# Anti-Ransomware

## Overview

Anti-Ransomware is a solution that protects against a ransomware attack and other kinds of malware that may change and/or access IBM i data on the IFS.

Ransomware blocks access to data files on a computer system until a sum of money is paid. It encrypts not only the files on the infected device, but also the contents of connected devices, mapped network drivers, shared local networks, and cloud storage services that are mapped to the infected computer. The IBM i is no longer an isolated system but connected to other databases through networked systems and connectivity. The data stored on the IFS is like any other file the mapped PC has access to.  Ransomware doesn't discriminate. It encrypts every data file that it has access to, including the IFS files, leaving organizations feeling paralyzed, exposed and without many options.

Anti-Ransomware is the first component of Raz-Lee's new iSecurity ATP, a comprehensive advanced threat protection solution for defending IBM i servers IFS files against offensive maneuvers targeted at distressing an organization.

# The Anti-Ransomware Solution

Raz-Lee Security's Anti-Ransomware module quickly detects high volume cyber threats deployed from an external source, isolates the threat, and prevents it from damaging valuable data that is stored on the IBM i while preserving performance. Anti-Ransomware is designed to protect the system quickly and efficiently from known and unknown threats as soon as malicious activity is diagnosed, prior to the demand for a ransom.

The Anti-Ransomware modules included in iSecurity ATP identify ransomware and similar malware activity in real-time and take the necessary measures to stop and report it.

# Key Features

- Identifies, stops, delays, and reports ransomware attack in real-time
- Based on a combination of methods which identify behavioral characteristics such as activity on files, names, extensions, encryption status, and honeypots
- Classifies the dangers and determines the appropriate way to neutralize the problem based on the existing situation and the customer's preferences.
- Suspends the attack and alerts the offending computer in real-time.
- Disconnects the intruder and sends email, messages and Syslog messages to up to 3 SIEMS in CEF/LEEF formats
- Full log. Query generator with PDF, HTML, Zip & email
- Ransomware definitions are updated from the web every two hours