Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments

The FBI anticipates cyber actors will exploit increased use of virtual environments by government agencies, the private sector, private organizations, and individuals as a result of the COVID-19 pandemic. Computer systems and virtual environments provide essential communication services for telework and education, in addition to conducting regular business. Cyber actors exploit vulnerabilities in these systems to steal sensitive information, target individuals and businesses performing financial transactions, and engage in extortion.

As of March 30 2020, the FBI's Internet Crime Complaint Center (IC3) has received and reviewed more than 1,200 complaints related to COVID-19 scams. In recent weeks, cyber actors have engaged in phishing campaigns against first responders, launched DDoS attacks against government agencies, deployed ransomware at medical facilities, and created fake COVID-19 websites that quietly download malware to victim devices. Based on recent trends, the FBI assesses these same groups will target businesses and individuals working from home via telework software vulnerabilities, education technology platforms, and new Business Email Compromise schemes.

Telework Vulnerabilities

The FBI advises you to carefully consider the applications you or your organization uses for telework applications, including video conferencing software and voice over Internet Protocol (VOIP) conference call systems. Telework software comprises a variety of tools that enable users to remotely access organizational applications, resources, and shared files. The COVID-19 pandemic has led to a spike in businesses teleworking to communicate and share information over the internet. With this knowledge, malicious cyber actors are looking for ways to exploit telework software vulnerabilities in order to obtain sensitive information, eavesdrop on conference calls or virtual meetings, or conduct other malicious activities. While telework software provides individuals, businesses, and academic institutions with a mechanism to work remotely, users should consider the risks associated with them and apply cyber best practices to protect critical information, safeguard user privacy, and prevent eavesdropping. Cyber actors may use any of the below means to exploit telework applications.

Software from Untrusted Sources

- Malicious cyber actors may use legitimate-looking telework software—which may be offered for free or at a reduced price—to gain access to sensitive data or eavesdrop on conversations.
- Cyber actors may also use phishing links or malicious mobile applications that appear to come from legitimate telework software vendors.

Communication Tools

- Malicious cyber actors may target communication tools (VOIP phones, video conferencing equipment, and cloud-based communications systems) to overload services and take them offline, or eavesdrop on conference calls.
- Cyber actors have also used video-teleconferencing (VTC) hijacking to disrupt conferences by inserting pornographic images, hate images, or threatening language.

Remote Desktop Access

- Some telework software allows for remote desktop sharing, which is beneficial for collaboration and presentations; however, malicious cyber actors historically have compromised remote desktop applications and can use compromised systems to move into other shared applications.

Supply Chain

- As organizations seek to obtain equipment, such as laptops, to enable teleworking, some have turned to laptop rentals from foreign sources. Previously used, improperly sanitized equipment potentially carries preinstalled malware.

Education Technology Services and Platforms

Today's rapid incorporation of education technology (edtech) and online learning could have privacy and safety implications if students' online activity is not closely monitored. For example, in late 2017, cyber actors exploited school information technology (IT) systems by hacking into multiple school district servers across the United States. They accessed student contact information, education plans, homework assignments, medical records, and counselor reports, and then used that information to contact, extort, and threaten students with physical violence and release of their personal information. The actors sent text messages to parents and local law enforcement, publicized students' private information, posted student personally identifiable information on social media, and stated how the release of such information could help child predators identify new targets.

Additionally, parents and caretakers should be aware of new technology issued to children who do not already have a foundation for online safety. Children may not recognize the dangers of visiting unknown websites or communicating with strangers online.

Business Email Compromise (BEC)

BEC is a scam that targets both individuals and businesses who have the ability to send wire transfers, checks, and automated clearing house (ACH) transfers. In a typical BEC scheme, the victim receives an email purported to be from a company the victim normally

conducts business with; however, the email requests money be sent to a new account, or for standard payment practices be altered. For example, during this pandemic, BEC fraudsters have impersonated vendors and asked for payment outside the normal course of business due to COVID-19. The FBI advises the public to be on the lookout for the following:

- The use of urgency and last-minute changes in wire instructions or recipient account information;
- Last-minute changes in established communication platforms or email account addresses;
- Communications only in email and refusal to communicate via telephone;
- Requests for advanced payment of services when not previously required; and
- Requests from employees to change direct deposit information.

TIPS TO PROTECT YOU AND YOUR ORGANIZATION

Teleworking Tips:

Do:

- Select trusted and reputable telework software vendors; conduct additional due diligence when selecting foreign-sourced vendors.
- Restrict access to remote meetings, conference calls, or virtual classrooms, including the use of passwords if possible.
- Beware of social engineering tactics aimed at revealing sensitive information. Make use of tools that block suspected phishing emails or allow users to report and quarantine them.
- Beware of advertisements or emails purporting to be from telework software vendors.
- Always verify the web address of legitimate websites or manually type it into the browser.

Don't:

- Share links to remote meetings, conference calls, or virtual classrooms on open websites or open social media profiles.
- Open attachments or click links within emails from senders you do not recognize.
- Enable remote desktop access functions like Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) unless absolutely needed.[1]

Education Technology Tips:

School districts across the United States are working to address a dynamically changing learning environment. The FBI acknowledges everyone is adjusting to these demands, but the FBI encourages parents and families to:

Do:

- Closely monitor children's use of edtech and online services.
- Research edtech service user agreements about data breach notifications, marketing, and/or selling of user data, data retention practices, and whether users and/or parents can elect to have student data deleted by request.
- Conduct regular internet searches of children's information to monitor the exposure and spread of their information on the internet.
- Consider credit or identity theft monitoring to check for any fraudulent use of their child's identity.
- Research parent coalition and information-sharing organizations available online for those looking for support and additional resources.
- Research school-related, edtech, and other related vendor cyber breaches, which can further inform families of student data and security vulnerabilities.

Don't:

- Provide exact information on children when creating user profiles (e.g., use initials instead of full names, avoid using exact dates of birth, avoid including photos, etc.)

BEC Tips:

Do:

- Check for last-minute changes in wiring instructions or recipient account information.
- Verify vendor information via the recipient's contact information on file—do not contact the vendor through the number provided in the email.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.
- If you discover you are the victim of a fraudulent incident, immediately contact your financial institution to request a recall of funds, and contact your employer to report irregularities with payroll deposits. As soon as possible, file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov or, for BEC and/or email account compromise (EAC) victims, BEC.IC3.gov.

Cyber Crime Vulnerability Tips:

The following tips can help protect individuals and businesses from being victimized by cyber actors:

Do:

- Verify the web address of legitimate websites and manually type them into your browser.

- Change passwords for routers and smart devices from default setting to unique passwords.
- Check for misspelled domain names within a link (for example, confirm that addresses for government websites end in .gov).
- Report suspicious activity on work computers to your employer.
- Use multi-factor authentication (MFA) when accessing organizational sites, resources, and files.
- Practice good cyber security when accessing Wi-Fi networks, including use of strong passwords and Wi-Fi Protected Access (WPA) or WPA2 protocols.
- Ensure desktops, laptops, and mobile devices have anti-virus software installed and routine security updates are applied; this includes regularly updating web browsers, browser plugins, and document readers.

Don't:

- Open attachments or click links within emails received from senders you do not recognize.
- Provide usernames, passwords, birth dates, social security numbers, financial data, or other personal information in response to an email or phone call.
- Use public or non-secure Wi-Fi access points to access sensitive information.
- Use the same password for multiple accounts.

If private sector partners have additional questions, you can reach out to local FBI Field Office Private Sector Coordinators. If you have evidence your child's data may have been compromised, if you are the victim of an internet scam or cybercrime, or if you want to report suspicious activity, please visit the FBI's Internet Crime Complaint Center at www.ic3.gov.

REFERENCE: https://www.ic3.gov/media/2020/200401.aspx