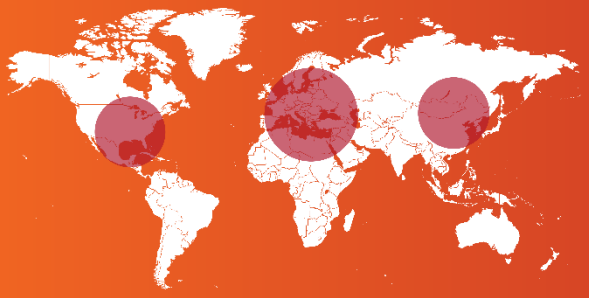
accenturesecurity

iDEFENSE
Part of Accenture Security

SITREP
CYBERSECURITY RISKS RELATED TO COVID-19

June 4, 2020, 16:00 UTC (12:00 p.m. ET), v.10.1

GEOGRAPHY



SEVERITY

INDUSTRY

- CMT
- Products
- FS
- H&PS
- Resources

SUMMARY

The worldwide COVID-19 outbreak, which the World Health Organization (WHO) declared a pandemic on March 11, 2020, continues to present global business with cybersecurity challenges, including opportunistic phishing campaigns, discontinuity of information security operations and long-term financial constraints. Companies in all industries should plan for these challenges to persist for months and to have long-term effects.

KEY CONSIDERATIONS

- Plan to execute months-long business continuity plans (BCP), including information security monitoring and response, while operating under quarantine conditions.
- The pandemic has created social engineering opportunities, including phishing campaigns. Phishing awareness is key, as cyberespionage and cybercriminal groups will take advantage of this condition while it remains active.
- BCPs, travel restrictions and remote work policies challenge enterprise monitoring, especially for companies that have not previously exercised BCPs. Companies should advise work-from-home employees on home router and Internet of Things (IoT) protection and virtual private network (VPN) best practices.
- The pandemic's economic and operational impact, which will create financial and budget challenges for companies' information security operations in the mid-to-long-term will pressure information security operations to maintain or increase coverage under tighter budgetary constraints. Companies will need advice on how to stratify, prioritize and outsource information security operations, and manage infrastructure and operational maintenance and growth.

ANALYSIS

COVID-19 INTRODUCES CYBERTHREAT OPPORTUNITIES

EXPLOITATION OF WORK-FROM-HOME POLICIES

To slow down infection rates and protect their workforces, companies worldwide have begun initiating work-from-home (WFH) policies. These conditions shift information security focus from enterprise infrastructure to cloud and virtualized infrastructure. WFH employees will rely on home Wi-Fi routers and VPN connections to company infrastructure, and misconfigurations risk the leakage and theft of sensitive company information. To help protect themselves from WFH vulnerabilities, companies should:

- Ensure employees are fully cognizant of company information protection procedures, including those regarding hard drives and file encryption in storage and in transit.
- Brief employees on home network best practices, including the use of non-default router and IoT passwords, SSID broadcast hiding and the configuration of trusted DNS providers.
- Ensure WFH employees understand how to configure and connect to company VPN providers and avoid split-tunneling.
- Plan fallback measures for phone-based and off-net communications and work, as many VPN providers may encounter scaling issues as large numbers of users join.
- Ensure the computers and devices WFH employees use are updated with the most current system and application versions.

CYBERTHREAT ACTORS AND GROUPS EXPLOITING COVID-19 CONCERNS

Threat actors will exploit unsecured conditions and numerous phishing campaigns, and potential mobile device vectors have already emerged, with these taking advantage of public concern and confusion about COVID-19 to use the pandemic as a lure. Researchers have attributed some campaigns to named groups while they have not been able to do so for others; some such actors and campaigns include:

- **ALBACORE** (a.k.a. APT15 and Ke3Chang), reportedly an advanced persistent threat (APT) group operating from China, is known to take advantage of well-known geopolitical events in its social network campaigns. This group's social engineering campaigns usually leverage malware attachments or malicious, embedded URLs that link to malware downloads that typically exploit older, more-reliable vulnerabilities across Microsoft Word, Oracle Java, and Adobe Reader. ALBACORE is reportedly associated with the CMStar malware variant observed in targeted attacks against the Belarus and Mongolian governments in the last several years.
- **ROHU** (a.k.a. Transparent Tribe, ProjectM and APT36), a threat group reportedly operating from Pakistan, has a history of diplomatic and political targets in the United States and India. This group reportedly produced a macro-based malicious Microsoft Word document spoofed to be a health advisory for COVID-19 from the Indian government. This malicious document drops Crimson RAT, a reported favorite of ROHU.
- **SNAKEMACKEREL** (a.k.a. Sofacy, APT28 and Fancy Bear), is a threat group reportedly of Russian origin. SNAKEMACKEREL operations continue to be some of the most far-reaching and sophisticated cyberespionage and intelligence campaigns to date. Actors reportedly associated with the group sent malicious documents, purporting to be the latest news on COVID-19, with an embedded C# backdoor Trojan to Ukrainian targets.
- **STICKLEBACK** (a.k.a. Kimsuky and Stolen Pencil), reportedly of North Korean origin, focuses its computer network intrusion operations against government and non-profit (e.g., think tank) organizations located in the United States and parts of East Asia, particularly South Korea. This threat actor group used COVID-19 as a lure to send documents with the Baby Shark malware to its intended victims.
- **POND LOACH** (a.k.a. OceanLotus and APT 32), reportedly an APT group operating in Vietnam, attacked the Chinese health department and agencies of Wuhan municipality using COVID-19-themed phishing lures, according to a Chinese information security report published on March 16. The POND LOACH group has been targeting Chinese energy-related industries, maritime agencies, marine construction, shipping companies and research institutes.
- **LUCIFERSHARK** (a.k.a. MUSTANG PANDA), reportedly operating from China, uses phishing to deliver weaponized Microsoft Office documents. The group deploys PlugLoadDLL, VMS Stager, and Cobalt Strike malware and traditionally targets non-governmental organizations and government agencies in Mongolia and Southeast Asia.

- **CANDLEFISH** (a.k.a. Patchwork and SideWinder), reportedly operating from India, allegedly targeted health organizations in Wuhan with COVID-19 phishing lures and triggered a Chinese patriotic hacktivist retaliation. This group also reportedly targeted Pakistan with a phishing attack using information regarding an alleged local Pakistani Army deployment to help combat COVID-19.

- **WINTERFLOUNDER** (a.k.a. Gamaredon), reportedly operating from Russia, allegedly targeted the Ukrainian government using COVID-19 as a lure and impersonating a Ukrainian journalist named Sashko Shevchenko.

- **ARCHERFISH** (a.k.a. APT27 and Emissary Panda), reportedly operating from China (https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox), purportedly used a .LNK file masquerading as a PDF file to infect victims with embedded malicious content using the COVID-19 pandemic as a lure (https://marcoramilli.com/2020/03/19/is-apt27-abusing-covid-19-to-attack-people/?utm).

- **SNIPEFISH** (a.k.a. DarkHotel), is reportedly behind an attack using a zero-day vulnerability in the Sangfor SSL VPN servers on Chinese government agencies in China and those operating in other countries (http://blogs.360.cn/post/APT_Darkhotel_attacks_during_coronavirus_pandemic.html). SNIPEFISH activity dates to at least 2007 and is likely responsible for thousands of successful compromises around the globe. Analysts have previously documented the group's use of zero-day vulnerabilities in many campaigns. These particular zero-day attacks appear related to the COVID-19 outbreak. VPNs serve as essential tools at the current time, with more people in many countries working from home.

  Syrian Electronic Army (a.k.a. SEA) is a prominent Arab hacktivist group that reportedly operates out of multiple cells both within Syria and in neighboring countries. A group with an IP address in the same block as the SEA reportedly used COVID-19 as lures to get users to install mobile applications targeting Arabic-language users; these malicious apps had names such as "Covid19," "Telegram Covid_19," "Android Telegram" and "Threema Arabic," among others (https://securityaffairs.co/wordpress/101754/malware/sea-targets-android.html).

- **NEEDLEFISH** (a.k.a. Lazarus, Bluenoroff, Hidden Cobra and APT38), a threat group reportedly operating out of North Korea (https://attack.mitre.org/groups/G0082/), is believed to have conducted both financially motivated and espionage operations, according to iDefense observations. The group uses an arsenal of tools during its operations, including a backdoor codenamed SYSCON (a.k.a. SANNY). The group reportedly distributed spear-phishing documents referencing COVID-19, specifically referencing the use of face masks and increases in cybercrime during the pandemic, to government targets in South Korea. These documents were the initial step in an infection chain that installed SYSCON to enable espionage operations (hxxps://s.tencent[.]com/research/report/969.html).

- Several COVID-19-themed phishing campaigns have targeted populations in the United States, the United Kingdom, Italy, Germany and Japan. Most of these campaigns have used common cybercrime malware, such as keyloggers, information stealers and banking Trojans, including Formbook, Lokibot, Ostap, TrickBot, AZORult and Emotet. Malicious actors have used some of these tools to steal credentials. These campaigns may impersonate official COVID-19 information providers such as the US Centers for Disease Control (CDC) and local experts.

- After 4-million Iranians installed it, Google removed an application to test and track infections of COVID-19 from Google Play; the Iranian government created the app, with the country's Health Ministry then persuading citizens to use it. Concerns were raised, as the developer of the app has connections with apps that in the past allegedly secretly collected user data (https://www.zdnet.com/article/spying-concerns-raised-over-irans-official-covid-19-detection-app/).

- Since January, parties have registered 4,000-6,000 COVID-19-related domains globally to support a wide array of malicious activity, including credential harvesting, carding fraud and malware installation. COVID-19 domains are reportedly 50 percent more likely to be fraudulent than are other domains.

- Criminal actors on Russian underground forums are soliciting people with Italian-language skills, suggesting a future increase in Italian-language phishing and mass spam campaigns; iDefense has observed some using the TrickBot malware. These solicitations have also targeted French- and Portuguese-speaking audiences. The malware campaign masquerading as a coronavirus map, which Reason Cyber Security Inc. discusses on its blog is an example of malicious domains that steal credentials (https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/).

- iDefense observed reporting to local police and news outlets of COVID-19-related extortion attempts in Denmark, Sweden, Portugal and the US. On average, these extortion attempts seek US$2,000-4,000 paid in bitcoins. Perpetrators typically send an e-mail stating that unless the target pays a certain amount in bitcoins, the perpetrator will ensure the victim becomes infected with COVID-19. Many of the targets are elderly, which indicates the threat actors behind this targeting possibly conducted some form of open-source intelligence before carrying out their attack. iDefense assesses with high confidence that the majority of these extortion attempts are scams with no actual threats behind them.
- Beginning on March 18, 2020, as news began circulating about the likelihood that the US would begin issuing stimulus checks to Americans, iDefense analysts observed discussions beginning on underground forums about how to exploit this. Several false-document sellers subsequently saw an increased demand for fake US documents. iDefense analysts assess with moderate confidence that some actors, especially US-domestic threat actors, will attempt to obtain fraudulent checks now that the CARES Act has become law. The trend will possibly increase the value of US personally identifiable information (PII) and may lead to the circulation of an increased number of false documents.
- iDefense has observed document sellers specifically mentioning the COVID-19 outbreak in reference to the obtaining of false documents, such as passports, driver's licenses, birth certificates and Social Security numbers for job requirements or to combat travel restrictions.
- iDefense continues to see daily phishing campaigns leveraging the COVID-19 theme, with most such campaigns delivering common cybercrime malware, such as keyloggers, information stealers, banking Trojans and a previously unknown backdoor dubbed BlackWater. iDefense also noticed new campaigns targeting additional locations such as Russian- and Spanish-speaking countries, along with India as the situation with COVID-19 worsens worldwide.
- A fake Android mobile app called "Coronavirus Finder" offers to show users infected people around them for 0.75 euros (US$0.82). This app requests and steals users' bank information and then infects users with the GINP banking Trojan (https://www.kaspersky.es/blog/ginp-trojan-coronavirus-finder/22193/).
- Actors who are presumably criminal in nature have sent hundreds of communications to direct consumers to a fraudulent UK website with the logo of the UK tax agency, Her Majesty's Revenue and Customs (HMRC). The website prompts users to provide their bank information to participate in a new (fake) tax refund program related to the COVID-19 outbreak. Once submitted, the malicious actors behind this site are able to use the input information to carry out credit card fraud and identity theft (https://www.ft.com/content/334ac60d-1f86-473f-a5dc-92b6f2d8bc56).
- According to information that cybersecurity and compliance solutions company Onapsis provided directly to iDefense, WFH policies, which organizations enacted to diminish the spread of COVID-19, have significantly increased those organizations' risks from Internet-accessible applications. For example, Onapsis observed a 35 percent increase in the number of Internet-accessible Oracle E-Business Suite Applications during the January-April 2020 period. Furthermore, Onapsis observed a 5-10 percent average monthly increase in the number of general business applications that vendors have made Internet-accessible since March 2020. Similarly, Onapsis observed a 44 percent increase in vulnerable, Internet-accessible SAP portals as organizations relax security controls to enable continued access to internal applications. Finally, Onapsis research shows the COVID-19 pandemic has coincided with the disclosure of an unprecedented number of SAP and Oracle vulnerabilities, with SAP releasing 11 notable "HotNews" security reports and Oracle releasing information about a record 399 vulnerabilities in April (https://www.oracle.com/security-alerts/cpuapr2020.html).
- Google's recent Threat Analysis Group update (https://blog.google/threat-analysis-group/updates-about-government-backed-hacking-and-disinformation) reports that "hack-for-hire" units have been conducting phishing activity distributing lure documents from Gmail accounts masquerading as the WHO. These groups, most of which Google claims are based in India, have targeted organizations in the financial services provider, consulting, and healthcare provider industries in the United States, Slovenia, Canada, India, Bahrain, Cyprus, and the United Kingdom.

COVID-19-RELATED DISCUSSIONS IN CYBERCRIME UNDERGROUND

While many threat actors are eager to take advantage of the global pandemic for monetary gain, some voices within cybercrime forums have expressed opposite opinions, refusing to use COVID-19 themes in cyberattacks:

- **Frenchy**, a vendor of a malicious Microsoft Excel macro has urged buyers to exploit COVID-19-themed cover stories to get better results from malware installations. This actor has built and is selling a malicious macro builder, offering discounts on this product on the Exploit forum, where Frenchy claims actors can use the product to "exploit Corona virus wave to get better results [sic]." iDefense sometimes observes product or service discounts in response to the emergence of a new threat vector, with threat actors making up the money lost due to reduced unit prices by the sheer volume of sales such discounts elicit. It would therefore seem that Frenchy's business is increasing.
- iDefense analysts found a significant increase in the sale of the popular Android banking Trojan "Cerberus" on criminal underground forums, including XSS, Exploit and Club2crd. Notably, the premier seller of the malware, the well-established threat actor on the XSS and Exploit forums who uses the name "Android," noted "I have sold more this week than the last 4 months" and claimed that "this week our bot was installed on 950,000 devices worldwide." iDefense analysts assess with moderate confidence that the increased demand and sale of Cerberus is due to the COVID-19 outbreak. Actor Android shares this sentiment, claiming "Due to the current threat of coronavirus to the world, mobile traffic has grown on the network" as the reason for the increased demand. iDefense notes this situation has created a significant threat to any Android user operating one of the affected applications as well as to targeted organizations. As of March 31, 2020, Cerberus operates overlays for seven French banking apps, seven US banking apps, one Japanese banking app and 15 non-banking apps.
- **jokerhttp**, a veteran threat actor who specializes in creating custom phishing lures, has posted new COVID-19-themed phishing kits for sale in the actor's usual advertisement space within the closed-door cybercriminal forum Exploit.
- **sweetMika7**, a threat actor running bulletproof hosting services, has offered seven days of service for free to existing customers in light of the COVID-19 situation.
- **Fireburn**, a fraudster in a Russian-speaking forum, showed some compassion in their comment on the threat actors offering fake COVID-19 maps leading to malware infections: "I decided to stay clear of this [targeting using COVID-19 themed attacks]. That's not like whacking $500 of PayPal or stealing PornHub accounts. At first I thought it'll be great with all the hype, but then I realized it's a tragedy and not just some mindless panic. I suggest everyone to stop exploiting this unfortunate event. I will also ask my customers to switch from COVID-19 landing pages to others."
- A threat actor running an online market selling high-capacity mailing server capabilities is offering a 20 percent discount promotion code, "COVID-2019," in light of the situation, and asks fellow threat actors to stay home.
- **Turnchoks**, a fraudster in a Russian-language forum, expressed interest in obtaining COVID-19-themed phishing lures for their own use.
- **madmobile**, in response to popular demand, has offered the sale of two false COVID-19-themed landing pages for the actor's Android inject service. madmobile offers injects as part of their own Trojan or for others to deploy via other Trojans. madmobile's landing pages are well crafted and therefore may cause victims to click on malicious links, making such pages especially threatening since they can deploy via multiple banking Trojans that actors are currently using to target major mobile banking apps. Moreover, according to data madmobile provided between January 23 and April 19, 2020, the actor has seen an explosive increase in the sale of their services, including 55,000 installations in April alone.
- **Mattcox** is a threat actor who has participated in a Dark Web market known for attacking Canadian entities. iDefense observed this actor offering a COVID-19-themed phishing kit targeting Canada Emergency Response Benefit (CERB), which provides income support for Canadian citizens whose incomes the pandemic has affected. The phishing lure, which Mattcox is selling for US$53, enables an attacker to set up a fake CERB application form. The threat actor stated that the lure supports 16 different Canadian banks, and asks recipients for an extensive amount of PII, such as security questions, Social Security numbers, birth dates, and more.
- **makdos92** is a threat actor who has participated in a closed-access cybercrime forum. iDefense observed this actor having posted a download link to a database

containing usernames and passwords for the website of the San Raffaele Hospital (HSR) cluster in Italy. The database contained 2,125 credentials to the hospital chain's website, http://hsr.it, which allows access to patients' PII and medical history. The Italian branch of the hacking group LulzSec originally tweeted a link to the data prior to makdos92's posting.

COVID-19-RELATED INDICATORS OF COMPROMISE (IOCS)

Please see the IoC addendum (Accenture_SITREPaddendum_IoCs_20200601_v12.docx).

VPN VULNERABILITIES

With increased use of VPNs, iDefense recommends organizations review their VPN security postures. Employee remote access to company networks has caused an increase in VPN traffic. To deal with the increase in monetary bandwidth costs, the VPN configuration that most organizations use most often is a "split-tunnel" configuration. In this configuration, a VPN client will only connect a user to an organization for the resources it needs from that organization and will connect the user directly to the Internet for everything else accessible only through an Internet connection. This setup saves a lot of bandwidth for organizations. Split-tunnel VPN configurations also lead to decreased monitoring from an organization's information security (infosec) team, as infosec teams will only be able to see organization-bound traffic, with no visibility into direct Internet traffic from remote hosts. iDefense recommends reviewing VPN configurations to make sure there are no unwitting DNS leaks of internal hostnames.

Since 2018, a handful of VPN vulnerabilities have become issues due to publicly available proof-of-concept exploits. This handful includes vulnerabilities in products from Citrix, Pulse Secure, Palo Alto Networks and Fortinet. Actors behind targeted attacks have also previously used some of the vulnerabilities in such attacks. iDefense actively monitors new exploits related to VPN applications and appliances and recommends patching and upgrading VPN applications to mitigate these threats. To mitigate VPN vulnerabilities, iDefense recommends:

- Applying patches to VPN servers.
- Upgrading to the latest firmware and operating system. After updating firmware and before reconnecting to an external network, iDefense recommends:
  - Resetting VPN credentials.
  - Revoking and generating new VPN server keys and certificates.

To harden VPN servers, iDefense recommends:

- Checking configurations to ensure no traffic leaks in split-tunnel configurations.
- Only using strong TLS (1.2 or greater) for SSL VPN servers.
- Avoid using self-signed certificates.
- Always using multi-factor authentication.
- Ensuring logging is enabled; include access, configuration and netflow information.
- Disabling any VPN management interfaces on external VPN interfaces.
- Disabling VPN server services not required.
- Dropping connections from countries in which no users connect.
- Analyzing logs and network traffic regularly to look for attack patterns and anomalous network traffic.
- Securing VPN Web applications by deploying a Web application firewall before it to inspect incoming traffic for attack patterns.
- Deploying an in-line distributed denial of service (DDoS) solution to scrub network traffic before it reaches VPN servers, for mission-critical networks.

SCALABILITY: PREPAREDNESS FOR DDOS ATTACKS AND SURGE IN DEMAND FOR CLOUD COMPUTING

Massive increases in bandwidth consumption puts most organizations at risk of DDoS attacks. Organizations that previously had over-provisioned bandwidth to deal with potential DDoS attacks have begun to use it for remote employees. This has led to decreases in bandwidth available to defend against DDoS attacks. With most of the workforce telecommuting, DDoS attacks have strong potential to cause operational downtime issues for organizations. There are ways to protect against DDoS attacks, but such techniques require some advanced preparedness. An organization's size may determine its options for DDoS protections. For example, medium-sized organizations can use appliances that provide in-line protection by scrubbing attack traffic. Organizations that see large-scale volumetric attacks would be better protected by scrubbing attack traffic at upstream providers but doing so requires such organizations to revise their routing configurations. Advanced planning and preparedness to protect against DDoS attacks will make a huge difference.

Since the WHO declared COVID-19 a pandemic, data center support teams have seen an increase in demand, leading to data center memory shortages. Organizations should plan to try to meet their cloud computing and data center resource needs and budget accordingly.

CYBERTHREAT ACTORS WILL TAKE FULLEST POSSIBLE ADVANTAGE OF RECENT HIGH-IMPACT VULNERABILITIES

Crisis conditions create short-term opportunities for cyberthreat actors. These actors are most likely to rely on recently announced vulnerabilities that targeted organizations may not have had time to fully patch. These will likely include the following high-severity vulnerabilities from the March 2020 Microsoft Security Bulletin, which iDefense recommends patching as quickly as possible: CVE-2020-0684, CVE-2020-0768, CVE-2020-0807, CVE-2020-0811, CVE-2020-0812, CVE-2020-0816, CVE-2020-0823, CVE-2020-0824, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0847, CVE-2020-0848, CVE-2020-0850, CVE-2020-0851, CVE-2020-0855, CVE-2020-0881, CVE-2020-0883, CVE-2020-0892 and CVE-2019-11510.

US GOVERNMENT WARNS OF TOP VULNERABILITIES

On May 12, 2020, the US Department of Homeland Security's (DHS') Cybersecurity and Infrastructure Security Agency (CISA) issued an alert naming top vulnerabilities that state, non-state and unattributed cyberthreat actors routinely exploit. The top 10 vulnerabilities in the 2016-2019 period were as follows: CVE-2017-11882, CVE-2017-0199, CVE-2017-5638, CVE-2012-0158, CVE-2019-0604, CVE-2017-0143, CVE-2018-4878, CVE-2017-8759, CVE-2015-1641 and CVE-2018-7600. Additionally, in 2020, cyberthreat actors were targeting unpatched VPN vulnerabilities CVE-2019-19781 and CVE-2019-11510, CISA wrote. The CISA alert also noted that cyberthreat actors were taking advantage of WFH arrangements to target poorly configured cloud collaboration services such as Microsoft Office 365. The CISA alert (https://www.us-cert.gov/ncas/alerts/aa20-133a) suggested mitigations for the noted vulnerabilities.

STATE-SPONSORED CYBERTHREAT ACTIVITY RATE STEADY; PREDICTED TO AFFECT HEALTHCARE-RELATED ORGANIZATIONS AND SERVICE GOVERNMENT REQUIREMENTS FOR INFORMATION AND INFORMATION CONTROL

After reviewing iDefense intelligence, open-source and government reporting, iDefense analysts have detected no change in state-sponsored cyberthreat activity related to the COVID-19 outbreak as of March 11, 2020. It should be noted that during the 2009 H1N1 outbreak, there was no noticeable reduction in what was presumably state-sponsored cyberthreat activity. Expectations are military and intelligence units are following strict infection control measures, as cyberespionage is a critical defense and economic development enabler for certain affected governments.

The effect of the pandemic on APT activity appears mixed as of March 17, 2020. On the one hand, Israeli media have noted a lull in regional activity originating from Iran, which could extend to cyberthreat activity. On the other hand, the virus panic serves as merely the latest tool in ongoing attempts to spy on, discredit and weaken adversary governments. Additional groups, including those based in or operating from Vietnam, North Korea and Russia, among others, are using virus fears as a lure in phishing campaigns targeting regional rivals.

Despite this steady rate of state-sponsored cyberthreat activity, Healthcare providers, vaccine developers, and government health and executive agencies have been targets of cyberespionage and ransomware. It is unclear whether the uptick in ransomware attacks is geopolitically motivated or not. If disruptive, financially motivated activity, including ransomware activity, continues to increase, prime targets (as in past activity) would include hospital groups, pharmaceutical labs, and crisis response agencies at the state and local levels. The healthcare and public health sectors, as well as other critical infrastructure sectors, remain attractive targets to adversaries and entities in those industries should maintain heightened awareness. Ransomware actors have taken advantage of the stress COVID-19 has had on medical organizations, likely seeking to extort higher ransoms. A Czechia hospital and an Illinois public health agency have each reported ransomware attacks related to COVID-19. The MailTo (Netwalker) malware the Illinois agency identified was recently used against an Australian logistics company, suggesting malicious actors are using the ransomware opportunistically rather than choosing medical targets (https://www.cyberscoop.com/czech-hospital-cyberattack-coronavirus/;

https://www.theregister.co.uk/2020/03/12/ransomware_illinois_health/).

Governments generally face pressure to obtain reliable pandemic information and control public information to minimize panic. As a result, state-sponsored cyberthreat actors will likely ramp up their efforts to gather controlled information from other governments, and some may use authorities to crack down on public information dissemination outlets domestically. Companies involved in healthcare and public services may find themselves in the crosshairs of these information-gathering efforts, which will not likely threaten such operations, but which could endanger the reliability of data that unauthorized parties access. Some state-sponsored threat groups have launched COVID-19-themed disinformation and influence operations to achieve political or economic goals. Please refer to iDefense's "2019 Cyber Threatscape Report" addressing "disinfodemics," which are epidemic-related disinformation threats.

CONTINUED ESPIONAGE, DISRUPTION AND DISINFORMATION AMONG STATES; CIVIL LIBERTY AND PRIVACY CONCERNS; CYBERSECURITY COMMUNITY FIGHTS BACK

As governments ramp up measures to contain COVID-19, they find it challenging to collect accurate data, stave off criminal opportunists, provide credible messages to their own populations, cooperate with other governments in tackling the virus, and balance public health with privacy and civil liberties concerns, noted below:

- Cyberespionage may increase as governments race to develop vaccines and tests, and as some attempt to lessen their dependence on foreign-made pharmaceuticals.
- Cybercriminals are targeting critical responders. Media have reported Netwalker ransomware attempts against a hospital and a government health agency, and persistent phishing campaigns against the WHO. Cybercriminal underground activity suggests more ransomware attempts in the future.
- Criminal activity is prompting swift public and private responses. Cybersecurity researchers have taken the initiative to share evidence and analyses of COVID-19-related cyberthreat activity and have even threatened retaliation against anyone targeting hospitals. The US Department of Justice has begun cracking down on COVID-19 fraud, as the prospect of US government relief payments has spawned the trade of stolen US identity documents. Underground activity shows cybercriminals are planning to target relief payments in the United States and United Kingdom at a minimum.

CYBERESPIONAGE CONTINUES, DESPITE SOFTER RHETORIC; SOCIAL STRAIN PROMPTS FURTHER INTERNET RESTRICTIONS

In the week of April 1-7, 2020, the leaders of Russia and China have discussed cooperation in phone calls with their US counterpart, signaling a softening of their harsh rhetoric of the week before. As Russia and Iran win support from UN officials for the easing of sanctions against them, these two countries may refrain from identifiable aggression in cyberspace in the hopes of attaining this long-held goal through diplomatic means.

Nevertheless, ongoing cyberespionage campaigns have not abated during the pandemic, as new reports indicate. Jorge Mieres, a threat intelligence researcher for MalwareIntelligence in Argentina, has purportedly observed a COVID-19-themed phishing campaign by WINTERFLOUNDER, reportedly operating out of Russia, appearing to target Ukrainian entities (https://twitter.com/jorgemieres/status/1244052428812701698).

As restricted movement pressures food supply chains, disruptions could prove fertile ground for Internet-based fraud. As an example, some customers seeking home food delivery have received malicious messages claiming there was a problem with their orders, requiring those recipients to provide their addresses and credit card information to resolve the supposed issue.

CONCERNS OVER CYBERCRIME, ESPIONAGE, AND DESTRUCTIVE ACTIVITY REMAIN

COVID-19-related economic, social and political disruptions bring new risks, as cybercrime and disease surveillance evolve in response. International tensions continue. Evidence, such as the following, continues to emerge about cyberespionage and possible state-sponsored destructive activity:

- **Cybercrime Risks for Government Programs Evolving:** Governments, in collaboration with the private sector, are quickly building and scaling relief programs, thereby creating a new attack vector, especially for attacking small- and medium-sized businesses.

- **Cybercrime Risks for Collaboration Tools Evolving:** The massive increase in telework, telehealth services and online classes is stressing some platforms and, in some cases, highlighting security and privacy concerns.
- **Espionage Continues:** After an apparent lull in Iranian cyberthreat activity, Reuters reported a phishing campaign targeting WHO employees' personal e-mail accounts, starting on March 2 and involving malicious websites with prior links to Iranian state-sponsored groups (https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC). It is unclear whether attackers successfully compromised any of the WHO e-mail accounts (https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC).
- **Possible Case of Border Gateway Protocol (BGP) Hijacking:** On April 1, 2020, Internet traffic for over 200 networks, affecting Google, Amazon, Facebook and others, was reportedly redirected through Rostelecom, Russia's state-owned telecommunications provider (https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others/). This could have merely been accidental; if it were intentional, it would have allowed Rostelecom to intercept traffic or spoof legitimate IP addresses for spamming.
- **Disruptive Attacks Continue with Possible State Influence in Targeting:** Microsoft has warned of ongoing human-operated ransomware attacks with malware such as Sodinokibi (a.k.a. REvil). Ransomware actors such as GandCrab (thought to control Sodinokibi) have paid deference to Russian government strategic priorities (https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf); state priorities could influence cybercriminals in their choices of targets and timing of ransomware attacks during the COVID-19 pandemic (https://dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/).
- **Potential Iranian Threat:** A February 2020 FBI alert (warned of a campaign using the Kwampirs remote access Trojan (https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf). Actors used Kwampirs against healthcare organizations and health-sector industrial control systems (ICS) as well as supply chains affecting numerous sectors. This malware has some code overlap with the Iran-linked Shamoon wiper, although the FBI did not see destructive code in Kwampirs and did not accuse Iran of being behind the malware.

DISINFORMATION, US AND UK WARNING, AND RISKS TO GOVERNMENT RELIEF EFFORTS

DISINFORMATION SPAWNS PHYSICAL ATTACKS

Extremists have used social media, drawing upon the COVID-19 pandemic, to threaten and urge violence against Muslims in India (https://www.reuters.com/article/us-health-coronavirus-india-paranoia-ins/vitriol-and-violence-a-coronavirus-death-exposes-paranoia-in-india-idUSKBN21G076). Additionally, extremist groups are leveraging social media to scapegoat target Jews, blacks, immigrants, politicians and law enforcement (https://www.vox.com/identities/2020/3/25/21190655/trump-coronavirus-racist-asian-americans; https://www.washingtonpost.com/national-security/far-right-wing-and-radical-islamist-groups-are-exploiting-coronavirus-turmoil/2020/04/10/0ae0494e-79c7-11ea-9bee-c5bf9d2e3288_story.html).

In the United Kingdom, false social media reports blaming the COVID-19 on 5G communications technology spawned attacks on 5G telephone masts and telecommunications company engineers. Well-organized networks of inauthentic social media accounts—in a pattern reminiscent of that of state-backed disinformation campaigns—initiated the campaign, according to Marc Owen Jones, a researcher at Hamad bin Khalifa University in Qatar. Since at least 2016, media sources like the website InfoWars and Russian state broadcaster RT have spread conspiracy theories linking 5G technology with various health risks, according to *Bloomberg* (https://www.bloomberg.com/news/articles/2020-04-09/covid-19-link-to-5g-technology-fueled-by-coordinated-effort).

JOINT US-UK ALERT OF COVID-19-THEMED ATTACKS

The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the UK's National Cyber Security Centre (NCSC) issued a joint alert on April 8, summarizing criminal and state-sponsored cyberthreat activity exploiting the COVID-19 crisis. This alert included summaries of phishing and short message service (SMS)-phishing campaigns that facilitate credential theft or the deployment of malware such as the Agent Tesla keylogger, the TrickBot malware, remote access Trojans or ransomware. Cyberthreat actors have also exploited the increased use of remote collaboration tools, with such actors launching phishing websites that spoof teleworking

platforms or launching attacks on unsecured Remote Desktop Protocol (RDP) endpoints (https://www.us-cert.gov/ncas/alerts/aa20-099a). The US-UK joint alert brings together lists of IoCs and public resources, many of which iDefense has already published as part of this SITREP series.

GOVERNMENT EFFORTS FACE CYBERSECURITY RISKS DUE TO COVID-19

Cybersecurity researchers in various countries have pointed out vulnerabilities in government relief program websites (https://krebsonsecurity.com/2020/04/new-irs-site-could-make-it-easy-for-thieves-to-intercept-some-stimulus-payments/) and privacy risks in government response programs COVID-19. (https://twitter.com/safe_runet/status/1249050167690645514; https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response).

Even sites without clear vulnerabilities have faced issues. For example, on April 10, Dutch police arrested a 19-year-old for suspected DDoS attacks on Dutch government sites that provide information on COVID-19 (https://securityaffairs.co/wordpress/101502/cyber-crime/ddos-for-hire-shutdown.html). In another case, users applying for benefits on an Italian social security website faced service delays and sometimes saw other people's personal data displayed on their screens during what initially appeared to be a cyberattack but which may have been due to overloading of the site (https://www.reuters.com/article/us-health-coronavirus-italy-cybercrime/italys-social-security-website-hit-by-hacker-attack-idUSKBN21J5U1).

The COVID-19 pandemic has affected government plans in other ways as well, such as the North American Electric Reliability Corp.'s (NERC's) request for the US Federal Energy Regulatory Commission (FERC) to delay enforcement of supply-chain cybersecurity standards due to COVID-19-pandemic-related work disruptions (https://www.eenews.net/stories/1062807343).

COVID-19 CYBERCRIME AND POLITICAL TARGETING MOUNT AS COUNTRIES TRADE BLAME

COVID-19-THEMED CYBERCRIME STATISTICS SOAR

There has been a clear increase in cybercrime exploiting the COVID-19 environment. Software and cybersecurity company VMWare Carbon Black observed a 148 percent increase in ransomware (https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/) while Google saw 18 million COVID-19-related malware and phishing e-mails daily over the week prior to reporting such on April 16 (https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond). Additionally, an FBI official said cybercrime reports to the FBI Internet Crime Complaint Center (IC3) website had risen from 1,000 daily a few months ago to 3,000-4,000 daily, with these complaints including a "good number" of COVID-19-related scams (https://news.yahoo.com/fbi-tracking-explosion-in-cybercrime-and-espionage-related-to-the-coronavirus-pandemic-200555069.html).

CYBERESPIONAGE CONTINUES

Several cases indicate cyberespionage cases related to COVID-19 have continued during this reporting period:

- A new campaign deploying the remote access Trojan PoetRAT targeted the government and utilities sectors in Azerbaijan, specifically targeting energy companies' supervisory control and data acquisition (SCADA) systems; the threat actors behind this likely sought credentials from Azerbaijan government officials, Cisco Talos reported (https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html).
- The FBI reported an uptick in "reconnaissance activity, and some intrusions" by unnamed state-backed hackers the FBI believes were likely seeking to steal intellectual property. These actors hacked into the systems of organizations engaged in biopharmaceutical research related to COVID-19. (https://www.reuters.com/article/health-coronavirus-cyber/update-1-foreign-state-hackers-target-u-s-coronavirus-treatment-research-fbi-official-idUSL1N2C41ZG).
- As nations and companies plan to improve resilience by reshaping supply chains, industrial espionage could increase (https://asia.nikkei.com/Editor-s-Picks/China-up-close/Xi-fears-Japan-led-manufacturing-exodus-from-China).

DISRUPTION AND EXTORTION AGAINST HEALTHCARE ORGANIZATIONS CONTINUES

The group behind the Maze ransomware leaked sample documents from patient payment services company Healthcare Fiscal Management Inc. (https://medium.com/@cyble/maze-ransomware-breached-healthcare-fiscal-management-inc-e4dd0ac8c5d3). On April 16, Czechia cybersecurity

officials warned of an unnamed "serious, advanced adversary" that had conducted spear phishing in advance of a "large-scale campaign of serious cyberattacks" on Czechia government- and health-related systems. The officials listed samples of malicious COVID-19-themed Windows documents that dropped malware capable of corrupting computers' master boot records (https://www.reuters.com/article/uk-czech-cyber/czechs-warn-of-imminent-large-scale-cyberattacks-on-hospitals-idUKKBN21Z00N). Czech officials did not name the adversary, but Czechia and Russia have been involved in a diplomatic tensions in recent weeks (https://news.expats.cz/weekly-czech-news/russian-extremists-attack-czech-embassy-in-moscow-over-pragues-removal-of-konev-statue/). In the following days, several hospitals and the Prague airport reportedly blocked cyberattacks (https://www.reuters.com/article/us-czech-cyber/prague-airport-says-thwarted-several-cyber-attacks-hospitals-also-targeted-idUSKBN2200GW).

ANTI-SURVEILLANCE ACTIVISM DAMAGES TELECOMMUNICATIONS SYSTEMS AGAIN

On April 14, the self-styled German anarchist collective Volcano Group claimed responsibility for a fire that damaged underground communications cables in Berlin that morning. An English-language version of the Volcano Group statement, on an anarchist blog post under the motto "Shut Down the Power / Sabotage Digital Infrastructure," said the group had damaged cables used by the Heinrich Hertz Institute, co-developers of an app tracing users' contact with those known to have COVID-19 infections, doing so in protest against the "repressive regulation of the population." The statement said the fire had also disrupted communications of nearby "climate killer" car dealerships (https://anarchistsworldwide.noblogs.org/post/2020/04/15/berlin-germany-arson-sabotage-attack-against-developers-of-the-new-corona-app/; https://www.morgenpost.de/berlin/polizeibericht/article228909289/Linke-Gruppe-bekennt-sich-zu-Brandstiftung.html). Eventually, the German government abandoned the Hertz Institute's contact tracing app in favor of a different app (https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKCN22807J).

TRADING BLAME ONLINE

Political messaging efforts continue. Social media analysis company Graphika reported on a campaign by a pro-Iranian news aggregator with the goal of amplifying content blaming the US for the pandemic's spread and praising China's work in limiting the disease (https://graphika.com/reports/irans-iuvm-turns-to-coronavirus/). Conversely, a "geopolitical Twitter war" has broken out between users in Thailand, Taiwan, Hong Kong and the Philippines and those in China, following a tweet claiming the virus may have originated in a Chinese laboratory (https://www.scmp.com/news/asia/southeast-asia/article/3079895/model-weeraya-sukarams-coronavirus-comment-sparks-twitter).

SECURITY ISSUES BEDEVIL GOVERNMENT EFFORTS AS COVID-19 PANDEMIC HEIGHTENS PRIOR COMPROMISE RISKS

New reports have detailed fraud involving COVID-19-related websites, including various governments' websites set up for relief payments:

- The FBI reported on April 22 that its IC3 had received over 3,600 complaints of COVID-19-related scams as of April 21. These scams included websites advertising fake vaccines, fake cures and fraudulent charity drives, as well as compromised legitimate websites; some of these domains harvested users' banking credentials or dropped malware. In addition, the FBI observed spoofed versions of domains the US Internal Revenue Service (IRS) set up to receive applications for COVID-19-related stimulus payments. The FBI noted that private sector cybersecurity researchers have helped enormously by identifying malicious domains and referring them to law enforcement for investigation. Cooperation between law enforcement, researchers and Internet domain registrars has led to the shutdown of hundreds of fraudulent domains (https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams).
- US relief efforts have prompted a rise in identity theft. *The New York Times* reported that calls to the Identity Theft Resource center, a San Diego nonprofit organization, soared 850 percent between March 2019 and March 2020. Threat actors can use stolen personal data, which they can purchase easily online, to apply for other people's unemployment and stimulus checks (https://www.nytimes.com/2020/04/22/technology/stimulus-checks-hackers-coronavirus.html).
- On April 21, the UK's National Cyber Security Centre announced it had taken down 2,000 COVID-19-related scams, including 471 fake online shops, and that it had launched a suspicious e-mail reporting service and a cyber-awareness education campaign (https://www.ncsc.gov.uk/news/public-urged-to-flag-covid-19-threats-new-campaign).

- A US Department of Defense cybersecurity program reported learning from a defense contractor that "a U.S. government Central Authentication Service login service was using a web service as an open redirect (proxy) to commit COVID-19 phishing" (https://www.defense.gov/Explore/Inside-DOD/Blog/Article/2156128/cyber-criminals-dont-brake-for-pandemics).
- Through its own research, iDefense analysts identified a phishing website exploiting the COVID-19 pandemic as lure to collect login credentials for customers of major Canadian banks. The actor-created main page presents what looks like the website for the Canada Emergency Response Benefit, a government relief program.

Cybersecurity lapses in government pandemic relief and control measures have resulted in the leaking of personal information:

- The US Small Business Administration (SBA) discovered on March 25 that its Economic Injury Disaster Loan (EIDL) loan application website may have inadvertently disclosed applicants' Social Security numbers, income amounts, names, addresses, and contact information to other program applicants, according to a letter it sent to applicants. The SBA confirmed on April 21 to media outlet Politico that the breach affected 7,900 EIDL program applicants and that the agency had relaunched the application portal after taking it offline to resolve the problem (https://www.washingtonpost.com/business/2020/04/21/sba-data-loan-small-business/; https://subscriber.politicopro.com/employment-immigration/whiteboard/2020/04/sba-data-breach-compromises-business-owners-data-3979643).
- A blockchain-based COVID-19 tracking app the Netherlands government reviewed accidentally leaked personal data when it published its code for public comment, according to RTL Nieuws (https://www.rtlnieuws.nl/tech/artikel/5095321/covid19-alert-datalek-crypto-digibyte-coronavirus-ministerie-app).

Cybercrime and cyberespionage involving health and public service organizations continues:

- iDefense and other researchers have observed threat group or actor the0time (Zero Time) offering for sale on multiple underground forums the source code and experimental data for artificial intelligence (AI)-assisted COVID-19 detection technology that a prominent Chinese AI company developed (https://www.forbes.com/sites/zakdoffman/2020/04/26/chinese-covid-19-detection-firm-just-got-hacked-data-for-sale-on-dark-web-new-report/#4b9b08ee5dec).
- Previously reported cyberespionage activity by Vietnam-based group POND LOACH against Wuhan health authorities and other Chinese government targets included the METALJACK remote-access malware, according to a new report (https://www.reuters.com/article/us-health-coronavirus-cyber-vietnam-idUSKCN2241C8).
- An April 22 report from Google's Threat Analysis Group detailed activity using spoofed versions of the WHO login page, likely designed to harvest login information from health organizations. Referring to previously reported activity appearing to originate from Iran, Google assessed that this "is consistent with" the threat group known as Charming Kitten, which iDefense tracks as SKATE. Google also identified similar activity from a South American actor known as Packrat, which iDefense tracks as RATFISH (https://blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats/). In the past, RATFISH has reportedly carried out espionage and disinformation campaigns as part of political conflict in Latin America (https://citizenlab.ca/2015/12/packrat-report/).
- Google reported a slight decrease in government-backed phishing e-mail volumes in March compared to January and February, with those phishing attacks possibly linked to quarantine-related staffing shortages. Google also reported having observed a government-backed campaign targeting US government employees' personal e-mail accounts (https://blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats/). In one of the government-backed campaigns Google did observe, threat actors targeted US government employees' personal e-mail accounts with phishing messages. In this campaign, phishing messages included links for free meals and coupons in response to COVID-19, or for purported online delivery services; the linked pages harvested users' Google account credentials.

The COVID-19 crisis highlights risks associated with previous infections:

- As a reminder of the continuing ransomware threat to hospitals, an April 16 alert from the DHS' CISA noted that the Pulse Secure VPN vulnerability tracked by CVE-2019-11510 continues to be a threat, even after patching it. Based on incidents at US government and commercial entities, CISA observed threat

actors obtaining plaintext Active Directory credentials after exploiting the CVE-2019-11510 vulnerability to gain access; threat actors can reuse those credentials even after organizations patch the VPN vulnerability if those organizations fail to change the stolen credentials. One threat actor made 30 unsuccessful attempts to connect to a target environment using compromised credentials, then gave up and attempted to sell the stolen credentials; CISA had previously observed this persistent threat actor successfully dropping ransomware on hospitals and US government targets (https://www.us-cert.gov/ncas/alerts/aa20-107a).

- On April 21, 2020, cybersecurity organization Team Cymru and Finnish company Arctic Security reported that research focusing on nine European countries and the United States found a surprising number of compromised corporate systems "lying dormant" behind corporate firewalls. After WFH policies went into effect and employees began to use VPNs to connect to corporate networks from outside their organizations' secure peripheries, the previously compromised corporate networks made malicious connections that the organizations' firewalls would have normally blocked (https://www.businesswire.com/news/home/20200421005295/en/Team-Cymru-Arctic-Security-Reveal-Number-Compromised; https://arcticsecurity.com/news/2020/04/17/number-of-potentially-compromised-organizations-more-than-doubles-since-january/).

Cyberthreat operations form a small subset of widespread fraud and self-dealing by numerous actors taking advantage of government spending on pandemic-related equipment and services worldwide; media reports indicate threat actors are carrying out identity theft, kickbacks, price-gouging and no-bid contracts in many countries (https://www.msn.com/en-us/news/world/a-pandemic-of-corruption-dollar40-masks-questionable-contracts-rice-stealing-bureaucrats-mar-coronavirus-response/ar-BB13dWG0?li=BBnb7Kz). Brokers who formerly dealt in cryptocurrency, financial technology and medical marijuana have flooded LinkedIn with fraudulent offers to procure scarce protective equipment from China (https://www.wired.com/story/linkedin-coronavirus-medical-equipment-ppe-shortage/; https://www.chinalawblog.com/2020/04/new-and-improved-china-ppe-scams.html).

CONTINUED FRAUD AND ESPIONAGE AGAINST GOVERNMENT RELIEF EFFORTS AND RESEARCH, RANSOMWARE AGAINST HOSPITALS, AND PRIVACY FLAWS IN DISEASE SURVEILLANCE TOOLS

LATE MAY STATISTICS SHOW CONTINUED HIGH LEVELS OF COVID-19-RELATED CYBERTHREAT ACTIVITY

Accenture's Cyber Investigation and Forensics Response (CIFR) incident response team has seen an approximately 25 percent increase in incidents, year over year, for the period of January-May 2020 compared to January-May 2019. Accenture does not have data to prove the year-over-year uptick is strictly related to COVID-19; the majority of the increase reflected incidents related to ransomware, account takeover (ATO), and business e-mail compromise (BEC) attacks. However, the timing of these events suggests a link with the pandemic, as most of the activity occurred in March and April 2020.

In a May 29 briefing, US Administration officials told a US Congressional subcommittee that the FBI's IC3 had received almost 10,000 complaints about COVID-19-related scams since the start of the outbreak, nearly tripling the figure reported on April 21. They added that CISA had blocked 7,000 malicious Internet domains used to collect sensitive information (https://oversight.house.gov/news/press-releases/agencies-brief-national-security-subcommittee-on-cybersecurity-risks-during).

Israel-based cybersecurity firm Check Point reported on May 12 that in the past three weeks it had observed COVID-19-related cyberthreat activity rise 30 percent to an average of 192,000 incidents per week (https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/).

Data on COVID-19-related phishing trends are mixed. US-based cybersecurity company Lastline reported on May 20 that it had seen a massive number of newly registered COVID-19-themed domains, but noted that only a fraction of those have been used in phishing attempts (https://www.lastline.com/labsblog/phishing-in-the-time-of-pandemic/). And, US cyberthreat research firm CrowdStrike reported on May 26 that it had detected fewer COVID-19-themed malicious lure documents over the previous three weeks, instead seeing spam e-mails that only briefly refer to the pandemic (https://www.crowdstrike.com/blog/covid-19-cyber-threats/).

GOVERNMENT ALERTS WARN OF CONTINUED FRAUD AGAINST COVID-19 RELIEF PROGRAMS AND GOVERNMENT-SUPPORTED RESEARCH

In mid-May the US Secret Service circulated a memo to field offices, describing a Nigerian identity theft ring that stole PII and used the data in fraudulent applications for unemployment benefits in numerous states, according to cybersecurity researcher Brian Krebs (https://krebsonsecurity.com/2020/05/u-s-secret-service-massive-fraud-against-state-unemployment-insurance-programs/). At least six US states warned residents who applied for the Pandemic Unemployment Assistance Program (PUA) and other unemployment programs that glitches in the PUA websites briefly leaked their data to other applicants (https://www.nbcnews.com/tech/security/four-states-warn-unemployment-benefits-applicants-about-data-leaks-n1212431; https://www.scmagazine.com/home/security-news/kentucky-is-6th-state-to-disclose-leak-of-unemployment-claims-amid-covid-19/). Accenture has found no evidence of actors selling this data or otherwise exploiting it.

Bank of America acknowledged that sensitive data from a small number of loan applicants under the US government SBA's Paycheck Protection Program had been inadvertently exposed on a testing platform on April 22. The SBA reportedly re-secured the data within a day (https://www.infosecurity-magazine.com/news/data-breach-at-bank-of-america/). Also reported on April 22, PII linked to 7,900 businesses that applied for Economic Injury Disaster Loans (EIDLs) may have been disclosed to other applicants of the program (https://www.infosecurity-magazine.com/news/us-covid19-relief-fund-leaks-data/).

At least nine supercomputer clusters throughout Germany, as well as in the United Kingdom and Spain, stood idle in mid-May after apparent cryptocurrency mining malware spread through academic computing networks via stolen SSH credentials. Many of these organizations had recently announced they were working on combating the COVID-19 outbreak, according to media reports (https://www.zdnet.com/article/supercomputers-hacked-across-europe-to-mine-cryptocurrency).

CRIMINAL SPOOFING OF GOVERNMENT DOMAINS AND REPUTABLE MEDICAL INSTITUTIONS CONTINUE

Microsoft documented a COVID-19-themed campaign that started on or around May 12, and featured e-mails that appeared to come from the "Johns Hopkins Center," referring to the reputable US medical center. Malicious attachments used Excel 4.0 macros to deliver the NetSupport Manager remote administration tool, a legitimate tool attackers use for malicious purposes (https://twitter.com/MsftSecIntel/status/1262504864694726656).

On May 19, 2020, a lure document referring to pandemic-related changes in the US Family and Medical Leave Act (FMLA) delivered the commodity banking malware BokBot (a.k.a. IcedID) (https://www.crowdstrike.com/blog/covid-19-cyber-threats/).

A spoofed version of a Russian government services website promised quarantine-related relief money but stole user data, according to Russian Web developer Dmitriy Belyayev (https://twitter.com/CuamckuyKot/status/1258031345739104257).

CYBERESPIONAGE TARGETS GOVERNMENT PERSONNEL AND LABS CONDUCTING COVID 19-RELATED RESEARCH

The UK NCSC warned on May 3 that foreign states—"experts" were attempting to steal vaccine and other COVID-19-related research data from British labs and universities. Such COVID-19-related intrusion attempts make up an increased proportion of all cyberthreat activity; however, activity against the UK overall had not increased during the pandemic (https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency).

On May 5, the NCSC and the US CISA issued an update to their April 8 joint alert, warning of espionage against pharmaceutical companies, medical research organizations, and universities. They reported observing state-linked threat actors scanning target organizations' websites for unpatched vulnerabilities and using password spraying to gain access to corporate e-mail accounts (https://www.us-cert.gov/ncas/alerts/AA20126A).

According to Indian press reporting, the Indian Army warned personnel in late April to download the government's COVID-19 contract tracing app AarogyaSetu only from official sources, saying Pakistani intelligence operatives were distributing malicious, mimicked versions of the app (https://www.newindianexpress.com/nation/2020/apr/30/indian-army-issues-warning-as-pakistani-spies-use-aarogyasetu-app-to-target-personnel-2137475.html). Other media reports attributed similar activity to cybercriminals (https://timesofindia.indiatimes.com/city/bhubaneswar/cops-sound-warning-on-fake-aarogya-setu-app/articleshow/75585902.cms).

A malicious e-mail campaign in April targeting Gilead, the drugmaker designing remdesvir, a promising COVID-19 treatment, used the same infrastructure as an e-mail campaign that targeted WHO personnel with malicious e-mails appearing to be from researchers and news organizations (https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV; https://www.bloomberg.com/news/articles/2020-05-07/hackers-target-who-by-posing-as-think-tank-broadcaster). The Iran-linked SKATE cyberthreat group appears to stand behind both campaigns. iDefense also reported earlier on a likely SKATE-linked campaign using spoofed versions of the WHO login page.

Ransomware attacks on hospitals continued as malware thought to be the Ekans (a.k.a. Snake) ransomware disrupted global IT operations of German-based hospital provider Fresenius on May 6. Researcher Brian Krebs cited an unnamed reader source as saying Fresenius had previously paid a US$1.5 million ransom (https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/).

PRIVACY CONCERNS REMAIN AS SURVEILLANCE TOOLS EVOLVE

Reports of privacy lapses in COVID-19 tracking and mobility apps continued, with one example being reports of excessive government surveillance of patients in Pakistan (https://www.codastory.com/authoritarian-tech/pakistan-coronavirus-surveillance/). The Care19 COVID_19 app US states North Dakota and South Dakota have been using sends location data to an outside company, according to *The Washington Post* (https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/?outputType=amp), while a flawed contact tracing app in Qatar exposed personal details of over a million people, according to Amnesty International (https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/).

INSIDER THREATS

There appears to have been a significant increase in risk from insider threats, especially from non-malicious insiders, due to COVID-19 and the resultant increase in WFH initiatives. This increased threat is mainly due to the volume of related phishing campaigns and people being more vulnerable to social engineering efforts than normal, as many are anxious to learn more about COVID-19 and how to prevent themselves from catching or spreading the virus. As a result, businesses should focus resources on training, awareness and communication of these increased security risks.

Insiders fall into two main categories: malicious and non-malicious, with the non-malicious category further divided into ignorant and complacent insiders. Non-malicious insiders increase security risks in this threat category the most, though malicious insiders are still likely to take advantage of the current environment surrounding COVID-19.

MALICIOUS INSIDERS

The COVID-19 pandemic is likely to increase opportunities for a premeditated malicious insider to take advantage of related situations. Such opportunities include: a lack of oversight, with WFH employees potentially feeling emboldened by working remotely and therefore more inclined to take risks; business processes that have become less rigorous due to new, temporary working practices; and easier data egress pathways. Coupled with potential motivating factors such as financial insecurity and job losses, these situations make it likely malicious insiders will be more inclined to commit fraud or steal intellectual property for future job opportunities or to sell. To protect against threats from malicious insiders, businesses can:

- Ensure key business processes or those that involve financial transactions are sufficiently rigorous and, if possible, monitor these processes.
- Revoke privileges belonging to furloughed or laid off staff as soon as possible (if appropriate in a furloughed situation).
- Monitor for large or critical data transfers and downloads, if possible, and/or increase monitoring of certain individuals of concern.

NON-MALICIOUS, IGNORANT INSIDERS

Ignorant insiders are more inclined to fall victim to the increasing numbers of phishing e-mails and texts related to COVID-19 than are insiders educated on such threats. COVID-19 has resulted in a huge increase in these types of e-mails and texts, which threat actors spoof to appear be from public bodies, demanding immediate actions. With COVID-19 increasing people's stress levels and related government orders making people potentially more compliant, incoming COVID-19-related phishing e-mails and texts may help create a recipe for disaster. It is also easy for criminals to impersonate senior leaders from businesses and demand actions from colleagues, such as making emergency payments etc., and malicious actors could take advantage of COVID-19 themes to do so.

Other ways cybercriminals may take advantage of COVID-19 relate to slow networks and IT issues. Cybercriminals could take advantage of such situations, purport to be from IT support teams and offer "help" with technical issues; in such scenarios, actors could use staff-granted system access to their advantage.

Criminals and state actors are likely to capitalize on the uncertainty, increased stress levels, and new working situations and processes to increase the volume and sophistication of social engineering attacks. To protect against threats from non-malicious, ignorant insiders, businesses can:

- Prioritize security training, employee awareness and communication of security risks, particularly with respect to COVID-19.
- Run security scans for spoofed e-mails and texts from both inside and outside of a given network and provide updates on results of these scans to staff as soon as possible for awareness.
- Ensure people have a clear line of reporting for security incidents and a mechanism to get help and advice if they need it.

NON-MALICIOUS, COMPLACENT INSIDERS

Risks involving complacent insiders include finding unsecured workarounds employees use to deal with WFH challenges (such as downloading unsecured online meeting apps and using unofficial document-sharing sites). These types of insiders are not likely to report security concerns, as they are unlikely to care to find out how to report such concerns; they may also start using unsecured devices for work purposes out of convenience, with both choices having the potential to create security issues. To protect against threats from non-malicious, complacent insiders, businesses can:

- Design and communicate easy "how to" guides for common WFH situations.
- Clearly communicate "dos and don'ts" related to work and define disciplinary actions that will follow non-compliance with such rules.
- Properly enable security information and event management (SIEM) solutions to detect unauthorized downloading and use of software and sites.

ADDITIONAL MITIGATIONS

Additional ways to protect against insider threats include using:

- Risk-based and/or multi-factor authentication (MFA) advanced access management systems to reduce the risk of compromise of company systems resulting from employee access to those systems.
- Identity governance (defining access, provisioning and deprovisioning access, implementing segregation of duties and recertification controls), as it reduces attack surfaces and limits opportunities for errors and malicious actions.
- Privileged access management for high-impact access points; this may include increased security measures, such as rotating passwords, recording sessions, and deploying analytics around privileged access. This solution can help reduce the risk of privilege escalation from an actor attacking via remote access routes.
- Organization-controlled phishing simulations and tests to improve employees' security behavior concerning phishing attacks.

All the above also enable logging and monitoring of activities pertaining to system access.

EXPERT, EXPERIENCED ADVICE WILL BE CRITICAL

To minimize targeting opportunities, companies should direct employees to the most-reliable local information source on COVID-19 and instruct employees not to fall prey to unfamiliar e-mails purporting to inform them about the pandemic; three reliable US sources are https://hub.jhu.edu/novel-coronavirus-information/, https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf and https://coronavirus.gov.

RECOMMENDATIONS

- Ensure employees are fully cognizant of company information protection procedures, including those regarding hard drives and file encryption in storage and in transit.
- Brief employees on home network best practices, including the use of non-default router and IoT passwords, SSID broadcast hiding and the configuration of trusted DNS providers.
- Ensure WFH employees understand how to configure and connect to company VPN providers and avoid split-tunneling.
- Plan fallback measures for phone-based and off-net communications and work, as many VPN providers may encounter scaling issues as large numbers of users join.
- Ensure the computers and devices work-from-home employees use are updated with the most current system and application versions.