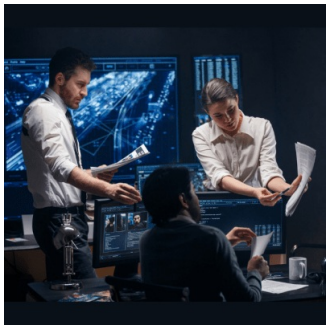
HealthManagement
Promoting Management and Leadership

Building Resilience: Law Enforcement's Advisory Against Akira Ransomware



The United States' Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber Security Centre (NCSC-NL) have collaborated to release a joint Cybersecurity Advisory (CSA) detailing the known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with the Akira ransomware. This ransomware has affected numerous businesses and critical infrastructure entities across North America, Europe, and Australia since March 2023. Initially targeting Windows systems, the threat actors behind Akira later developed a Linux variant aimed at VMware ESXi virtual machines in April 2023. As of January 1, 2024, over 250 organisations have been impacted, resulting in approximately $42 million USD in ransom payments. While early versions of Akira were coded in C++ and encrypted files with a .akira extension, later attacks since August 2023 have utilised Megazord, written in Rust and encrypting files with a .powerranges extension. The threat actors have been observed using both Akira and Megazord interchangeably, including a variant known as Akira_v2 as identified by third-party investigations.

Understanding the Akira Ransomware Actors' Tactics

The FBI and cybersecurity experts have observed the Akira ransomware group utilising various methods to gain initial access to organisations, including exploiting vulnerabilities in VPN services lacking multifactor authentication and known Cisco vulnerabilities. They also use external-facing services like RDP, spear phishing, and credential abuse. Once inside, they manipulate domain controllers and use post-exploitation techniques like Kerberoasting and credential scraping to escalate privileges. Akira actors disable security software and leverage tools like PowerTool to exploit antivirus drivers. They exfiltrate data using tools like FileZilla and establish command and control channels via AnyDesk and other tools. They employ a double-extortion model and use a sophisticated encryption scheme combining ChaCha20 and RSA. Encrypted files are given extensions like .akira or .powerranges, and the ransom note is provided through a .onion URL. The newer variant, Akira_v2, enhances encryption speed and efficiency, adds protection layers, and includes functionalities specific to virtual machines. After encryption, the Linux ESXi variant may add "akiranew" extensions to encrypted files or include "akiranew.txt" ransom notes.

Cybersecurity Performance Goals: Recommendations for Resilience

NIST recommends that all organisations implement cybersecurity performance goals (CPGs) developed in collaboration with CISA. These goals are based on existing cybersecurity frameworks and guidance to mitigate common threats and tactics. Key recommendations include implementing a recovery plan for data, enforcing strong password standards, employing multifactor authentication, keeping software updated, segmenting networks, monitoring for abnormal activity, filtering network traffic, using antivirus software, auditing accounts, disabling unused ports, adding email banners, implementing time-based access controls, disabling command-line activities, and maintaining offline backups of encrypted and immutable data covering the entire organization's infrastructure. These measures collectively enhance cybersecurity resilience and minimise the impact of potential threats like ransomware.

Testing and Validating Security Programmes Against MITRE ATT&CK Framework

The FBI, CISA, EC3, and NCSC-NL recommend organisations not only apply mitigations but also exercise, test, and validate their security programmes against threat behaviours outlined in the MITRE ATT&CK for Enterprise framework. They suggest testing existing security controls against specific techniques described in the advisory, analysing their performance, and tuning the security programme based on the results. This process should be repeated for all security technologies to gather comprehensive performance data. Continual testing at scale in a production environment is advised to ensure optimal performance against identified MITRE ATT&CK techniques.

The FBI is interested in various information, including boundary logs, ransom notes, communications with threat actors, Bitcoin wallet details, decryptor files, and samples of encrypted files. Additional details, such as contact information, infection status, loss estimates, and attack vectors, are also valuable. The FBI, CISA, EC3, and NCSC-NL advise against paying ransom as it does not guarantee file recovery and can encourage further attacks. Regardless of ransom payment decisions, prompt reporting of ransomware incidents to the FBI is strongly encouraged.

Source: FBI

Image Source: iStock

Published on : Thu, 25 Apr 2024