CALIFORNIA CYBER SECURITY INTEGRATION CENTER

CYBERSECURITY ADVISORY | 17 MARCH 2020

COVID-19 Telework Activities Susceptible to Cyber Threats

Cyber criminals and nation-state actors are capitalizing on COVID-19 fears by registering malicious domains, distributing phishing emails, and developing malware containing Coronavirus themes. In some cases, healthcare provider networks are experiencing denial of service attacks. As employees increasingly shop and work from home to ease national infection rates, targeting of online retailers and VPN services is likely to intensify. Risk to telework activities may increase substantially as persistent threat actors and unforeseen vulnerabilities continue to materialize during global states of emergency.

On March 4th, 2020 the Governor of California declared a state of emergency to combat Corona Virus Disease 2019 (COVID-19) infections in the region. [1] Nearly a week later, as COVID-19 officially became a pandemic, the President of the United States (POTUS) declared a state of emergency for the country. [2] As California public and private entities implement telework plans across the state, there's increasing evidence of cyber threat actors capitalizing on the fear and panic gripping the globe. Consequently, the confidentiality, integrity, and availability of systems required for the successful execution of mission essential tasks are at increased risk of being compromised. The potential for loss of life is real, therefore methodically applying mitigations to counter the threat is highly prudent.

Spikes in Coronavirus-themed phishing, malware, and domain registrations are now widespread, along with some indications of distributed denial of service (DDoS) attacks targeting healthcare providers. The motives for these malicious activities vary, but financial gain, espionage, and malign influence conducted by criminals and nation-state actors are the primary objectives.

- **Domain Registrations**: In mid-February, as reported cases of infections increased, corresponding surges in domain registrations followed. Typical of pre-attack preparations, threat actors procure new domains [3] and perhaps SSL certificates to impersonate legitimate Internet services [4] while obfuscating domain whois records using privacy services in order to evade attribution. [5] Domain name variations for the terms "coronavirus" and "covid19" have been common. [6]

- **Phishing**: By leveraging newly registered malicious domains and spoofing email addresses of legitimate healthcare organizations such as the Centers for Disease Control and Prevention (CDC), threat actors are able to lure victims into clicking hyperlinks or opening attachments which lead to compromise. [7] Due to COVID-19 opportunists, the magnitude of email scams is the worst seen in years. Targeted industries include aerospace, transport, manufacturing, hospitality, healthcare and insurance while phishing content is written in English, French, Italian, Japanese, and Turkish languages. Victims are lured by emails promising cures, offering tax refunds, suggesting novel safety measures, declaring new high-risk zones, and soliciting bitcoin donations. [8]

- **Malware**: Aside from delivering malware via phony domains, in one instance a threat actor developed a portable executable to display a Coronavirus infection map masquerading as a John Hopkins University service. Once executed, the map drops information-stealing malware known as AZORult. [9] A malicious Android app named "CovidLock" also poses as a COVID-19 heatmap, but encrypts a user's phone with ransomware once installed. [10]

  Some hackers have no qualms about attacking healthcare facilities. [11] Following an unspecified attack at the University Hospital Brno in the Czech Republic where COVID-19 treatments take place, test results were delayed for days and examinations prolonged as medical staff resorted to completing paperwork by hand. [12]

- **DDoS:** Unknown threat actors attempted to degrade the United States Health and Human Services (HHS) website via a DDoS attack on 16 March without success, followed by a disinformation campaign which spread rumors about a nationwide quarantine. The fake claims were subsequently dispelled by the National Security Council (NSC). [13]

As cyber threat activity continues to propagate, it exacerbates challenges already faced by an overstretched medical services industry. An organization's limited resources coupled with the elevated sense of urgency may degrade cybersecurity defenses as individuals rush through high priority tasks and divert their attention to address frequent deadlines, perhaps letting their guard down during the process.

Recent upsurges in online shopping and telework – triggered by medical advice to "social distance" and "self-quarantine" during the pandemic – expose additional vulnerabilities. Online retailers such as Amazon regularly experience upticks in phishing activity during the holidays [14] and special events. [15] As Amazon hires thousands of additional employees to keep up with demand during the coronavirus outbreak, [16] the company's customers may again become an attractive target. Many of those same customers could be teleworkers involved in performing critical objectives for the state.

Telework comes with its own set of challenges. As outlined by the Cybersecurity and Infrastructure Security Agency (CISA), employees who utilize virtual private network (VPN) solutions to gain remote access to privileged employer data must beware of credential harvesting attempts, exploitable (unpatched) access points, and denials of service caused by limited VPN connections or sabotage. [17]

CALIFORNIA CYBER SECURITY INTEGRATION CENTER

CYBERSECURITY ADVISORY | 17 MARCH 2020

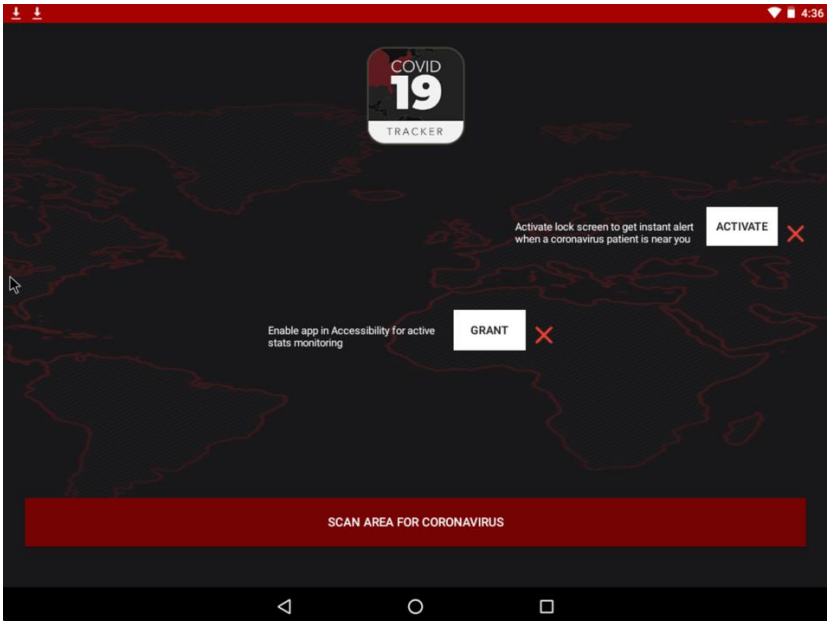

FIGURE 1 – Malicious COVID-9 Tracker app for Android attempting to take full control

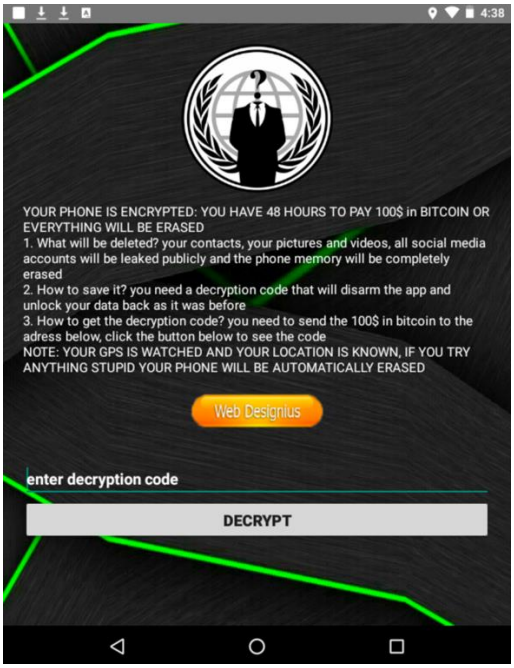

FIGURE 2 – Ransom note produced by COVID-19 Tracker app for Android

CALIFORNIA CYBER SECURITY INTEGRATION CENTER

CYBERSECURITY ADVISORY | 17 MARCH 2020

Indicator Type	Indicator Value
Host	dating4sex[.]us
Host	coronavirusapp[.]site
Host	coronavirusupdate[.]tk
Host	bestcoronavirusprotect[.]tk
Host	coronavirus[.]cc
Host	vaccine-coronavirus[.]com
Host	survivecoronavirus[.]org
Host	corona-virus[.]healthcare
Host	coronavirusaware[.]xyz
Host	bgvfr[.]coronavirusaware[.]xyz
Host	coronavirus-realtime[.]com
Host	coronavirus[.]zone
Host	blogcoronacl[.]canalcero[.]digital
Host	coronavirus-map[.]com
Host	coronavirusstatus[.]space

TABLE 1 – Indicators of Compromise (IOCs)

In light of the threat, the following mitigations should be considered:

- Enable Multifactor Authentication (MFA) for email and VPN services
- Narrow COVID-19 situational awareness consumption to a handful of trusted, familiar sources in order to more easily detect social engineering attempts. Trusted sources may include the following:
    - California Department of Public Health (**cdph.ca.gov**)
    - U.S. Department of Health & Human Services (**hhs.gov**)
    - Centers for Disease Control and Prevention (**cdc.gov**)
    - World Health Organization (**who.int**)
- Conduct user training by integrating telework and COVID-19 themes
- Mitigate the impact of DDoS activity by filtering network traffic using on-premise address, port, and/or protocol blocking methods or garner technical assistance from Internet Service Providers (ISPs) and Content Delivery Networks (CDNs)
- Install mobile phone apps from trusted distributors who prevent malicious code
- Detect and block indicators of compromise (IOCs) such as IP addresses, email addresses, file hashes, domains, and URLs

- Refer to CISA's Risk Management for Novel Coronavirus (COVID-19) guide for further information. [18]
- Visit the Cal-CSIC website for further information concerning telework risk management. [19]

ADMINISTRATIVE NOTE

For further information concerning this report, please contact Cal-CSIC at CalCSIC@caloes.ca.gov or (833) REPORT1.

ENDNOTES

[1] Online publication; *California Office of Governor; Proclamation of a state of emergency*; 4 March 2020; https://www.gov.ca.gov/wp-content/uploads/2020/03/3.4.20-Coronavirus-SOE-Proclamation.pdf; accessed on 16 March 2020.
[2] Online publication; *FEMA; COVID-19 Emergency Declaration*; 13 March 2020; https://www.fema.gov/news-release/2020/03/13/covid-19-emergency-declaration; accessed on 16 March 2020.
[3] Online database; *MITRE ATT&CK; Buy domain name*; 17 October 2018; https://attack.mitre.org/techniques/T1328/; accessed on 16 March 2020.
[4] Online database; *MITRE ATT&CK; SSL certificate acquisition for domain*; 17 October 2018; https://attack.mitre.org/techniques/T1337/; accessed on 16 March 2020.
[5] Online database; *MITRE ATT&CK; Private whois services*; 17 October 2018; https://attack.mitre.org/techniques/T1305/; accessed on 16 March 2020.
[6] Online article; *Forbes; Coronavirus Scam Alert: Watch Out For These Risky COVID-19 Websites And Emails*; 12 March 2020; https://www.forbes.com/sites/thomasbrewster/2020/03/12/coronavirus-scam-alert-watch-out-for-these-risky-covid-19-websites-and-emails/#2c6187651099; accessed on 16 March 2020.
[7] Ibid.
[8] Online article; *BBC; Coronavirus: How hackers are preying on fears of Covid-19*; 13 March 2020; https://www.bbc.com/news/technology-51838468; accessed on 16 March 2020.
[9] Online article; *Reason Security; COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report*; 9 March 2020; https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/; accessed on 16 March 2020.
[10] Online article; *Domain Tools; CovidLock Update: Deeper Analysis of Coronavirus Android Ransomware*; 16 March 2020; https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware; accessed on 17 March 2020.
[11] Online article; *Data Breach Today; COVID-19 Complication: Ransomware Keeps Hitting Healthcare*; 16 March 2020; https://www.databreachtoday.com/covid-19-complication-ransomware-keeps-hitting-healthcare-a-13941; accessed on 17 March 2020.
[12] Online article; *Bleeping Computer; COVID-19 Testing Center Hit By Cyberattack*; 14 March 2020; https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/; accessed on 16 March 2020.
[13] Online article; *Bleeping Computer; U.S. Health Department Site Hit With DDoS Cyber Attack*; 16 March 2020; https://www.bleepingcomputer.com/news/security/us-health-department-site-hit-with-ddos-cyber-attack/; accessed on 16 March 2020.
[14] Online article; *ABC 10 News San Diego; Fake Amazon delivery notices targeting holiday shoppers*; 17 December 2019; https://www.10news.com/money/consumer/dont-waste-your-money/fake-amazon-delivery-notices-target-holiday-shoppers; accessed on 16 March 2020.
[15] Online article; *Wired; An Amazon Phishing Scam Hits Just in Time For Prime Day*; 12 July 2019; https://www.wired.com/story/amazon-prime-day-phishing-campaign/; accessed on 16 March 2020.
[16] Online article; *NPR; Amazon To Hire 100,000 Workers To Meet 'Surge In Demand'*; 16 March 2020; https://www.npr.org/2020/03/16/816704442/amazon-to-hire-100-000-workers-to-meet-surge-in-demand; accessed on 16 March 2020.
[17] Online publication; *CISA; Alert (AA20-073A), Enterprise VPN Security*; 13 March 2020; https://www.us-cert.gov/ncas/alerts/aa20-073a; accessed on 16 March 2020.
[18] Online publication; *CISA; CISA Insights, Risk Management for Novel Coronavirus (COVID-19)*; 6 March 2020; https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf; accessed on 16 March 2020.
[19] Online publication; *Cal-CSIC; California Cybersecurity Integration Center*; 2020; https://www.caloes.ca.gov/cyber; accessed on 16 March 2020.