BLACKSWAN CYBERSECURITY

THREAT ANALYSIS

Mar 14, 2023

IceFire Ransomware Now Encrypts Both Linux and Windows Systems

SUMMARY

SentinelOne's SentinelLabs recently reported that the IceFire ransomware campaign has expanded and now has a dedicated Linux systems encryptor. IceFire Ransomware, first discovered in 2021, is known for its advanced encryption techniques that are difficult to decrypt files without paying the ransom.

TECHNICAL DETAILS

According to SentinelOne, this malware strain has mostly been deployed in Iran, Pakistan, Turkey, and the UAE. Attackers capitalized on the patched deserialization vulnerability (CVE-2022-47986) in IBM Aspera Faspex to deploy the malware. IceFire malware is currently a 2.18 MB, 64-bit ELF binary that was built with GCC for AMD64 architecture. Many legitimate OpenSSL routines that are statically linked into the malicious program's binary are also hardcoded, along with the RSA public key. A vulnerable version of Aspera Faspex is running on CentOS machines under IceFire. Two payloads are downloaded by the system and saved to an Aspera subdirectory using wget. A DigitalOcean droplet is used to host the payloads.

Upon execution, IceFire encrypts files and adds the ".ifire" extension to the filename. The attackers' Tor-based ransom payment portal is used in conjunction with the unique hardcoded username and password that are immediately dropped in the victim's ransom letter. IceFire does not encrypt every file under Windows or Linux and stays away from certain paths, preserving the functionality of critical parts of the system. The malware eventually deletes itself to hide its tracks by deleting the binary.

INDICATORS OF COMPROMISE (IOCs)

SHA-1:

- b676c38d5c309b64ab98c2cd82044891134a9973

Payload URLs:

- hxxp[://]159.65.217.216:8080/demo

ADDITIONAL COMMENTS

Based on the IceFire discovery in 2021 and other organizations like BlackBasta, Hive, Qilin, and Vice Society, we believe that ransomware attacks on Linux environments will continue grown through 2023.

REFERENCES

- https://www.sentinelone.com/labs/icefire-ransomware-returns-now-targeting-linux-enterprise-networks/
- https://thehackernews.com/2023/03/icefire-linux-ransomware.html
- https://www.bleepingcomputer.com/news/security/icefire-ransomware-now-encrypts-both-linux-and-windows-systems/