مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Volcano Demon: New Ransomware Threat

Tracking #:432316012

Date:03-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed new ransomware threat actor, Volcano Demon, responsible for recent attacks utilizing the LukaLocker encryptor (.nba file extension).

TECHNICAL DETAILS:

Halcyon researchers have identified a new ransomware threat actor, Volcano Demon, responsible for recent attacks utilizing the LukaLocker encryptor (.nba file extension). This group has carried out several successful attacks in the past two weeks, locking both Windows, Linux workstations and servers by exploiting common administrative credentials. Prior to the encryption, the attackers exfiltrated data for potential double extortion. The threat actor features no leak site and instead uses threatening phone calls to leadership and IT executives to demand payment.

- **Ransomware**: LukaLocker (.nba file extension) - Windows and Linux variants identified.
- **Attack Vector**: Common administrative credentials harvested from the network.
- **Data Exfiltration**: Exfiltrates data to C2 servers before encryption for double extortion.
- **Impact**: Locks critical systems and data, disrupts operations.
- **Extortion Methods**: Uses phone calls to pressure victims into payment, with aggressive tactics.

Indicators of Compromise:

Name	Description	SHA256 Hash
Protector.exe	Trojan	f83abe3d9717238755f1276c87b3b320d8c30421984a897099ce3741d9143906
Locker.exe	Encryptor	4e58629158a6c46ad420f729330030f5e0b0ef374e9bb24cd203c89ec3262669
Linux locker.bin	Linux Encryptor	ac08ab5bfc5f2cfa0703115a0e2b61decc5158ec0d8a99ebc0824da2b4c3d25
Reboot.bat	Command line scripts as precursors to encryption event	ed32ebb15d4abe262a34e54408ebb0680b62dc975bf6c02652d28006f45fca14

RECOMMENDATIONS:

- Block the IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Patch Systems: Ensure all systems are up-to-date with the latest security patches from operating system and software vendors.
- Enforce Strong Passwords: Implement strong and unique passwords for all administrative accounts and enforce multi-factor authentication (MFA) wherever possible.
- Segment Networks: Segment network to limit the lateral movement of attackers in case of a breach.
- Monitor User Activity: Implement security solutions that monitor user activity for

anomalous behaviors.

- Endpoint Detection and Response (EDR): Deploy EDR solutions to detect and respond to malicious activity on endpoints.
- Regular Backups: Maintain regular backups of critical data with offline storage isolated from the production network.
- Incident Response Plan: Develop and test an incident response plan to effectively respond to a ransomware attack.
- Employee Training: Train employees on cybersecurity best practices, including phishing awareness and social engineering techniques

REFERENCES:

- https://www.halcyon.ai/blog/halcyon-identifies-new-ransomware-operator-volcano-demon-serving-up-lukalocker