مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Linux Malware Campaign Targeting Docker, Apache Hadoop, Redis, and Confluence

Tracking #:432315690
Date:12-03-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a New Linux Malware Campaign Targets misconfigured web-facing servers running Apache Hadoop YARN, Docker, Confluence and Redis instances.

TECHNICAL DETAILS:

The "Spinning YARN" campaign targets misconfigured servers running web-facing services like Apache Hadoop YARN, Docker, Confluence, and Redis. Attackers leverage unique Golang binaries to automate the discovery and infection of hosts by exploiting common misconfigurations and n-day vulnerabilities. Once initial access is achieved, the malware delivers a cryptocurrency miner, spawns a reverse shell, and enables persistent access to compromised hosts.

The shell script payloads delivered in the campaign resembles previously linked to cloud attacks by TeamTNT, WatchDog, and the Kiss a Dog campaign.

Targeted Services:

- Apache Hadoop YARN
- Docker
- Confluence
- Redis

Attack Techniques:

- **Exploit of Unpatched Vulnerabilities:** The attackers exploit unpatched vulnerabilities, including CVE-2022-26134 in Confluence, to gain remote code execution (RCE) on targeted systems.
- **Custom Golang Payloads:** The campaign utilizes unique Golang binaries designed to automate the discovery and compromise of vulnerable hosts.
- **Delivery of Cryptocurrency Miner:** After gaining access, the attackers deploy a cryptocurrency miner to steal computational resources for mining cryptocurrency.
- **Reverse Shell and Persistence:** A reverse shell is established for remote access, and user-mode rootkits are used to maintain persistence and hide malicious processes.

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Regularly update all software, including operating systems and applications, to patch vulnerabilities.
- Patch systems promptly, especially for known vulnerabilities like CVE-2022-26134.
- Ensure the Docker Engine API is properly secured by deploying firewalls or using a secure cloud service provider with suitable security configurations.
- Implement strong authentication methods, such as multi-factor authentication (MFA), for all

critical systems and applications.

- Monitor network traffic for unusual or suspicious activities using intrusion detection systems (IDS) and intrusion prevention systems (IPS).
- Regularly back up the data and store it in a secure location.
- **User Awareness Training:** Educate employees on phishing, social engineering, and secure password practices.

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.cadosecurity.com/spinning-yarn-a-new-linux-malware-campaign-targets-docker-apache-hadoop-redis-and-confluence/