AL2024_05 AcidPour: A New Variant of Data Wiping Malware Targeting Linux x86 Devices (26th March 2024)

Description

A new variant of data wiping malware, named AcidPour, has emerged in the cyber threat landscape, specifically designed to target Linux x86 devices. AcidPour is an ELF binary compiled for x86 architectures, distinct from its predecessor AcidRain, which targeted Linux devices running on MIPS architectures. This malicious software can erase content from RAID arrays and Unsorted Block Image (UBI) file systems, posing a significant threat to the integrity and security of affected systems.

Details

AcidPour exhibits significant differences from its predecessor AcidRain. While AcidRain primarily targeted KA-SAT modems from U.S. satellite company Viasat, AcidPour extends its reach by targeting Linux x86 devices. It employs a distinct codebase and utilizes file paths such as "/dev/dm-XX" and "/dev/ubiXX" to erase content from RAID arrays and UBI file systems, respectively. The exact scale of the attacks and the identity of the intended victims remain unclear, although Ukrainian agencies have been notified of the threat.

Remediation

To mitigate the risk posed by AcidPour and similar data wiping malware, organizations and individuals are advised to implement robust cybersecurity measures. This includes keeping systems and software up to date with the latest security patches, implementing strong access controls, and regularly backing up critical data to secure, offsite locations. Additionally, organizations should enhance network monitoring capabilities to detect and respond to suspicious activity promptly. Collaboration with cybersecurity experts and information sharing within the industry can also aid in threat intelligence gathering and mitigation efforts.

Indicators of Compromise (IOCs):

- File Paths:
  - /dev/dm-XX
  - /dev/ubiXX
- ELF Binary: compiled for x86 architectures
- Filesystem wiping activity targeting RAID arrays and UBI file systems

References:

- The Hacker News. (2024, March 19). Suspected Russian Data-Wiping “AcidPour” Malware Targeting Linux x86 Devices. Retrieved from https://thehackernews.com/2024/03/suspected-russian-data-wiping-acidpour.html
- Toulas, B. (2024, March 19). New AcidPour data wiper targets Linux x86 network devices. BleepingComputer. https://www.bleepingcomputer.com/news/security/new-acidpour-data-wiper-targets-linux-x86-network-devices/