ALSTON & BIRD

WWW.ALSTON.COM

CYBER ALERT ■

APRIL 7, 2020

Cybersecurity and COVID-19: Four Categories of Cyber Threats and Practical Tips in Response

By Kim Peretti, Amy Mushahwar, and Nameir Abbas

In our previous Cyber Alert, we noted that the shift to remote work in response to the coronavirus (COVID-19) pandemic could pose cybersecurity and information technology risks to companies, focusing on immediate concerns relating to an expanded work-from-home environment. In the midst of this environment, cybercriminals enjoy a target-rich world, with some individuals using unfamiliar technologies, employees finding workarounds for technologies that create inconveniences, and security teams either implementing technologies with known security risks or allowing exceptions with interim risk to support business needs during the crisis. We offered six practical tips for companies to consider as they prepared for the risks of the shift to remote work.

With companies now several weeks into this new reality, we have seen an explosion of cybercriminal activity taking advantage of the unique uncertainties of the COVID-19 pandemic. A recent FBI alert notes that the FBI's Internet Crime Complaint Center (IC3) has received over 1,200 complaints related to COVID-19 scams, and media reports and other government guidance point to the proliferation of phishing and similar exploits as well. At the same time, non-COVID-19 threats still exist, with cybercriminals and nation-state actors continuing to pursue other avenues of attack.

Scams That Target Individuals

Risks

As we previously warned, scammers and cyber threat actors follow the headlines, and COVID-19 is no different. Cybercriminals continue to find creative ways to trick users into falling for phishing emails. Successful phishing attempts can lead to additional unauthorized activity, such as business email compromise (BEC), installation of malware (including ransomware), theft of credentials or personal information, or account takeover.

One FBI alert from mid-March highlights the occurrence of fraudulent emails purporting to be from the Centers for Disease Control and Prevention, as well as emails that claim to be related to charitable contributions, general financial relief, airline carrier refunds, fake cures and vaccines, and fake testing kits. The IRS similarly expects criminals to take advantage of the government's COVID-19 relief programs as a fresh phishing lure, with the IRS urging taxpayers to be on the lookout for a surge of calls and email phishing attempts along those lines. These alerts and updates track U.S. Secret Service guidance from early March indicating that cyber criminals were posing as legitimate medical and health organizations to make phishing emails more convincing.

Practical Tips

- Companies should remain vigilant in monitoring for such threats and ensure that email threat prevention tools are operational.
- Consistent with government guidance, companies should consider reminding employees to avoid clicking on links or opening attachments from unsolicited email, and to otherwise be aware of other types of social engineering and scams. Companies should also consider testing their awareness of the issues through phishing simulations involving COVID-19-related topics.
- Given the unprecedented uptick in phishing activity, an additional consideration is whether email and related security tools are configured to appropriately reduce the volume of malicious emails or limit the risk of an unsafe click or download (e.g., what URL IP or URLs have been whitelisted by users, and may these whitelists be too broad?).

Attempts to Compromise Company Systems, Including Criminal and State-Sponsored Actors

Risks

The proliferation of phishing activity could result in an uptick in malware infections. As just one example of many, Interpol has warned of a significant increase in the rate of attempted ransomware attacks against hospitals and other organizations involved in the response to the COVID-19 pandemic, primarily via phishing. On a different note, in a recent alert the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) cites the resurfacing of the Zeus banking trojan in COVID-19-themed phishing campaigns targeting major banks in the U.S., Canada, and Australia. Another alert from the NJCCIC cites the occurrence of phishing emails that purport to be from the U.S. Small Business Administration and attempt to deliver a remote access trojan, targeting small and midsized businesses.

Of course, phishing is not the only method of delivering malware and compromising systems. For example, recent warnings from Microsoft caution that organizations in the health care sector are being targeted by cybercriminals seeking to exploit vulnerable gateway and VPN appliances in their efforts to deploy ransomware. More generally, there are reports of cybercriminals targeting organizations that use single-factor VPN, taking advantage of insecure wireless router configurations, and exploiting unpatched vulnerabilities.

Along those lines, and as described in our previous alert, COVID-19 and the shift to telework may strain company resources and staff at even the most sophisticated enterprises. At the same time, monitoring and analysis of systems is more important than ever due to the evolving threat landscape. While many cybercriminals look to exploit COVID-19-related fear and uncertainty, others – including those associated with nation-states – will continue to search for and exploit known or as-of-yet undiscovered vulnerabilities. For example, a recent FBI alert has highlighted continuing advanced persistent threat (APT) activity targeting a variety of industries using the Kwampirs malware. Similarly, the Center for Strategic & International Studies has identified several recent cybersecurity incidents involving APTs, with numerous and varied examples from the past few months.

These examples represent only a small sample of the wide array of attack vectors and malware that cybercriminals may use in COVID-19-related campaigns or other unrelated efforts.

Practical Tips

- Consistent with existing guidance from the NSA, which ranks updating and upgrading of software as the most effective mitigation strategy against known APT tactics, companies should ensure that existing software is appropriately updated and upgraded by doing the following:
  - Validate the IP ranges scanned by your vulnerability tool and enumerated network nodes (compare against an inventory scan, like NMAP).
  - Scan for vulnerabilities pre-upgrade and post-upgrade to validate the fix.
  - Review and address configuration vulnerabilities in accordance with risk in addition to patch-related vulnerabilities (both matter).
- More generally, CISA's broad range of insights on cybersecurity may provide a useful roadmap for mitigation strategies against these often sophisticated threats.

Telework Vulnerabilities

Risks

The shift to telework has changed how employees interact with company systems and data, introducing new risks. These risks include vulnerabilities in remote access tools or infrastructure such as VPN, reliance on insecure communication tools, and even supply-chain risks. Notably, the FBI recently issued guidance warning companies about unauthorized activity on video teleconferencing (VTC) platforms. In addition to the potential for disruption by unauthorized parties, the FBI warned that criminals could attempt to eavesdrop on VTC or other communications platforms.

Practical Tips

- Companies should consider whether VTC and other communications platforms are up to date and appropriately secured.

- Several large VTCs have issued security blogs or other guidance on what employees can do to better secure their meetings; consider appropriate training on VTC security.
- Companies should also consider reminding employees to carefully share links to VTC meetings or corresponding dial-in information, and to configure their VTCs to prevent access or intrusion by unauthorized parties.
- More generally, NIST offers a number of resources on telework cybersecurity that companies may wish to review in a broader assessment of their infrastructure.

Business Email Compromise

Risks

BEC remains a significant risk for companies, particularly in such uncertain times. In these types of fraudulent schemes, a criminal impersonates a key company or vendor contact and attempts to direct a payment or transfer to the criminal rather than the legitimate recipient. According to a recent FBI alert as well as recent FBI guidance, fraudsters have been observed impersonating vendors and asking for changes in payment due to COVID-19. A recent Federal Trade Commission (FTC) blog post similarly suggests that companies should be on the lookout for BEC activity. As the FTC notes, the COVID-19 pandemic complicates BEC prevention efforts by making the unusual seem usual or understandable. Companies may undertake atypical or rushed financial transactions due to economic circumstances, while at the same time employees work from home, potentially hampering communication between employees.

Practical Tips

- The FTC recommends identifying a central in-house resource for verifying payment instructions, and along the same lines the FBI recommends verifying changes via the contact on file.
- For employee payroll, consider issuing a paper check before changing the electronic transfer instruction with a direct deposit change notice in the check envelope.
- Consistent with these recommendations, it may make sense for companies to consider additional controls or protections for external payments, such as those destined for business partners or vendors.
- Companies should also consider reminding employees to be on the lookout for potential warning signs for BEC activity, such as last-minute changes to payment methods or instructions, account information, or communications platforms.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, TX 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor, Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 950 Page Mill Road ■ Palo Alto, California USA, 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333