مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Akira Ransomware Threat

Tracking #:432315778

Date:22-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed the Akira ransomware, a sophisticated threat impacting organizations globally.

TECHNICAL DETAILS:

The Akira ransomware, a sophisticated threat impacting organizations globally, has been identified as a significant cyber threat. This ransomware variant has targeted a wide range of businesses and critical infrastructure entities in worldwide causing substantial financial losses and data breaches. Akira ransomware has evolved from targeting Windows systems to deploying a Linux variant, impacting over 250 organizations and claiming approximately $42 million USD in ransom proceeds.

Details:

Initial Access: Akira threat actors exploit vulnerabilities in VPN services, known Cisco vulnerabilities(CVE-2020-3259 and CVE-2023-20269), and external-facing services like RDP and spear phishing to gain initial access to organizations.

Persistence and Discovery: After gaining access, threat actors establish persistence by creating new domain accounts, leveraging post-exploitation techniques like Kerberoasting, and using credential scraping tools for privilege escalation.

Defense Evasion: Akira threat actors deploy multiple ransomware variants “Megazord” ransomware & Akira_v2 against different system architectures, disable security software, and exploit vulnerabilities to avoid detection.

Exfiltration and Impact: Threat actors exfiltrate data using tools like FileZilla and WinSCP, establish command and control channels through various protocols, and employ a double-extortion model to encrypt systems and demand ransom payments in Bitcoin.

Encryption: Akira ransomware utilizes a sophisticated encryption scheme combining ChaCha20 and RSA public-key cryptosystem, encrypting files with .akira or .powerranges extensions, and deleting volume shadow copies to hinder recovery.

Indicators of Compromise:

Attached 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
- Patch Vulnerabilities: Prioritize remediating known vulnerabilities, especially those exploited by Akira threat actors, to prevent initial access.
- Implement Multifactor Authentication: Enable multifactor authentication (MFA) for all services, particularly for critical systems and webmail, to enhance security.
- Regularly Update Software: Keep all software and applications up-to-date with the latest patches and conduct vulnerability assessments regularly.
- Network Segmentation: Segment networks to prevent the spread of ransomware and control traffic flows between subnetworks.
- Enhance Monitoring: Implement network monitoring tools to detect abnormal activities

and potential ransomware traversal.

- Backup Data: Maintain offline backups of data, ensuring they are encrypted, immutable, and cover the entire organization's data infrastructure.

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.cisa.gov/news-events/cybersecurity-advisories/aa24-109a