Incident Report: CISA Iranian APT

Summary:

This report details an incident involving an Iranian Advanced Persistent Threat (APT) group that exploited the Log4Shell vulnerability to gain initial access to a target network. The attackers deployed XMRig cryptocurrency mining software on compromised systems and used various tactics, techniques, and procedures (TTPs) to maintain persistence, escalate privileges, and move laterally within the network.

Attack Details:

The Iranian APT group gained initial access to the target network by exploiting the Log4Shell vulnerability (CVE-2021-44228) in a VMware Horizon server. The attackers used an LDAP server (51.89.181.64) to exploit the vulnerability and execute arbitrary code on the compromised server.

After establishing a foothold, the attackers executed a PowerShell command on the compromised server to add an exclusion rule to Windows Defender, allowing the entire C:\ drive. The command also executed a Base64-encoded payload to download and execute the next stage of the attack.

The attackers then downloaded a malicious PowerShell script named "mde.ps1" from the IP address 182.54.217.2. This script served as a downloader and was used to retrieve a ZIP file named "file.zip" from the same IP address. The ZIP file contained four malicious components: WinRing0x64.sys (an XMRig Miner driver), wuacltservice.exe (the XMRig Miner itself), RuntimeBroker.exe (an associated trojan), and config.json (the XMRig Miner configuration file).

To maintain persistence, the attackers created a scheduled task named "RuntimeBrokerService.exe," which executed the malicious RuntimeBroker.exe daily as the SYSTEM user. RuntimeBroker.exe was capable of creating local user accounts, checking for internet connectivity by pinging 8.8.8.8, and communicating with the command-and-control (C2) server.

The attackers used the built-in Windows account "DefaultAccount" to move laterally to a VMware VDI-KMS host. From there, they downloaded additional tools, including PsExec, Mimikatz, and Ngrok, from a server associated with the IP address 144.76.136.153.

Using Mimikatz, the attackers created a rogue domain administrator account, which they used to move laterally to multiple hosts on the network via RDP. They manually disabled Windows Defender on several compromised hosts and implanted Ngrok executables and configuration files to facilitate further access.

The attackers moved laterally to the domain controller using RDP and executed PowerShell commands to perform remote system discovery, obtaining a list of all machines attached to the domain. They also changed the password for the local administrator account on several hosts.

In an attempt to gather credentials, the attackers tried to dump the LSASS process using the Windows Task Manager. However, this attempt was stopped by additional antivirus software installed on the compromised systems.

The attackers used Ngrok to proxy RDP connections, allowing them to access the compromised network using generated subdomains at .ngrok.io, ngrok..tunnel[.]com, or korgn.*.lennut[.]com.