مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Outlaw Linux Malware Threat

Tracking #:432317061

Date:11-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that the 'OUTLAW' malware, a persistent yet unsophisticated Linux-based threat, uses SSH brute-force attacks to infiltrate systems, establish control, and deploy cryptocurrency mining operations.

TECHNICAL DETAILS:

Outlaw is a persistent Linux malware that has been active for several years. It employs simple yet effective techniques such as SSH brute-forcing, SSH key manipulation, and cron-based persistence to maintain a long-lasting botnet. Despite its lack of sophistication, Outlaw achieves widespread impact by leveraging commodity tooling and worm-like propagation.

Technical Details

Initial Infection & Deployment

The attack starts when tddwrt7s.sh downloads the dota3.tar.gz package from a C2 server. The extracted initall.sh script executes, initiating the infection chain.

Gaining Control & Persistence

The malware ensures dominance by killing competing brute-forcers and miners. It then deploys:

- Modified XMRIG for crypto mining (connecting to a mining pool).
- STEALTH SHELLBOT for remote control via IRC C2.
- BLITZ to perform SSH brute force attacks.

Propagation & Expansion

The brute-force module retrieves target lists from an SSH C2 server and attempts SSH brute-force attacks on new machines. Successfully compromised systems are infected, repeating the cycle. This automated infection loop allows OUTLAW to remain active and profitable with minimal effort from attackers.

Execution Chain Analysis

Outlaw effectively covers a wide range of tactics and techniques in the MITRE ATT&CK framework.

- **Initial Access**: SSH brute-forcing using the blitz component.
- **Execution**: The tddwrt7s.sh script downloads and executes the initial payload.
- **Persistence**:
  - Cron-based persistence via init scripts.
  - SSH key manipulation by injecting attacker-controlled SSH public keys.
  - STEALTH SHELLBOT for remote control via IRC C2.
- **Defense Evasion**:
  - Killing competing brute-forcers and miners.
  - Obfuscation of scripts using variable-based string concatenation.
- **Credential Access**: SSH brute-forcing to gain access to new systems.
- **Discovery**: Gathering system information to optimize mining performance.
- **Resource Hijacking**: Crypto mining using modified XMRig.
- **Command and Control**: IRC C2 communication via STEALTH SHELLBOT.

Key Components

- **tddwrt7s.sh**: Initial dropper script.
- **dota3.tar.gz**: Archive containing the malware components.
- **initall.sh**: Main initialization script.
- **blitz**: SSH brute-forcing tool.
- **XMRig**: Modified cryptocurrency miner.

- **STEALTH SHELLBOT**: IRC-based backdoor for remote control.

Indicators of Compromise:
Attached File

RECOMMENDATIONS:

1. **Strengthen SSH Security**:
   - Enforce strong password policies.
   - Disable SSH access for accounts with default credentials.
   - Implement multi-factor authentication.
   - Monitor SSH logs for suspicious activity.
2. **Regularly Update and Patch Systems**:
   - Keep all systems and software up to date with the latest security patches.
   - Use a centralized patch management system to ensure timely updates.
3. **Implement Network Segmentation**:
   - Divide the network into isolated segments to limit the spread of malware.
   - Implement strict access control policies between network segments.
4. **Monitor System Processes**:
   - Monitor for unusual processes, especially those related to crypto mining (XMRig) or IRC communication.
   - Use endpoint detection and response (EDR) solutions to detect and block malicious processes.
5. **Inspect Cron Jobs**:
   - Regularly review cron jobs for suspicious or unauthorized entries.
   - Use a configuration management tool to manage and monitor cron jobs.
6. **Network Monitoring and Intrusion Detection**:
   - Implement network-based intrusion detection systems (IDS) to detect brute-force attacks and other suspicious network activity.
   - Monitor network traffic for communication with known malicious IPs and domains.
7. **User Awareness Training**:
   - Educate users about the risks of weak passwords and the importance of security best practices.
   - Conduct regular phishing simulations to test and improve user awareness.
8. **Backup and Recovery**:
   - Implement a robust backup and recovery plan to ensure business continuity in the event of a successful attack.
   - Regularly test backup and recovery procedures.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.elastic.co/security-labs/outlaw-linux-malware