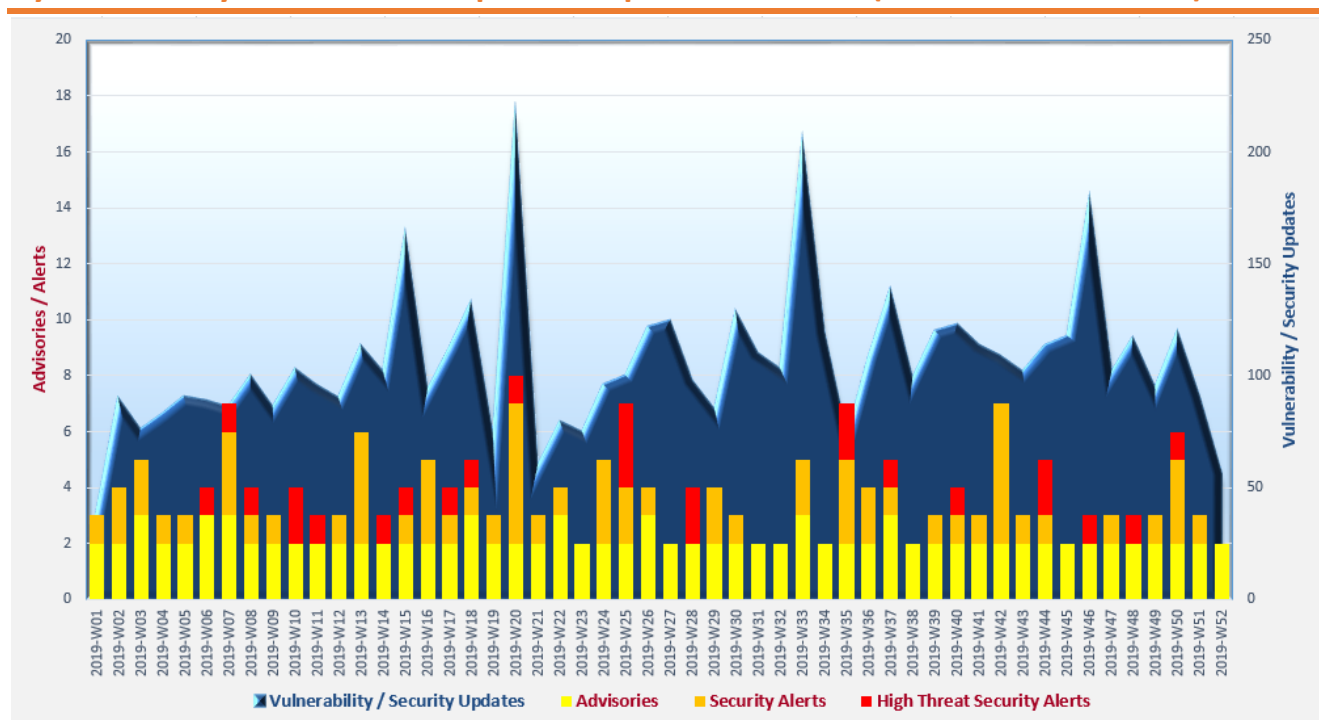


Cyber Security Threat Trends 2019-M12

December 2019

With reference to the FIRST Traffic Light Protocol (TLP) standard¹, 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 Internet-facing network attached storage (NAS) devices have emerged. To protect the devices and data, it is essential to have regular offline backup, timely software update, restricted network access, strong password or multi-factor authentication, and encrypted data storage.
- ✧ **5G networks** bring bandwidth surge and device proliferation, which could ease traffic manipulation and distributed denial-of-service attacks. Businesses should keep their cyber security policies and defense systems up-to-date to prepare for the additional risk exposure.
- ✧ **Social engineering attacks** are on the rise. Organisations should train staff on the know-how to respond to the attacks for better defence, in addition to making them fully aware of the threats.

¹ <https://www.first.org/tlp/>

CERT Advisories



Protect against Ransomware attacks

HKCERT² released an advisory on new trends of ransomware, the preventive measures against the threat and actions could be taken when infected by ransomware. It also revealed an emerged cyberattack targeting vulnerable network attached storage (NAS) accessible through the Internet. **Users should follow the best practices to protect against ransomware.**



Mitigate the risk on Citrix Application Delivery Controller and Citrix Gateway critical vulnerability

Australian Cyber Security Centre (ACSC)³ warned organisations about a critical vulnerability (CVE-2019-19781) found in Citrix Application Delivery Controller (ADC) (formerly known as NetScaler ADC) and Citrix Gateway (formerly known as NetScaler Gateway). Unauthenticated remote attackers could exploit the vulnerability to execute arbitrary commands on the targeted system. **System administrators should follow the recommendations provided by the product vendor and take immediate actions to mitigate the risk. The affected system should be patched immediately once upon the fix was released.**



Prevent, detect, contain cyberattacks

New Zealand Computer Emergency Response Team (CERT NZ)⁴ issued the annual list of ten critical controls on how to protect, detect or contain against cyberattacks. The list aimed to facilitate organisations prioritising their security controls based on CERT NZ's updated statistics. Protecting organisation's authentication, asset management and secure defaults for Microsoft Office macros were newly added to this critical controls list.



Share data securely with external parties

The UK National Cyber Security Centre (NCSC)⁵ prepared a guidance "Design Pattern: Safely Exporting Data" for implementing a secure end-to-end data export solution. The solution should be built on the four techniques mentioned in the guidance, including controlling the release of information, preventing hidden data in documents, defending attacks over the network and encrypting data for the recipient.

² https://www.hkcert.org/my_url/en/blog/19123001

³ <https://www.cyber.gov.au/news/acsc-aware-critical-vulnerability-citrix-application-delivery-controller-and-citrix-gateway>

⁴ <https://www.cert.govt.nz/it-specialists/critical-controls/10-critical-controls/>

⁵ <https://www.ncsc.gov.uk/guidance/design-pattern-safely-exporting-data>

CERT Advisories



Beware of Emotet

SingCERT⁶ issued an advisory on ongoing and widespread Emotet malware campaign. Emotet evolved from banking trojans into botnet for spreading other malware like Trickbot Trojan. Trickbot, after infected the victim, would attempt to steal emails and credentials, move laterally within a network, and deploy other malware to the infected networks. The new Emotet variants possessed the capability of evading from detection by anti-malware solutions. The advisory provided recommendations to help organisations defend against Emotet.

⁶ <https://www.csa.gov.sg/singcert/advisories/emotet-malware-campaign-2019>

Industry Insight on Cyber Security Threat Trends

Emerging threats put cyber risk to a higher level

Trend Micro and Ponemon Institute surveyed over 1,000 IT managers and practitioners of United States organisations in the second half year of 2019. Their responses were studied and analysed to prepare "The 2H 2019 Cyber Risk Index (CRI)"⁷ on organisations' readiness for handling cyber-attacks and their likelihood of being attacked. The highlights from CRI included:

- **For -10 represented the highest risk, CRI decreased from -0.15 in 2H 2018 to -0.27 in 2H 2019, driven by a perceived increase in risks from new threats targeting organisations.** That represented an increase in risk from last year's survey. There was a threefold decrement in CRI for medium-sized organisations (with 100 - 999 employees), from -0.15 to -0.45. Small-sized organisations (with less than 100 employees) got a slight drop from -0.59 to -0.61. Both CRIs were at elevated level. CRI for organisations with more than 1,000 staff, was at moderate level, with a slight increase to 0.23 from 0.21.
- **Almost four-fifths organisations anticipated at least one successful cyberattack or a data breach in 2020.** During 2H 2018 to 2H 2019, 73% organisations suffered one or more successful cyberattacks and 21% organisations encountered more than 6 cyberattacks.
- **Large organisations were more ready to defend against cyberattacks, as reflected by the Cyber Preparedness Index (CPI).** The CPI of large organisations was 6.04, higher than the CPI of all organisations (5.07). Nevertheless, in general, all organisations were at elevated cyber risk level.
- **R&D information, financial information, companies' confidential information and customer accounts were the data types at the highest risk subject to loss or theft.** In mitigation of data risks, the respondents had most concern on their security solutions' zero day attacks detection capability.
- **Phishing, social engineering, clickjacking, botnets, fileless attack and denial of service (DoS) were the top cyber threat concerns from the respondents.** They also concerned about their organisations' spending on employing or retaining IT security staff and security training were insufficient.
- **Organisations were recommended to fine tune their cyber security strategy and follow security best practices to protect their critical data, devices and infrastructure against ever emerging new threats.**

Source: Trend Micro and Ponemon Institute

⁷ https://www.trendmicro.com/en_us/security-intelligence/breaking-news/cyber-risk-index.html

Industry Insight on Cyber Security Threat Trends

Old software vulnerabilities were still popular for threat actors

Verint and Thales studied 525 attack tools, attack techniques used and 98 CVEs exploited in 490 attack campaigns by 66 attack groups targeting 39 sectors over 147 countries and disclosed the results and key observations in “The Ultimate Threat Actor Landscape”⁸ report. The major observations were:

- **The United States was most targeted by attackers (13.2%), followed by the United Kingdom, France, Israel and the Mainland of China which targeted by 8.2%, 6.8%, 6.4% and 5.7% of threat actors respectively.** Most of the cyber-attacks worldwide were for the purpose of cyber espionage and ideology. Government agencies was the most targeted sector world-wide, followed by critical infrastructure except in Latin America and Africa where financial services were the second most targeted sector.
- **Microsoft Windows, Office and Internet Explorer grabbed the first, second and fourth place in the list of most exploited software after analysing 490 attack campaigns.** Adobe Flash Player held the third place and Adobe Acrobat Reader shared the fifth place with Oracle JDK.
- **Over one-third attack campaigns leveraged a memory corruption vulnerability (CVE-2017-0199) and a remote code execution vulnerability (CVE-2017-11882) of Microsoft Office.** Nine out of eleven most exploited vulnerabilities were from Microsoft products. Over 80% of the most exploited vulnerabilities aged more than two years. 14.6% of attack campaigns exploited a 7-years old Microsoft vulnerability (CVE-2012-0158). The oldest vulnerability of the eleven most exploited vulnerabilities was CVE-2010-3333, a 9-years old vulnerability, which was still exploited in 6.25% of attack campaigns.
- **Cyberattacks by nation-states threat actors were mostly for cyber espionage and were typically well-crafted and surgical by using sophisticated attack tools and techniques.** The attacks mostly targeted government agencies (26.3%), critical infrastructure (22.5%) and defense (20%). At least 50% of the attack campaigns in Europe, Asia Pacific, Middle East and North America were from nation-states threat actors.
- **Valid accounts (16.9%), scheduled task execution (11.1%), scripting execution (10.9%), remote file copy (9.9%) and input capture (8.1%) were the top five most used attack techniques.**

Source: Verint and Thales

⁸ <https://cis.verint.com/resources/the-ultimate-threat-actor-landscape-booklet/>

Industry Insight on Cyber Security Threat Trends

Upsurge of network attacks using old Apache Struts exploits and zero day malware detections

WatchGuard collected anonymised information on threat detected from 36,794 globally deployed appliances and summarised the latest malware and exploit trends observed from the collected threat data in its "Internet Security Report – Q3 2019"⁹. The highlights from the report included:

- **6 out of 10 detected network attacks (i.e. exploitation of network-accessible servers' vulnerabilities or client software) targeted the Americas region (AMER) in Q3 2019.** The attack volume for Europe and Middle East region (EMEA) and Asia Pacific region (APAC) were 23% and 17% respectively.
- **Threat actors actively targeted Apache Struts vulnerabilities in Q3 2019.** Two Apache Struts exploits became top 10 network attacks. One of the top 5 most widespread network attacks also targeted Apache Struts vulnerability. *System administrators should upgrade and patch their Apache Struts immediately.*
- **The "WEB-CLIENT Generic JavaScript Remote Code Execution" exploit showed a sharp increase, which targeted the Adobe Flash player vulnerability disclosed in 2011.** *Website owners should replace all Adobe Flash implementations by HTML5, CSS3 and JavaScript (without Flash Player) as Adobe Flash would be end of support by 31 December 2020.*
- **Almost half of the detected malware in Q3 2019 was zero day malware which could circumvent typical signature-based anti-malware solution.** The number of malware increased by 30% in Q3 2019 overall. *Organisations were recommended to adopt multi-layers of defense and detection mechanisms.*
- **Two Microsoft Office exploits took up the first and second place of most widespread malware especially targeting EMEA and APAC, amounting to over 80% of the distribution.** Hong Kong had the highest detection of SpamMalware-RAR (7.5%), the fourth most widespread malware. *Users were reminded to be cautious on links or attachments in the emails and should examine the links carefully.*
- **Similar to the observations for network attacks, AMER recorded the highest malware detection (42%), followed by EMEA and APAC recorded 30% and 28% respectively.** Compared with Q2 2019, the amount for EMEA and APAC decreased slightly, while AMER had a significant increase in the number of malware.

Source: WatchGuard

⁹ <https://www.watchguard.com/wgrd-resource-center/security-report-q3-2019>

Industry Insight on Cyber Security Threat Trends

Cybercrime will be exacerbated by 5G, social engineering and Operational Technology (OT) networks of critical infrastructures

Group-IB published its “Hi-Tech Crime Trends 2019/2020”¹⁰ which analysed the attacks carried out by 38 cybercriminal groups and state-sponsored attackers and the global cybercrime trend. The key observations were:

- **More attacks on domain name registrars to destabilise the Internet access were expected.** Cybercriminals could attack domain name registrars and then manipulate the traffic of the registered website, mail and DNS servers, as well as all services connected to them.
- **5G networks pose new threats.** Routers being used could become vulnerable if their settings were insecure and they were not timely updated or patched. Traffic manipulation and DDoS attacks would become much more frequent and effective regarding the huge number of insecure devices connected to 5G and the wide 5G bandwidth. Cybercriminals could leverage telecom networks to penetrate customer networks for espionage and supply chain attacks. *Organisations should update the security policy to cater for increased risk exposure brought by 5G deployment.*
- **Compromising IT networks and supply-chain attacks through software and hardware vendors allowed infiltrating the isolated OT networks of the energy industry.** The threats could be even greater for those attacks originated from the cybercriminals from developed countries due to their higher capabilities to conduct less detectable attacks.
- **Surge in JavaScript (JS) sniffer attacks for stealing credit card information would continue.** With just a few lines of codes injected onto e-commerce web sites, JS sniffers could skim the victims’ credit card data and made profit. Moreover, these JS sniffers were hard to detect as well as difficult to be scrubbed. In 2019, 38 different JS sniffer malware families were identified. Compromised bank cards by JS sniffers and card dumps recorded 38% and 46% annual increase respectively.
- **Rise of social engineering techniques including phone calls, messaging apps, and social media to steal credit card information, login password and other sensitive information were expected.** A new social engineering attack method was used to entice victims to install malicious apps such as remote control tools on their mobile devices. *Organisations should promote high user awareness and well-trained responses on the latest social engineering attacks.*

Source: Group-IB

¹⁰ <https://www.group-ib.com/resources/threat-research/2019-report.html>

Summary of Microsoft December 2019 Security Updates

10

Product Families
with Patches

4

Critical

6

Important or
below

Product Family	Impact ¹¹	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems	Remote Code Execution	Critical ★★★★	KB4530681 , KB4530684 , KB4530689 , KB4530714 , KB4530715 , KB4530717
Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1903)	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4530689 Windows Server 2019: KB4530715 Windows Server v1803: KB4530717 Windows Server v1903 & v1909: KB4530684
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4530691 , KB4530692 , KB4530695 , KB4530698 , KB4530702 , KB4530719 , KB4530730 , KB4530734
Microsoft Visual Studio	Remote Code Execution	Critical ★★★★	Visual Studio 2017 version 15.0: Release Notes Visual Studio 2017 version 15.9 (includes 15.1 – 15.8): Release Notes Visual Studio 2017 version 16.0 and 2019 version 16.0: Release Notes Visual Studio 2019 version 16.4 (includes 16.0 - 16.3): Release Notes Visual Studio Live Share extension: Release Notes
Internet Explorer	Remote Code Execution	Important ★★★	IE 9: KB4530677 , KB4530695 IE 10: KB4530677 , KB4530691 IE 11: KB4530677 , KB4530681 , KB4530684 , KB4530689 , KB4530702 , KB4530714 , KB4530715 , KB4530717 , KB4530734


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-related software	Remote Code Execution	Important ★ ★ ★	<p>Microsoft Office 2010 SP2: KB4475598, KB4484192, KB4484193</p> <p>Microsoft Office 2013 and 2013 RT: KB4484184, KB4484186</p> <p>Microsoft Office 2016: KB4484180, KB4484182</p> <p>Microsoft Office 2019 Security Update: Click to Run</p> <p>Microsoft Office 2016 & 2019 for Mac Security Update: Release Notes</p> <p>Microsoft Office 365 ProPlus Security Update: Click to Run</p> <p>Microsoft Outlook for Android: Release Notes</p> <p>Microsoft Excel 2010 SP2: KB4484196</p> <p>Microsoft Excel 2013 SP1 & 2013 RT SP1: KB4484190</p> <p>Microsoft Excel 2016: KB4484179</p> <p>Microsoft Word 2010 SP2: KB4475601</p> <p>Microsoft Word 2013 SP1 & 2013 RT SP1: KB4484094</p> <p>Microsoft Word 2016: KB4484169</p> <p>Microsoft Power Point 2010 SP2: KB4461613</p> <p>Microsoft Power Point 2013 SP1 & 2013 RT SP1: KB4461590</p> <p>Microsoft Power Point 2016: KB4484166</p>
Microsoft Authentication Library (MSAL) for Android	Information Disclosure	Important ★ ★ ★	Microsoft Authentication Library (MSAL) for Android: Download
Power BI Report Server	Spoofing	Important ★ ★ ★	Power BI Report Server: Download
Skype for Business Server 2019 CU2	Spoofing	Important ★ ★ ★	Skype for Business Server 2019 CU2: KB4534761
SQL Server-related software	Spoofing	Important ★ ★ ★	<p>SQL Server 2017 Reporting Services: Download</p> <p>SQL Server 2019 Reporting Services: Download</p>

Learn more:

High Threat Security Alert (A19-12-03): Multiple Vulnerabilities in Microsoft Products (December 2019)
(https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=439)

Sources:

 Microsoft December 2019 Security Updates
(<https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2019-Dec>)