AL2025_15 Auto-Color Linux Backdoor Targets North American Governments and Universities (27th February 2025)

Description

A newly discovered Linux backdoor named Auto-Color has been identified in cyberattacks targeting government institutions and universities in North America and Asia. The malware, first observed between November and December 2024, is highly evasive and designed for long-term persistence. Researchers at Palo Alto Networks Unit 42 identified Auto-Color as a sophisticated threat capable of maintaining unauthorized access and evading detection through stealthy persistence mechanisms and encryption techniques.

Auto-Color shares some similarities with the Symbiote Linux malware family, previously documented by BlackBerry in 2022. However, researchers have confirmed that it is a distinct strain, featuring unique persistence mechanisms and stealth capabilities.

Attack Details

While the initial infection vector remains unknown, the malware executes using files disguised under common names such as "door," "egg," and "log." If it gains root privileges, it deploys a malicious library implant (libcext.so.2), masquerading as a legitimate library (libcext.so.0), and modifies system files to ensure persistent execution. Auto-Color modifies the '/etc/ld.preload' file to execute before legitimate system libraries, establishing remote access to a command-and-control (C2) server that allows attackers to issue commands stealthily. The malware encrypts communications with a custom algorithm and dynamically changes encryption keys to avoid detection. It also functions as a rootkit by hooking libc functions to intercept system calls, modifying files like '/proc/net/tcp' to conceal its presence. Furthermore, Auto-Color includes a kill switch that erases infection traces, hindering forensic analysis. Once connected to the C2 server, attackers can open a reverse shell for full remote access, execute arbitrary commands, modify or create files to expand the infection, act as a proxy to forward traffic, and dynamically adjust its configuration.

Indicators of Compromise (IoCs)

There are several indicators of compromise, including:

File Paths:

- /var/log/cross/auto-color
- /etc/ld.preload modifications referencing libcext.so.2

Network Indicators:

- Anomalous connections in /proc/net/tcp
- Encrypted traffic patterns indicating dynamic encryption key changes

Suspicious File Names:

- Executables disguised as “door,” “egg,” or “log”

Remediation

To defend against Auto-Color and similar threats, security teams should implement the following measures:

1. **Monitor for Persistence Mechanisms:**
    a. Regularly check for unauthorized modifications to **/etc/ld.preload**.
    b. Ensure all shared libraries, particularly **libcext.so**, are verified as legitimate.
2. **Network Traffic Analysis:**
    a. Inspect **/proc/net/tcp** for anomalies or hidden C2 communications.
    b. Use behavioral-based threat detection tools to identify encrypted traffic linked to malware activity.
3. **System Hardening:**
    a. Enforce the principle of least privilege to limit root access.
    b. Apply security updates and patches to prevent exploitation of system vulnerabilities.
4. **Incident Response and Forensic Analysis:**
    a. Monitor system logs for unusual process executions.
    b. Investigate unauthorized file modifications and sudden traffic spikes.
    c. Conduct regular audits to detect and remove unauthorized software.
5. **Threat Intelligence Utilization:**
    a. Cross-reference logs with the provided IoCs.
    b. Stay updated with security advisories and emerging threat reports.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Mandvi. (2025, February 25). New Auto-Color malware targets Linux devices to gain full remote access. Retrieved from Cyber Security News. https://cyberpress.org/new-auto-color-malware-targets-linux-devices/
- Toulas, B. (2025, February 25). New Auto-Color Linux backdoor targets North American govts, universities. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/new-auto-color-linux-backdoor-targets-north-american-govts-universities/