Iran-Based Threat Actor Exploits VPN Vulnerabilities

us-cert.cisa.gov/ncas/alerts/aa20-259a

Summary

This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

This product was written by the Cybersecurity and Infrastructure Security Agency (CISA) with contributions from the Federal Bureau of Investigation (FBI). CISA and FBI are aware of an Iran-based malicious cyber actor targeting several U.S. federal agencies and other U.S.-based networks. Analysis of the threat actor's indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) indicates a correlation with the group known by the names, Pioneer Kitten and UNC757. This threat actor has been observed exploiting several publicly known Common Vulnerabilities and Exposures (CVEs) dealing with Pulse Secure virtual private network (VPN), Citrix NetScaler, and F5 vulnerabilities. This threat actor used these vulnerabilities to gain initial access to targeted networks and then maintained access within the successfully exploited networks for several months using multiple means of persistence.

This Advisory provides the threat actor's TTPs, IOCs, and exploited CVEs to help administrators and network defenders identify a potential compromise of their network and protect their organization from future attacks.

Click here for a PDF version of this report.

Technical Details

CISA and FBI are aware of a widespread campaign from an Iran-based malicious cyber actor targeting several industries mainly associated with information technology, government, healthcare, financial, insurance, and media sectors across the United States. The threat actor conducts mass-scanning and uses tools, such as Nmap, to identify open ports. Once the open ports are identified, the threat actor exploits CVEs related to VPN infrastructure to gain initial access to a targeted network. CISA and the FBI have observed the threat actor exploiting multiple CVEs, including CVE-2019-11510, CVE-2019-11539, CVE-2019-19781, and CVE-2020-5902.

After gaining initial access to a targeted network, the threat actor obtains administrator-level credentials and installs web shells allowing further entrenchment. After establishing a foothold, the threat actor's goals appear to be maintaining persistence and exfiltrating data. This threat actor has been observed selling access to compromised network infrastructure in

an online hacker forum. Industry reporting indicates that the threat actor operates as a contractor supporting Iranian government interests, but the malicious activity appears to also serve the threat actor's own financial interests. The FBI notes this threat actor has the capability, and likely the intent, to deploy ransomware on victim networks.

CISA and FBI have observed this Iran-based threat actor relying on exploits of remote external services on internet-facing assets to gain initial access to victim networks. The threat actor also relies heavily on open-source and operating system (OS) tooling to conduct operations, such as ngrok; fast reverse proxy (FRP); Lightweight Directory Access Protocol (LDAP) directory browser; as well as web shells known as ChunkyTuna, Tiny, and China Chopper.

Table 1 illustrates some of the common tools this threat actor has used.

Table 1: Common exploit tools

Tool	Detail
ChunkyTuna web shell	ChunkyTuna allows for chunked transfer encoding hypertext transfer protocol (HTTP) that tunnels Transmission Control Protocol (TCP) streams over HTTP. The web shell allows for reverse connections to a server with the intent to exfiltrate data.
Tiny web shell	Tiny uses Hypertext Preprocessor (PHP) to create a backdoor. It has the capability to allow a threat actor remote access to the system and can also tunnel or route traffic.
China Chopper web shell	China Chopper is a web shell hosted on a web server and is mainly used for web application attacks; it is configured in a client/server relationship. China Chopper contains security scanners and can be used to upload files and brute-force passwords.
FRPC	FRPC is a modified version of the open-source FRP tool. It allows a system—inside a router or firewall providing Network Address Translation—to provide network access to systems/operators located outside of the victim network. In this case, FRPC was used as reverse proxy, tunneling Remote Desktop Protocol (RDP) over Transport Layer Security (TLS), giving the threat actor primary persistence.
Chisel	Chisel is a fast TCP tunnel over HTTP and secured via Secure Shell (SSH). It is a single executable that includes both client and server. The tool is useful for passing through firewalls, but it can also be used to provide a secure form of communication to an endpoint on a victim network.
ngrok	ngrok is a tool used to expose a local port to the internet. Optionally, tunnels can be secured with TLS.

Tool	Detail
Nmap	Nmap is used for vulnerability scanning and network discovery.
Angry IP Scanner	Angry IP Scanner is a scanner that can ping a range of Internet Protocol (IP) addresses to check if they are active and can also resolve hostnames, scan ports, etc.
Drupwn	Drupwn is a Python-based tool used to scan for vulnerabilities and exploit CVEs in Drupal devices.

Notable means of detecting this threat actor:

- CISA and the FBI note that this group makes significant use of ngrok, which may appear as TCP port 443 connections to external cloud-based infrastructure.
- The threat actor uses FRPC over port 7557.
- Malware Analysis Report MAR-10297887-1.v1 details some of the tools this threat actor used against some victims.

The following file paths can be used to detect Tiny web shell, ChunkyTuna web shell, or Chisel if a network has been compromised by this attacker exploiting CVE-2019-19781.

Tiny web shell

```
/netscaler/ns_gui/admin_ui/rdx/core/css/images/css.php
/netscaler/ns_gui/vpn/images/vpn_ns_gui.php
/var/vpn/themes/imgs/tiny.php
```

ChunkyTuna web shell

```
/var/vpn/themes/imgs/debug.php
/var/vpn/themes/imgs/include.php
/var/vpn/themes/imgs/whatfile
```

Chisel

```
/var/nstmp/chisel
```

MITRE ATT&CK Framework

Initial Access

As indicated in table 2, the threat actor primarily gained initial access by using the publicly available exploit for CVE-2019-19781. From there, the threat actor used the Citrix environment to establish a presence on an internal network server.

Table 2: Initial access techniques

ID	Technique/Sub-Technique	Context
T1190	Exploit Public-Facing Application	The threat actor primarily gained initial access by compromising a Citrix NetScaler remote access server using a publicly available exploit for CVE-2019-19781. The threat actor also exploited CVE-2019-11510, CVE-2019-11539, and CVE-2020-5902.

Execution

After gaining initial access, the threat actor began executing scripts, as shown in table 3.

Table 3: Execution techniques

ID	Technique/Sub-Technique	Context
T1059.001	Command and Scripting Interpreter: PowerShell	A PowerShell script (`keethief` and `kee.ps1`) was used to access KeePass data.
T1059.003	Command and Scripting Interpreter: Windows Command Shell	`cmd.exe` was launched via sticky keys that was likely used as a password changing mechanism.

Persistence

CISA observed the threat actor using the techniques identified in table 4 to establish persistence.

Table 4: Persistence techniques

ID	Technique/Sub-Technique	Context
T1053.003	Scheduled Task/Job: Cron	The threat actor loaded a series of scripts to `cron` and ran them for various purposes (mainly to access NetScaler web forms).
T1053.005	Scheduled Task/Job: Scheduled Task	The threat actor installed and used FRPC (`frpc.exe`) on both NetScaler and internal devices. The task was named `lpupdate` and the binary was named `svchost` , which was the reverse proxy. The threat actor executed this command daily.

ID	Technique/Sub-Technique	Context
T1505.003	Server Software Component: Web Shell	The threat actor used several web shells on existing web servers. Both NetScaler and web servers called out for ChunkyTuna.
T1546.008	Event Triggered Execution: Accessibility Features	The threat actor used sticky keys (`sethc.exe`) to launch `cmd.exe` .

Privilege Escalation

CISA observed no evidence of direct privilege escalation. The threat actor attained domain administrator credentials on the NetScaler device via exploit and continued to expand credential access on the network.

Defense Evasion

CISA observed the threat actor using the techniques identified in table 5 to evade detection.

Table 5: Defensive evasion techniques

ID	Technique/Sub-Technique	Context
T1027.002	Obfuscated Files or Information: Software Packing	The threat actor used base64 encoding for payloads on NetScaler during initial access, making the pre-compiled payloads easier to avoid detection.
T1027.004	Obfuscated Files or Information: Compile After Delivery	The threat actor used base64 encoding schemes on distributed (uncompiled) scripts and files to avoid detection.
T1036.004	Masquerading: Masquerade Task or Service	The threat actor used FRPC (`frpc.exe`) daily as reverse proxy, tunneling RDP over TLS. The FRPC (`frpc.exe`) task name was `lpupdate` and ran out of Input Method Editor (IME) directory. In other events, the threat actor has been observed hiding activity via ngrok.

ID	Technique/Sub-Technique	Context
T1036.005	Masquerading: Match Legitimate Name or Location	The FRPC (`frpc.exe`) binary name was `svchost` , and the configuration file was `dllhost.dll` , attempting to masquerade as a legitimate Dynamic Link Library.
T1070.004	Indicator Removal on Host: File Deletion	To minimize their footprint, the threat actor ran `./httpd-nscache_clean` every 30 minutes, which cleaned up files on the NetScaler device.

Credential Access

CISA observed the threat actor using the techniques identified in table 6 to further their credential access.

Table 6: Credential access techniques

ID	Technique/Sub-Technique	Context
T1003.001	OS Credential Dumping: LSASS Memory	The threat actor used `procdump` to dump process memory from the Local Security Authority Subsystem Service (LSASS).
T1003.003	OS Credential Dumping: Windows NT Directory Services (NTDS)	The threat actor used Volume Shadow Copy to access credential information from the NTDS file.
T1552.001	Unsecured Credentials: Credentials in Files	The threat actor accessed files containing valid credentials.
T1555	Credentials from Password Stores	The threat actor accessed a `KeePass` database multiple times and used `kee.ps1` PowerShell script.
T1558	Steal or Forge Kerberos Tickets	The threat actor conducted a directory traversal attack by creating files and exfiltrating a Kerberos ticket on a NetScaler device. The threat actor was then able to gain access to a domain account.

Discovery

CISA observed the threat actor using the techniques identified in table 7 to learn more about the victim environments.

Table 7: Discovery techniques

ID	Technique/Sub-Technique	Context
T1018	Remote System Discovery	The threat actor used Angry IP Scanner to detect remote systems.
T1083	File and Directory Discovery	The threat actor used WizTree to obtain network files and directory listings.
T1087	Account Discovery	The threat actor accessed `ntuser.dat` and `UserClass.dat` and used Softerra LDAP Browser to browse documentation for service accounts.
T1217	Browser Bookmark Discovery	The threat actor used Google Chrome bookmarks to find internal resources and assets.

Lateral Movement

CISA also observed the threat actor using open-source tools such as Plink and TightVNC for lateral movement. CISA observed the threat actor using the techniques identified in table 8 for lateral movement within the victim environment.

Table 8: Lateral movement techniques

ID	Technique/Sub-Technique	Context
T1021	Remote Services	The threat actor used RDP with valid account credentials for lateral movement in the environment.
T1021.001	Remote Services: Remote Desktop Protocol	The threat actor used RDP to log in and then conduct lateral movement.
T1021.002	Remote Services: SMB/Windows Admin Shares	The threat actor used PsExec. and PSEXECSVC pervasively on several hosts. The threat actor was also observed using a valid account to access SMB shares.

ID	Technique/Sub-Technique	Context
T1021.004	Remote Services: SSH	The threat actor used Plink and PuTTY for lateral movement. Artifacts of Plink were used for encrypted sessions in the system registry hive.
T1021.005	Remote Services: Virtual Network Computing (VNC)	The threat actor installed TightVNC server and client pervasively on compromised servers and endpoints in the network environment as lateral movement tool.
T1563.002	Remote Service Session Hijacking: RDP Hijacking	The threat actor likely hijacked a legitimate RDP session to move laterally within the network environment.

Collection

CISA observed the threat actor using the techniques identified in table 9 for collection within the victim environment.

Table 9: Collection techniques

ID	Technique/Sub-Technique	Context
T1005	Data from Local System	The threat actor searched local system sources to accessed sensitive documents.
T1039	Data from Network Shared Drive	The threat actor searched network shares to access sensitive documents.
T1213	Data from Information Repositories	The threat actor accessed victim security/IT monitoring environments, Microsoft Teams, etc., to mine valuable information.
T1530	Data from Cloud Storage Object	The threat actor obtained files from the victim cloud storage instances.
T1560.001	Archive Collected Data: Archive via Utility	The threat actor used 7-Zip to archive data.

Command and Control

CISA observed the threat actor using the techniques identified in table 10 for command and control (C2).

Table 10: Command and control techniques

ID	Technique/Sub-Technique	Context
T1071.001	Application Layer Protocol: Web Protocols	The threat actor used various web mechanisms and protocols, including the web shells listed in table 1.
T1105	Ingress Tool Transfer	The threat actor downloaded tools such as PsExec directly to endpoints and downloaded web shells and scripts to NetScaler in base64-encoded schemes.
T1572	Protocol Tunneling	The threat actor used `FRPC.exe` to tunnel RDP over port 443. The threat actor has also been observed using ngrok for tunneling.

Exfiltration

CISA currently has no evidence of data exfiltration from this threat actor but assesses that it was likely due to the use of 7-Zip and viewing of sensitive documents.

Mitigations

Recommendations

CISA and FBI recommend implementing the following recommendations.

- If your organization has not patched for the Citrix CVE-2019-19781 vulnerability, and a compromise is suspected, follow the recommendations in CISA Alert AA20-031A.
- This threat actor has been observed targeting other CVEs mentioned in this report; follow the recommendations in the CISA resources provided below.
- If using Windows Active Directory and compromise is suspected, conduct remediation of the compromised Windows Active Directory forest.
    If compromised, rebuild/reimage compromised NetScaler devices.
- Routinely audit configuration and patch management programs.
- Monitor network traffic for unexpected and unapproved protocols, especially outbound to the internet (e.g., SSH, SMB, RDP).
- Implement multi-factor authentication, especially for privileged accounts.
- Use separate administrative accounts on separate administration workstations.
- Implement the principle of least privilege on data access.
- Secure RDP and other remote access solutions using multifactor authentication and “jump boxes” for access.

- Deploy endpoint defense tools on all endpoints; ensure they work and are up to date.
- Keep software up to date.

Contact Information

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at central@cisa.dhs.gov.

Resources

CISA Alert AA20-031A: Detecting Citrix CVE-2019-19781
CISA Alert AA20-073A: Enterprise VPN Security
CISA Alert AA20-107A: Continued Threat Actor Exploitation Post Pulse Secure VPN Patching
CISA Alert AA20-206A: Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902
CISA Security Tip: Securing Network Infrastructure Devices

Revisions

September 15, 2020: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.