JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

Product ID: AA22-320A

November 16, 2022

Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester

SUMMARY

From mid-June through mid-July 2022, CISA conducted an incident response engagement at a Federal Civilian Executive Branch (FCEB) organization where CISA observed suspected advanced persistent threat (APT) activity. In the course of incident response activities, CISA determined that cyber threat actors exploited the Log4Shell vulnerability in an unpatched VMware Horizon server, installed XMRig crypto mining software, moved laterally to the domain controller (DC), compromised credentials, and then implanted Ngrok reverse proxies on several hosts to maintain persistence. CISA and the Federal Bureau of Investigation (FBI) assess that the FCEB network was compromised by Iranian government-sponsored APT actors.

CISA and FBI are releasing this Cybersecurity Advisory (CSA) providing the suspected Iranian government-sponsored actors' tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help network defenders detect and protect against related compromises.

CISA and FBI encourage all organizations with affected VMware systems that did not immediately apply available patches or workarounds to assume compromise and initiate threat hunting activities. If suspected initial access or compromise is detected based on IOCs or TTPs described in this CSA, CISA and FBI encourage organizations to assume lateral movement by threat actors, investigate connected systems (including the DC), and audit privileged accounts. All organizations, regardless of identified evidence of compromise, should apply the recommendations in the Mitigations section of this CSA to protect against similar malicious cyber activity.

For more information on Iranian government-sponsored Iranian malicious cyber activity, see CISA's Iran Cyber Threat Overview and Advisories webpage and FBI's Iran Threats webpage.

For a downloadable copy of IOCs, see: AA22-320A.stix, 155 mb.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282- 0870. 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.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.
For more information on the Traffic Light Protocol, see cisa.gov/tlp/.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 12. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques with corresponding mitigation and/or detection recommendations.

Overview

In April 2022, CISA conducted retrospective analysis using EINSTEIN—an FCEB-wide intrusion detection system (IDS) operated and monitored by CISA—and identified suspected APT activity on an FCEB organization's network. CISA observed bi-directional traffic between the network and a known malicious IP address associated with exploitation of the Log4Shell vulnerability (CVE-2021-44228) in VMware Horizon servers. In coordination with the FCEB organization, CISA initiated threat hunting incident response activities; however, prior to deploying an incident response team, CISA observed additional suspected APT activity. Specifically, CISA observed HTTPS activity from IP address `51.89.181[.]64` to the organization's VMware server. Based on trusted third-party reporting, `51.89.181[.]64` is a Lightweight Directory Access Protocol (LDAP) server associated with threat actors exploiting Log4Shell. Following HTTPS activity, CISA observed a suspected LDAP callback on port 443 to this IP address. CISA also observed a DNS query for `us-nation-ny[.]cf` that resolved back to `51.89.181[.]64` when the victim server was returning this Log4Shell LDAP callback to the actors' server.

CISA assessed that this traffic indicated a confirmed compromise based on the successful callback to the indicator and informed the organization of these findings; the organization investigated the activity and found signs of compromise. As trusted-third party reporting associated Log4Shell activity from `51.89.181[.]64` with lateral movement and targeting of DCs, CISA suspected the threat actors had moved laterally and compromised the organization's DC.

From mid-June through mid-July 2022, CISA conducted an onsite incident response engagement and determined that the organization was compromised as early as February 2022, by likely Iranian government-sponsored APT actors who installed XMRig crypto mining software. The threat actors also moved laterally to the domain controller, compromised credentials, and implanted Ngrok reverse proxies.

Threat Actor Activity

In February 2022, the threat actors exploited Log4Shell [T1190] for initial access [TA0001] to the organization's unpatched VMware Horizon server. As part of their initial exploitation, CISA observed a connection to known malicious IP address `182.54.217[.]2` lasting 17.6 seconds.

The actors' exploit payload ran the following PowerShell command [T1059.001] that added an exclusion tool to Windows Defender [T1562.001]:

```
powershell try{Add-MpPreference -ExclusionPath 'C:\'; Write-Host 'added-exclusion'} catch {Write-Host 'adding-exclusion-failed' }; powershell -enc "$BASE64 encoded payload to download next stage and execute it"
```

The exclusion tool allowlisted the entire `c:\drive`, enabling threat actors to download tools to the `c:\drive` without virus scans. The exploit payload then downloaded `mdeploy.text` from `182.54.217[.]2/mdepoy.txt` to `C:\users\public\mde.ps1` [T1105]. When executed, `mde.ps1` downloaded `file.zip` from `182.54.217[.]2` and removed `mde.ps1` from the disk [T1070.004].

`file.zip` contained XMRig cryptocurrency mining software and associated configuration files.

- `WinRing0x64.sys` – XMRig Miner driver
- `wuacltservice.exe` – XMRig Miner
- `config.json` – XMRig miner configuration
- `RuntimeBroker.exe` – Associated file. This file can create a local user account [T1136.001] and tests for internet connectivity by pinging `8.8.8.8` [T1016.001]. The exploit payload created a Scheduled Task [T1053.005] that executed `RuntimeBroker.exe` daily as `SYSTEM`. **Note**: By exploiting Log4Shell, the actors gained access to a VMware service account with administrator and system level access. The Scheduled Task was named `RuntimeBrokerService.exe` to masquerade as a legitimate Windows task.

See MAR 10387061-1.v1 for additional information, including IOCs, on these four files.

After obtaining initial access and installing XMRig on the VMWare Horizon server, the actors used RDP [T1021.001] and the built-in Windows user account `DefaultAccount` [T1078.001] to move laterally [TA0008] to a VMware VDI-KMS host. Once the threat actor established themselves on the VDI-KMS host, CISA observed the actors download around 30 megabytes of files from `transfer[.]sh` server associated with `144.76.136[.]153`. The actors downloaded the following tools:

- PsExec – a Microsoft signed tool for system administrators.
- Mimikatz – a credential theft tool.
- Ngrok – a reverse proxy tool for proxying an internal service out onto an Ngrok domain, which the user can then access at a randomly generated subdomain at `*.ngrok[.]io`. CISA has observed this tool in use by some commercial products for benign purposes; however, this process bypasses typical firewall controls and may be a potentially unwanted application in production environments. Ngrok is known to be used for malicious purposes.[1]

The threat actors then executed Mimikatz on VDI-KMS to harvest credentials and created a rogue domain administrator account [T1136.002]. Using the newly created account, the actors leveraged RDP to propagate to several hosts within the network. Upon logging into each host, the actors manually disabled Windows Defender via the Graphical User Interface (GUI) and implanted Ngrok executables and configuration files. The threat actors were able to implant Ngrok on multiple hosts to ensure Ngrok's persistence should they lose access to a machine during a routine reboot. The actors were able to proxy [T1090] RDP sessions, which were only observable on the local network as outgoing HTTPS port 443 connections to `tunnel.us.ngrok[.]com` and `korgn.su.lennut[.]com` (the prior domain in reverse). It is possible, but was not observed, that the threat actors configured a custom domain, or used other Ngrok tunnel domains, wildcarded here as `*.ngrok[.]com`, `*.ngrok[.]io`, `ngrok.*.tunnel[.]com`, or `korgn.*.lennut[.]com`.

Once the threat actors established a deep foothold in the network and moved laterally to the domain controller, they executed the following PowerShell command on the Active Directory to obtain a list of all machines attached to the domain [T1018]:

```
Powershell.exe get-adcomputer -filter * -properties * | select
name,operatingsystem,ipv4address &gt;
```

The threat actors also changed the password for the local administrator account [T1098] on several hosts as a backup should the rogue domain administrator account get detected and terminated. Additionally, the threat actor was observed attempting to dump the Local Security Authority Subsystem Service (LSASS) process [T1003.001] with task manager but this was stopped by additional anti-virus the FCEB organization had installed.

MITRE ATT&CK TACTICS AND TECHNIQUES

See table 1 for all referenced threat actor tactics and techniques in this advisory, as well as corresponding detection and/or mitigation recommendations. For additional mitigations, see the Mitigations section.

Table 1: Cyber Threat Actors ATT&CK Techniques for Enterprise

Initial Access			
Technique Title	**ID**	**Use**	**Recommendations**
Exploit Public-Facing Application	T1190	The actors exploited Log4Shell for initial access to the organization's VMware Horizon server.	**Mitigation/Detection:** Use a firewall or web-application firewall and enable logging to prevent and detect potential Log4Shell exploitation attempts [M1050]. **Mitigation:** Perform regular vulnerability scanning to detect Log4J vulnerabilities and update Log4J software using vendor provided patches [M1016],[M1051].

Execution			
Technique Title	**ID**	**Use**	**Recommendation**
Command and Scripting Interpreter: PowerShell	T1059.001	The actors ran PowerShell commands that added an exclusion tool to Windows Defender. The actors executed PowerShell on the AD to obtain a list of machines on the domain.	**Mitigation:** Disable or remove PowerShell for non-administrative users [M1042],[M1026] or enable code-signing to execute only signed scripts [M1045]. **Mitigation:** Employ anti-malware to automatically detect and quarantine malicious scripts [M1049].
Persistence			
Technique Title	**ID**	**Use**	**Recommendations**
Account Manipulation	T1098	The actors changed the password for the local administrator account on several hosts.	**Mitigation:** Use multifactor authentication for user and privileged accounts [M1032]. **Detection:** Monitor events for changes to account objects and/or permissions on systems and the domain, such as event IDs `4738`, `4728`, and `4670`. Monitor for modification of accounts in correlation with other suspicious activity [DS0002].
Create Account: Local Account	T1136.001	The actors' malware can create local user accounts.	**Mitigation:** Configure access controls and firewalls to limit access to domain controllers and systems used to create and manage accounts. **Detection:** Monitor executed commands and arguments for actions that are associated with local account creation, such as `net`

			`user /add` , `useradd`, and `dscl -create` [DS0017]. **Detection:** Enable logging for new user creation [DS0002].
Create Account: Domain Account	T1136.002	The actors used Mimikatz to create a rogue domain administrator account.	**Mitigation:** Configure access controls and firewalls to limit access to domain controllers and systems used to create and manage accounts. **Detection:** Enable logging for new user creation, especially domain administrator accounts [DS0002].
Scheduled Task/Job: Scheduled Task	T1053.005	The actors' exploit payload created Scheduled Task `RuntimeBrokerService.exe`, which executed `RuntimeBroker.exe` daily as `SYSTEM`.	**Mitigation:** Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as `SYSTEM` [M1028]. **Detection:** Monitor for newly constructed processes and/or command-lines that execute from the `svchost.exe` in Windows 10 and the Windows Task Scheduler `taskeng.exe` for older versions of Windows [DS0009] **Detection:** Monitor for newly constructed scheduled jobs by enabling the `Microsoft-Windows-TaskScheduler/Operational` setting within the event logging service [DS0003].
Valid Accounts: Default Accounts	T1078.001	The actors used built-in Windows user account `DefaultAccount`.	**Mitigation:** Change default usernames and passwords immediately after the installation and before deployment to a production environment [M1027].

			Detection: Develop rules to monitor logon behavior across default accounts that have been activated or logged into [DS0028].
Defense Evasion			
Technique Title	**ID**	**Use**	**Recommendations**
Impair Defenses: Disable or Modify Tools	T1562.001	The actors added an exclusion tool to Windows Defender. The tool allowlisted the entire `c:\drive`, enabling the actors to bypass virus scans for tools they downloaded to the `c:\drive`. The actors manually disabled Windows Defender via the GUI.	**Mitigation:** Ensure proper user permissions are in place to prevent adversaries from disabling or interfering with security services. [M1018]. **Detection:** Monitor for changes made to Windows Registry keys and/or values related to services and startup programs that correspond to security tools such as `HKLM:\SOFTWARE\Policies\Microsoft\Windows` Defender [DS0024]. **Detection:** Monitor for telemetry that provides context for modification or deletion of information related to security software processes or services such as Windows Defender definition files in Windows and System log files in Linux [DS0013]. **Detection:** Monitor processes for unexpected termination related to security tools/services [DS0009].
Indicator Removal on Host: File Deletion	T1070.004	The actors removed malicious file `mde.ps1` from the dis.	**Detection:** Monitor executed commands and arguments for actions that could be utilized to unlink, rename, or delete files [DS0017].

			Detection: Monitor for unexpected deletion of files from the system [DS0022].
Credential Access			
Technique Title	**ID**	**Use**	**Recommendations**
OS Credential Dumping: LSASS Memory	T1003.001	The actors were observed trying to dump LSASS process.	**Mitigation:** With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping [M1043] **Mitigation:** On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing [M1040]. **Mitigation:** Ensure that local administrator accounts have complex, unique passwords across all systems on the network [M1027]. **Detection:** Monitor for unexpected processes interacting with `LSASS.exe`. Common credential dumpers such as Mimikatz access `LSASS.exe` by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. [DS0009]. **Detection:** Monitor executed commands and arguments that may attempt to access credential material stored in the process memory of the LSASS [DS0017].

Credentials from Password Stores	T1555	The actors used Mimikatz to harvest credentials.	**Mitigation:** Organizations may consider weighing the risk of storing credentials in password stores and web browsers. If system, software, or web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in improper locations [M1027]. **Detection:** Monitor for processes being accessed that may search for common password storage locations to obtain user credentials [DS0009]. **Detection:** Monitor executed commands and arguments that may search for common password storage locations to obtain user credentials [DS0017].
Discovery			
Technique Title	**ID**	**Use**	**Recommendations**
Remote System Discovery	T1018	The actors executed a PowerShell command on the AD to obtain a list of all machines attached to the domain.	**Detection:** Monitor executed commands and arguments that may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for lateral movement [DS0017]. **Detection:** Monitor for newly constructed network connections associated with pings/scans that may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for lateral movement [DS0029].

			Detection: Monitor for newly executed processes that can be used to discover remote systems, such as ping.exe and tracert.exe, especially when executed in quick succession [DS0009].
System Network Configuration Discovery: Internet Connection Discovery	T1016.001	The actors' malware tests for internet connectivity by pinging `8.8.8.8`.	**Mitigation:** Monitor executed commands, arguments [DS0017] and executed processes (e.g., `tracert` or `ping`) [DS0009] that may check for internet connectivity on compromised systems.
Lateral Movement			
Technique Title	**ID**	**Use**	**Recommendations**
Remote Services: Remote Desktop Protocol	T1021.001	The actors used RDP to move laterally to multiple hosts on the network.	**Mitigation:** Use MFA for remote logins [M1032]. **Mitigation:** Disable the RDP service if it is unnecessary [M1042]. **Mitigation:** Do not leave RDP accessible from the internet. Enable firewall rules to block RDP traffic between network security zones within a network [M1030]. **Mitigation:** Consider removing the local Administrators group from the list of groups allowed to log in through RDP [M1026]. **Detection:** Monitor for user accounts logged into systems associated with RDP (ex: Windows EID `4624` Logon Type 10). Other factors, such as access patterns (ex: multiple systems over a relatively short period of time) and activity that occurs after a remote login, may indicate suspicious or

			malicious behavior with RDP [DS0028].
Command and Control			
Technique Title	**ID**	**Use**	**Recommendations**
Proxy	T1090	The actors used Ngrok to proxy RDP connections and to perform command and control.	**Mitigation:** Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network allow and block lists [M1037]. **Detection:** Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g., extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure) [DS0029].
Ingress Tool Transfer	T1105	The actors downloaded malware and multiple tools to the network, including PsExec, Mimikatz, and Ngrok.	**Mitigation:** Employ anti-malware to automatically detect and quarantine malicious scripts [M1049].

INCIDENT RESPONSE

If suspected initial access or compromise is detected based on IOCs or TTPs in this CSA, CISA encourages organizations to assume lateral movement by threat actors and investigate connected systems and the DC.

CISA recommends organizations apply the following steps **before applying** any mitigations, including patching.

1. Immediately isolate affected systems.
2. Collect and review relevant logs, data, and artifacts. Take a memory capture of the device(s) and a forensic image capture for detailed analysis.

3. Consider soliciting support from a third-party incident response organization that can provide subject matter expertise to ensure the actor is eradicated from the network and to avoid residual issues that could enable follow-on exploitation.
4. Report incidents to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870) or your local FBI field office or FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov.

MITIGATIONS

CISA and FBI recommend implementing the mitigations below and in table 1 to improve your organization's cybersecurity posture on the basis of threat actor behaviors.

- **Install updated builds to ensure affected VMware Horizon and UAG systems are updated to the latest version**.
    - If updates or workarounds were not promptly applied following VMware's release of updates for Log4Shell in December 2021, treat those VMware Horizon systems as compromised. Follow the pro-active incident response procedures outlined above prior to applying updates. If no compromise is detected, apply these updates as soon as possible.
        - See VMware Security Advisory VMSA-2021-0028.13 and VMware Knowledge Base (KB) 87073 to determine which VMware Horizon components are vulnerable.
        - **Note:** Until the update is fully implemented, consider removing vulnerable components from the internet to limit the scope of traffic. While installing the updates, ensure network perimeter access controls are as restrictive as possible.
        - If upgrading is not immediately feasible, see KB87073 and KB87092 for vendor-provided temporary workarounds. Implement temporary solutions using an account with administrative privileges. Note that these temporary solutions should not be treated as permanent fixes; vulnerable components should be upgraded to the latest build as soon as possible.
        - Prior to implementing any temporary solution, ensure appropriate backups have been completed.
        - Verify successful implementation of mitigations by executing the vendor supplied script `Horizon_Windows_Log4j_Mitigations.zip` without parameters to ensure that no vulnerabilities remain. See KB87073 for details.
- **Keep all software up to date** and prioritize patching known exploited vulnerabilities (KEVs).
- **Minimize the internet-facing attack surface** by hosting essential services on a segregated DMZ, ensuring strict network perimeter access controls, and not hosting internet-facing services that are not essential to business operations. Where possible, implement regularly updated web application firewalls (WAF) in front of public-facing services. WAFs can protect against web-based exploitation using signatures and heuristics that are likely to block or alert on malicious traffic.

- **Use best practices for identity and access management (IAM)** by implementing phishing resistant MFA, enforcing use of strong passwords, regularly auditing administrator accounts and permissions, and limiting user access through the principle of least privilege. Disable inactive accounts uniformly across the AD, MFA systems, etc.
  - If using Windows 10 version 1607 or Windows Server 2016 or later, monitor or disable Windows `DefaultAccount`, also known as the Default System Managed Account (DSMA).
- **Audit domain controllers to log** successful Kerberos Ticket Granting Service (TGS) requests and ensure the events are monitored for anomalous activity.
  - Secure accounts.
  - Enforce the principle of least privilege. Administrator accounts should have the minimum permission necessary to complete their tasks.
  - Ensure there are unique and distinct administrative accounts for each set of administrative tasks.
  - Create non-privileged accounts for privileged users and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).
- **Create a deny list of known compromised credentials** and prevent users from using known-compromised passwords.
- **Secure credentials by restricting where accounts and credentials can be used** and by using local device credential protection features.
  - Use virtualizing solutions on modern hardware and software to ensure credentials are securely stored.
  - Ensure storage of clear text passwords in LSASS memory is disabled. **Note:** For Windows 8, this is enabled by default. For more information see Microsoft Security Advisory Update to Improve Credentials Protection and Management.
  - Consider disabling or limiting NTLM and WDigest Authentication.
  - Implement Credential Guard for Windows 10 and Server 2016 (refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
  - Minimize the AD attack surface to reduce malicious ticket-granting activity. Malicious activity such as “Kerberoasting” takes advantage of Kerberos’ TGS and can be used to obtain hashed credentials that threat actors attempt to crack.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA and FBI recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA and FBI recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see table 1).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA and FBI recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

REFERENCES

[1] MITRE ATT&CK Version 12: Software – Ngrok