COVID-19
ESF-17 Cyber Risk Management

COVID-19 Themed Cyber Attacks

In addition to the health concerns and significant disruption to businesses we are experiencing, there is an increase in phishing and malware campaigns exploiting the COVID-19 pandemic. Some examples include:

- The most common type of attack is credential phishing through email that looks legitimate
- Business email compromise cybercrime exploiting COVID-19; this campaign states that they are changing their banking details in response to COVID-19 and asks for payments to new account
- Advanced Persistent Threat (APT) groups distributing malware through coronavirus themed documents
- Several hospitals and other organizations having organizational emails spoofing the hospital's/organization's IT team, inviting staff to register with their user account details for a 'Corona Virus Awareness Seminar"
- Coordinated DDOS attacks disrupting access to information on websites

Emergency Support Function-17 (ESF-17) assesses that criminal cyber threat actors will attempt to gain access through indiscriminate phishing campaigns leading to compromised website or weaponized documents. They will exploit successful access for financial gain through blackmail, ransomware or payment redirection fraud.

COVID-19 Information Operations

Bottom Line Up Front[i]

- While COVID-19 continues to spread, so does disinformation surrounding the virus and national/state/local responses
- This merging of public health crisis and malicious online activity has amplified the threat posed by COVID-19
- Strong leadership that conveys accurate information at the local level regarding the depth and breadth of the threat is the best way to counter the 'infodemic' that has now run parallel to the outbreak

The COVID-19 pandemic has likely spurred state actors to launch disinformation campaigns according to the U.S. Department of State.[ii] There have also been multiple text and social media messages designed to insight fear and panic in recent days and weeks. One of the more common messages cited the Stafford Act as the legal authority to implement martial law and national lockdown – all of which are untrue. The World Health Organization (WHO) is working with Facebook, Twitter, and other social media outlets to combat misinformation during this pandemic.

Key Steps to Prevent Misinformation

- **Take the time to research before sharing**
- **Do not spread misinformation about prevention or cures**
- **Beware of posts that traffic in fear**
- **Don't trust everything you see online**

Recommendations & General Advice for Users

The Cybersecurity and Infrastructure Security Agency (CISA) and ESF-17 both encourage individuals to guard against COVID-19-related phishing attacks and disinformation campaigns by taking the following precautions:

- **Avoid** clicking on links in unsolicited emails and be wary of email attachments
- **Do not reveal** personal or financial information in emails, and do not respond to email solicitations for this information
- **Use** trusted sources – such as legitimate, government websites – for up-to-date, fact-based information about COVID-19
- **Verify** a charity's authenticity before making donations by reviewing the Federal Trade Commission (FTC) Charity Scams page

Additional physical security and data protection best practices should also be implemented:

- **Ensure** home router, firewall, WiFi default passwords have been changed to strong passwords
- **Update** firmware and software on home network equipment used to connect back to work through VPN
- **Store** sensitive or confidential information on encrypted media provided by your organization
- **Ensure** confidential paper documents are properly disposed of (e.g. shredding)
- **Always** lock your computer when leaving it unattended
- **Always** comply with your organizations policies and procedures to protect specific high-risk data elements regulated by HIPPA, IRS, PCI, etc.
- **Validate** you are running anti-malware/anti-virus software on work and personal computers

Cybersecurity Actions for your IT Team

The Cybersecurity and Infrastructure Security Agency (CISA) has identified that with remote work – or telework – as the new normal during the COVID-19 pandemic, IT teams must expand their view of the risk management horizon to include the typical enterprise virtual private network (VPN) solution and more. Some of the considerations recommended are as follows:

Telework Vulnerabilities

- Malicious cyber actors are identifying and exploiting VPN vulnerabilities
- VPN security updates are lagging due to the 24/7 operations
- Phishing emails targeting teleworkers to steal usernames and passwords
- Organizations that do not use multi-factor authentication (MFA) for remote access are more susceptible to phishing attacks
- Limitations of VPN connections availability can lead to impacting business operations to include IT security personnel's ability to perform cybersecurity tasks
- Users implementing "Shadow IT" (e.g. unmanaged software/assets)
- IT teams deferring patches on critical assets to keep network operations stable and available
- Network flattening in order to facilitate cross-enterprise resource access which would ordinarily prevent or detect a threat actor from gaining access
- Help desk task saturation leading to pressure to skip authentication or authorization steps

Mitigations

The following recommendations can assist in ensuring the security of enterprise operations while teleworking.

Mitigation Recommendations[iii][iv]
• Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations • Alert employees to an expected increase in phishing attempts • Ensure IT security personnel are prepared to ramp up the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery • Implement MFA on all VPN connections to increase security. If MFA is not implemented, required teleworkers to use strong passwords • Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications – such as rate limiting – top prioritize users that will require higher bandwidths. • Block or monitor file types that are not normally needed for business operations (e.g. ISO files) or should not be delivered as email attachments (e.g. SCR files) • Update firewall settings and whitelist only pre-approved websites and IP addresses • Leverage role-based rather than location-based identity and access management solutions, analytics, and controls • Establish second-factor authentication for formerly in-person processes, such as manual phone calls, etc. • Establish formal and transparent channels for corporate messaging to highlight what the enterprise is doing to address this pandemic

Additional Resources

NIST Telework Security Basics: https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics

DHS Teleworking and Protecting PII: https://www.dhs.gov/xlibrary/privacy_training/resources/teleworkbestpractices.pdf

CISA Coronavirus: https://www.cisa.gov/coronavirus

DHS Coronavirus: https://www.dhs.gov/coronavirus

LADH Coronavirus: http://ldh.la.gov/coronavirus/

Reporting

Report any cyber incident related to COVID-19-themed emails, attachments, or scams to the Louisiana FUSION Center at lafusion.center@la.gov or call 800-434-8007

---

[i] https://thesoufancenter.org/intelbrief-disinformation-and-the-coronavirus-covid-19/
[ii] https://www.theguardian(.)com/world/2020/feb/22/coronavirus-russia-disinformation-campaign-us-officials.
[iii] https://www.cisa.gov/coronavirus
[iv] https://www.ncsc.gov.ie/pdfs/COVID19Advice.pdf