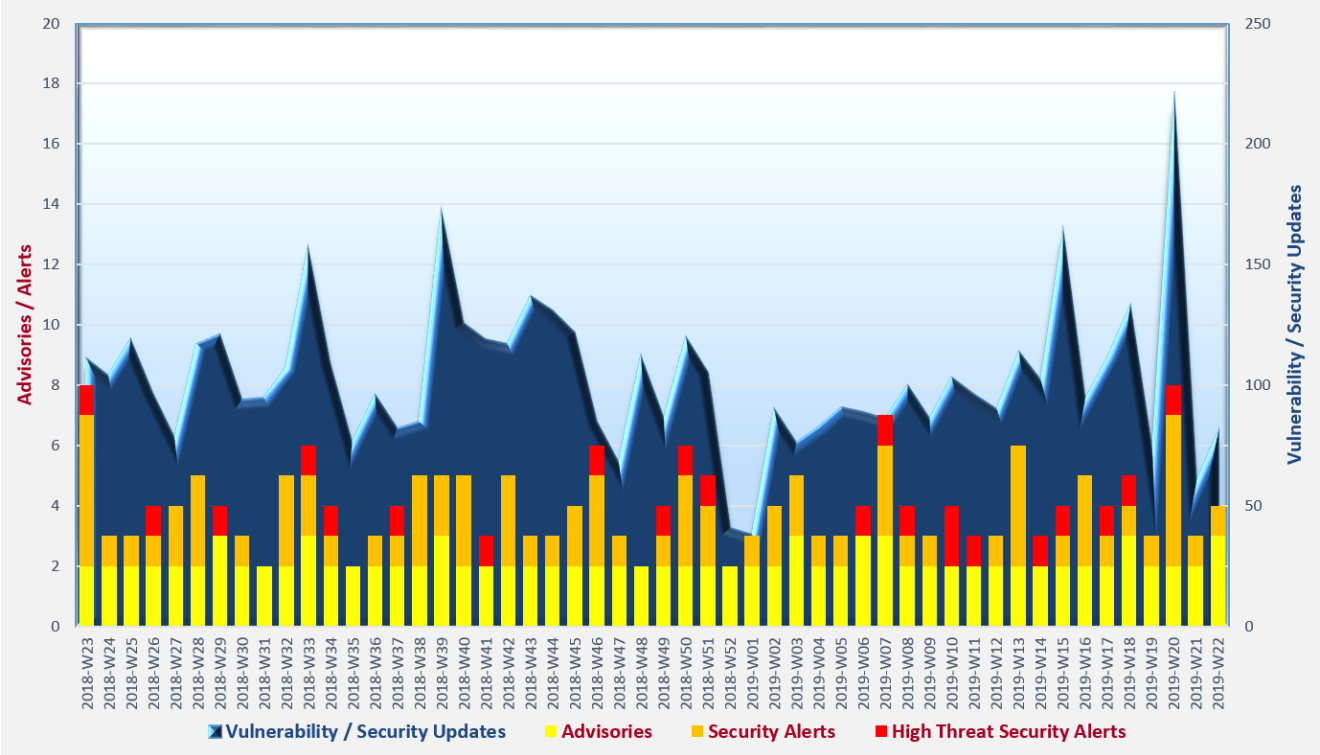
TLP:WHITE

Cyber Security Threat Trends 2019-M05

May 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:

- ✧ **Obsolete systems** could impose risks to cyber security. Organisations should plan for upgrading system components before they become end-of-support or deprived of security patches.
- ✧ **Attacks follow money** since threat actors are mostly motivated by financial gains. Businesses should conduct rigorous security risk assessments and protect their information assets accordingly.
- ✧ **Exploits** against system vulnerabilities can emerge rapidly. System administrators should race to patch known system vulnerabilities to stop potential exploitations.

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

CERT Advisories

Update your WhatsApp

GovCERT.HK[2], HKCERT[3,4], US-CERT[5], the UK National Cyber Security Centre (NCSC)[6], SingCERT[7], MyCERT[8] and Australian Cyber Security Centre (ACSC)[9] issued alerts on a security vulnerability identified in WhatsApp which allowed a remote attacker to install malicious code such as spyware on targeted mobile devices. Users were advised to update WhatsApp to the latest version offered by the official app stores immediately.

Attackers can exploit the Remote Desktop Services vulnerability (CVE-2019-0708) in Microsoft Windows products for remote code execution. Patch your system immediately

GovCERT.HK[10], HKCERT[11,12], US-CERT[13], NCSC[14], SingCERT[15], MyCERT[16] and ACSC[17] issued alerts on a vulnerability in the Remote Desktop Services. An attacker could exploit this vulnerability to remotely take control of an affected system. System administrators should patch the affected systems immediately.

Design and operate systems with security consideration

NCSC issued a guidance "Cyber security design principles"[18] for reference in designing systems, including identification of system elements need to be protected, securing the systems against compromise and service disruption, enabling detection on suspicious activities, and minimising the impact caused by compromise.

2 https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=390
3 https://www.hkcert.org/my_url/en/blog/19051401
4 https://www.hkcert.org/my_url/en/alert/19051402
5 https://www.us-cert.gov/ncas/current-activity/2019/05/14/Facebook-Releases-Security-Advisory-WhatsApp
6 https://www.ncsc.gov.uk/guidance/whatsapp-vulnerability
7 https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-exploit-targeting-whatsapp-vulnerability-cve-2019-3568-observed
8 https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=32444791-0bd9-45bb-bf29-260b8e15c363
9 https://www.cyber.gov.au/news/update-whatsapp
10 https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=391
11 https://www.hkcert.org/my_url/en/alert/19051507
12 https://www.hkcert.org/my_url/en/blog/19052301
13 https://ics-cert.us-cert.gov/Microsoft-Releases-Security-Update-Remote-Desktop-Services-Vulnerability
14 https://www.ncsc.gov.uk/report/weekly-threat-report-17th-may-2019
15 https://www.csa.gov.sg/singcert/news/advisories-alerts/microsoft-remote-desktop-services-remote-code-execution-vulnerability-cve-2019-0708
16 https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=6d136d13-2dfc-4c1d-bdd8-915335b08af5
17 https://www.cyber.gov.au/news/patch-to-protect-your-business
18 https://www.ncsc.gov.uk/collection/cyber-security-design-principles

Industry Insight on Cyber Security Threat Trends

71% of data breaches were motivated by financial gain, and 25% were for the purpose of espionage

Verizon analysed 41,686 security incidents, including 2,013 cases of confirmed data breaches. The observations and insights derived from the analysis results were published in the "2019 Data Breach Investigations Report"[19]. More details were presented below:

- **Public sector was at the top of the victim list, accounted for over 56% (23,399) of the analysed security incidents.** 330 of them were confirmed data breaches. The most prominent pattern in data breaches was Cyber-Espionage, recorded an increase of 68% from last year. It took months or even years to discover breach cases in the Public sector. Some of the data breaches were due to human erroneous or malicious behaviour such as inappropriately sent or published data. So regular review of user privileges should be conducted. Besides, organisations should detect any suspicious egress traffic that could be an indication of backdoor or Command and Control (C2) malware installation. In addition, up-to-date anti-malware software should be implemented in the end point devices.

- **Financial gain was the top driving force for data breaches since 2010, and it accounted for 71% of data breach cases in 2018.** The gain of strategic advantage, or espionage, was involved in 25% of data breach cases in 2018. 69% of data breach cases in 2018 were carried out by external threat actors.

- **Phishing was a common attack vector in data breach.** 32% of data breach cases still involved use of phishing, although findings from security awareness vendors indicated that the click rates in phishing continued to drop to around 3% in 2018. The report also revealed that 18% of clicks from the studied phishing data were from mobile devices, probably stemmed from the relatively small screen size and users often interacting with their mobile devices while performing other activities such as walking, talking, etc., which could side-track their security awareness to incoming messages.

- **Different industries encountered different attack patterns and actions, number and trend of attacks and targeted assets**, as indicated in the comparison presented in the report. Organisations should understand what assets attracted threat actors' interests, and apply multi-layers protection on their perimeter.

Source: Verizon

[19] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Industry Insight on Cyber Security Threat Trends

Phishing targeted Software-as-a-Service (SaaS) and Webmail services ranked as the top category of phishing for the first time, accounting for 36% of all phishing attacks

Anti-Phishing Working Group (APWG) analysed the phishing attacks information collected from its member companies and global research partners, and published the analysis results in its "Phishing Activity Trends Report Q1 2019"[20]. The key observations were:

- **Phishing targeted SaaS and Webmail services reached 36% in Q1 2019, became the most common category of phishing.** This was a notable increase when compared with 30% in Q4 2018 and 20.1% in Q3 2018. For the first time it overtaken phishing against payment services category, which accounted for 27% of all phishing attacks in Q1 2019.

- **The total number of detected phishing sites grew remarkably to 180,768,** a significant increase when compared with the 138,328 sites detected in Q4 2018. There was also an increasing trend within the 3 months of Q1 2019, with around 81,000 sites being detected in March. Number of phishing sites reported in January and February were around 49,000 and 51,000 respectively.

- **There was a steady increase within Q1 2019 regarding the number of unique phishing reports.** These unique phishing reports were "email campaigns", in which unique emails were sent to multiple users, enticing them to phishing web sites. The figure for January 2019 was 34,630, and rose to 35,364 and 42,399 in February and March respectively.

- **Phishers tended to use HTTPS protocol to deceive Internet users**, taking the advantage of misunderstanding on the padlock icon shown at the address bar of the browser. There were 58% of phishing sites used SSL certificates in Q1 2019, which was a record high since Q1 2015, and a noteworthy increase comparing to 46% in Q4 2018. Such increase was due to phishers could create free Domain Validated certificates easily, and more web sites were using SSL in general. Users should understand that the padlock icon was not assuring the web site was “safe” and avoid falling into the pitfall.

Source: Anti-Phishing Working Group (APWG)

[20] https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

Industry Insight on Cyber Security Threat Trends

Fraudulent emails from BEC (Business Email Compromise) scammers tended to adopt a more personalised approach to deceive their victims

Agari analysed data from 328 million domains, and examined 6.75 million domains with recognisable Domain-based Message Authentication, Reporting and Conformance (DMARC) to observe the current trends in phishing and email fraud and organisations' adoption of DMARC. It published the "Agari Q2 2019 Email Fraud & Identity Deception Trends Report"[21], and the highlights of the report included:

- **27% of identity-deception email attacks were launched from compromised accounts of trusted individuals and brands,** an increase of nearly 30% in the quarter, and made it the second common type of identity deception technique. Email attacks from compromised accounts were more difficult to be detected and handled, and hence they were considered as a competent means of deceiving the victims. Display name deception remained the most common type of attack, accounted for 53% of identity-deception email attacks.

- **Phishing attacks reported by employees increased by 25%, reaching 29,028 cases per organisation a year.** The time taken by the security operations centers (SOCs) to handle such reported phishing attack was around 6.5 hours per case, which increased 32% in the quarter. Despite 55% of the reported phishing cases were false positives, users should stay vigilant and report any suspicious email.

- **Only 6.75 million domains out of the surveyed 328 million domains had valid DMARC records.** This figure was increased for merely 1% over the period. Majority of those domains adopted DMARC used the default monitor-only setting. Organisation were suggested to implement a reject policy, which could stop unauthenticated emails from being delivered, and hence could block phishing that attempted to impersonate the organisation.

- **67% of BEC attacks used free and easily-acquired webmail accounts.** 20% of BEC emails were personalised to include the name of the recipients, making the scams to be more legitimate. Some of the BEC emails did not have malicious links or payloads, making them more difficult to be blocked by email security solutions. The subjects of most of the BEC emails were generic, but used words such as "Quick", "Request", "Urgent", etc. so as to give recipients a sense of urgency.

Source: Agari

[21] https://www.agari.com/email-fraud/ebooks/q2-2019-report.pdf

Industry Insight on Cyber Security Threat Trends

Fraud Attacks launched by rogue mobile apps tripled in Q1 2019

RSA published the "Quarterly Fraud Report Q1 2019"[22], showing their observations on global fraud trends on different attack vectors and digital channels. The highlights of the report were:

- **There were 41,313 fraud attacks from rogue mobile apps in the quarter, represented a 300% increase when compared with the 10,390 cases in Q4 2018.** In fact, attacks from rogue mobile apps ranked top in the quarter, accounted for around 50% of the 82,938 identified fraud attacks around the world. Phishing, Trojan horse, and brand abuse (such as misusing the brand of an organisation to mislead users) positioned the second (29%), third (12%), and fourth (9%) places respectively.

- **Canada (52%), Spain (16%), and the Netherlands (10%) were the top 3 countries victimised in phishing attacks**, accounting for 78% of total attack volume. The top 3 phishing hosting countries were the United Sates, India and Russia.

- **A 17% increase in card-not-present (CNP) fraud transactions was observed in the quarter.** 60% of the transactions value came from new devices with trusted accounts, indicating that threat actors used account takeover to conduct these fraudulent transactions.

- **In the quarter, 14.2 million unique compromised cards and card previews were found from online fraud stores,** a 33% increase when compared with Q4 2018.

- **Fraud-as-a-Service continued to develop.** A growing trend on using account takeover was observed in recent years, creating an increasing demand for account checkers, which were designed to test the credentials and hence verify the validity of accounts. Account checker web site which offer studio to facilitate the development of new account checkers emerged. Fraudsters could develop their own account checkers which did not exist before. With the proliferation of new account checkers available, organisations were expected to encounter more automated credential stuffing and account takeover activities. To counter the increasing threat, organisations should consider to deploy protective measures such as multi-factors authentication, behaviour analytics, and so on.

Source: RSA

[22] https://www.rsa.com/content/dam/premium/en/report/rsa-fraud-report-q1-2019.pdf

Summary of Microsoft May 2019 Security Updates

15 Product Families with Patches

8 Critical

7 Important or below

Product Family	Impact[23]	Severity	Associated KB and / or Support Webpages
Windows 10 for both 32-bit and x64-based Systems (not including Edge)	Remote Code Execution	Critical ★★★★	KB4494440, KB4494441,KB4497936, KB4499154, KB4499167, KB4499179, KB4499181
Windows Server 2016, 2019 and Server Core installations (2016, 2019, v1803, v1903)	Remote Code Execution	Critical ★★★★	Windows Server 2016: KB4494440 Windows Server 2019: KB4494441 Windows Server v1803: KB4499167 Windows Server v1903: KB4497936
Windows 7, 8.1 and Windows Server 2008, 2008 R2, 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB4499151, KB4499165, KB4499171, KB4499158, KB4499164, KB4499175, KB4499149, KB4499180
Microsoft Edge	Remote Code Execution	Critical ★★★★	KB4494440, KB4494441, KB4497936, KB4499154, KB4499167, KB4499179, KB4499181
Internet Explorer	Remote Code Execution	Critical ★★★★	IE 9: KB4498206, KB4499149 IE 10: KB4498206, KB4499171 IE 11: KB4494440, KB4494441, KB4497936, KB4498206, KB4499151, KB4499154, KB4499164, KB4499167, KB4499179, KB4499181
ChakraCore	Remote Code Execution	Critical ★★★★	ChakraCore
Microsoft Office-related software	Remote Code Execution	Critical ★★★★	Microsoft Office 2010: KB4464567 Microsoft Office 2013 and 2013 RT: KB4464561 Microsoft Office 2016: KB4464551 Microsoft Office 2019 Security Update: Click to Run

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

Product Family	Impact[23]	Severity	Associated KB and / or Support Webpages
			Microsoft Office 2016 & 2019 for Mac Security Update: Release Notes Microsoft Office 365 ProPlus Security Update: Click to Run Microsoft Office Online Server: KB4462169 Microsoft Word 2016: KB4464536
Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2003 R2	Remote Code Execution	Critical ★★★★	Windows XP, Windows Server 2003 and Windows Server 2003 R2: KB4500331 Windows Vista: KB4499180
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	Microsoft SharePoint Server 2019: KB4464556 Microsoft SharePoint Foundation 2013 SP1: KB4464564 Microsoft SharePoint Foundation 2010 SP2: KB4464573 Microsoft SharePoint Enterprise Server 2016: KB4464549
Microsoft SQL Server	Information Disclosure	Important ★★★	Microsoft SQL Server 2017 for x64-based Systems (GDR): KB4494351 Microsoft SQL Server 2017 for x64-based Systems (CU+GDR): KB4494352
Microsoft Dynamics	Security Feature Bypass	Important ★★★	Microsoft Dynamics 365 (on-premises) version 8.2 : KB4494412 Microsoft Dynamics 365 (on-premises) version 9.0 : KB4498363 Microsoft Dynamics CRM 2015 (on-premises) version 7.0: KB4499386
Microsoft .NET Framework	Denial of Service	Important ★★★	KB4499167, KB4494440, KB4495610, KB4495611, KB4495613, KB4495616, KB4495620, KB4498961, KB4498962, KB4498963, KB4498964, KB4499405, KB4499406, KB4499407, KB4499408, KB4499409, KB4499154, KB4499179, KB4499181

Product Family	Impact[23]	Severity	Associated KB and / or Support Webpages
.NET Core and ASP.NET Core	Denial of Service	Important ★★★	.NET Core and ASP.NET Core: Download
Microsoft Visual Studio	Elevation of Privilege	Important ★★★	Visual Studio 2015 Update 3: KB4489639 Visual Studio 2017 version 15.0 & 15.9 and Visual Studio 2019 version 16.0: Download
Azure DevOps Server, Team Foundation Server, and Nuget	Information Disclosure	Important ★★★	Azure DevOps Server, Team Foundation Server, and Nuget: Security Update Guide

Learn more:
High Threat Security Alert (A19-05-07): Multiple Vulnerabilities in Microsoft Products (May 2019) (https://www.crisp.govcert.gov.hk/portal/govcert/en/alerts_detail.xhtml?id=391)

Sources:

- Microsoft May 2019 Security Updates (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/e5989c8b-7046-e911-a98e-000d3a33a34d)