FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

28 APRIL 2023

FLASH Number

TC-000171-TT

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients 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 actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:AMBER**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact FBI Cyber Watch (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.*

IOCs and TTPs Associated With Compromises Targeting Identified Distributor of Government, Law Enforcement, and Non-Profit Organization Equipment

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate known IOCs and TTPs associated with system compromises identified as recently as 10 April 2023. The compromises appear to target the products of a distributor of equipment to government, law enforcement, and non-profit organizations. These products include, but are not limited to, License Plate Reader (LPR) Communication Boxes, Emergency Operations Center (EOC) video wall systems, and general access terminals. The malicious files on these systems can facilitate keylogging, cryptocurrency mining, exfiltration of data, and/or remote access capabilities.

The FBI encourages organizations to implement the recommendations in the Mitigations section of this FLASH to reduce the likelihood and impact of the identified compromise.

Technical Details

The actors leveraged Windows scripting to deploy cryptominers and maintain their presence on the system. For example, an identified US company acting as a distributor used a standard Windows system image and this image had a zip file containing batch scripts used to establish crypto miners, a keylogger, and a backdoor. First, the actors established a connection to the system then gained access to the command line through “loadhost.cmd” and download “xmrig.cmd” from their C2. With command line access, the actors installed new services using “RuntimeBroker.exe” and “loadhost.exe” to create a backdoor “IntelSvc.exe” connecting to IP address 37.48.87.53. The actors also downloaded “killvr.exe” which was used to kill the windows defender process.

Once access was established, actors created a hidden folder containing cryptomining binaries, such as those listed below, used for cryptocurrencies, usually within “C:\ProgramData\Internet Explorer”. Upon attempted deletion, these files, such as RtkAudio.exe (located at “C:\USERS\PUBLIC\RTKAUDIO.EXE” and masquerading as a Real Tech Audio file), recreated themselves as the registry continually checked for their existence. Once installed, actors ran “tv_x64.vbs” which hid the command line UI (screen.exe) and started the cryptominers (Exists.bat / edge.cmd).

- nvrtc-builtins64_100.dll
- nvrtc-builtins64_102.dll
- nvrtc64_100_0.dll
- nvrtc64_102_0.dll
- RtkAudio.exe
- service.dll
- tv_x64.vbsWinRing0x64.sys

The image also installed a Keylogger “Systemfont.exe” found in “C:\ProgramData” that actively logged all mouse clicks, keyboard captures, and window openings. “Netserver.exe” then sent emails containing the keylog “webfont.txt” back to the actors for further exploitation. In order to access “Systemfont.exe”, two malicious registry keys were removed:

- HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM|DISABLETASKMGR
- HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM|DISABLETASKMGR

The backdoor IntelSvc.exe ensured actors can regain access to the system if files are removed. One victim company observed the cryptomining activity occurred with approximately 300,000 connection requests per day to four domains:

- donate.ssl.xmrig.com
- pool.supportxmr.com
- donate.v2.xmrig.com

- xmr.2miners.com

Indicators

The FBI assesses the following indicators of compromise (IOCs) are likely associated with this malicious cryptomining and keylogger activity.

Cryptomining Binaries	
RtkAudio.exe	nvrtc64_102_0.dll
WinRing0x64.sys	service.dll
nvrtc-builtins64_102.dll	

Malicious Registry Entries
HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM|DISABLETASKMGR
HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM|DISABLETASKMGR

C2 Domains	
sellview.xyz	btc257.xyz
xemhang.vn	btc247.xyz

Domain	Context	Timeframe
nicehash.com		2023-03-09
nanopool.org		2023-03-09
nanominer.org		2023-03-09
ezil.me		2023-03-09
rustpool.xyz		2023-03-09
shardpool.io		2023-03-09
ethermine.org		2023-03-09
donate.ssl.xmrig.com		2021-12-15
pool.supportxmr.com		2021-12-15
donate.v2.xmrig.com		2021-12-15
xmr.2miners.com		2021-12-15

Cryptomining		
Monero Address	87cy4ywNH3BWgv3dPU7VraakVWE8N9zWMB1zLtgBG877TwMn3NQiXmkMkPGcHyMp2cecQneuqCVXHTeMKzb	• supportxmr.com • 2miners.com
Wallet	thuyhue7481.831982597_1601405516	• dxpool.net

Batch Scripts	
Name	**MD5 Hash**
tv_x64.vbs	5D3E2B2EE668B2BC071B8D4027C6B8F1
Exists.bat	CE4502063C6E3984E0E38E8AAB66D24C
tv_x64.vbs	5D3E2B2EE668B2BC071B8D4027C6B8F1
Exists.bat	429EF72759D45172D7C1E4E2A1B8E6F4

Executables and DLLs	
File Name	**MD5 Hash**
service.dll	A531FE822618B6A917D50BEE001C95A1
nvrtc-builtins64_100.dll	0A0A463E17AF03587BC9D89F6AED9ED1
nvrtc64_100_0.dll	553113E0299FBA3B17C7E16C25FC593D
scren.exe	a1cd6a64e8f8ad5d4b6c07dc4113c7ec
Taskmg.exe	8C04808E4BA12CB793CF661FBBF6C2A0
netserver.exe	483421FB3DA24E88AE3B3337967CF4A4
edge.cmd	B747AEDF0F3E4457C6D02BC5AF7C0980
loadhost.exe	B1407576A1CB581EFBD8AB445615660C
screen.exe	A1CD6A64E8F8AD5D4B6C07DC4113C7EC
netserver.exe	483421FB3DA24E88AE3B3337967CF4A4
RuntimeBroker.exe	AC27DE51896A5BA2FD0DDA9B7955A201
Systemfont.exe	3C47D45F09948B8E6FDB5F96523BC60B
nvrtc-builtins64_100.dll	0A0A463E17AF03587BC9D89F6AED9ED1
service.dll	A531FE822618B6A917D50BEE001C95A1
cmdow.exe	DDD12566B99343B96609AFA2524ECEC3
killvr.exe	0A50081A6CD37AEA0945C91DE91C5D97
Taskmg.exe	8C04808E4BA12CB793CF661FBBF6C2A0
IntelSvc.exe	A7CDE18F991E97037A7899B7669E2548
nvrtc64_100_0.dll	553113E0299FBA3B17C7E16C25FC593D
RtkAudio.exe	227FA5D690A943114FF3CCFE7977192A
xmrig-cuda.dll	1DA8E7C92C86FC8DBAB5287BDCA91CA1
WinRing0x64.sys	0C0195C48B6B8582FA6F6373032118DA
unpro.exe	75375C22C72F1BEB76BEA39C22A1ED68
Taskmg.exe	F8247397AE65792524D949C825969391
screen.exe	A1CD6A64E8F8AD5D4B6C07DC4113C7EC
RtkAudio.exe	D41D8CD98F00B204E9800998ECF8427E
nvrtc-builtins64_102.dll	D816D6C6A543FF4C19486E36546436D8
nvrtc64_102_0.dll	EE49D4EE7259A23219A20E6498009897
loadhost.cmd	DDAB66730A84583B98D3415F9181D092

Data and Configuration Files	
File Name	**MD5 Hash**
webfont.txt	A33772B9006AA2D0E92746AA59D69389
loadlink.txt	844AFD44FF5361DF28129DF1E3EF8915
kernel.dat	37FC4B471DEDB296DD2112702AA48560
config.json	00CA6F0B57DDD25717D0227977342599

Killed Applications	
Windows Defender	

Tools	
NirCmd	GNU Wget

Information Requested:

If you believe you have been affected by the threat activity identified in this FLASH, please contact your local FBI field office or ic3.gov. In addition to your contact information, please provide what indicators of compromise you have found on your systems. Include which types of devices you believe to be compromised, how many of each type of device, and which vendor(s) they were acquired from. Please include how long you have been in possession of the compromised devices and if you have had any service conducted on the compromised devices.

Recommended Mitigations:

Vulnerability Management:

- Ensure proper migrating steps or compensating controls are implemented for vulnerabilities that cannot be patched in a timely manner.
- Recommend that organizations routinely audit their configuration and patch management programs to ensure they can track and mitigate emerging threats. Implementing a rigorous configuration and patch management program will hamper sophisticated cyber threat actors' operations and protect organizations' resources and information systems.
- Flag and delete listed registry entries.

Protect Credentials:

- 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. Regularly change passwords and do not reuse passwords for multiple accounts.

- Audit all remote authentications from trusted networks or service providers.
- Detect mismatches by correlating credentials used within internal networks with those employed on external-facing systems.
- Log use of system administrator commands, such as net, ipconfig, and ping.
- Audit logs for suspicious behavior.

Network Hygiene and Monitoring:

- Actively scan and monitor internet-accessible applications for unauthorized access, modification, and anomalous activities.
- Actively monitor server disk use and audit for significant changes.
- Log DNS queries and consider blocking all outbound DNS requests that do not originate from approved

DNS servers. Monitor DNS queries for C2 over DNS:

- Develop and monitor the network and system baselines to allow for the identification of anomalous activity. Identify and suspend access of users exhibiting unusual activity.
- Use whitelist or baseline comparison to monitor Windows event logs and network traffic to detect when a user maps a privileged administrative share on a Windows system.
- Leverage multi-sourced threat-reputation services for files, DNS, URLs, IPs, and email addresses.
- 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.

Reporting Notice

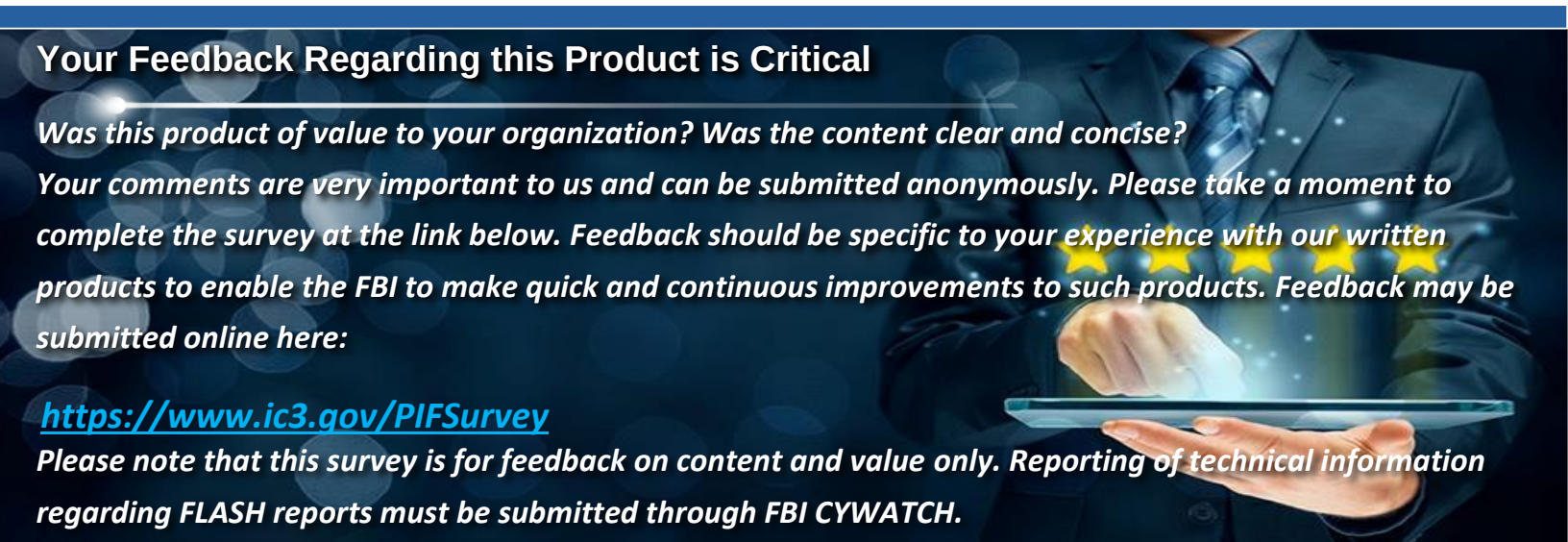
The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. 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, 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

The information in this report is being provided "as is" for informational purposes only. The FBI does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI.

This product is marked TLP:AMBER The information in this product may be shared with members of your organization, and with clients and customers who need to know the information to protect themselves or prevent future harm.



Your Feedback Regarding 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.