Anti-Ransomware

DATASHEET (iSecurity Suite Cyber Protection)

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.

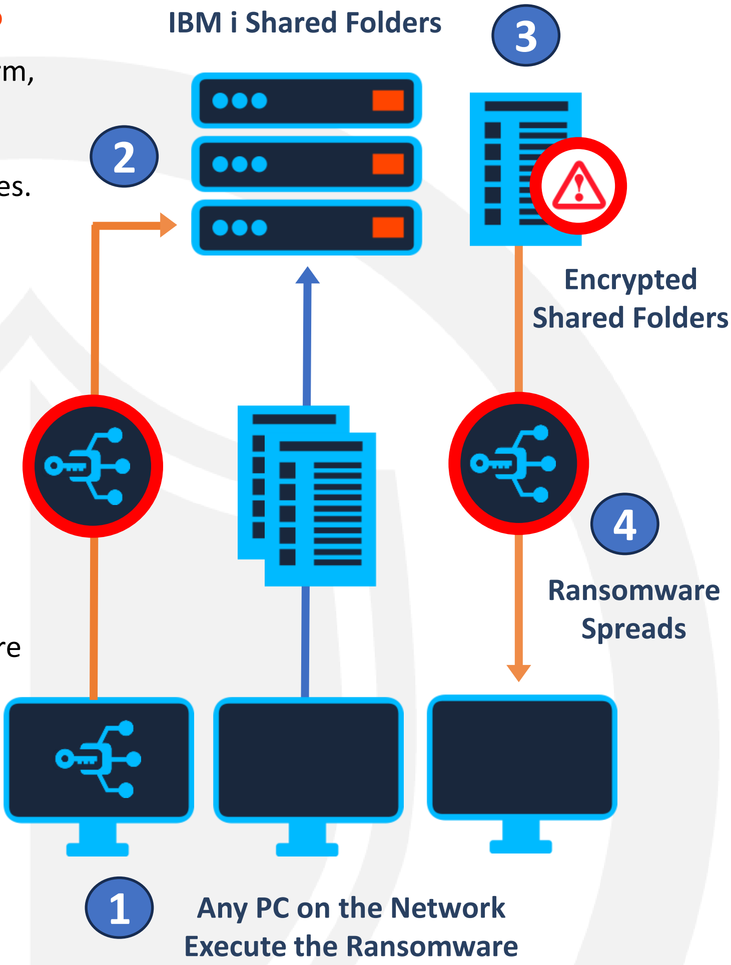
IFS directory files can easily become ransomware victims and unintentional ransomware propagators, through infected mapped drives.

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

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.



Advanced Ransomware Threat Protection for IFS

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

- iSecurity Anti-Ransomware software is the first component of iSecurity ATP
- A comprehensive advanced threat protection solution for defending IBM i IFS files against ransomware and other kinds of malware
- It prevents ransomware from damaging valuable data while preserving performance.

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
- User-friendly, multilingual interface (green screen and GUI)
- Supports V5R3 Scanning Enablement
- Integration with OS/400 Scheduler
- History Log for review and analysis
- 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 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.

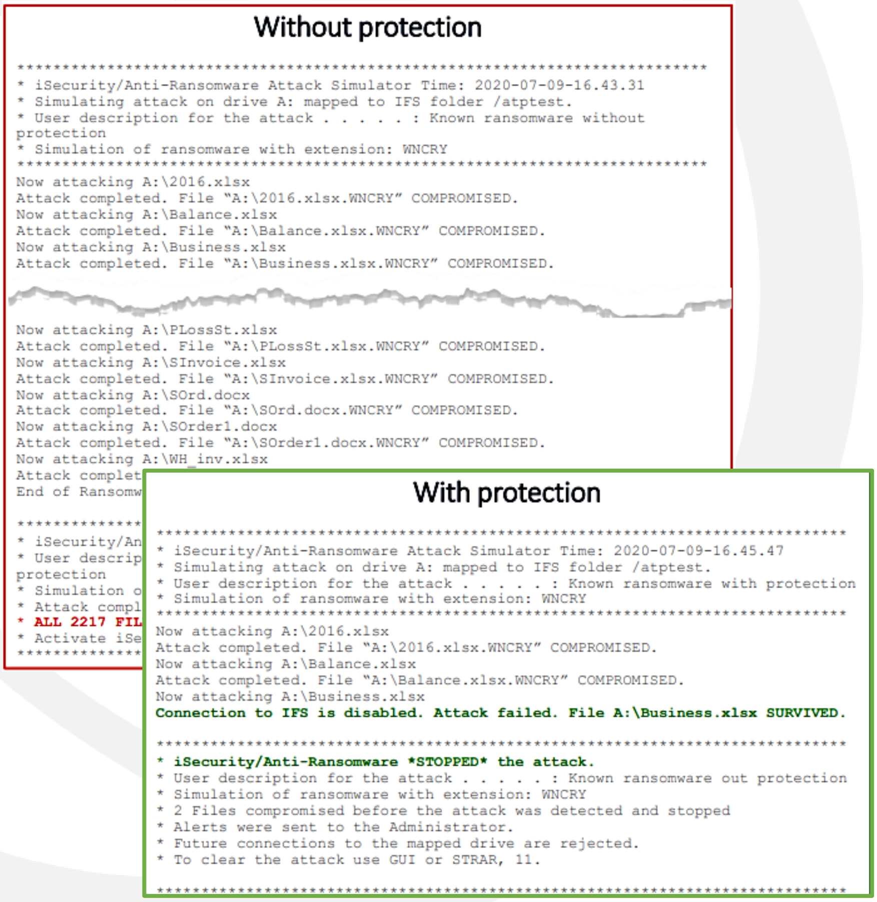
Results speaks for their own

iSecurity Anti Ransomware was tested in a completely isolated lab which included:

- 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!



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 complet
End of Ransomw

*************
* iSecurity/An
* User descrip
protection
* Simulation o
* Attack compl
* ALL 2217 FIL
* Activate iSe
*************
```

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.

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

Let's Get Started

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

RAZ-LEE iSecurity