FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 July 2020

Alert Number

AC-000128-TT

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact **FBI CYWATCH** immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email:
cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP:WHITE**: The information in this product may be distributed or briefed without restriction to the private sector and the public.

Indictment of Chinese Cyber Actors associated with the Ministry of State Security (MSS) Guangdong State Security Department (GSSD) for Intrusion Activities

Summary

The US Department of Justice (DOJ) indicted two People's Republic of China (PRC) cyber actors for stealing hundreds of millions of dollars' worth of trade secrets, intellectual property, and other high-value information from biotechnical, commercial, and government victims in the United States and abroad. The actors, Li Xiaoyu and Dong Jiazhi—each a hacker conducting computer network exploitation (CNE) operations originating from China—are associated with China's Ministry of State Security (MSS) Guangdong State Security Department (GSSD).

These MSS-affiliated actors targeted victims in the following sectors:

- Biotechnology
- Medical device manufacturers
- Defense contractors
- Pharmaceutical
- High-tech manufacturers

- Gaming and software
- Government
- Military
- Education
- US naval and maritime
- Aerospace
- Information technology

Technical Details

These MSS-affiliated cyber actors conducted reconnaissance on targets through publicly available web pages and reviewed documents posted online prior to conducting intrusions. They used various techniques to compromise victims, including taking advantage of common vulnerabilities and exposures (CVEs) to target vulnerable web servers. Known CVEs used by these actors to gain or attempt to gain access to the victim networks include but are not limited to: CVE-2017-5638, CVE-2017-3066, CVE-2018-15961, CVE-2018-8120, CVE-2019-8394, CVE-2019-3396, CVE-2019-11510, and CVE-2019-11580. A significant portion of recent intrusions have used CVE-2019-11510, exploiting a vulnerability in Pulse Secure VPN. More detailed information on CVE-11510 can be found at: https://www.us-cert.gov/ncas/alerts/aa20-107a.

Additional details on the remaining CVEs, as well as patching information, can be found on the National Vulnerability Database website: https://nvd.nist.gov.The MSS-affiliated cyber actors typically conducted their intrusions by accessing compromised servers called hop points from numerous China-based IP addresses resolving to different Chinese internet service providers.

During the initial attack phase, the MSS-affiliated actors predominantly targeted vulnerable, external-facing web servers, using the above referenced CVEs, and uploaded a China Chopper Web shell to review and steal information. China Chopper Web shells allow for remote access to the victim host and can be used to upload and download files, and alter existing files. Additional details on the China Chopper tool can be found at: https://www.us-cert.gov/ncas/alerts/AA18-284A.

Additional information on the exploitation of web servers via web shells can be found at: https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2159419/detect-prevent-cyber-attackers-from-exploiting-web-servers-via-web-shell-malware/.

The MSS-associated cyber actors also deployed publicly available tools such as Mimikatz to gather user credentials. We have also observed the actors using a zero-day exploit provided by the MSS. In one instance, the actors received a zero-day exploit from email address asls1027@***.com. Frequently, the cyber actors stored tools and files in the Recycle Bin on victim hosts, or within directories related to the associated vulnerability. The actors also enumerated directories to learn about the network prior to data exfiltration. Additional details on publically available tool Mimikatz can be found at: https://www.us-cert.gov/ncas/alerts/AA18-284A.

The actors executed commands to package select directories into multi-part RAR files. Once packaged, the MSS cyber actors renamed the files to JPG from RAR.

Hop points were routinely accessed via remote desktop protocol (RDP) when preparing to transfer files from the victim network.

Recommended Mitigations

Activity that is similar to the actions of the MSS-associated cyber actors referenced above should be considered an indication of a compromise and should be reported to law enforcement. The FBI recommends a thorough incident response effort be carried out to ensure any lateral movement or follow-on intrusion activity is contained. The FBI recommends the following steps to help reduce the overall risk from these exploitation attempts.

Patch Management

- Immediately install patches released by vendors, especially for web-facing appliances. The best mitigation against China Chopper Web shells is to protect public-facing web servers.

Protect Credentials

- Enforce principle of least privilege.

- Restrict local accounts to reduce the amount of usable credentials found within a network.
- Restrict where administrators can use their accounts and what they can use their accounts for.
- Force different passwords and credentials for user, local administrator, and domain administrator accounts to prevent an adversary from reusing stolen credentials.
- Use multifactor authentication as a measure of security beyond passwords, which allows you to differentiate a user from an attacker.
- Reset all credentials if adversary activity is detected.

Network Hygiene

- Implement network segmentation to limit lateral movement.
- Identify and establish a network baseline to aid in the identification of potentially malicious scanning activity, and check regularly for any suspicious scripts or running processes.
- Enable network-based antivirus programs and firewalls.
- Block or monitor malicious IP addresses, as well as any other IP addresses conducting remote logins outside of regular business hours.
- Conduct regular system vulnerability scans.

Publicly Available Information

- Review company information publicly available on websites, especially about sensitive projects. Adversaries use this information to target your organization.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). 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 e-mail 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.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:

https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.