FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 July 2020

Alert Number

AC-000129-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 to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

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

Chinese Government-Mandated Tax Software Contains Malware, Enabling Backdoor Access

Summary

The FBI seeks to inform US companies in the healthcare, chemical, and finance sectors of potential targeting activity by the Chinese government against their business and operational components based in China. As early as March 2019, at least two Western companies operating in China detected malware that was delivered through Chinese vendors that were responsible for releasing tax software upgrades following changes in 2018 to China's value-added tax (VAT). The malware launched a backdoor into victim systems, which the FBI assesses likely allows cyber actors to preposition to conduct remote code execution and exfiltration activities on the victim's network.

Although all companies conducting business in China may be vulnerable to such activity, the US healthcare and chemical sectors have been a common target of Chinese cyber operations for many years. Pharmaceutical companies form a critical interdependency between the manufacturing components of the chemical sector and the supply chain of the Healthcare and Public Health Sector.

Compromise of the pharmaceutical supply chain provides malicious actors opportunities for theft of US intellectual property, while public disclosure can cause cascading effects including loss of public trust in both chemical and healthcare institutions. As previously highlighted in FBI PIN 20200521-001 released on 21 May 2020 and the US Department of Homeland Security's joint advisory with Britain's National Cyber Security Centre, hackers continue to "actively target organizations that include healthcare bodies, pharmaceutical companies, academia, medical research organizations, and local governments."

Threat

Baiwang and Aisino are the only government-authorized tax software service providers to operate the Chinese value added tax (VAT) system. The use of either software provider is required by the China Tax Bureau in order for US companies to operate within China's market. Both companies operate the VAT system under the management and oversight of state-owned enterprise the National Information Security Engineering Center (NISEC). The NISEC has foundational links to the 3PLA.

In July 2018, an employee of a US pharmaceutical company with business interests in China downloaded the Baiwang Tax Control Invoicing software program from baiwang.com. Since at least March 2019, Baiwang released software updates which installed a driver automatically along with the main tax program. In April 2019, employees of the pharmaceutical company discovered that the software contained malware that created a backdoor on the company's network.

In June 2020, a private cybersecurity firm reported that Intelligence Tax, a tax software from Aisino Corporation that is required by a Chinese bank under the same VAT system, likely contained malware that installed a hidden backdoor to the networks of organizations using the tax software. The malware, named GoldenSpy, was designed to provide cyber actors with unfettered access to victim networks and is believed to have been around since 2016. It is unclear how many organizations may have been compromised.

Indicators of Compromise

The following domains are associated with this activity:

Domains
help.tax-helper.ltd
help.tax-assistant.com
help.tax-assistant.info
info.tax-assistant.com
info.tax-assistant.info
info.tax-helper.ltd

tip.tax-helper.ltd
bbs.tax-helper.info
update.tax-helper.ltd
download.tax-helper.com
tools.tax-helper.info
update.tax-helper.com

The following were characteristics of the USB drive used in this specific attack. The USB name likely reflects the name of the state-owned provider, National Information Security Engineering Center.

- Key created - 21 March 2019, 011637 UTC,
- Name - NISEC TCG-01 USB Device.

The following were characteristics of the malicious files and associated hash values:

Filename	MD5 Hash
WMIASSSRV.DLL	26e71f1d387298162c1b19e858d001a1
mshkos014.dat	490d17a5b016f3abc14cc57f955b49b3
n/a	7a7ef986808ebb7781f5d64da9d7900c

In addition to the indicators of compromise listed above, the FBI will provide a document with more in-depth technical analysis at a later date.

Recommended Mitigations

- Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected servers for known vulnerabilities and software processing Internet data, such as web browsers, browser plugins, and document readers.
- 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, particularly for webmail and VPN access and for accounts that access critical systems. Change passwords and do not reuse passwords for multiple accounts.
- Recommend developing a network baseline to allow for the identification of anomalous account activity. 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 WAN interfaces and secured with strong passwords and encryption when enabled.
- Identify and suspend access of users exhibiting unusual activity.
- 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 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.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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 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.