Homeland Security

30 March 2020

# (U) Cyber Mission Center

# (U//FOUO) Cyber Actors Almost Certainly View Growing Telework During the Novel Coronavirus Pandemic as an Opportunity to Exploit Enterprise Networks

**(U//FOUO) Scope.** This *Article* warns US public sector policymakers and private sector leaders of likely cyber threats associated with the rapid widespread shift of workers from their workplaces to telework during the novel coronavirus (COVID-19) pandemic. The information cutoff date for this *Article* is 19 March 2020.

*(U//FOUO) Prepared by the DHS Intelligence Enterprise (DHS IE) Cyber Mission Center (CYMC). Coordinated with CBP, CISA, CWMD, FEMA, ICE, S&T, TSA, USCG, USSS, CIA, DIA, Department of Energy, Department of State, Department of the Treasury, FBI, NASIC, NGA, NIC, and NSA.*

(U//FOUO) We assess malicious cyber actors almost certainly view the shift to telework of public and private sector employees during the COVID-19 crisis as an opportunity to gain access to enterprise networks and sensitive information. We base this judgment on the demonstrated ability of malicious cyber actors to access sensitive data or to install malware within internal corporate networks by exploiting remote employees' personal and business devices, remote access applications and networking protocols, teleconferencing devices, or collaboration software. We also base this assessment on malicious cyber actors conducting COVID-19-themed social engineering that could lead to compromise of user or administrator credentials. We also assume malicious cyber actors believe network defense and mitigation are less robust during the COVID-19 pandemic because of reduced resources and focus on mission critical functions.

» (U) **Growing number of teleworking employees:** The Office of Management and Budget (OMB) directed federal departments and agencies to maximize telework across the nation for the federal workforce and US corporations asked employees to work remotely as a precaution against COVID-19, according to an OMB memorandum and a US media outlet that covers business news.[1,2] A US cybersecurity company vice president noted a surge in queries from companies that anticipated employees will work from home until mid-June, possibly leaving company data more vulnerable, according to a 10 March US media article that describes a spike in malicious online activity capitalizing on growing fears of COVID-19.[3]

» (U) **Threats from personal devices:** Russian Main Intelligence Directorate of the General Staff (GRU) cyber actors in 2016 compromised a hotel's Wi-Fi network in Lausanne, Switzerland, to gain access to a Canadian Centre for Ethics in Sports (CCES) official's laptop and user credentials. The GRU actors used the CCES official's credentials to pivot into the CCES network in Canada, according to a US Department of Justice indictment of seven GRU actors.[4]

» (U) **Threats from remote access applications and networking protocols:** An unknown actor in January 2018 used valid TeamViewer credentials to gain access to an entertainment company's internal network, according to a whitepaper from a US cybersecurity firm with expertise in cyber threat analysis describing observations of adversarial activities during incident response engagements throughout 2018.[5,a] The actor moved laterally within and enumerated the network, created malicious scheduled tasks, and installed malware enabling extensive follow-on activity, according to the same source. Cyber threat actors between 2016 and 2018

[a] (U) TeamViewer is a remote access application that enables desktop sharing and file transfer capabilities between computers.

IA-43325-20

increasingly leveraged the remote desktop protocol (RDP) as an attack vector from which to steal login credentials, compromise identities, and install ransomware, according to a joint DHS-FBI public service announcement.[6,b]

» (U) **Threats from teleconferencing devices:** Cyber actors in late 2018 scanned for and sought to exploit Voice over Internet Protocol (VoIP) phones, video conferencing equipment, conference phones, VoIP routers, and cloud-based communication systems to identify vulnerabilities, which could later be used to gain access and unlawfully acquire information about victim organizations, according to an FBI private industry notification bulletin.[7]

» (U) **Threats from collaboration software:** Cybercriminals in April 2019 exploited a critical Atlassian Confluence server flaw to install ransomware with native tools to avoid detection, according to a US cybersecurity company's blog.[8,c] The source judged that since Confluence potentially holds valuable company information that is possibly not backed up, the actors might have chosen to deploy ransomware because the likelihood of a significant payout was greater than what could have been expected by deploying cryptocurrency mining malware on the host.

» (U) **COVID-19-themed social engineering:** Cybercriminals and state-sponsored advanced persistent threat groups since January 2020 have used COVID-19-themed lures (specifically requests for donations, updates on virus transmissions, safety measures, tax refunds, and fake vaccines) in spear-phishing messages to deliver commodity and custom malware capable of data exfiltration and downloading secondary payloads, according to a UK advisory and consultancy firm. The South Korean Government also noted short messaging service (SMS) phishing attacks against mobile devices with COVID-19 lures designed to entice victims to click on links that would harvest sensitive information and account credentials, according to the same source.[9]

## (U) Mitigation

» (U) The Cybersecurity and Infrastructure Security Agency (CISA) advises organizations to review the recommendations regarding hardware and software solutions that enable remote access to enterprise networks, phishing attempts, log review, attack detection, incident response and recovery, multifactor authentication, and virtual private network (VPN) capabilities.[10] For more information, please see https://www.us-cert.gov/ncas/alerts/aa20-073a.

» (U) The National Institute of Standards and Technology (NIST) recommends that organization-issued and personally owned devices be secured against expected threats. NIST provides information security considerations for several types of remote access solutions, and it makes recommendations for securing a variety of telework, remote access, and personally owned device technologies.[11] For more information, see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf.

(U) NIST has developed a comprehensive telework resource guide that provides information on security enterprise telework, remote access, and bring-your-own-device solutions. Some key concepts in the guide include development and enforcement of telework security policy, multifactor authentication for enterprise access, and telework client device security.[12] For more information, see https://crsc.nist.gov/News/2020/telework-cybersecurity-itl-bulletin-blog.posts.

[b] (U) RDP is a proprietary network protocol that allows an individual to control the resources and data of a computer over the Internet. This protocol provides complete control over the desktop of a remote machine by transmitting input such as mouse movements and keystrokes and sending back a graphical user interface. Cyber actors can infiltrate the connection between the machines and inject malware or ransomware into the remote system. Attacks using the RDP protocol do not require user input, making intrusions difficult to detect.

[c] (U) Confluence is an integrated collaboration platform.

» (U) CISA encourages caution when handling any e-mail with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19. Cyber actors may send e-mails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes.[13]

| (U) Reporting Computer Security Incidents |
| --- |
| **(U) To report a computer security incident, either contact CISA at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.<br><br>**(U) To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov.** DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption. |

**(U) Tracked by:** HSEC-1.1, HSEC-1.2.2, HSEC-1.2.3, HSEC-1.5, HSEC-1.5.1, HSEC-1.6.2.4, HSEC-1.7.1, HSEC-1.7.4, HSEC-1.8.1

## (U) Source Summary Statement

(U//FOUO) This *Article* is based on two US media outlets' online articles, a US cybersecurity company's blog post, a US cybersecurity company's whitepaper, an OMB memorandum, a US Department of Justice indictment, a joint DHS-FBI public service announcement, a UK-based risk advisory and consultancy firm's report, and an FBI private industry notification bulletin.

(U//FOUO) We assess malicious cyber actors almost certainly view the shift to telework of public and private sector employees during the COVID-19 crisis as an attractive target of opportunity into enterprise networks and sensitive information. We have **high confidence** in this assessment based on an OMB memorandum directing maximum telework and reports from two US media outlets that show employees are expected to work remotely during the COVID-19 outbreak. Our **high confidence** is also based on a reliable Department of Justice indictment that describes how a GRU actor compromised a laptop that belonged to a CCES official who had traveled to Switzerland. The indictment describes how the GRU actor moved laterally into the organization's enterprise network in Canada. A whitepaper from a US cybersecurity company with expertise in cyber threat analysis provided an example of how threat actors used TeamViewer—a collaboration platform—to access a company's internal network and conduct follow-on cyber activity. A reliable jointly published public service announcement describes the increase in exploitation of RDP to steal credentials and install malware on remote computers. A credible FBI private industry notification bulletin describes how cyber actors sought to exploit teleconferencing equipment to gain access to sensitive information and internal networked resources. A reliable US-based cybersecurity company's blog provides an example of cybercriminals exploiting vulnerable Confluence instances to install ransomware. A report from a credible UK-based risk advisory and consultancy firm describes
COVID-19 social engineering techniques in spear-phishing and SMS-phishing attacks.

---

[1] (U) OMB; "Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19; 17 March 2020.

[2] (U) Business Insider; "Oracle, Apple, Google, and Amazon are among the largest global companies who have restricted travel or asked their employees to work remotely as a precaution against the novel coronavirus."; accessed on 20 March 2020, https://www.businessinsider.com/companies-asking-employees-to-work-from-home-due-to-coronavirus-2020.

[3] (U); CBS news; "Cybercriminals are capitalizing on coronavirus fears, security firm warns"; 10 March 2020; https://www.cbsnews.com/news/coronavirus-cybercriminals-capitalize-on-fears-cyber-firm-crowdstrike-says/; accessed on 11 March 2020; Source is a US-based media outlet with a history of credible reporting.

[4] (U): US District Court of the Western District of Pennsylvania; "United States of America v. Aleksei Sergeyevich Morenets, Evgenii Mikhaylovich, Serebriakov, Ivan Sergeyevich Yermakov, Artem Andreyevich Malyshev, Dmitriy Sergeyevich Badin, Oleg Mikhaylovich Sotnikov, and Alexey Valerevich Minin"; 3 October 2018; pp 21-22; Source consistently produces reliable documentation for use in US legal proceedings.

[5] (U); Crowdstrike; "Observations from the Front Lines of Threat Hunting: A 2018 Mid-Year Review from Falcon OverWatch"; 9 October 2018; p. 7; https://go.crowdstrike.com/rs/281-0BQ-266/images/Report2018OverwatchReport.pdf; accessed on 13 March 2020; Source is a credible, US-based, information technology and cybersecurity research firm.

[6] (U); FBI; Internet Crime Complaint Center; "Cyber Actors Increasingly Exploit The Remote Desktop Protocol to Conduct Malicious Activity"; 27 September 2018; https://www.ic3.gov/media/2018/180927.aspx; accessed on 19 March 2020; Source is hub to receive, develop, and refer criminal complaints regarding the rapidly expanding occurrences of Internet crime, and provides law enforcement agencies at the federal, state, local and international level with reliable leads to criminal activities.

[7] (U); FBI; PIN 20190102-001; 02 January 2020; (U) "Cyber Actors Target Audio and Visual Communication Devices on Business Networks to Identify Vulnerabilities for Exploitation"; Extracted information is U; Overall document classification is U; Source is a credible federal agency that investigates and reports on cyber attacks by criminals, overseas adversaries, and terrorists.

[8] (U); Alert Logic; "Active Exploitation of Confluence Vulnerability CVE-2019-3396 Dropping Gandcrab Ransomware"; 23 April 2019; https://blog.alertlogic.com/active-exploitation-of-confluence-vulnerability-cve-2019-3396-dropping-gandcrab-ransomware/; accessed on 18 March 2020; Source is a US provider of managed cloud security and compliance solutions delivered in a Software-as-a-Service model.

[9] (U); Deloite; "COVID-19 (Coronavirus) related information leveraged in ongoing cyber-attacks"; 17 March 2020; Serial: G-TR-EN-01-12352; Source is a credible UK-based multinational professional risk advisory and consultancy firm.

[10] (U); CISA; "Enterprise VPN Security"; 13 March 2020; https://www.us-cert.gov/ncas/alerts/aa20-073a; accessed on 18 March 18, 2020; Source is a federal civilian agency responsible for providing cybersecurity assistance to government and critical infrastructure partners.

[11] (U); NIST; "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security"; July 2016; https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final#pubs-abstract-header; accessed on 18 March 18, 2020; Source is a federal civilian agency responsible for the promotion of innovation and industrial competitiveness.

[12] (U); NIST, "Telework Cybersecurity Resources: New ITL Bulletin and Blog Posts"; 19 March 2020; https://crsc.nist.gov/News/2020/telework-cybersecurity-itl-bulletin-blog.posts; accessed on 20 March 2020; Source is a federal civilian agency responsible for the promotion of innovation and industrial competitiveness.

[13] (U); CISA; "Defending Against COVID-19 Cyber Scams"; 6 March 2020; https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams; accessed on 18 March 2020; Source is a federal civilian agency responsible for providing cybersecurity assistance to government and critical infrastructure partners.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

*Office of Intelligence and Analysis*

# Customer Feedback Form

Product Title: (U//FOUO) Cyber Actors Almost Certainly View Growing Telework During the Novel Coronavirus Pandemic

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

**1. Please select partner type:** Select One **and function:** Select One

**2. What is the highest level of intelligence information that you receive?** Select One

**3. Please complete the following sentence: "I focus most of my time on:"** Select One

**4. Please rate your satisfaction with each of the following:**

| | Very Satisfied | Somewhat Satisfied | Neither Satisfied nor Dissatisfied | Somewhat Dissatisfied | Very Dissatisfied | N/A |
|---|---|---|---|---|---|---|
| Product's overall usefulness | ○ | ○ | ○ | ○ | ○ | ○ |
| Product's relevance to your mission | ○ | ○ | ○ | ○ | ○ | ○ |
| Product's timeliness | ○ | ○ | ○ | ○ | ○ | ○ |
| Product's responsiveness to your intelligence needs | ○ | ○ | ○ | ○ | ○ | ○ |

**5. How do you plan to use this product in support of your mission?** ***(Check all that apply.)***

- ☐ Drive planning and preparedness efforts, training, and/or emergency response operations
- ☐ Observe, identify, and/or disrupt threats
- ☐ Share with partners
- ☐ Allocate resources (e.g. equipment and personnel)
- ☐ Reprioritize organizational focus
- ☐ Author or adjust policies and guidelines
- ☐ Initiate a law enforcement investigation
- ☐ Intiate your own regional-specific analysis
- ☐ Intiate your own topic-specific analysis
- ☐ Develop long-term homeland security strategies
- ☐ Do not plan to use
- ☐ Other:

**6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.**

**7. What did this product *not* address that you anticipated it would?**

**8. To what extent do you agree with the following two statements?**

| | Strongly Agree | Agree | Neither Agree nor Disagree | Disagree | Strongly Disgree | N/A |
|---|---|---|---|---|---|---|
| This product will enable me to make better decisions regarding this topic. | ○ | ○ | ○ | ○ | ○ | ○ |
| This product provided me with intelligence information I did not find elsewhere. | ○ | ○ | ○ | ○ | ○ | ○ |

**9. How did you obtain this product?** Select One

**10. Would you be willing to participate in a follow-up conversation about your feedback?** Yes

***To help us understand more about your organization so we can better tailor future products, please provide:***

| | | | |
|---|---|---|---|
| *Name:* | | *Position:* | |
| *Organization:* | | *State:* | |
| *Contact Number:* | | *Email:* | |

Submit Feedback

*Privacy Act Statement*