COVID-19 Related Cyber Fraud and Misinformation Campaigns Disrupt Critical Industries

Threat actors are using the COVID-19 pandemic to cause greater business disruption by targeting front-line organizations across industries with cyber-attacks, phishing scams, fraudulent schemes, and misinformation. While the tactics may appear traditional, the exploitation of public fear, growing remote workforce, and rapidly changing global circumstances are resulting in a sharp increase in new and malicious activities by financially motivated actors and extremist groups.

Emerging Cyber Trends Linked to COVID-19

Aon's Cyber Solutions has observed the following recent trends related to the targeting of critical infrastructure, international organizations, essential industries, and individuals since the global outbreak of COVID-19.

- **Cyber actors target health organizations and essential retailers with DDoS attacks, malware or account takeovers**: Cyber-attacks against the health sector have surged since January 2020, according to reporting by global media outlets. Government agencies and international organizations such as the U.S. Department of Health and Human Services, and the World Health Organization have recently experienced attempted cyber-attacks by Advanced Persistent Threat (APT) groups, while hospitals across the U.S. and Europe are being shut down by malware and ransomware. Online retailers selling essential goods are also reporting record levels of malicious traffic and account takeovers as major cities enforce shutdowns.
- **Financially motivated threat actors sell custom exploit kits on the dark web:** Research conducted by Aon in late March across multiple underground marketplaces catering to English, Russian and Chinese speakers found threat actors offering signed or unsigned malware loaders that claim to be undetectable by commercial anti-virus tools for USD$400-1,000. These malware delivery kits use COVID-19 related topics as lures, resulting in victims downloading malicious attachments. The posts indicate that the malware runs on most Windows versions and may require a Java Runtime Environment installation.
- **Fraudsters exploit PPE supply chain disruptions:** Supply chain disruptions globally are resulting in an uptick in fraud schemes that exploit manufacturing shortages of essential items and Personal Protective Equipment (PPE). Due to the high demand and low supply of goods, official and open sources have reported a significant increase in online scams related to the sale of counterfeit medical supplies and treatments through clickbait and phishing as organizations attempt to procure PPE for their employees.
- **Cyber criminals lure individuals with economic stimulus checks:** Media reporting on economic stimulus plans by multiple governments has resulted in a recent spike in phishing and spear-phishing campaigns. These are where cyber criminals send fake emails from accounts that appear official such as a government agency or local tax organization to offer economic stimulus payouts. These emails typically contain malicious attachments or links that deploy malware, request payment, and steal personal information.
- **Extremist groups rally followers to attack critical infrastructure by spreading misinformation:** Global extremists groups such as ISIS and U.S.-based white supremacists are leveraging misinformation campaigns to exploit public fears associated with COVID-19, calling for attacks on critical infrastructure, faith-based organizations, and the health care industry. While their mobilization efforts appear to be unorganized and splintered, these groups are using social media and online platforms to spread false information about national and local government efforts to mitigate COVID-19, as well as rallying followers to take advantage of stretched police, security and medical resources.

We're here to empower results

Find out how our cyber security solutions can help you.

Visit **aon.com/cyber-solutions**
or call +1 212.981.6540

Continued >

Recommendations to Help Protect Your Organization

Organizations can take the following proactive measures to assess cyber risks related to infrastructure, assets and employees, as well as to mitigate potential security vulnerabilities.

- **Conduct vulnerability management for critical technologies and platforms**: Perform routine scanning, analysis, and testing for vulnerabilities on major corporate infrastructure. Does the organization have a holistic approach to identifying, tracking and remediating gaps across the environment?
- **Identify online security vulnerabilities and reputational risks**: Assess the organization's online footprint on the open, deep and dark web to identify active targeting, sensitive data exposure, leaked corporate credentials, fraud, and other types of reputational risks to the business and its employees.
- **Collect threat intelligence from official sources and peer networks:** Indicators of compromise such as malware samples, YARA rules, malicious IPs, suspicious email headers, and other artifacts are constantly evolving with the emergence of new cyber campaigns. Leverage cyber security alerts published by official sources, industry networks, and peer organizations to collect up-to-date data.

Recent threats include:

- A recent COVID-19 phishing scam used the email subject "COVID-19 – Now Airborne, Increased Community Transmission" followed by a spoofed display name (CDC INFO) and fake email (CDC-Covid19@cdc[.]gov).
- Another recent phishing campaign spoofing the World Health Organization aimed to deliver the Agent Tesla keylogger using the subject "Attention: List Of Companies Affected With Coronavirus March 02, 2020."
- Multiple business email compromise scams are using the subject line "Requesting COVID-19 Donations" or "COVID-19 Tax Refund."

- **Implement threat monitoring for the organization**: Triage threat intelligence collection efforts to monitor for security anomalies, suspicious or malicious behavior, and advanced persistent threats on or off the network. Does the organization have a monitoring program or tools to flag threats on an ongoing basis?
- **Evaluate critical third parties**: The organization should evaluate what its most critical third parties, supply chain, and business partners are doing in response to COVID-19 related security vulnerabilities or cyber threats. Have cyber due diligence or background checks been conducted to assess vendors?
- **Update security awareness training for employees**: Provide updated training to employees on cyber security best practices for remote working and managing corporate devices, as well as how to identify and report phishing scams. Do key personnel know "what to be on the lookout for," and do they know "what to do" in the event of a suspected incident?
- **Plan for cyber incidents**: Is the organization prepared for a cyber incident or breach, including options for cyber insurance? Have key processes, accountability, roles, responsibilities, partners, and tools been evaluated, defined, tested, and updated? Does the organization have relationships with incident response and digital forensics providers? When was the last time a tabletop or other "test" of current plans and processes was performed?

Continued >

References

1. https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN
2. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
3. https://healthitsecurity.com/news/covid-19-cyber-threats-hackers-target-dns-routers-remote-work
4. https://www.scmagazine.com/home/security-news/cybercrime/report-account-takeover-and-data-scraping-attacks-on-e-retailers-up-as-covid-19-surges/
5. https://kms.dsac.gov/communities/intelligence-products/files/trss-research-and-insights_covid-19-ppe.pdf/
6. https://hbr.org/2020/03/coronavirus-is-a-wake-up-call-for-supply-chain-management
7. https://www.businessinsider.com/covid-19-disrupting-global-supply-chains-how-companies-can-react-2020-3
8. https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-takes-further-steps-help-mitigate-supply-interruptions-food-and
9. https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf
10. https://www.ftc.gov/news-events/press-releases/2009/03/ftc-warns-consumers-about-economic-stimulus-scams
11. https://www.forbes.com/sites/kellyphillipserb/2020/03/28/beware-of-stimulus-check-scams-and-related-hoaxes/#6fbec11e4730
12. https://www.cnet.com/news/fbi-issues-warning-for-covid-19-stimulus-package-scams/
13. https://www.bbc.com/news/technology-51838468
14. https://kms.dsac.gov/communities/intelligence-products/files/u-fouo-jib-disruption-of-a-racially-or-ethnically-motivated-violent-extremist-2019-s-plot-to-attack-a-missouri-medical-center-03302020.pdf/
15. https://kms.dsac.gov/communities/intelligence-products/files/u-fouo-terrorists-exploiting-covid-19-pandemic-to-incite-violence-03-23-2020.pdf/
16. https://abcnews.go.com/Politics/homeland-security-warns-terrorists-exploit-covid-19-pandemic/story?id=69770582
17. https://www.dailysabah.com/politics/war-on-terror/turkey-fighting-terrorists-fake-news-campaigns-amid-covid-19-battle

About Cyber Solutions: Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon: Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates.

Stroz Friedberg, LLC, an Aon company, has provided the information contained in this paper in good faith and for general informational purposes only. The information provided does not replace the advice of legal counsel or a cyber security expert and should not be relied upon for any such purpose.

Empower Results®