Welcome to the COVID-19 Cyber Threat Roundup, a new NTIC Cyber Center threat intelligence product designed to keep our members apprised of the latest cyber threats and social engineering scams exploiting the COVID-19 pandemic. Unfortunately, even in these unprecedented times, profit-motivated cyber criminals and advanced persistent threats continue to take advantage of victims by exploiting their concerns about COVID-19 to gain unauthorized access to networks and data. The NTIC Cyber Center team continues to work diligently to bring you the latest open-source cyber threat information and we encourage you to forward all of our TLP:White products to whomever you feel would benefit. If you have received this product from a friend or colleague, you can subscribe directly through our website here.

Please consider letting us know how we're doing by answering our short survey.

We hope that all of our readers remain safe and in good health and we especially want to express our heartfelt gratitude to all who are on the front lines working tirelessly to battle this pandemic and helping those in need.

Sincerely,

The NTIC Cyber Center Team

Federal Partner Guidance and Announcements

FBI and CISA Warn against Chinese Targeting of COVID-19 Research Organizations
The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a public service announcement last week warning organizations researching COVID-19 of likely targeting and network compromise by the People’s Republic of China (PRC). Health care, pharmaceutical, and research sectors working on COVID-19 response should all be aware they are the prime targets of this activity and take the necessary steps to protect their systems.

China’s efforts to target these sectors pose a significant threat to our nation’s response to COVID-19. This announcement is intended to raise awareness for research institutions and the American public and provide resources and guidance for those who may be targeted.

The FBI requests organizations who suspect suspicious activity contact their local FBI field office. CISA is asking for all organizations supporting the COVID-19 response to partner with the agency in order to help protect these critical response efforts.

Additional technical details regarding the threat will be released in the coming days. CISA and the United Kingdom’s National Cyber Security Agency released a similar alert earlier this month warning of malicious actors targeting COVID-19 response organizations using a tactic of password spraying.

Current and Emerging COVID-19 Cyber Threats

Microsoft Detects COVID-19 Phishing Campaign Delivering LokiBot Malware

Researchers at Microsoft Security Intelligence uncovered a phishing campaign that uses COVID-19 lures to distribute the LokiBot information-stealing Trojan, which can pilfer credentials from web browsers, FTP, email accounts, and terminal programs. Threat actors are masquerading as official entities such as government agencies and financial institutions and sending COVID-19 related emails with malicious attachments. The malicious attachments are actually ARJ archive files disguised as PDF files, making them difficult to scan with antivirus software, especially if these files are password-protected. The NTIC Cyber Center recommends users remain vigilant for email phishing campaigns disguised as COVID-19 relief, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this campaign, notify your organization’s IT security team immediately.

Palo Alto Networks Observes COVID-19 Themed Malware Hosted within Public Could Infrastructure
Palo Alto Networks Unit 42 researchers discovered communication between public cloud infrastructure and domains known to distribute COVID-19 themed malware and analyzed attack patterns of the associated cyber threat actors. During this investigation, Unit 42 discovered more than 300 COVID-19 related malware samples, 20 unique IP addresses and domain names, and discovered over 450,000 network connections to potential COVID-19 themed malware hosts. The NTIC Cyber Center recommends all network administrators review Palo Alto Network’s report and proactively block the associated indicators of compromise (IoCs).

COVID-19 Cyber Threat Resources

Anomali COVID-19 Attack Resource Center
Anomali has created a free COVID-19 Resource Center to consolidate threat intelligence and guidance, share updates, and point to free resources and tools to help keep networks and systems protected against cyber threats exploiting the COVID-19 pandemic.

Cloudflare Offers Assistance to Governments during COVID-19
Cloudflare is providing a free package of services to state and local governments until September 1, 2020 to help them secure their web infrastructure and internal teams. These services include DDoS mitigation, web application firewalls (WAFs), support for custom SSL certificates, rate limiting, team security and authentication, and DNS filtering.

COVID-19 Cyber Threat Coalition
The COVID-19 Cyber Threat Coalition is a global community of volunteer cybersecurity analysts who collect and share cyber threat intelligence associated with campaigns exploiting the COVID-19 pandemic. Their resources include blacklists, a Slack Workspace for real-time sharing of indicators of compromise, and an Open Threat Exchange Group powered by AlienVault.

DomainTools: Free COVID-19 Threat List
DomainTools is providing a free, curated list of high-risk COVID-19-related domains to support the community during the Coronavirus crisis. The list will be updated daily and available for CSV download.

GreyNoise Provides Free Network Monitoring Service Alerts
Threat intelligence company GreyNoise is now offering a free alert service for organizations that
want to track and be notified of malicious activity originating from their networks.

**Microsoft AccountGuard Now Offered to Healthcare Organizations**

Microsoft is now offering its AccountGuard service for free to healthcare organizations such as hospitals, clinics, labs, frontline service providers, device manufacturers, and life science companies researching treatments for COVID-19 to help protect them from state-sponsored cyber attacks.

**Microsoft: Open-Sourcing New COVID-19 Threat Intelligence**

Microsoft has made some indicators of compromise associated with COVID-19 cyber threats publicly available through its Azure Sentinel GitHub repository and the Microsoft Graph Security API.

**National Cyber Security Alliance COVID-19 Security Resource Library**

To help individuals and organizations find resources they can use and share, NCSA has launched the COVID-19 Security Resource Library. This library features free and updated information on current scams, cyber threats, remote working, disaster relief, and more.

**PhishLabs COVID-19 Threat Intelligence**

PhishLabs is providing intelligence on coronavirus-themed attacks as a free resource to defenders. The intelligence is updated every business day with the latest email lures, URLs, and domains.

**SANS Security Awareness Work-From-Home Deployment Kit**

SANS has released a Security Awareness Work-From-Home Deployment Kit, which offers a wide variety of SANS public resources and paid training materials at no cost.

**SpyCloud Malicious COVID-19 and Coronavirus-Themed Domain Dataset**

To assist the information security community, SpyCloud researchers have compiled, enriched, and analyzed a list of over 136,000 hostnames and fully qualified domain names with COVID-19 or coronavirus themes from a variety of open-source feeds.

---

**COVID-19 Scams in the News**

![Coronavirus Scams](image)

**Beware of Contact Tracing Scams in Washington, Police Warn**

**Analytic Comment:** Law enforcement agencies in Olympia, Washington are warning residents of scammers posing as COVID-19 contact tracing investigators who are attempting to obtain personal
information from unsuspecting victims. These scammers send unsolicited SMS messages containing links that prompt victims to enter sensitive personal information that legitimate investigators would not normally collect, such as Social Security numbers, financial information, marital status, or immigration status. To avoid becoming victimized by this or similar scams, never provide sensitive personal or financial information during unsolicited phone calls, or in response to unsolicited SMS messages and emails.

Scams Exploit COVID-19 Giveaways via Venmo, PayPal, and Cash App

Analytic Comment: Researchers at Tenable are highlighting Peer-to-Peer (P2P) payment scams in which profit-motivated cyber threat actors are using social media platforms to promote "money flipping" scams masquerading as COVID-19 relief campaigns. Scammers spoof accounts of celebrities or other public figures and advertise financial relief, but ultimately trick victims into sending money to criminal accounts. For more information on these and similar scams, please see the NTIC Cyber Center’s blog titled Securing Our Communities: Peer-to-Peer Payment Scams.

Watch Out for the Coming Tsunami of Mortgage Rescue Phishing Scams

Analytic Comment: Researchers at KnowBe4 suggest a high probability that mortgage "rescue" scams will soon surface and target struggling homeowners throughout the remainder of 2020. Profit-motivated cyber threat actors will likely leverage and spoof legitimate relief programs to target homeowners who are struggling to make their mortgage payments, playing on their fears to collect sensitive personal and financial information. These scams could also be used to collect login credentials for work-based accounts, increasing the risk of successful cyber attacks conducted against organizations. When applying for financial relief, it is important to remember to visit the legitimate organization’s website directly, and to never provide sensitive personal or financial information through links provided in unsolicited emails or SMS messages.

Beware of SBA Loan Scams, Government Officials Warn

Analytic Comment: Government officials have issued a warning about US Small Business Administration (SBA) loan scams. Small business owners are advised to remain vigilant in guarding their sensitive business and personal information as profit-motivated threat actors are constantly seeking new ways to target victims, using email, SMS messages, and phone calls to collect this data. The current largest financial assistance program, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) has recently been exploited in this way to deceive and defraud victims. Prospective financial relief recipients are urged to check official sites for financial assistance.

Ready-Made COVID-19 Themed Phishing Templates Copy Government Websites Worldwide

Analytic Comment: Website spoofing is one of the most successful methods that threat actors use to steal sensitive data and deliver malware to victims. These techniques are especially effective during times of crisis and disaster, as people searching for information and assistance can easily be fooled into thinking the websites displaying official logos and verbiage are legitimate. Unfortunately, in today's ever-growing cyber threat landscape, everyone must remain aware of these types of threats and all organizations must commit to educating end users about these and other cyber threat campaigns.

Banks' DMARC Fail Puts #COVID19 Business Loans at Risk of Phishing

Analytic Comment: The most effective way today to combat the threat of phishing and email
spoofing is to implement and configure Domain-based Message Authentication, Reporting, and Conformance (DMARC), including Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM), on domain and email servers. Properly configuring and deploying DMARC, SPF, and DKIM on an enterprise network will improve email authentication, prevent your organization's emails from being spoofed, and reduce the risk of successful inbound and outbound phishing attacks. For more information about DMARC, including information about implementation, visit www.dmarc.org.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.

Disclaimer: The NTIC Cyber Center COVID-19 Cyber Threat Roundup is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up through our website, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on Subscribe to Receive Our Products at the top of the page, and enter your information.