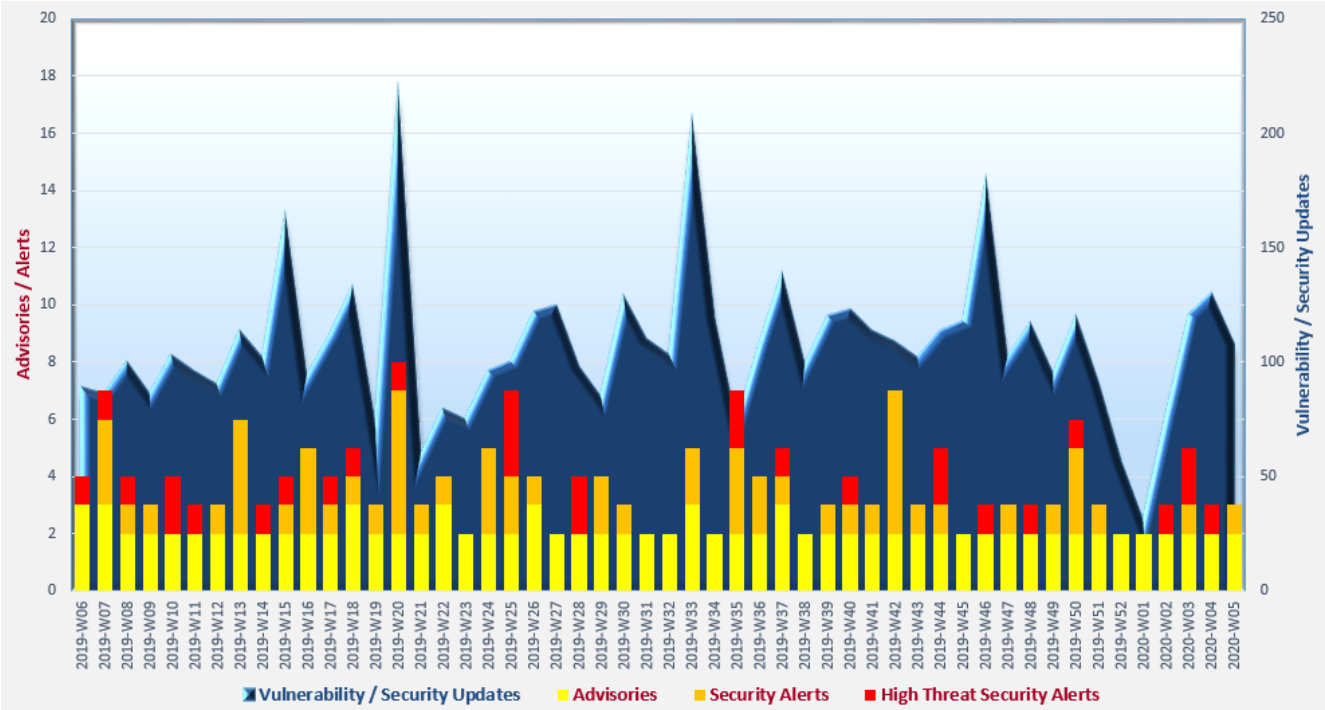
TLP:WHITE

Cyber Security Threat Trends 2020-M01

January 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:

- ✧ **Phishing attacks** become more targeted and personalised. Organisation-wide awareness training on new phishing techniques should be conducted, supplemented by focus training to specific groups of high risk users.
- ✧ **Threat actors** target new attack surface on public cloud, 5G network and Internet of Things (IoT) technologies. Organisations should fully understand threats introduced by adopting the technologies and deploy risk mitigations together with the technologies.
- ✧ **Worm-based malware always** spreads laterally across networks. Network administrators should adopt network segmentation, least privilege access control and zero-trust defense approach to contain the spread of malware.

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

CERT Advisories

Critical Vulnerability in Citrix Application Delivery Controller, Gateway and SD-WAN WANOP

HKCERT[2], MyCERT[3], JPCERT[4], Australian Cyber Security Centre (ACSC)[5], Cybersecurity and Infrastructure Security Agency (CISA)[6,7], Canadian Centre for Cyber Security[8], and New Zealand Computer Emergency Response Team (CERT NZ)[9] issued alert/advisory regarding on a critical vulnerability (CVE-2019-19781) that affected certain versions of Citrix Application Delivery Controller (ADC) (formerly known as NetScaler ADC) and Citrix Gateway (formerly known as NetScaler Gateway). This critical vulnerability also affected multiple models of Citrix SD-WAN WANOP appliance. If attackers successfully exploited this vulnerability, they could trigger remote code execution and even take control of the vulnerable servers. System administrators should install the latest security updates or firmware updates promptly.

Critical Vulnerabilities of Microsoft Windows Operating Systems

CISA[10], CERT NZ[11], HKCERT[12], SingCERT[13], and ACSC[14] issued alert/advisory in mid of January 2019 to remind system administrators and computer users to patch one important spoofing vulnerability CVE-2020-0601, and three critical remote code execution vulnerabilities, CVE-2020-0609, CVE-2020-0610 and CVE-2020-0611. CVE-2020-0601 affects all Windows 10 versions and Windows Server 2016 or later. CVE-2020-0609 and CVE-2020-0610 exists in Windows Remote Desktop Gateway (RD Gateway) that affects Windows Server 2012 or later. CVE-2020-0611 exists in the Windows Remote Desktop Client that affects all supported versions of Windows operating systems (included Windows 7 and Windows 2008 R2 that were end of support on 14 January 2020).

[2] https://www.hkcert.org/my_url/en/blog/20011702
[3] https://www.mycert.org.my/portal/advisory?id=MA-760.012020
[4] https://www.jpcert.or.jp/english/at/2020/at200003.html
[5] https://www.cyber.gov.au/threats/advisory-2020-001-active-exploitation-critical-vulnerability-citrix-application-delivery-controller-and-citrix-gateway
[6] https://www.us-cert.gov/ncas/alerts/aa20-020a
[7] https://www.us-cert.gov/ncas/alerts/aa20-031a
[8] https://www.cyber.gc.ca/en/alerts/active-exploitation-citrix-vulnerabilities
[9] https://www.cert.govt.nz/it-specialists/advisories/exploitation-of-critical-citrix-vulnerability/
[10] https://www.us-cert.gov/ncas/alerts/aa20-014a
[11] https://www.cert.govt.nz/it-specialists/advisories/critical-vulnerabilities-in-microsoft-windows/
[12] https://www.hkcert.org/my_url/en/blog/20011701
[13] https://www.csa.gov.sg/singcert/advisories/advisory-on-critical-vulnerabilities-in-microsoft-windows-operating-system
[14] https://www.cyber.gov.au/threats/advisory-2020-002-critical-vulnerabilities-microsoft-windows-announced-patch-urgently

Security events in Hong Kong declined in Q4 2019

HKCERT released its Hong Kong Security Watch Report (Q4 2019)[15]. The number of security events declined for three consecutive quarters in 2019. The peak was 80,266 in Q1 2019 and dropped gradually to 8,864 in Q4 2019. The number of defacement events and phishing events were reduced by 529 and 592, respectively. Scammers' favourite phishing targets were some popular platforms such as Apple iCloud. Nevertheless, phishing event related to eBay was increased due to fraudster took the chance of final year sales. The most significant change was the number of malware hosting, which fell from 17,273 in Q3 2019 to 1,185 in Q4 2019. Although the number of defacement events was reduced by 529, HKCERT's analysis deemed that the possible main causes of defacement incidents may be due to security vulnerabilities on the servers and using end-of-support (EOS) operating systems. System administrators are urged to strengthen the protection of servers, such as timely patching.

Comprehensive guide for protecting mobile device

The UK National Cyber Security Centre (NCSC)[16] published its Mobile Device Guidance. The guidance covers a wide range of topics including selection and procurement of devices, mobile device management (MDM), device hardening, supporting infrastructure for mobile devices, and so on.

Professional guidelines for assessing the security of communication services

The UK NCSC also published an alpha release of secure communications principles[17]. This guidance provides a set of principles to help risk owners and security professionals, particularly those in public sector and government, on choosing secure communication services such as voice, video, email and messaging services.

Beware of Shortened URLs

SingCERT[18] and Government Technology Agency (GovTech) of Singapore jointly delivered an advisory reminding users to exercise caution before clicking on shortened URLs (such as bit.ly and tinyurl) to avoid victimised by scammers.

[15] https://www.hkcert.org/my_url/en/blog/20013101
[16] https://www.ncsc.gov.uk/collection/mobile-device-guidance
[17] https://www.ncsc.gov.uk/guidance/secure-communication-principles-alpha-release
[18] https://www.csa.gov.sg/singcert/advisories/advisory-on-risks-of-shortened-urls

Industry Insight on Cyber Security Threat Trends

Phishing attacks became more targeted and customised

Proofpoint analysed data collected from different sources, including survey results from more than 3,500 people and 600 IT security professionals in seven countries, around 50 million simulated phishing attacks and more than 9 million reported suspicious emails and presented the study results in their "2020 State of the Phish"[19] report. The key findings were:

- **Instead of launching generic and mass volume attack campaigns, threat actors increasingly used a more targeted and personalised approach to attack.** More than 85% of the IT security professional respondents indicated that their organisations encountered spear phishing and Business Email Compromise (BEC) in 2019. 20% of organisations encountered at least 50 spear phishing attacks while 16% of them faced not fewer than 50 BEC attacks. Besides phishing emails, more than 80% of organisations encountered other forms of phishing such as phishing by social media (86%), smishing (84%) and vishing (83%).

- **55% of organisations were victimised by successful phishing attacks.** More than 50% of the IT security professional respondents indicated that successful phishing attacks caused data loss to their organisations. Other adverse impacts included compromise of credentials, infection of ransomware and malware and financial loss.

- **95% of IT security professional respondents indicated that their organisations conducted phishing awareness training.** 78% of the organisations opined that security awareness training could make them less susceptible to phishing attacks. However, there were still areas for improvement. Almost 30% of organisations did not offer phishing awareness training to all of their users. It would be more effective by offering organisation-wide awareness training, supplemented by targeted training to specific groups of users.

- **Almost 30% of users who opened simulated phishing emails were tricked.** Among those phishing tests with high percentage of users phished, 65% were attachment based and 35% were link based. Almost 90% of them had senders from recognisable internal accounts. Phishing messages with high hit rate used subjects such as "Lost Watch" or "Lost Ring" to take advantage of recipients' curiosity and empathy.

- **Compared with 2018, there was a 67% increase in number of suspicious emails reported by users in 2019, amounted to around 9.2 million emails.** Organisations were recommended to have a reporting mechanism on suspicious emails, as high quality user reports could help catching attacks which evaded the organisations' email defence and reached users' inbox.

Source: Proofpoint

[19] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

Industry Insight on Cyber Security Threat Trends

Cyber attacks became more sophisticated, targeted and deceitful

Check Point published its "2020 Cyber Security Report"[20] which reviewed major cyber security incidents in 2019, analysed and predicted the cyber threat trends, and provided recommendations to organisations to protect against cyber attacks. The key observations were:

- **Attacks targeted cloud and mobile devices, together with targeted ransomware attacks, continued to grow in 2019.** Attackers also increasingly conducted supply chain attacks, victimising service or product providers as stepping stones to attack their prime targets. Multiple e-commerce web sites were infected by Magecart style code injection attacks.

- **Cryptominers continued to be the most popular malware type in 2019 even though there was minor decrease in most regions.** Botnet and mobile malware were the second and third most common malware types respectively.

- **Attacks targeting Microsoft Remote Desktop Protocol (RDP) vulnerabilities (CVE-2019-0708 and CVE-2019-1182), Oracle WebLogic Servers remote code execution vulnerabilities (CVE-2017-10271 and CVE-20192725) and EXIM Mail server remote code execution vulnerability (CVE-2019-10149) were the top attacks detected in 2019.** Nevertheless, more than 80% of the detected attacks in 2019 targeted old vulnerabilities earlier than 2018.

- **Targeted ransomware attacks would continue the increasing trend in 2020.** Attackers would spend more effort to profile their victims so as to cause more serious impact and attain higher profits. More attacks targeting the Tokyo 2020 Olympics would be expected. On the phishing battlefront, more variety of phishing technique such as smishing, phishing by social media and gaming platform would be employed by the threat actors. Attacks targeting mobile users, particularly mobile malware, would increase in 2020. Attackers would also take advantage of the speedy 5G networks and enormous IoT devices to launch attacks. AI would be a double edged sword: security vendors would improve their solutions using this technology, while attackers would also use it to probe networks, identify weaknesses and improve the evasive ability of malware.

- **Organisations were recommended to adopt a prevention over detection approach to protect against cyber attacks.** Multi-layer protection covering different elements such as networks, mobile devices, various endpoints and cloud should be adopted, supplemented by up to date threat intelligence. Adoption of network segmentation, least privilege access control and zero-trust approach was also recommended for preventing malicious lateral movement within corporate network.

Source: Check Point

[20] https://pages.checkpoint.com/cyber-security-report-2020.html

Industry Insight on Cyber Security Threat Trends

New attack surface emerged with wider adoption of public cloud, 5G network and IoT technologies

Radware surveyed 561 individuals from various industries worldwide for their experiences and views on cyber attacks and compiled the "2019-2020 Global Application & Network Security Report"[21]. Predictions on the threat landscape in 2020 were also included in the report. The highlights from the report included:

- **94% of respondents experienced at least one cyber attack in 2019, whereas 20% of respondents experienced cyber attacks daily.** The most frequent attacked industries were education, retail, banking and finance. Nation-state attacks increased from 19% in 2018 to 27% in 2019.

- **Nearly one-third of respondents experienced DDoS attacks in 2019.** 42% of DDoS attacks lasted less than one hour and 10% of DDoS attacks were above 10Gbps. For those encountered DDoS attacks, 91% of respondents experienced DDoS attack against the application layer. 38% of them were not sure whether the DDoS attacks were originated by IoT botnet or not.

- **Almost 75% of respondents indicated that their organisations used at least one public cloud, whereas 44% adopted two or more public cloud solutions**. Almost 60% of respondents considered their data less secured in the public cloud. Web and application intrusion, and credential threats, accounted for 27% and 20% respectively, were the largest security threats to public cloud. Organisations should recognise that their existing protection mechanism for on-premises data and application might not be sufficient for protecting their data and applications in the public cloud environment.

- **26% of respondents opined the distributed nature of 5G networks could introduce new cyber threats.** On the contrary, 20% of respondents expected 5G networks could provide better information security and 31% of respondents anticipated the security level would be unvaried.

- **Researchers predicted that attackers would use bots to attack APIs and exploit the flaws in Kubernetes in 2020.** Moreover, hackers would abuse IoT devices to form the cyber arsenal and launch cyber attacks via 5G networks. Amplification attacks were expected to resurge in 2020. Major application breaches would also be expected in 2020.

Source: Radware

[21] https://www.radware.com/ert-report-2020/

Summary of Microsoft January 2020 Security Updates

10 Product Families with Patches

6 Critical

4 Important or below

Product Family	Impact[22]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems	Remote Code Execution	Critical ★★★★	KB4528760, KB4534271, KB4534273, KB4534276, KB4534293, KB4534306
Windows Server 2016, 2019 and Server Core installations	Remote Code Execution	Critical ★★★★	KB4534271, KB4534273, KB4534293, KB4528760
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4534283, KB4534288, KB4534297, KB4534303, KB4534309, KB4534310, KB4534312, KB4534314
Internet Explorer	Remote Code Execution	Critical ★★★★	KB4528760, KB4534251, KB4534271, KB4534273, KB4534276, KB4534283, KB4534293, KB4534297, KB4534303, KB4534306, KB4534310
Microsoft .NET Framework	Remote Code Execution	Critical ★★★★	KB4532933, KB4532935, KB4532936, KB4532938, KB4534271, KB4534276, KB4534293, KB4534306, KB4534976, KB4534977, KB4534978, KB4534979, KB4535101, KB4535102, KB4535103, KB4535104, KB4535105
.NET Core and ASP.NET Core	Remote Code Execution	Critical ★★★★	2.1: Security Update 3.0: Security Update 3.1: Security Update
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4484236, KB4484227, KB4484221, KB4484223, KB4484243, KB4484234, KB4484217 Microsoft Office 2019: Click to Run Microsoft Office for Mac: Release Notes

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

Product Family	Impact[22]	Severity	Associated KB and / or Support Webpages
			Microsoft Office 365 ProPlus: Click to Run
Microsoft SharePoint-related software	Information Disclosure	Important ★★★	KB4484165, KB4484157, KB4484143, KB4484142
Dynamics 365 Field Service (on-premises)	Spoofing	Important ★★★	Release Notes
OneDrive for Android	Security Feature Bypass	Important ★★★	Release Notes

Learn more:
High Threat Security Alert (A20-01-03): Multiple Vulnerabilities in Microsoft Products (January 2020) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=445)

Sources:

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