27 May 2021

Alert Number

MI-000148-MW

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 was coordinated with DHS/CISA.

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

APT Actors Exploiting Fortinet Vulnerabilities to Gain Access for Malicious Activity

Summary

The FBI is continuing to warn about Advanced Persistent Threat (APT) actors exploiting Fortinet vulnerabilities. As of at least May 2021, an APT actor group almost certainly exploited a Fortigate appliance to access a webserver hosting the domain for a U.S. municipal government. The APT actors likely created an account with the username “elie” to further enable malicious activity on the network.

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) previously warned in April 2021 that APT actors had gained access to devices on ports 4443, 8443, and 10443 for Fortinet FortiOS CVE-2018-13379, and enumerated devices for FortiOS CVE-2020-12812 and FortiOS CVE-2019-5591.

Access gained by the APT actors can be leveraged to conduct data exfiltration, data encryption, or other malicious activity. The APT actors are actively targeting a broad range of victims across multiple sectors, indicating the activity is focused on exploiting vulnerabilities rather than targeted at specific sectors. Please see Joint Cybersecurity Advisory AA21-092A, published 2 April 2021, for more information on this activity.

Technical Details

The FBI identified the following indicators of compromise (IOCs) that we assess are likely associated with this APT activity.

New User Accounts

The APT actors may have established new user accounts on domain controllers, servers, workstations, and the active directories. Some of these accounts appear to have been created to look similar to other existing accounts on the network, so specific account names may vary per organization. In addition to unrecognized user accounts or accounts established to masquerade as existing accounts, the following account usernames may be associated with this activity:

- "elie"
- "WADGUtilityAccount"

Executable Files

Filename:	Audio.exe or frpc.exe
MD5:	b90f05b5e705e0b0cb47f51b985f84db
SHA-1	5bd0690247dc1e446916800af169270f100d089b
SHA-256:	28332bdbfaeb8333dad5ada3c10819a1a015db9106d5e8a74beaaf03797511aa
Vhash:	017067555d5d15541az28!z
Authentihash:	ed463da90504f3adb43ab82044cddab8922ba029511da9ad5a52b8c20bda65ee
Imphash:	93a138801d9601e4c36e6274c8b9d111
SSDEEP:	98304:MeOuFco2Aate8mjOaFEKC8KZ1F4ANWyJXf/X+g4:MeHFV2AatevjOaDC8KZ1xNWy93U
Note:	Identical to "frpc.exe" available at: https://github[.]com/fatedier/frp/releases/download/v0.34.3/frp_0.34.3_windows_amd64.zip

Filename:	Frps.exe
MD5:	26f330dadcdd717ef575aa5bfcdbe76a
SHA-1	c4160aa55d092cf916a98f3b3ee8b940f2755053
SHA-256:	d7982ffe09f947e5b4237c9477af73a034114af03968e3c4ce462a029f072a5a
Vhash:	017057555d6d141az25!z
Authentihash:	40ed1568fef4c5f9d03c370b2b9b06a3d0bd32caca1850f509223b3cee2225ea
Imphash:	91802a615b3a5c4bcc05bc5f66a5b219
SSDEEP:	196608:/qTLyGAlLrOt8enYfrhkhBnfY0NIPvoOQiE:GLHiLrSfY5voO
Note:	Identical to “frps.exe” available at: https://github[.]com/fatedier/frp/releases/download/v0.33.0/frp_0.33.0_windows_amd64.zip

Associated Tools

- Mimikatz (credential theft)
- MinerGate (crypto mining)
- WinPEAS (privilege escalation)
- SharpWMI (Windows Management Instrumentation)
- BitLocker activation when not anticipated (data encryption)
- WinRAR where not expected (archiving)
- FileZilla where not expected (file transfer)

Outbound Traffic

Any FTP transfers over port 443

Unrecognized Scheduled Tasks

The APT actors may have made modifications to the Task Scheduler that may display as unrecognized scheduled tasks or “actions.” Specifically, the below established task may be associated with this activity:

- SynchronizeTimeZone

Recommended Mitigations

- Immediately patch CVEs 2018-13379, 2020-12812, and 2019-5591.
- If FortiOS is not used by your organization, add the key artifact files used by FortiOS to your organization's execution denylist. Any attempts to install or run this program and its associated files should be prevented.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system defined or recognized scheduled tasks for unrecognized "actions" (for example: review the steps each scheduled task is expected to perform).
- Review antivirus logs for indications they were unexpectedly turned off.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multifactor authentication where possible.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts. Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update antivirus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field.

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.