TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 MAY 2020

PIN Number

20200521-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats.

This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This PIN has been released TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Criminals and Nation-State Cyber Actors Conducting Widespread Pursuit of US Biological and COVID-19 Related Research

Summary

Criminal and nation-state cyber actors since February 2020 have been increasingly targeting US pharmaceutical, medical, and biological research facilities to acquire or manipulate sensitive information, to include COVID-19 vaccine and treatment research amid the evolving global pandemic. The US Healthcare and Public Health Sector (HPH), including pharmaceutical and medical companies, has been a common target of malicious cyber activity even prior to the pandemic. This notification seeks to raise awareness in the HPH sector by highlighting the current threat and cyber tactics used by our adversaries.

Threat

Cyber-enabled criminal and state actors continue to target US clinical trials data, personally identifiable information (PII), personal health information (PHI), trade secrets, means of producing critical HPH goods, and sensitive data and proprietary research of US universities and research facilities. Likely due to the current global public health crisis, the FBI has observed some nation-states shifting cyber resources to collect against the HPH sector, while criminals are targeting similar entities for financial gain. The FBI has observed malicious actors successfully compromising US victim networks through social engineering, hacking emails, and exploiting common vulnerabilities of connected devices and Internet of Things (IoT) equipment used in laboratories.

The scale and urgency of the COVID-19 health crisis exacerbates the threat against the HPH sector in two ways:

- As entities are focused on meeting urgent demands for research and product development, potential neglect of critical cyber security practices may compound existing known vulnerabilities.
- Nation-state cyber actors are targeting COVID-19-related research as many foreign governments seek to accelerate their own R&D processes and clinical trials. The compromise of US research and sensitive data undermines the effectiveness of US pharmaceutical, medical, and biological companies and harms US response efforts for health crises, including the pandemic.

Adversaries are targeting a wide range of US-based entities with access to research using network intrusions, including:

- academic institutions;
- biological facilities;
- bioscience industries;
- medical facilities;
- medical device manufacturers;
- pharmaceutical facilities;
- scientific collaborations; and
- university laboratories.

The following examples illustrate targeting of the HPH sector observed by the FBI since February 2020.

- An identified healthcare-related company notified the FBI of suspected Advanced Persistent Threat (APT) activity on its network. The threat actors leveraged a Confluence server vulnerability to install a backdoor on a Windows server, which was identified by the beacon activity to a Command and Control (C2) IP address. The threat actor then leveraged a valid domain administrator account to move laterally within the network. After containment, threat actors were observed trying to unsuccessfully regain access via the same initial critical vulnerability.

- An identified US university reported an attempted intrusion into its computer network. The university received thousands of authentication requests against its hybrid exchange servers. The attackers unsuccessfully attempted to use previously acquired account credentials, likely acquired in a previous known breach.

- Likely nation-state cyber actors conducted a multi-month campaign targeting multiple external-facing devices (primarily Juniper VPN endpoints and Citrix devices) of an identified US research entity. The actors used legitimate credentials and VPN controls. When defensive measures were taken, the actors made extensive attempts to regain access to the network. The actors predominately conducted their activity through the evening and early morning US time.

- A biological research facility experienced a ransomware attack that encrypted its data. The facility was able to restore most of the encrypted data with backups and paper records.

The following examples illustrate targeting of the HPH sector prior to this year.

- In mid-2019, an unidentified actor used social engineering to impersonate an employee to gain access to an identified university's Biosafety Level (BSL) 3 facility. The actor attempted to reset passwords and phone numbers of the victim employee to bypass two-factor identification. The actor successfully gained access to the victim employee's account before the university changed the password.

- In early 2019, a US-based DNA sequence company's email account was hacked by unidentified actors. The actors impersonated company employees and sent emails to individuals associated with the company and requested money transfers.

- In early 2019, an unidentified actor gained unauthorized access to a pharmacy's network and successfully escalated their network privileges; however, they were unsuccessful in attempts to access medical records and PII.

- In late 2018, a separate US BSL-3 laboratory reported an unidentified actor attempted to gain access to its networks by hacking a laboratory printer.

Cyber Actors and Activity

Criminal and nation-state cyber actors routinely leverage open source information, such as social media postings, press releases, and official publications, to identify targets of interest. After gaining access, usually through an unpatched vulnerability or previously acquired legitimate credentials, the actors target information on a company's internal network, networked equipment, shared drives, and email servers, as well as information available through managed service providers or cloud providers. Some actors exfiltrate information to pass to foreign governments or foreign competitors. Others may seek to modify or delete data on a network or to encrypt the data with ransomware, making it unavailable to the owners. Specific to COVID-19 related research, data manipulation and deletion attempts could undermine the credibility and integrity of ongoing research efforts and the results of clinical trials, delaying the delivery of a potential vaccine and treatment. Information sought by the actors could include, but is not necessarily limited to:

- research proposals, development, and production plans of new vaccines, drugs, and related technology;
- drafts of research grant or contract submissions, including manuscripts for publication;
- virus testing kits/equipment and related technology;
- clinical trial information and results;
- drugs with expiring international patents;
- cancer-related treatments/drugs;
- marketing information; and
- financial information, including manufacturing/production and retail costs.

The FBI observed cyber actors using tactics to include but not limited to:

- Exploitation of unpatched vulnerabilities on web-facing servers to gain access to systems;

- Installation of web shells on a compromised network and/or obtaining legitimate credentials to log onto a system;
- Reconnaissance of companies' networks and identification of remote access systems; actors could exploit unpatched vulnerabilities to gain access and/or log on with legitimate credentials;
- Exploitation of third-party connections, such as managed services providers, to gain access to a network;
- Sending of spear-phishing messages to employees with malicious links and/or malware; and,
- Targeting employee or family member emails and telework applications to compromise home networks.

Recommendations

- Assume press attention affiliating your organization with COVID-19 research will lead to increased interest and activity by nation-state and cyber criminal actors to penetrate your network.
- Patch critical vulnerabilities on all systems. Prioritize patching of Internet-connected servers for known vulnerabilities as well as software that processes Internet data, such as web browsers, browser plugins, and document readers. For additional guidance on identifying and patching the most commonly exploited vulnerabilities, refer to Alert (AA20-133A): ***Top 10 Routinely Exploited Vulnerabilities*** published by the FBI and CISA on 12 May 2020. [Reference link: https://www.us-cert.gov/ncas/alerts/aa20-133a]
- Actively scan and monitor web applications for unauthorized access, modification, and anomalous activities.
- Strengthen credential requirements and implement multi-factor authentication to protect individual accounts. Change passwords and do not use the same passwords for multiple accounts.
- Identify and suspend access of users exhibiting unusual activity.
- Network device management interfaces such as Telnet, SSH, Winbox, and HTTP should be turned off for wide-area network (WAN) interfaces and secured with strong passwords and encryption, when enabled.
- When possible, segment critical information on air-gapped systems. Use strict access control measures for critical data.
- Be mindful of new and existing cyber infrastructure for work and bioscience collaborations.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office, the FBI's 24/7 Cyber Watch (CyWatch), the FBI's InfraGuard, or local field office WMD Coordinator. Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by email at CyWatch@fbi.gov.

When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.
For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey