RAZ-LEE

iSecurity

Anti-Ransomware

iSecurity
Anti-Ransomware

Protecting IBM i from the Inside

Advanced threat protection solution for defending IBM i IFS files against ransomware.

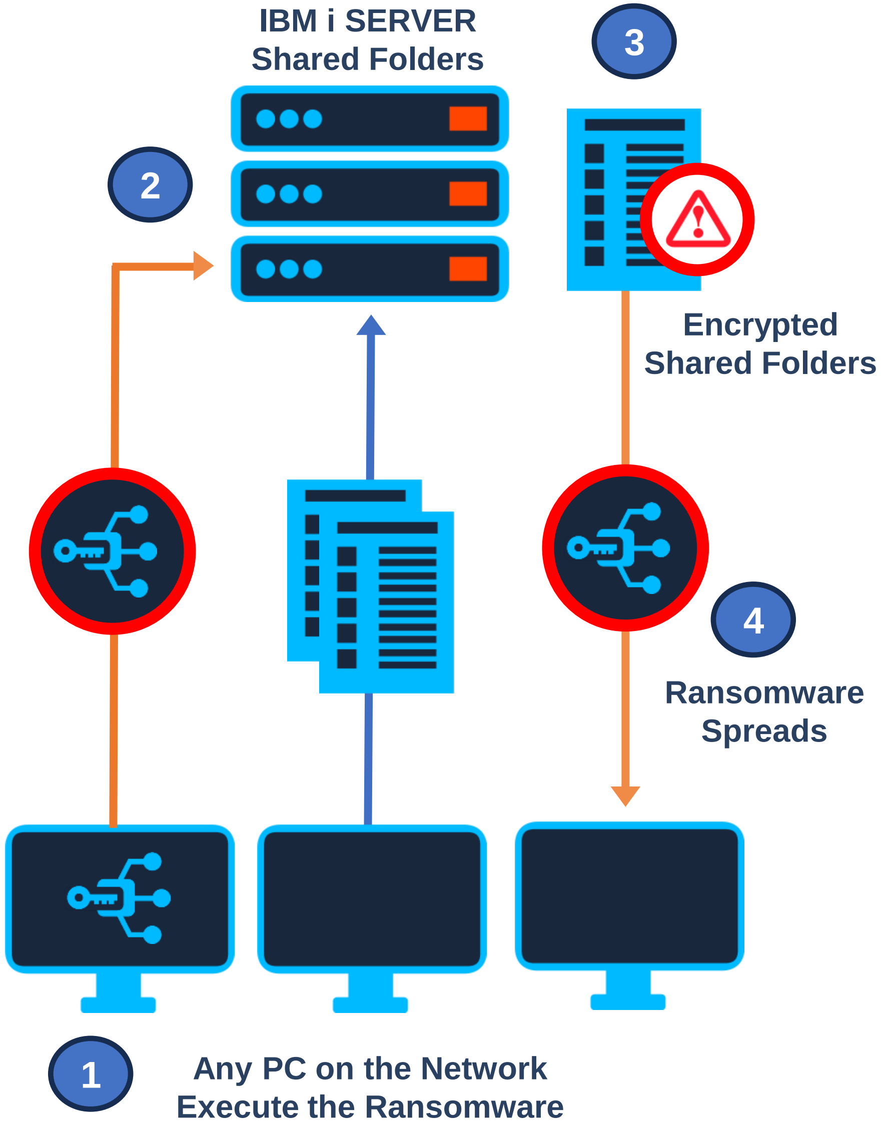
RAZ-LEE

Is IBM i affected by Ransomware?

Since the IBM i is no longer an isolated platform, there is a real risk of malware & ransomware spreading to it and other devices and systems via networked drives and cloud storage services.

IFS directory files can easily become ransomware victims and unintentional ransomware propagators, through infected mapped drives.

Ransomware encrypts every file that it has access to, including IFS files, leaving organizations feeling paralyzed, exposed and without many options.



RAZ-LEE iSecurity

iSecurity Anti-Ransomware Insights

Anti-Ransomware quickly detects high volume cyber threats deployed from an external source, isolates the threat, and prevents it from damaging valuable data.

Our Solution:

- ✓ **iSecurity Anti-Ransomware** STOPS Ransomware attacks immediately as they starts. Even if it is a Zero-Day Attack.
- ✓ A comprehensive advanced threat protection solution for defending IBM i IFS files against ransomware and other kinds of malware.

RAZ-LEE iSecurity

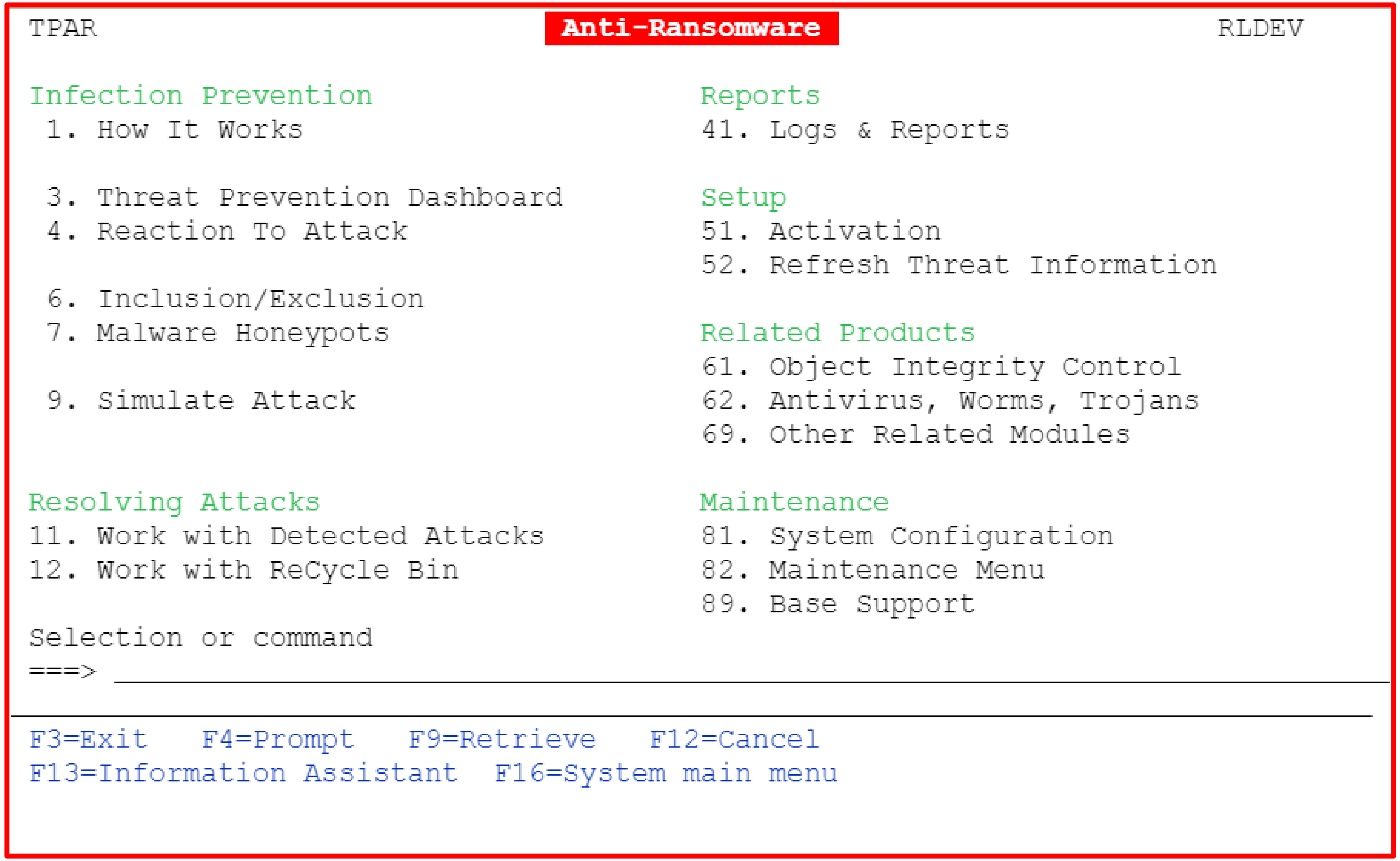
iSecurity
Anti-Ransomware

Let’s see our Product in Action!

The best way to see how it works is a demo with **iSecurity Anti-Ransomware** running on a real environment.

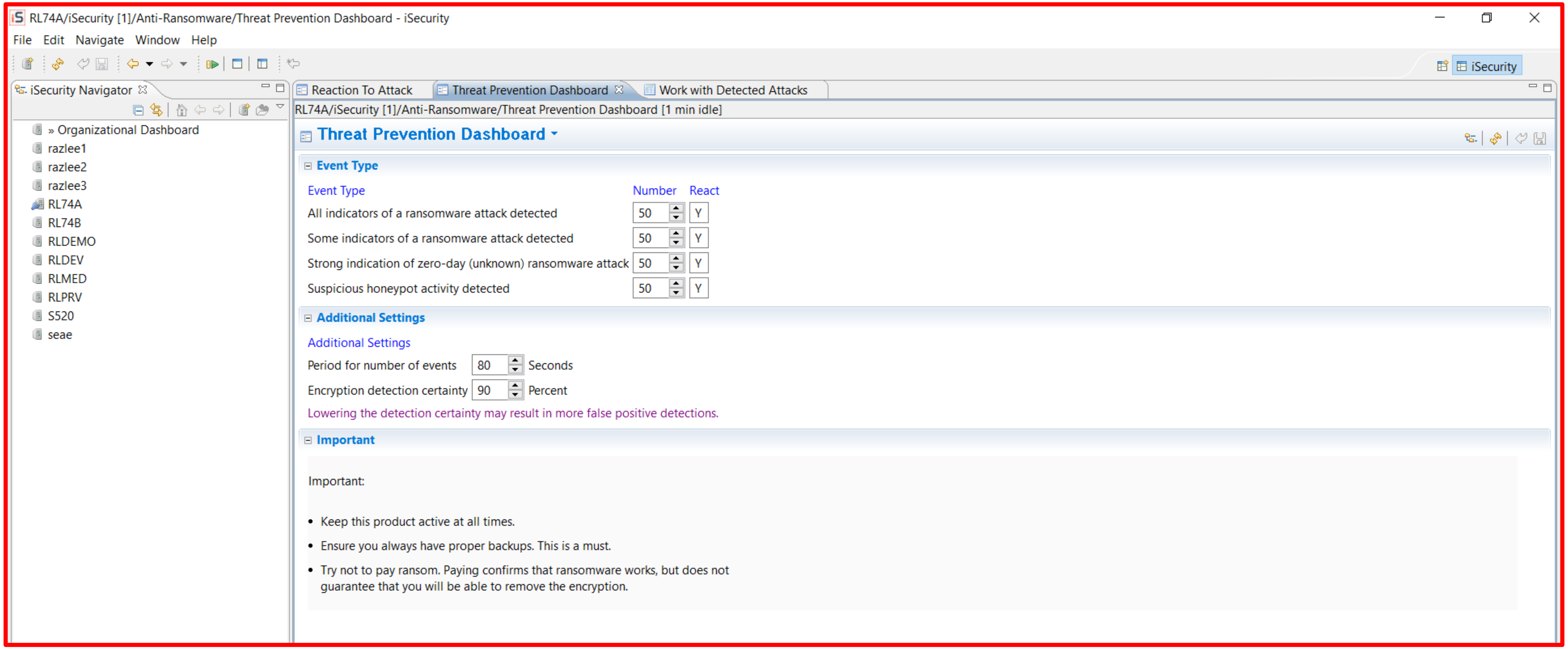
RAZ-LEE

Anti-Ransomware in Action (Native Interface)



```
TPAR                         Anti-Ransomware                                RLDEV

Infection Prevention                     Reports
 1. How It Works                         41. Logs & Reports

 3. Threat Prevention Dashboard          Setup
 4. Reaction To Attack                   51. Activation
                                         52. Refresh Threat Information
 6. Inclusion/Exclusion
 7. Malware Honeypots                    Related Products
                                         61. Object Integrity Control
 9. Simulate Attack                      62. Antivirus, Worms, Trojans
                                         69. Other Related Modules

Resolving Attacks                        Maintenance
11. Work with Detected Attacks           81. System Configuration
12. Work with ReCycle Bin                82. Maintenance Menu
                                         89. Base Support
Selection or command
===> ____________________________________________________________________________

F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel
F13=Information Assistant  F16=System main menu
```

Activation Screen (GUI)



RL74A/iSecurity [1]/Anti-Ransomware/Threat Prevention Dashboard - iSecurity
File Edit Navigate Window Help
iSecurity
iSecurity Navigator
» Organizational Dashboard
razlee1
razlee2
razlee3
RL74A
RL74B
RLDEMO
RLDEV
RLMED
RLPRV
S520
seae
Reaction To Attack
Threat Prevention Dashboard
Work with Detected Attacks
RL74A/iSecurity [1]/Anti-Ransomware/Threat Prevention Dashboard [1 min idle]
Threat Prevention Dashboard

Event Type

Event Type	Number	React
All indicators of a ransomware attack detected	50	Y
Some indicators of a ransomware attack detected	50	Y
Strong indication of zero-day (unknown) ransomware attack	50	Y
Suspicious honeypot activity detected	50	Y

Additional Settings

Additional Settings

Period for number of events 80 Seconds

Encryption detection certainty 90 Percent

Lowering the detection certainty may result in more false positive detections.

Important

Important:

- Keep this product active at all times.
- Ensure you always have proper backups. This is a must.
- Try not to pay ransom. Paying confirms that ransomware works, but does not guarantee that you will be able to remove the encryption.

Results speaks for their own

iSecurity Anti Ransomware was tested in a completely isolated lab.

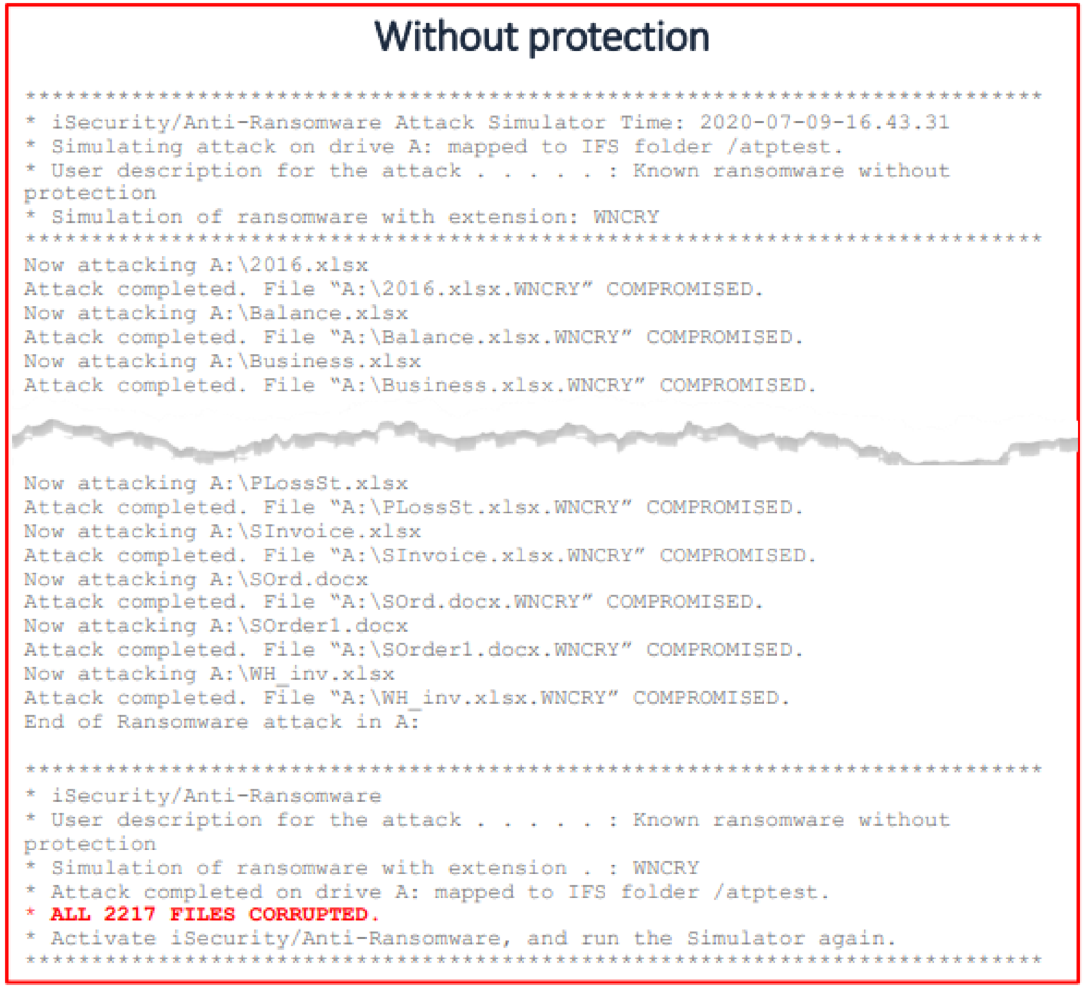
TEST ELEMENTS

- IBM i
- Windows based PC with mapped IBM i folder.
- Set of 10+ real ransomwares (not emulators).

TEST OUTCOME

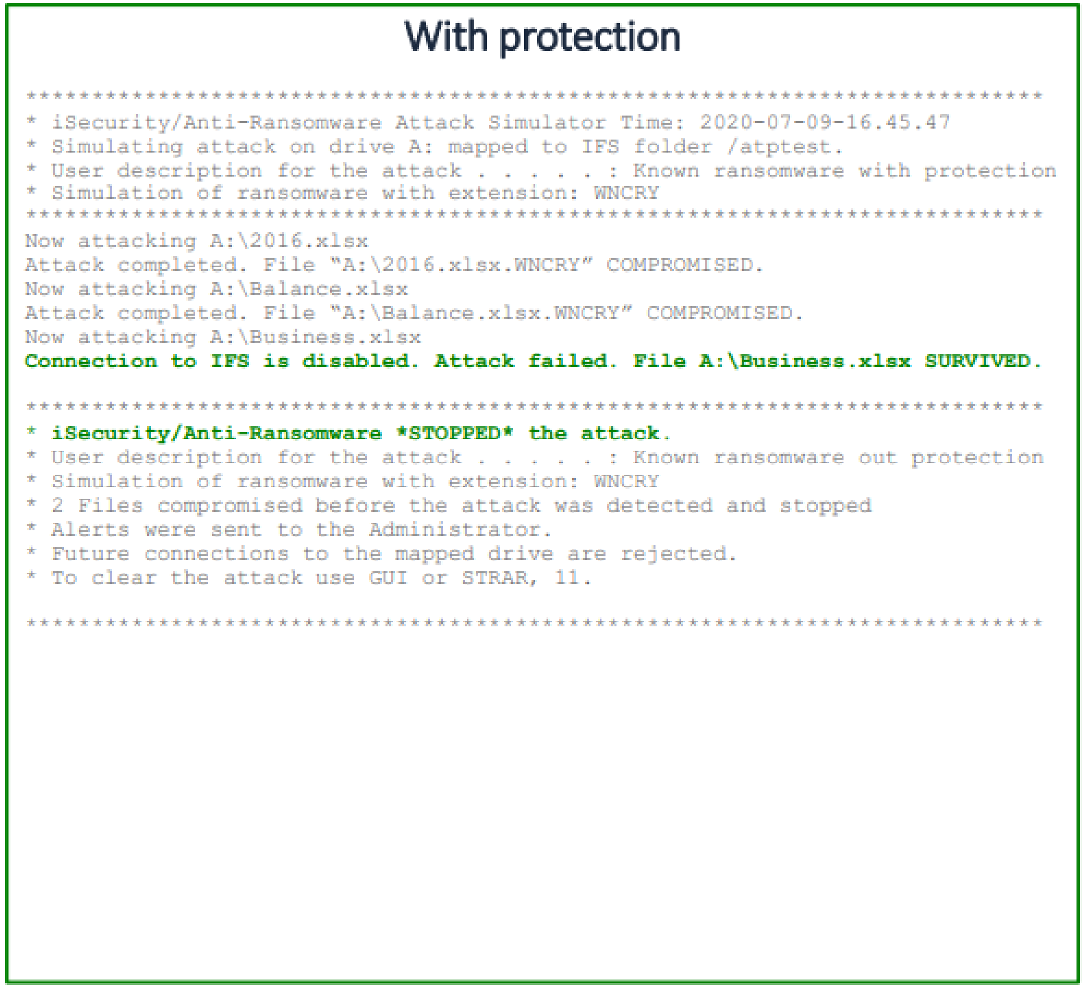
- PC data files are encrypted (as expected).
- When IFS file was attacked, the **Anti-Ransomware** stopped the attack before even the first file was compromised.
- Alert was raised.
- IBM i was disconnected from the attacking PC.
- IBM i survived the attack!

Report after the Attack



Without protection

```
****************************************************************************
* iSecurity/Anti-Ransomware Attack Simulator Time: 2020-07-09-16.43.31
* Simulating attack on drive A: mapped to IFS folder /atptest.
* User description for the attack . . . . . : Known ransomware without
protection
* Simulation of ransomware with extension: WNCRY
****************************************************************************
Now attacking A:\2016.xlsx
Attack completed. File “A:\2016.xlsx.WNCRY” COMPROMISED.
Now attacking A:\Balance.xlsx
Attack completed. File “A:\Balance.xlsx.WNCRY” COMPROMISED.
Now attacking A:\Business.xlsx
Attack completed. File “A:\Business.xlsx.WNCRY” COMPROMISED.

Now attacking A:\PLossSt.xlsx
Attack completed. File “A:\PLossSt.xlsx.WNCRY” COMPROMISED.
Now attacking A:\SInvoice.xlsx
Attack completed. File “A:\SInvoice.xlsx.WNCRY” COMPROMISED.
Now attacking A:\SOrd.docx
Attack completed. File “A:\SOrd.docx.WNCRY” COMPROMISED.
Now attacking A:\SOrder1.docx
Attack completed. File “A:\SOrder1.docx.WNCRY” COMPROMISED.
Now attacking A:\WH_inv.xlsx
Attack completed. File “A:\WH_inv.xlsx.WNCRY” COMPROMISED.
End of Ransomware attack in A:

****************************************************************************
* iSecurity/Anti-Ransomware
* User description for the attack . . . . . : Known ransomware without
protection
* Simulation of ransomware with extension . : WNCRY
* Attack completed on drive A: mapped to IFS folder /atptest.
* ALL 2217 FILES CORRUPTED.
* Activate iSecurity/Anti-Ransomware, and run the Simulator again.
****************************************************************************
```



With protection

```
****************************************************************************
* iSecurity/Anti-Ransomware Attack Simulator Time: 2020-07-09-16.45.47
* Simulating attack on drive A: mapped to IFS folder /atptest.
* User description for the attack . . . . . : Known ransomware with protection
* Simulation of ransomware with extension: WNCRY
****************************************************************************
Now attacking A:\2016.xlsx
Attack completed. File “A:\2016.xlsx.WNCRY” COMPROMISED.
Now attacking A:\Balance.xlsx
Attack completed. File “A:\Balance.xlsx.WNCRY” COMPROMISED.
Now attacking A:\Business.xlsx
Connection to IFS is disabled. Attack failed. File A:\Business.xlsx SURVIVED.

****************************************************************************
* iSecurity/Anti-Ransomware *STOPPED* the attack.
* User description for the attack . . . . . : Known ransomware out protection
* Simulation of ransomware with extension: WNCRY
* 2 Files compromised before the attack was detected and stopped
* Alerts were sent to the Administrator.
* Future connections to the mapped drive are rejected.
* To clear the attack use GUI or STRAR, 11.

****************************************************************************
```

iSecurity
Anti-Ransomware

Advantages on our Solution

iSecurity Anti-Ransomware prevents ransomware from damaging valuable data while preserving performance.

RAZ-LEE

Why to choose iSecurity Anti-Ransomware?

Protects against ransomware attacks and other kinds of malware that may access and change IBM i data on the IFS. It prevents ransomware from damaging valuable data while preserving performance.

- ✓ Identifies, stops, delays, and reports attacks in real-time.
- ✓ Suspends the attack and alerts the offending computer in real-time.
- ✓ Disconnects the intruder and sends Email Alert.
- ✓ Syslog messages to up to 3 SIEMS in CEF/LEEF formats.
- ✓ Gets ransomware definitions updates every two hours.

Advantages when being evaluated against competition

- ✓ Ability to work asynchronous achieving a huge performance impact.
- ✓ Ability to work multithread as IBM recommends it. It results in having a single job for all the user-shares, rather than a job for each one – If you have 100 users and each has 3 shares = 300 jobs.
- ✓ Sandbox, Remember the Wolf, Wolf story? This will reduce False alert to virtually zero. Files that are suspected to have been compromised, are passed to a sandbox which tries to run them. If they run in the sandbox, they are not compromised, and vice versa. The Sandbox runs in the IBM i. No additional hardware/software is needed.
- ✓ Attack simulator.
- ✓ Ability to shutdown (or put in sleep mode) the attacker, before disconnecting him from IBM i.
- ✓ Recycle Bin.

iSecurity Anti-Ransomware Advantages

All detections are logged to a native WORM (Write Once, Read Many) native file, in addition to the standard IFS logs.

- ✓ Automatic, regularly updated database.
- ✓ Disconnect Intruder Automatically.
- ✓ Command-line scanner.
- ✓ Database updater with support for digital signatures.
- ✓ Cannot be disabled by viruses.
- ✓ Built-in support for zip, gzip, jar, and tar files.
- ✓ User-friendly, multilingual interface (green screen and GUI).
- ✓ Supports V5R3 Scanning Enablement.
- ✓ Integration with OS/400 Scheduler.
- ✓ SIEM LOG compatible.
- ✓ History Log for review and analysis.

RAZ-LEE

Contact us About our Products

Sales Representatives

sales@razlee.com

Visit Our Website

www.razlee.com

iSecurity

Anti-Ransomware