مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

WolfsBane and FireWood - New Linux Threats

Tracking #:432316555

Date:25-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed ESET researchers have identified new Linux malware, WolfsBane and FireWood, attributed to the Gelsemium advanced persistent threat (APT) group.

TECHNICAL DETAILS:

ESET researchers have identified new Linux malware, WolfsBane and FireWood, attributed to the Gelsemium advanced persistent threat (APT) group. WolfsBane is the Linux counterpart to the Windows-based Gelsevirine, while FireWood is linked to Project Wood. These backdoors are used for cyberespionage, targeting sensitive data and maintaining persistent access on compromised systems. The shift towards Linux malware is driven by enhanced security measures on Windows platforms, prompting threat actors to exploit vulnerabilities in Linux-based internet-facing systems. Gelsemium has previously targeted entities in Eastern Asia and the Middle East.

Key Insights from the Analysis:

1. **WolfsBane Backdoor**:
   - **Linux Version of Gelsevirine**: WolfsBane is closely associated with **Gelsevirine**, a Windows backdoor used by Gelsemium. ESET's analysis reveals several shared features, such as custom libraries for network communication, a similar command execution mechanism, and analogous configuration structures. WolfsBane is attributed to Gelsemium with high confidence, based on the consistent patterns and technical similarities with previously known Gelsemium malware.
   - **Persistence and Stealth**: The backdoor is part of a loading chain with a dropper, launcher, and backdoor, designed to maintain persistent access and execute commands covertly.
   - **Technical Details**: WolfsBane's dropper uses a modified open-source userland rootkit for hiding its activities in the user space of the operating system. This stealth technique is similar to Gelsemine, the dropper used in the Gelsevirine backdoor.
2. **FireWood Backdoor**:
   - **Connection to Project Wood**: FireWood shows strong similarities to **Project Wood**, a backdoor also used by Gelsemium in a previous operation (TooHash). The connection includes matching naming conventions, file extensions, encryption algorithms (TEA), and command-and-control (C&C) communication patterns.
   - **Caution in Attribution**: While FireWood exhibits clear connections to Project Wood, the evidence linking it directly to other Gelsemium tools is weaker. As a result, ESET attributes FireWood to Gelsemium with **low confidence**, acknowledging the possibility that it might be a tool used by multiple China-aligned APT groups.
3. **Additional Tools**:
   - ESET found several additional tools, such as web shells, that allow remote access to compromised servers. These tools are generally based on publicly available code and help maintain control over infected systems.
4. **Trend Towards Linux Malware**:
   - **Shift from Windows**: The discovery of these Linux-based tools reflects a growing trend among APT groups to target Linux systems, likely due to enhanced security measures in Windows environments (e.g., endpoint detection and response tools, disabled VBA macros).
   - **Targeting Internet-Facing Systems**: Many of these Linux systems are vulnerable

internet-facing servers, which are attractive targets for espionage operations.

Indicators of Compromise:
Attached File

RECOMMENDATIONS:

1. **Review and Patch Vulnerabilities**:
   - Ensure that all Linux systems, especially internet-facing servers, are up-to-date with the latest security patches. APT groups often exploit known vulnerabilities to gain access.
2. **Monitor for Indicators of Compromise (IoCs)**:
   - Track **WolfsBane** and **FireWood**-specific IoCs, including domains like **dsdsei[.]com** and file extensions like **.k2** and **.v2**.
3. **Enhance Logging and Monitoring:**
   - Implement centralized logging and monitoring to detect suspicious activities such as unusual network connections or command execution from external sources.
4. **Strengthen Endpoint Detection**:
   - Deploy advanced Endpoint Detection and Response (EDR) solutions across both Windows and Linux systems to improve the visibility of malicious activity and reduce the time to **Security Awareness Training**:
   - Conduct regular security training for employees, focusing on recognizing phishing attempts, malicious attachments, and other social engineering tactics commonly used by APT groups to gain initial access.
5. **Backup and Recovery**:
   - Ensure that all critical data is backed up regularly and securely. Test recovery procedures to minimize downtime in case of a successful attack

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.welivesecurity.com/en/eset-research/unveiling-wolfsbane-gelsemiums-linux-counterpart-to-gelsevirine/#Technical%20analysis