24 Aug 2020

Alert Number

AC-000131-MW

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 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.

Tactics, Techniques, and Procedures Associated with Malware within Chinese Government-Mandated Tax Software

Summary

On 23 July 2020, the FBI disseminated the FLASH message "**Chinese Government-Mandated Tax Software Contains Malware, Enabling Backdoor Access**" (AC-000129-TT) after the FBI observed reporting of malware distributed through Chinese Government-mandated tax software. FLASH message AC-000129-TT provided several indicators of compromise (IOCs) and a summary of security risks associated with the "Golden Tax System" tax software.

The FBI is disseminating this FLASH message based on the identification of additional IOCs and tactics, techniques, and procedures (TTPs) associated with the malware. The FBI advises all organizations conducting business in China to review FLASH message AC-000129-TT. Observed TTPs associated with the malware can be mapped to the MITRE[1] Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK[2]) for Enterprise framework, Version 7.0.

[1] MITRE is a registered trademark of The Mitre Corporation. Information about Mitre can be found at *https://mitre[.]org*.

[2] ATT&CK is a registered trademark of The Mitre Corporation. This FLASH utilizes ATT&CK for Enterprise, Version 7.0. Information about ATT&CK can be found at *https://attack.mitre[.]org*.

Threat

Following the recent disclosure of the GoldenSpy malware, cyber actors have made determined efforts to remove the malware from victim networks. Each subsequent attempt to remove the malware involves increasing levels of obfuscation and detection avoidance techniques in an effort to evade newly implemented network security rules. This reveals the actors' high level of sophistication and operational awareness. The software service providers have not provided a statement acknowledging the software supply chain compromise. The FBI assesses that the cyber actors' persistent attempts to silently remove the malware is not a sign of resignation. Rather, it is an effort to hide their capabilities. Organizations conducting business in China continue to be at risk from system vulnerabilities exploited by the tax software and similar supply chains.

Recently Observed TTPs:

Initial Access	
Supply Chain Compromise: Software Supply Chain Compromise (T1195.002) *MITRE ATT&ACK Reference: https://attack.mitre.org/techniques/T1195/002/*	Aisino Version: Numerous, published software versions with a trojanized file within the tax software. The tax software and the loaders for the malware were digitally signed.
	Baiwang Version: Numerous, published software versions were distributed that contain malicious components. The tax software and the loaders for the malware were digitally signed.

Execution	
User Execution: Malicious File (T1204.002)	Aisino Version: See T1195.002 (above)
	Baiwang Version: See T1195.002 (above)
Command and Scripting Interpreter: Windows Command Line (T1159.003)	Aisino Version: Use of numerous executable files in order to install the malware like "plugin.exe" and "svm.exe".
	Baiwang Version: Use of numerous executable files and *INF* functions in order to install the malware like "taxver.exe" and "kp.exe".
Inter-Process Communication: Component Object Model (T1559.001)	Baiwang Version: *INF* functions are invoked to use COM to bypass UAC to execute using CMSTP.
System Services: Service Execution (T1569.002)	Aisino Version: The malware installs, establishes presence, and runs as system processes via "svm.exe" and "svmm.exe".
	Baiwang Version: The malware installs, establishes presence, and runs as system processes via "WMPAssis".

Persistence	
Scheduled Task/Job: Scheduled Task (T1053.005)	Aisino Version: The trojanized file schedules the malware download two hours after the tax software install.
Create or Modify System Process: Windows Service (T1543.003)	Aisino Version: See T1569.002 (above)
	Baiwang Version: See T1569.002 (above)

Event Triggered Execution (T1546)	Aisino Version: “Svm.exe” and “svmm.exe” will download and reinstall its partner process if it is deleted.

Privilege Escalation / Defensive Evasion	
Boot/Logon Auto-start Execution: Registry Run Keys/Startup Folder (T1547.001)	Aisino Version: “Svm.exe” generates and stores uuid on HKLM\Software\IDG\DA.
	Baiwang Version: Numerous values were added under HKLM\SYSTEM\CurrentControlSet\services\WMPAssis”.
Abuse Elevation Control Mechanism: Bypass User Access Control (T1548.002)	Baiwang Version: See T1559.001 (above)
Signed Binary Proxy Execution: CMSTP (T1218.003)	Baiwang Version: See T1559.001 (above)
Indicator Removal on Host: File Deletion (T1070.004)	Aisino Version: Numerous GoldenSpy uninstallers deployed to remove "svm.exe" files and directories after 25 June report.
	Baiwang Version: *INF* functions execute and delete upon completion.
Indicator Removal on Host: Timestomp (T1070.004)	Baiwang Version: Files were timestamped with randomly generated "Creation" and "Last write".
Hide Artifacts: Hidden Files and Directories (T1564.002)	Baiwang Version: *WriteStartINF* is executed and then subsequently hides the file system.
Execution Guardrails (T1480)	Baiwang Version: The malware checks if the victim system is running 64-bit version of Windows 7 or above before continuing the process.
Subvert Trust Controls: Code Signing (T1553.002)	Aisino Version: See T1195.002 (above)
	Baiwang Version: See T1195.002 (above)
Masquerading (T1063)	Baiwang Version: Downloaded executables use fake filenames and file extensions like .gif, .jpg, .zip. Additionally, a randomly generated dat file name is created.
Obfuscated files or Information (T1027)	Aisino Version: “Plugin.exe” and “mplugin.exe” logs are encrypted with SM4 Block cipher with a 16-byte key and then encoded in Base64.

Discovery	
System Information Discovery (T1087)	Aisino Version: "Svm.exe" sends host environment information to threat actor C2.
	Baiwang Version: See T1480 (above)

Command and Control	
Non-Standard Port (T1571)	Aisino Version: Use of port 7357, 9002, 9005, 9006 for telnet and malware network traffic.
Fallback Channels (T1008)	Aisino Version: Numerous IP/domains are coded for the malware to communicate.

	Baiwang Version: Numerous IP/domains are coded for the malware to download its additional files.
Remote File Copy (T1544)	Aisino Version: NCAT is downloaded to the victim system.
Traffic Signaling: Port Knocking (T1205.001)	Aisino Version: “Svm.exe” uses a series of custom "UserAgent" strings to enable communication to the C2 server.
Dynamic Resolution: Domain Generation Algorithms (T1568.002)	Baiwang Version: “Mshkos014.dat” utilize IP-based DGA to switch download domains.
Remote Access Software (T1219)	Aisino Version: The malware enables telnet via 7357.
Non-Application Layer Protocol (T1095)	Aisino Version: See T1219 and T1571 (above)
Application Layer Protocol: Web Protocol (T1071.001)	Aisino Version: The legitimate tax software (plugin.exe) uses of port 80/http download "svminstall.exe".

Indicators of Compromise

The following domains are associated with this activity:

Domains			
help.tax-helper[.]ltd	info.tax-assistant[.]info	download.tax-helper[.]com	info.tax-helper[.]ltd
help.tax-assistant[.]com	tip.tax-helper[.]ltd	tools.tax-helper[.]info	
help.tax-assistant[.]info	bbs.tax-helper[.]info	update.tax-helper[.]com	
info.tax-assistant[.]com	update.tax-helper[.]ltd	ningzhidata[.]com	

The following IP addresses are associated with this activity:

IP Addresses			
42.56.76[.]93	110.18.246[.]13	223.112.21[.]2	3.3.1[.]2
124.152.41[.]85	49.232.159[.]177	172.46.16[.]23	2.2.1[.]2
59.83.204[.]14	159.89.176[.]244	192.168176[.]1	1.3.1[.]8

The following characteristics identify USB drives used in this specific attack. The USBs are used to distribute the tax software with malicious files. The USB name likely reflects the name of the Chinese 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(64 bit)	490d17a5b016f3abc14cc57f955b49b3
mshkos014.dat- (32 bit)	7a7ef986808ebb7781f5d64da9d7900c
Skpc.dll (v2.1.0.11)	9e2ebdbc9ba4dca69a712e3268f3ab77
SVMV1.0-20200310.exe	09b4079b039d13b47944e4cc7182f96f
kp.exe (v2.0.17.0)	bf2b45fb30452fc3982d5a4d768b8d0f

IDG-FEILONGV1.0-20200310.exe	e104c1deefaf379787677fcdc2ec3efc
svm.exe	eb1c4f73efdedd8cd2ed29203efc3341
svminstall.exe	b363e855f613233848a0a89216488bfb
usv.exe	c2e51a827d684412a97a61ed5d02bcd7
dga.exe	3fc537665e2154ce9e80c6f4c784cef9
MPlugin.exe	946945ee4555fc7f7aced80904fe802f
BWXT.exe	f2a7363cf43b5900bb872b0d4c627a48
AWX.exe	573adb1569a08472094f0cfbb6264360
idgclient.exe	c21307b7bc2889e0318eb25dacfe4fcc

Please see the attached document for additional indicators of compromise.

Recommended Mitigations

- Evaluate risk exposure and security considerations associated with conducting business in China and when using third-party software.
- 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 (see attachment for guidance).
- 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.

Administrative Note:

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

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.