KPMG

COVID-19 | Cyber Security

Threat Update

May 2020

While organized crime volumes remain broadly constant, there has been a shift to COVID-19 themed phishing campaigns and fraudulent websites, as organized crime groups seek to monetise the fear, uncertainty and doubt many people feel during the pandemic.

Financial scams

A wide range of COVID-19-related financial scams are under way:

- The US Federal Bureau of Investigation[1] warns that government and healthcare buyers are being targeted by frauds with fake sellers and brokers purporting to provide personal protective equipment, ventilators and COVID-19 supplies.
- The Times of India[2] reports that Indian banks have raised concerns over scams tricking people into downloading applications via a SMS link to opt for the government payment moratorium.

Infrastructure

Organised crime groups have been building out attack infrastructure since mid January. MarkMonitor reports[3] that over 100,000 COVID-19-related domains have been registered since mid-January, with the greatest rate during the period 11-18 March.

Phishing and smishing campaigns

Extensive COVID-19-themed phishing campaigns are underway with cyber criminals exploiting the financial and healthcare sectors, and IT infrastructure:

- Hong Kong Monetary Authority (HKMA)[4] has alerted the public to phishing emails purported to be sent by The Hong Kong and Shanghai Banking Corporation Limited (HSBC).
- Fortinet reports[5] that the Lokibot malware is being spread via spear phishing emails purporting to be from the World Health Organization (WHO).
- Anomali reports[6] that threat actors are continuing to use COVID-19-themed lures to target multiple healthcare organisations, including a campaign which uses RTF to distribute HawkEye malware.
- PhishLabs reports[7] that criminals are exploiting workplace concerns such as outbreak prevention and shipment delays to distribute malware. Examples include Excel documents downloading Zloader and the Zeus Trojan, along with a second attack using the Nanocore remote access Trojan.
- Inky reports[8] the use of quarantine related emails sent by attackers masquerading as the US White House relating to extended quarantine, and detailing groundbreaking steps to slow the virus.
- Google reports[9] seeing 18 million COVID-19-related phishing emails a day in early April 2020, which it seeks to block on a daily basis.
- Malwarebytes[10] reports that cyber criminals and state advanced persistent threat (APT) groups have moved to use COVID-19 lures. Attacks include lure documents with links to malicious Microsoft Office templates, malicious macros, RTF exploits using OLEI related vulnerabilities, and malicious LNK files.

Fraudulent websites

Bank of China (Hong Kong) (BOCHK)[11] has issued a statement about a fraudulent website that intends to steal data, such as Internet Banking number/ user name of its customers.

Conferencing Platforms

While the most of these phishing attacks are attributable to malwares, a range of other exploitation techniques are being attempted targeting conferencing platforms:

- Threatpost reports[12] that attackers use emails purporting to be a CISO critical security advisory as the basis of phishing campaigns to steal WebEx credentials. It also reports[13] that fake apps masquerading as conferencing applications are being widely distributed. Skype dominates such fake email campaigns, with 42% of incidents targeting it.
- Security Affairs reports[14] that thousands of compromised conferencing platform credentials have been discovered on a Dark Web forum.

Mobile malware

Mobile devices are not immune from COVID-19 themed attacks:

- Singapore Police have warned[15] of WhatsApp scams involving takeover of accounts by targeting users using compromised accounts.
- Check Point research reports[16] discovery of 16 different malicious applications masquerading as legitimate COVID-19 applications. The applications embed malware to steal sensitive information or exploit premium-rate services. None of the apps were on official app stores.

Broader threat landscape

- Unit 42 reports[17] a global attack campaign by APT41 targeting Citrix, CISCO and Zoho network appliances using recently disclosed vulnerabilities. Multiple victims across healthcare, higher education, manufacturing, government and technology services.
- Threatpost reports[18] that the APT group known as DarkHotel has exploited a VPN zero day vulnerability of Chinese government agencies.
- Aqua reports[19] that hackers are targeting vulnerable Docker servers to deploy the malicious 'Kinsing cryptocurrency miner' using a misconfigured Docker API to run an Ubunto container.

Other Observations

Microsoft Security

Microsoft has issued a new threat intelligence and security bulletin[20] along with advice on how to secure remote working scenarios.[21]

Microsoft has also released patches for 113 CVEs with three vulnerabilities under active attack:

- CVE-2020-1020 – Adobe Font Manager Library Remote Code Execution Vulnerability.[22]
- CVE-2020-0938 – OpenType Font Parsing Remote Code Execution Vulnerability.[23]
- CVE-2020-0993 – Windows DNS Denial of Service Vulnerability.[24]

Attacks on 5G masts

And lastly, the BBC reports[25] damage to multiple 5G masts in the UK following ill informed rumours of links to COVID-19 incidence.

Recommendations

With an increasing number of countries encouraging citizens to stay, learn or work from home, cyber security remains as important as ever, but pragmatism is required.

KPMG has produced a range of advice which may assist:

- COVID-19: Immediate actions for the CIO and CISO
- COVID-19: Steps to staying cyber secure
- COVID-19: 10 considerations for working from home securely
- COVID-19: 9 security tips for video conferencing

Sources

1. https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic
2. https://timesofindia.indiatimes.com/business/india-business/emi-moratorium-fraud-banks-ask-customers-to-be-alert-not-to-share-otp-with-imposters/articleshow/75067375.cms
3. https://markmonitor.com/mmblog/covid-19-domains-whats-going-on/
4. https://www.hkma.gov.hk/eng/smart-consumers/beware-of-fraudsters/#fraudulent-bank-websites-phishing-emails-and-similar-scams
5. https://www.fortinet.com/blog/threat-research/latest-global-covid-19-coronavirus-spearphishing-campaign-drops-infostealer.html
6. https://www.anomali.com/blog/covid-19-themed-hawkeye-phishing-campaign-targets-healthcare-sector-dissection-of-the-maldoc-and-the-two-way-approach?&web_view=true
7. https://info.phishlabs.com/blog/covid-19-phishing-update-workplace-concerns-exploited-to-distribute-malware
8. https://www.inky.com/blog/white-house-phishing-scam-inky-catches-another-coronaphish
9. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond
10. https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure/
11. https://www.bochk.com/dam/bochk/desktop/top/aboutus/notice/20200428_Statement_EN.pdf
12. https://threatpost.com/cisco-critical-update-phishing-webex/154585/?web_view=true
13. https://threatpost.com/skype-apps-hide-malware/154566/
14. https://securityaffairs.co/wordpress/101475/deep-web/zoom-dark-web.html
15. https://www.todayonline.com/singapore/police-warn-resurgence-whatsapp-scams-involving-takeover-accounts
16. https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/
17. https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/
18. https://threatpost.com/government-vpn-servers-zero-day-attack/154472/
19. https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability
20. https://www.microsoft.com/security/blog/2020/04/08/microsoft-shares-new-threat-intelligence-security-guidance-during-global-crisis/
21. https://news.microsoft.com/en-my/2020/04/10/alternative-ways-for-security-professionals-and-it-to-achieve-modern-security-controls-in-todays-unique-remote-work-scenarios/
22. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1020
23. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0938
24. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0993
25. https://www.bbc.co.uk/news/technology-52281315

Contacts

Mark Bowra
Partner - Forensic
KPMG in Hong Kong
T: +852 2140 2323
E: mark.bowra@kpmg.com

Henry Shek
Partner – Head of IT Advisory
KPMG in China
T: +852 2143 8799
E: henry.shek@kpmg.com

Ravindranath Patil
Director - Cyber Response
KPMG in Hong Kong
T: +852 2826 7295
E: ravindranath.patil@kpmg.com

David Ferbrache
Global Head - Cyber Futures
KPMG International
T: +44 (0) 7545 124116
E: david.ferbrache@kpmg.co.uk

Pratiksha Doshi
Director - Cyber
KPMG in India
T: +91 22 6134 9200
E: pratikshadoshi@kpmg.com

You can learn more about **KPMG Cyber Response Services** via the QR code

kpmg.com/cn/socialmedia