Anti-Ransomware AIX

DATASHEET (iSecurity Suite Cyber Protection)

Is AIX affected by Ransomware?

IBM AIX is not immune to ransomware and cyber threats, though it is less frequently targeted for mass-market ransomware than Windows or Linux.

Mission-Critical Targets: AIX systems often run core financial, healthcare, and industrial infrastructure, making them high-value targets for attackers seeking maximum disruption or extortion.

Vulnerabilities: Critical remote code execution flaws—such as the Network Installation Management (NIM) vulnerabilities tracked under IBM Security Guidance—have demonstrated that UNIX-based master services can be leveraged for unauthorized access or payload deployment.

Indirect and Shared Risks: Ransomware or malware can also impact AIX environments via connected network storage protocols (like NFS) where compromised external clients propagate file corruption across shared directories

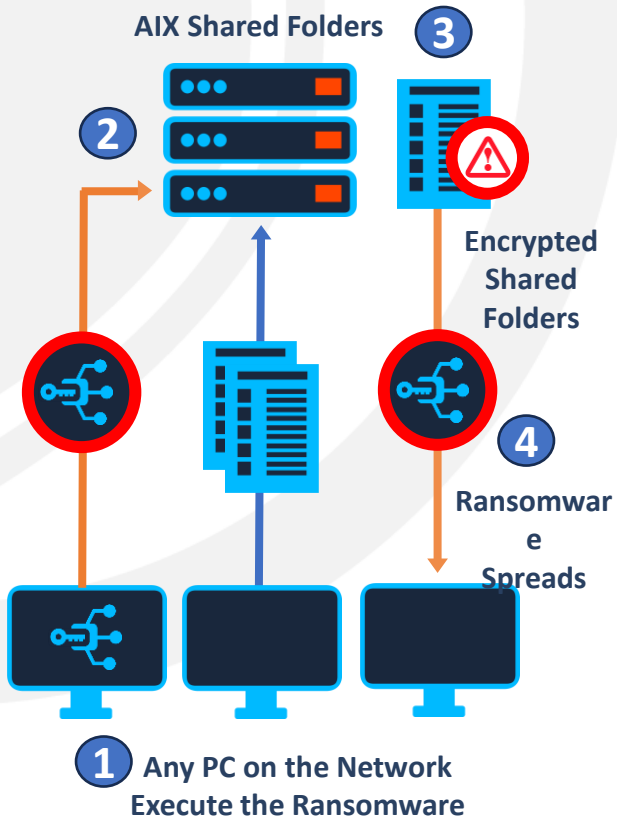
iSecurity Anti-Ransomware AIX will STOP Ransomware attacks immediately as they starts.

Even if it is a Zero-Day Attack.

Because traditional Endpoint Detection and Response (EDR) agents designed for Windows or Linux cannot run natively on AIX, Raz-Lee's native solution closes that security gap through several key mechanisms

How Anti-Ransomware AIX helps:

If it detects high-volume, suspicious file activity (such as a mass encryption process characteristic of a ransomware payload), it can automatically isolate the offending threat to limit data damage across your partitions.



Key Features

- Automatic, regularly updated database
- Command-line scanner
- Database updater with support for digital signatures
- Can not be disabled by viruses
- Built-in support for zip, gzip, jar, and tar files
- Stops the attack as it starts
- Live tested with Ryuk ransomware attack
- Heuristic engine for zero-day threats
- Automatic disconnection of the attacking source
- Tamper protection prevents disabling malware
- Protection continues without internet connectivity
- Full history log of all detections

Blocking Lateral Contamination via Network Shares

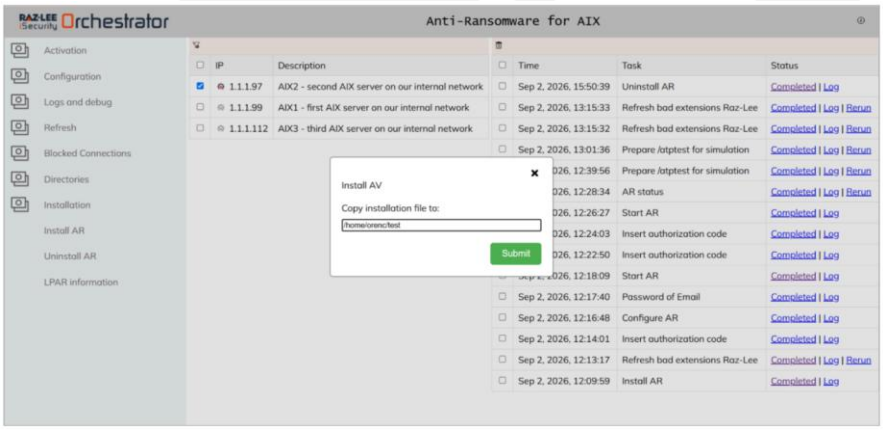
As mentioned previously, one of the biggest risks to AIX is when an infected Windows client encrypts AIX directories mounted via network shares (like NFS or Samba).

Anti-Ransomware AIX uses real-time, On-Access scanning to monitor files as they are being modified or transferred. If a compromised Windows machine attempts to write or encrypt files on the AIX server, Raz-Lee catches the activity at the server level, preventing AIX from acting as a blind host or spreading malware

Managing Scale with Orchestrator

For enterprise environments deploying dozens or hundreds of AIX LPARs (logical partitions), managing individual security policies is unfeasible.

Raz-Lee includes an **Orchestrator for AIX**, which automates definition distribution, centralizes history logs, and coordinates scanning across thousands of AIX and Linux partitions from a unified web interface



Let's Get Started

Schedule your Demo and start protecting your Systems with iSecurity Anti-Ransomware AIX.

RAZ-LEE iSecurity