



iSecurity Anti-Ransomware

User Guide
Version 7.40

www.razlee.com

Contents

- Contents 2
- About this Manual 3
 - Intended Audience 3
 - Native IBM i (OS/400) User Interface 4
 - Conventions Used in the Document 4
 - Menus 4
 - Data Entry Screens 5
 - Legal Notice 5
 - Contacts 6
- Ransomware Best Practices 7
- Installation, Upgrade and Setup 9
 - Configuring Anti-Ransomware 10
- Starting Anti-Ransomware 15
- Setting Thresholds for Ransomware Detection 25
- Setting Reactions to Ransomware Attacks 27
- Excluding Files and Directories from Scanning 29
 - Excluding Files by Extension 31
 - Including Files by Name or Extension 33
- Activating and De-Activating Ransomware Detection 35
- Setting Up Malware Honeypots 39
- Managing Default Honeypot Files 44
- Updating Anti-Ransomware Definitions 46
- Simulating a Ransomware Attack 50
 - Examining and Recovering Files in the Recycle Bin 51
 - Enabling the Recycle Bin 51
 - Viewing the Recycle Bin 52
 - Processing Multiple Files 53
 - Viewing Detected Attacks 55

About this Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on IBM i systems. However, any user with basic knowledge of IBM i operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: <http://www.adobe.com/>. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the-box" security. To learn more about the iSecurity Suite, visit our website at <http://www.razlee.com/>.

Intended Audience

The Anti-Ransomware User Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on IBM® AS/400 systems. However, any user with a basic knowledge of System i operations is able to make full use of this document following study of this User Guide.

NOTE: Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

Native IBM i (OS/400) User Interface

Anti-Ransomware is designed to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard IBM i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands. Many features are also accessible via the command line, for the convenience of experienced users.

Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on the previous page.

Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.

Key combinations are in Bold and separated by a dash, for example: **Enter, Shift-Tab**.

Emphasis is written in **Bold**.

A sequence of operations entered via the keyboard is marked as

STRAR > 81 > 32

meaning: Syslog definitions activated by typing ***STRAR*** and selecting option: **81** then option: **32**.

Menus

Product menus allow easy access to all features with a minimum of keystrokes. Menu option numbering and terminology is consistent

throughout this product and with other Raz-Lee products. To select a menu option, simply type the option number and press **Enter**. The command line is available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press **F10** to display it.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press Enter or Field Exit
- To move from one field to another without changing the contents press Tab
- To view options for a data field together with an explanation, press F4
- To accept the data displayed on the screen and continue, press Enter

The following function keys may appear on data entry screens.

- **F1: Help** Display context-sensitive help
- **F3: Exit** End the current task and return to the screen or menu from which the task was initiated
- **F4: Prompt** Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
- **F6: Add New** Create a new record or data item
- **F8: Print** Print the current report or data item
- **F9: Retrieve** Retrieve the previously-entered command
- **F12: Cancel** Return to the previous screen or menu without updating

Legal Notice

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

Please check your End User License Agreement (EULA) for terms and Conditions.

2022 © Copyright Raz-Lee Security Inc. All rights reserved.

Manual Revised: Wednesday, May 18, 2022

Contacts

Raz-Lee Security Inc. www.razlee.com

Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)

Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

Ransomware Best Practices

While several routines, protocols and operations can dramatically reduce the exposure of your business to Ransomware attacks, you also need ways to handle the crises once they are detected.

Safety Recommendations for Prevention

- Set Antivirus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed, and those who need administrator accounts should only use them when necessary.
- Implement your security incident response and business continuity plan. Ideally, organizations ensure they have appropriate backups, so their response to an attack will simply be to restore the data from a known clean backup. Having a data backup can eliminate the need to pay a ransom to recover data.
- Keep all software up to date, including the most recent releases and patches of critical products.

Business Continuity Considerations

- Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure that it works.
- Secure your backups. Ensure that backups are not connected permanently to the computers and networks that they are backing up. For example, secure your backups in the cloud or physically store them offline. Backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data.

Disaster Recovery Plan (DRP) guidelines

- Isolate the infected computer immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or shared drives.

- Immediately secure backup data or systems by taking them offline. Ensure that backups are free of malware.

Installation, Upgrade and Setup

Time Allocation

You must allocate sufficient time for installations and upgrades.

Installing Anti-Ransomware for the first-time takes up to fifteen minutes.

Upgrading an existing installation takes up to sixty minutes.

During the installation or upgrade, no iSecurity products installed on the target computer will be available.

System Requirements

The Anti-Ransomware software requires:

- Operating System (OS) 6.1 and higher
- Disk Space: 150 MB

NOTE: To install the Anti-Ransomware software, you may need to install iSecurity Audit base software as well.

The Antivirus software may have additional System Requirements. Consult the documentation for **iSecurity Audit** for its system requirements.

Installation Procedure

The Anti-Ransomware software product is available for download as a link through e-mail.

The Installation Guide document, available as a link through email, details the full procedure for installing and upgrading Raz-Lee products.

Configuring Anti-Ransomware

To **configure** Anti-Ransomware, select **81. System Configuration** from the main **Anti-Ransomware** screen (STRAR).

The **AntiVirus & AntiRansomware (ATP) Configuration** screen appears:

```
Antivirus & AntiRansomware (ATP) Configuration 15/10/20 11:50:20
RLDEV
Antivirus *Not Active* Advanced Messaging
 1. General Definitions 31. SIEM Definitions
 2. Real-Time ("on access")
 9. Alerting

11. Force Re-Scan ("on access") More Settings
41. Proxy Setup for Antivirus

Anti-Ransomware *Active*
21. Protection General
25. Recycle Bin 91. Language Support
99. Copyright Notice

Selection ==> _ Restart Real-Time activities to activate changes

Release ID . . . . . 07.39 20-10-14 788C500 41A EP10 2
Authorization code . . . . . V##### 2 RLDEV

F3=Exit F22=Enter Authorization Code
```

To **set your authorization code** for Anti-Ransomware, press the **F22 (Shift+F10)** key. Enter your key in the **Authorization code** field and press **Enter**.

To **enable the recycle bin**, select **25. Recycle Bin**. The **Anti-Ransomware Protection Setting** screen appears, as shown in "Examining and Recovering Files in the Recycle Bin" on page 51.

Setting Real Time Activities and Internal Logging

To set whether Anti-Ransomware is to **monitor activity**, either real time or in FYI Simulation mode, and to set whether it is to **keep an internal log**, select **21. Protection** from the main **AntiVirus & AntiRansomware (ATP) Configuration** screen (*STRAR > 81*).

The **Real-Time Activities Setting** screen appears:

```
Anti-Ransomware Protection Setting      15/10/20 14:41:59
                                          RLDEV
Anti-Ransomware active . . . Y          Y=Yes, I=FYI, N=No
*FYI* is an acronym for "For Your Information".
In this mode, no global stop occurs.

Internal log . . . . . Y          Y=Yes, N=No
Activate only as per Raz-Lee Support instruction for limited time. Data is
collected in SMZVDTA/TPFILSL*. Clear file after sending it to Raz-Lee Support.

F3=Exit  F12=Cancel
```

The **Anti-Ransomware/Malware** field controls whether Anti-Ransomware runs in real time. The choices are:

- **Y**: Anti-Ransomware runs in **real time**, monitoring activity and acting on what it detects.
- **I**: Anti-Ransomware runs in **FYI Simulation mode**, monitoring activity and logging what its responses would be if it were running in real time without taking action.
- **N**: Anti-Ransomware **does not run** in real time.

The **Internal log** field controls whether Anti-Ransomware events are captured to a log in **SMZVDTA/TPFILSL***. The files can grow large. Set this field to Y only if directed to do so by Raz-Lee support. Remove them when they are no longer needed.

To **select a language**, place the cursor in either field and press the **F4** key. The **Select Language Attributes** window appears, from which you can select the language from a predefined set of numeric CCSID codes representing the language.

CCSID to use as origin of data

To select a different language when receiving data, place the cursor in either field and press the **F4** key select the language from a predefined set of numeric CCSID codes representing the language.

Replacement of special characters

Use this field to replace characters when presenting text in this language.

In some languages, the keyboard settings are different. When creating an HTML file via one of the commands, such as **DSPAULOG** or **DSPFWLOG**, the machine writes to a text file that HTML translator understands.

When, for example, a keyword for HTML has to be between "[keyword]", but the user notices that his text file looks like this ... "!keyword^", then, defining the field as follows:

```
Replacement of special characters.  !^  
(original value)                  [ ]@#$...1...+...2...+...3...+...4
```

This will obtain as result: "[keyword]" which will be readable to HTML.

Setup Workflow

To set up Anti-Ransomware after installation, follow these steps in order. Each step is documented at the provided links.

1. **Start** Anti-Ransomware by entering **STRAR** on any command line, as shown in "Starting Anti-Ransomware" on the facing page.
2. Set needed **Base System parameters**, including the **Anti-Ransomware authorization code**, as shown in the iSecurity Base Support manual.
3. Set whether Anti-Ransomware is to **monitor activity** in real time or in a simulation, as shown in Setting Real Time Activities and Internal Logging.
4. Set **thresholds** and durations for Anti-Ransomware responses, as shown in "Setting Thresholds for Ransomware Detection" on page 25.
5. Set the methods by which Anti-Ransomware **responds to alerts**, as shown in "Setting Reactions to Ransomware Attacks" on page 27.
6. Set specific **files and directories to exclude** from scans for ransomware, as shown in "Excluding Files and Directories from Scanning" on page 29.
7. **Exclude files with specific extensions** from scans, as shown in "Excluding Files by Extension" on page 31.
8. Set up the **default set of honeypot** files, as shown in "Managing Default Honeypot Files" on page 44.
9. Set up and manage **honeypots in specified directories**, as shown in "Setting Up Malware Honeypots" on page 39.
10. If needed, change the **program run after Anti-Ransomware**, as shown in "Activating and De-Activating Ransomware Detection" on page 35
11. **Activate** real-time detection, as shown in "Activating and De-Activating Ransomware Detection" on page 35.
12. **Simulate a ransomware attack**, as shown in "Simulating a Ransomware Attack" on page 50.

Starting Anti-Ransomware

Log into your IBM i computer.

On the command line, type **STRAR** and press the **Enter** key.

The main **Anti-Ransomware** screen appears:

```
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 Honey Pots              Related Products
61. Object Integrity Control        62. Antivirus, Worms, Trojans
9. Simulate Attack
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
```

You can perform the following tasks from the options on this screen:

- "Setting Reactions to Ransomware Attacks" on page 27
- "Excluding Files and Directories from Scanning" on page 29
- "Managing Default Honey Pot Files" on page 44
- "Activating and De-Activating Ransomware Detection" on page 35
- "Updating Anti-Ransomware Definitions" on page 46
- "Simulating a Ransomware Attack" on page 50
- "Examining and Recovering Files in the Recycle Bin" on page 51

Setting Anti-Ransomware Reactions to Suspected Attacks

To set the **thresholds and durations** for Anti-Ransomware responses, select **3. Threat Prevention Dashboard**. The **Threat Prevention Dashboard** screen appears, as shown in "Setting Thresholds for Ransomware Detection" on page 25.

To set the **methods** by which Anti-Ransomware responds to alerts of different levels, select **4. Reaction To Attack**. The **Reaction To Attack** screen appears, as shown in "Setting Reactions to Ransomware Attacks" on page 27.

Setting Inclusions and Exclusions

To set the **names and extensions** of files and directories that Anti-Ransomware should specifically include in or exclude from checks for ransomware, select **6. Inclusion/Exclusion** from the main **Anti-Ransomware** screen. The **Exclusions and Inclusions** screen appears:

```
TPRANS                               Exclusions and Inclusions                               iSecurity/ATP
                                                                              System:  RAZLEE3

Exclusions
  1. Files and Directories to exclude
  5. Extensions to exclude
No check will take place for the above

Inclusions
11. Locally added Ransomware File name and Extensions
Use this to add Ransomware information that has just became public

===> _____

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

To set specific **files and directories to exclude**, select **1. Files and Directories to exclude** from the **Exclusions and Inclusions** screen. The **Objects to exclude** screen appears, as shown in "Excluding Files and Directories from Scanning" on page 29.

To set specific **extensions to exclude**, select **5. Extensions to exclude** from the **Exclusions and Inclusions** screen. The **Locally Verified Extensions** screen appears, as shown in "Excluding Files by Extension" on page 31.

To set specific **file names and extensions to include**, select **11. Locally added Ransomware File name and Extensions** from the **Exclusions and Inclusions** screen. The **Ransomware Files and Extensions** screen appears, as shown in "Setting Up Malware Honeypots" on page 39.

Managing Malware Honey pots

To define and manage **malware honey pots**, select **7. Malware Honey pots** from the main **Anti-Ransomware screen**. The **Malware Honey pots** screen appears:

```
TPHONY                               Malware Honey pots                               iSecurity/ATP
                                         System: RAZLEE3

Work with Honey pots
1. Deploy Honey pots

5. Setup Honey pot Template

Malware honey pots are sacrificial files. If they are accessed, this is
considered as a contributing sign that an attack takes place.
Most Ransomware accesses files sequentially. It is recommended to name
honeypot files in a way which will place them first in the folder list
(i.e. AAA 0011 etc.).

iSecurity honey pot files are recognized even if they are renamed or moved.

===> _____

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

To set up and manage honey pots, select **1. Deploy Honey pots**. The **Deploy Honey pots** screen appears, as shown in "Setting Up Malware Honey pots" on page 39.

To manage the default set of honey pots, select **5. Setup Honey pot Template** from the **Deploy Honey pots** screen. The **Setup Honey pot Template** screen appears, as shown in "Managing Default Honey pot Files" on page 44.

Activating and De-Activating Anti-Ransomware

To **activate and de-activate** real-time ransomware detection and to work with related jobs, select **51. Activation** from the main **Anti-Ransomware** screen. The **Activation** screen appears:

```
TPACTV                               Activation                               iSecurity/ATP
System: RLDEV
Anti-Ransomware / Anti-Malware
1. Activate Real-Time Detection
2. De-activate Real-Time Detection

5. Activate NETSERVER with RESET(*YES)
7. Work with Subsystem QSERVER Jobs
8. Work with Active QZLS* Jobs

Selection or command
===> _____

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

To **activate** real-time detection, select **1. Activate Real-Time Detection**. The **Anti-Ransomware - Activation** screen appears, as shown in "Activating and De-Activating Ransomware Detection" on page 35.

To **de-activate** real-time detection, select **2. De-activate Real-Time Detection**. The **Anti-Ransomware - De-Activation** screen appears, as shown in "Activating and De-Activating Ransomware Detection" on page 35.

To **manage jobs from the QSERVER subsystem**, which Anti-Ransomware uses, select **7. Work with Subsystem QSERVER Jobs**. The standard **Work with Subsystem Jobs** screen appears, with information on the QSERVER subsystem.

To **manage active jobs** with names beginning with **QZLS***, which Anti-Ransomware uses, select **8. Work with Active QZLS* Jobs**. The standard **Work with Active Jobs** screen appears, showing jobs with names that begin with the string "**QZLS**".

Displaying Anti-Ransomware Logs and Reports

To display logs and journaled information for Anti-Ransomware, select **41 . Logs and Reports** from the main **Anti-Ransomware** screen. The **ATP Logs and Reports** screen appears:

```
TPRPRT                                ATP Logs & Reports                                iSecurity/ATP
System:  RAZLEE3
Logs
1. Display ATP Log

5. Display ATP Journaled Info

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

To display Anti-Ransomware logs, select **1. Display ATP Log**. The standard **Display Audit Log Entries (DSPAULOG)** screen appears, with the **Audit Type** field set to ***BYENTTYP**.

To display journaled information for Anti-Ransomware, select **5. Display ATP Journaled Info**. The standard **Display Journal (DSPJRN)** screen appears, with the **Journal** field set to **SMZV** and the **Library** field set to **SMZVDTA**.

Refreshing Threat Information

To manually **refresh** threat information, select **52. Refresh Threat Information** from the main **Anti-Ransomware** screen. The **Threat Information Refresh** screen appears:

```
TPRFRS                               Threat Information Refresh                               iSecurity/ATP
                                                                              System: RAZLEE3

1. Refresh
2. Schedule Refresh

9. Display Last Refresh Time

Threats Information might be updated every 2 hours.

===> _____

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

NOTE: By default, threat information is automatically updated every two hours.

To **refresh threat information on demand**, select **1. Refresh**. The **Update ATP Definitions (UPDATPDFN)** screen appears, as shown in "Updating Anti-Ransomware Definitions" on page 46

To **schedule a refresh** of threat information, select **2. Schedule Refresh**. The standard **Work with Job Schedule Entries** screen appears, with information on the job **AV\$UPDATP**, which performs the update on schedule.

To **display the time of the last update**, select **9. Display Last Refresh Time**. A window appears showing information on the update:

Exiting Anti-Ransomware

To exit the **Anti-Ransomware** screen, press the **F3** key.

Setting Thresholds for Ransomware Detection

Anti-Ransomware tests interactions for ransomware attacks in several different ways. Some give a clear indication that an attack is in progress. Others note suspicious activity that suggests that an attack may be happening. You can set thresholds for response, based on:

- the type of activity
- the certainty that an attack is in progress, and
- the number of times in a set number of seconds that the activity has been detected.

To set the **thresholds and durations** for Anti-Ransomware responses, select **3. Threat Prevention Dashboard** from the main **Anti-Ransomware screen (STRAR)** as shown in "Starting Anti-Ransomware" on page 15. The **Threat Prevention Dashboard** screen appears:

```
Active Threat Prevention Dashboard RLDEV
Number of React
Checks Y/N
Detected Attack
All indicators of a ransomware attack detected . . . 3 Y
Some indicators of a ransomware attack detected . . 5 Y
Strong indication of zero-day (unknown) ransomware attack. 9 Y
Suspicious honeypot activity detected . . . . . 10 Y
Checks are not equal to files. Several checks may correspond to a single file.

Additional Settings
Period for number of checks . . . . . 30 Seconds
Encryption detection certainty . . . . . 50 Percent
Lowering the detection certainty may result in more false positive detections.

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

F3=Exit
```

Anti-Ransomware can react to threats based on several levels of detection, as shown in the first column on the screen:

All indicators of a ransomware attack detected

The activity matches every indicator that a known type of ransomware attack is in progress.

Some indicators of a ransomware attack detected

The activity matches some, but not all, indicators that a known type of ransomware attack is in progress.

Strong indication of zero-day (unknown) ransomware attack

The activity matches several general indicators of ransomware attacks, although it doesn't specifically match those of a known attack type.

Suspicious honeypot activity detected

A honeypot trap (as shown in "Setting Up Malware Honeypots" on page 39) has detected attempts to access decoy files that you have set up to spot suspected attacks.

For each of those items, if Anti-Ransomware detects:

- the number of suspected attacks shown in its **Number of Checks** field
- of that **level** of detection
- within the number of seconds shown in the **Period for number of checks** field,
- with the degree of certainty shown in the **Encryption detection certainty** field,
- it triggers the reaction indicated in its **React Y/N** field (as set in "Setting Reactions to Ransomware Attacks" on the facing page).

In the example shown here, if Anti-Ransomware detects

- even **one** instance where
- **all** indicators show that known ransomware is attacking or
- **three** of the indicators show that known ransomware is attacking
- within a period of **30** seconds
- with **50%** certainty,
- it triggers a reaction.

In the **Encryption detection security** field, a higher number means that, to trigger a reaction, Anti-Ransomware must be more certain of what it has detected. To reduce false alarms, keep its value above **50**.

Setting Reactions to Ransomware Attacks

In the **Reaction To Attack** screen, you can define two reactions to detected attacks, based on criteria set in the **Threat Control Center** screen, as shown in "Setting Thresholds for Ransomware Detection" on page 25.

To set the **methods** by which Anti-Ransomware responds to alerts of different levels, select **4. Reaction To Attack** from the **Anti-Ransomware** main screen, as shown in "Starting Anti-Ransomware" on page 15.

The **Reaction To Attack** screen appears:

```

                                Reaction To Attack                                RLDEV
Alert
Message to QSYSOPR . . . . . Y           Y=Yes
Inform SIEM . . . . . -               Y=Yes
Email system admin . . . . . xxxxxx@razlee.com
-----
Stop the Attack - Even in *FYI (simulation), the attack is stopped.
Stop attack of User from IP . Y           Y=Yes

If Mode is *REAL:
  End system wide File Server . -         Y=Yes
  Stops all remote access to shares.

  Hibernate/Shutdown attacker . -        Y=Yes
  See procedure and restrictions in SMZV/AVSOURCE ATP4RMT

  Submit/Call on this system . . S        S=Submit, C=Call
  Program . . . . . _____          Name
  Library . . . . . _____          Name *LIBL
  See example program in SMZV/AVSOURCE ATPALERTR
F3=Exit
  
```

The body of the screen lists different possible reactions. You can also set further details and specifications for some of the reactions.

To **choose that reaction**, set the field in that column to **Y** (except as shown below). Otherwise, leave the field blank.

Possible reactions are:

Alert

Message to QSYSOPR

Send a system message to QSYSOPR.

Inform SIEM

Alert up to three SIEM systems as set from the **iSecurity/Base System Configuration** screen within the **iSecurity Base System** (*STRAUD > 81*).

Email system admin

Send an email to the system administrator at the email address in this field.

Stop the Attack

Stop attack of user from IP

End the attack.

If Node is *REAL

End system wide File Server

End all activity on the file server that is being attacked.

Hibernate/Shutdown infected PC

Hibernate or shutdown the PC with which the system is communicating.

See **SMZV/AVSOURCE ATP4RMT** for more information.

Submit/Call on this system

Set this to **C** to call the program or **S** to submit it. Enter the name and library of the program in the **Program to run** and **Library** fields, respectively.

See **SMZV/AVSOURCE ATPALERTR** for a sample program.

Excluding Files and Directories from Scanning

To set specific **files and directories to exclude** from scans for ransomware, select **1. Files and Directories to exclude** from the **Exclusions and Inclusions** screen (*STRAR > 6*), as shown in "Starting Anti-Ransomware" on page 15.

The **Objects to exclude** screen appears:

```
Objects to exclude

Type options, press Enter.          Position to . . .
  1=Select  4=Delete                Subset . . . _____

Opt Object                          Text
- /db_gate_backup/DB-Gate/mysql-connector-ja > DB gate
- /tmp/av.txt.log-saved              Antivirus EEEE
- /tmp/clamav-cf620b3fcf19cb99c2d971c22a097f > Test Each exception must start
- /tmp/clamav-913671717f85d71dbe8d6e91784e21 > Group Job handling tries to co

F3=Exit  F6=Add New  F12=Cancel  F22=Display entire field
There are 4 entries defined, out of the 500 allowed.

Bottom
```

NOTE: As shipped, this screen lists objects chosen by Raz-Lee. Contact Raz-Lee Support before making any changes on this screen.

The body of the screen contains lines referring to each of up to two hundred objects. Each contains two fields after the standard **Opt** field:

Object

The path and name of the file or directory.

The value may contain asterisks (*****), which represent one or more characters in a generic name. Names beginning with an asterisk indicate that they may appear in any directory. If the name does not begin with an asterisk, it must begin with a slash (**/**) and show the absolute path from the top of the file system.

If the complete file name or path is too long to fit onscreen, the ">" character appears at the end of the field. To see the full path and name, place the cursor in the **Opt** field for that line and press the **F22 (Shift+F10)** key.

Text

A free-form description of the field.

If the text is truncated, enter **1** in the **Opt** field on that line. The **Modify Object to Exclude** screen appears, showing the complete text.

To **add files and directories** to the list, press the **F6** key. The **Add Object to Exclude** screen appears. It contains two fields:

- **Object**, corresponding to the **Links** field of the **Objects to Exclude** screen, and
- **Description**, corresponding to the **Text** field of the **Objects to exclude** screen.

To **modify information on a file or directory**, enter **1** in the **Opt** field on that line. The **Modify Object to Exclude** screen appears, showing the complete **Object** and **Description** fields.

To **delete a file or directory from the list**, enter **4** in the **Opt** field for that line. The **Delete Excluded links for Ransomware** screen appears. Press **Enter** to confirm the deletion or the **F12** key to cancel it.

Excluding Files by Extension

To exclude files with specific extensions, select **5. Well-Known Extensions** from the **Exclusions and Inclusions** screen (*STRAR > 2*) as shown in "Starting Anti-Ransomware" on page 15. The **Well-Known Extensions** screen appears:

```
Well-Known Extensions

Type options, press Enter.
  1=Select  4=Delete                Subset . . . . . _____

Opt      Extension      Entered extensions that are known ransomware are in blue
-        .$$$
-        .$DB
-        .001
-        .003
-        .113
-        .123
-        .208
-        .264
-        .2BP
-        .2FS
-        .36
-        .386
-        .386
-        .3D
                                                More...

F3=Exit   F6=Add New   F12=Cancel
```

NOTE: As shipped, this screen lists objects chosen by Raz-Lee. Contact Raz-Lee Support before making any changes on this screen.

Each line on the screen refers to a single extension that is excluded from scanning. After the standard **Opt** column, the **Extension** field shows the extension to be excluded. An asterisk (*) means that one or more characters are in the string. Thus, ***.ENG** means any file names that end in **".ENG"**.

To **add a new extension**, press the **F6** key. The **Add Locally Verified Extension** screen appears. The screen has the following fields:

Extension

Corresponds to the **File or Extension** field on the **Locally Verified Extensions** screen.

Source

(Read only) Corresponds to the **Type** field on the **Locally Verified Extensions** screen.

Related to malware

The name of the malware that uses that extension.

Description

A free-form description of the extension.

To **modify the information on an extension**, enter **1** in the **Opt** column for that line. The **Modify Well-Known Extensions** screen appears, with the same fields as the **Add Locally Verified Extension** screen.

To **delete an extension from the list**, enter **4** in the **Opt** field for that line. The **Delete Extensions** screen appears. Press **Enter** to confirm the deletion or the **F12** key to cancel it.

Including Files by Name or Extension

To include files or extensions that are not yet listed as possible malware, select **11. Locally added Ransomware File name and Extensions** from the **Exclusions and Inclusions** screen (*STRAR > 6*) as shown in "Starting Anti-Ransomware" on page 15.

The **Ransomware Files and Extensions** screen appears.

```

                                Ransomware Files and Extensions

Type options, press Enter.
  1=Select  4=Delete                Subset . . . . . _____

Opt Type File or Extension
_  USR  XYZ

                                Bottom

F3=Exit   F6=Add New   F12=Cancel
```

The body of the screen contains a line for each filename or extension that has been added to the list. For each, it shows the type of file in the **Type** field and the file or extension name in the **File or Extension** field.

To add a new file or extension to the list, press the **F6** key. The **Add Ransomware File or Extension** screen appears, as shown below.

To view and modify information on a file or extension, enter **1** in the **Opt** field in its line. The **Modify Ransomware File or Extension** screen, which has the same fields as the **Add Ransomware File or Extension** screen, appears.

To delete a file or extension from the list, enter **4** in the **Opt** field in its line. The **Delete Ransomware File or Extension** screen appears, confirming that you want to delete the listing.

Add Ransomware File or Extension

Type choices, press Enter.

File or Extension . _____

Source USR

Related to malware. _____

Description _____

F3=Exit F12=Cancel

The body of the **Add Ransomware File or Extension** screen contains these fields:

File or Extension

The file name or extension to be included in the list. Extensions begin with a period (".").

Source

The source of the information. If the User is supplying it, set the field to **USR**.

Related to malware

Names of malware that uses this name or extension.

Description

A free-form description of the name or extension.

Activating and De-Activating Ransomware Detection

To activate or de-activate real-time ransomware detection, select **51 . Activation** from the main **Anti-Ransomware** screen (*STRAR*).

The **Activation** screen appears:

```
TPACTV                               Activation                               iSecurity/ATP
System:  RLDEV
Anti-Ransomware / Anti-Malware
  1. Activate Real-Time Detection
  2. De-activate Real-Time Detection

  5. Activate NETSERVER with RESET(*YES)
  7. Work with Subsystem QSERVER Jobs
  8. Work with Active QZLS* Jobs

Selection or command
===> _____

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

Activating Real-Time Detection

To activate real-time detection, select **1. Activate Real-Time Detection**.

The **Anti-Ransomware - Activation** screen appears.

```
Anti-Ransomware - Activation                                RLDEV

Anti-Ransomware status . . *Active*
Protect when active . . . Y                               Y=Yes, I=Yes in FYI (Simulation),
Change by 81. System Configuration.                       N=No

If before activation there was a program in the Exit Point, it will also run:
Program . . . . . *NONE                                  Name, *NONE
Library . . . . .                                       Name

Press Enter to activate, F3 to cancel.

Explanation
The File Server exit point can run only one program. If the exit point
already has a program assigned, Anti-Ransomware ensures that the
existing program is called following the Anti-Ransomware detection program.

F3=Exit   F22=Enable change of program name
```

When the screen appears, all the fields are read-only, showing whether the exit point and Anti-Ransomware itself is active, inactive, or running in FYI Simulation Mode (in which the program reacts to events and logs what its responses would be if running, which not making any changes to the system). The **Program** and **Library** fields show the program called after Anti-Ransomware runs.

To change the Anti-Ransomware activation status, use the **Anti-Ransomware Protection Setting** screen, as shown in Setting Real Time Activities and Internal Logging.

Before you activate TP, use the **WRKREGINF** command to check the **QIBM_QPWFS_FILE_SERV** exit point for the program that is called after Anti-Ransomware is run.

To **change the program** called after Anti-Ransomware, press the **F22 (Shift+F10)** key. You can then change the values of the **Program** and **Library** fields. If they are blank, leave them blank.

To **activate** Anti-Ransomware, press **Enter**.

To **cancel** and exit to the previous screen, press the **F3** key.

De-activating Real-Time Detection

To de-activate real-time detection, select **2. De-activate Real-Time Detection** from the **Activations** screen (**STRAR > 51**).

The **Anti-Ransomware - De-Activation** screen appears.

```
Anti-Ransomware - De-Activation

De-Activation of Anti-Ransomware malware detection resets the exit program
to the program that it had run before activation.

Program to set back . . . *FIREWALL           Name, *NONE
Library . . . . . Name

Press Enter to continue, F3 to cancel.

F3=Exit
```

The screen's read-only **Program to set back** and **Library** fields show the program that is set as the exit program when you de-activate Anti-Ransomware.

To **de-activate** Anti-Ransomware, press **Enter**.

To **cancel** and exit to the previous screen, press the **F3** key.

Setting Up Malware Honey pots

A **honeypot** is a computer system that is set up as a decoy to tempt cyber-attackers and to detect, deflect or study attempts to gain unauthorized access to information systems. Generally, it consists of a computer, applications, and data that simulate the behavior of a real system that appears to be part of a network but is actually isolated and closely monitored.

NOTE: Legitimate users have no reason to access a honeypot. All communications with honeypots are considered hostile.

Viewing and logging this activity can provide an insight into the level and types of threats that a network infrastructure faces, while distracting attackers away from assets of real value.

Raz-Lee's malware honeypot mechanism generates honeypot files that:

- Allow the users to discover where such fake targets are required and to control their implanting repositories.
- Even if they are copied or distributed or their contents or names are altered, will always be recognized by Raz-Lee's Anti-Ransomware software.
- Like all other Anti-Ransomware mechanisms, are not inspected based on single events but related to the rhythm of occurrences.

To **set up and manage honeypots**, select **1. Deploy Honey pots** from the **Malware Honey pots** screen (**STRAR > 7**) as shown in "Starting Anti-Ransomware" on page 15. The **Deploy Honey pots** screen appears:

```

                                Deploy Honeypots

List the directory tree and show the number of honeypot files (H-P) files that
exist in it and in any of its sub-directories.

Start at directory . . . . _____
Selecting a high level _____
directory may increase _____
loading time.                _____

Subset by:
Directory name contains . _____
Directories without H-P . - _____      Y=Yes, N=No, A=All

F3=Exit

```

To **search a directory for honeypots**, enter the pathname of the directory to be searched in the Start at directory field. (The field wraps over five lines, allowing for a very long pathname.) Search as specifically as you can, since searching at too high a level can take a long time.

To **specify subdirectory names** that contain a particular string, enter that string in the **Directory name contains** field.

To **specify whether to display subdirectories with or without honeypots**, enter one of these values in the **Directories without H-P** field:

- **Y**: Only list directories without honeypots.
- **N**: Only list directories with honeypots.
- **A**: List all directories.

To **run the search**, press **Enter**.

A second **Deploy Honeypots** screen appears:


```

Deploy Honey Pots
Start Dir: /tmp

Type choices, press Enter.
  1=Work with H-P  4=Remove H-P  6=Add H-P  8=WRKLNK  9=Set as Start Dir

Filter by name . . .
Missing H-P  A      Y, N, A=All
Window. . . 1

File-Count
Opt H-P  Other  Folder
-
-      44      3  /tmp/.com_ibm_tools_attach/
-      7      7  /tmp/tstaud/
-      3      3  /tmp/tstaud/.com_ibm_tools_attach/
-      2      2  /tmp/tstaud/.com_ibm_tools_attach/1374741/
-      2      2  /tmp/tstaud/.com_ibm_tools_attach/1398595/
-      2      2  /tmp/tstaud/.com_ibm_tools_attach/851898/
-      2      2  /tmp/tstaud/.com_ibm_tools_attach/851915/
-      2      2  /tmp/tstaud/.com_ibm_tools_attach/852048/
-      2      2  /tmp/tstaud/.com_ibm_tools_attach/852049/

Bottom
F3=Exit  F12=Cancel  F13=Repeat  F14=End repeat  F19=Left  F20=Right
F22=Display entire name

```

The body of the screen lists the directory that you specified and subdirectories within it. After the standard **Opt** column, each line shows, for one of the folders:

Count of H-P

The number of honeypot files in the directory

Count of Other

The number of files in the directory that are not honeypots.

Folder

The pathname of the directory. If the name is truncated, to see the full name, place the cursor in the **Opt** field on that line and press the **F22 (Shift+F10)** key.

In the example, the **/tmp/.com_ibm_tools_attach/** subdirectory of the **/tmp** starting directory contains 44 honeypot files and 3 other files.

To **add the default honeypot files** (as defined on the **Work with Default Honeypot Files** screen, shown in "Managing Default Honeypot Files" on page 44) to a directory, enter **6** in the **Opt** field of that line.

To **remove all honeypot files** from a directory, enter **4** in the **Opt** field of that line.

To **limit the list** to only the subdirectories of one of the displayed directories, enter **9** in the **Opt** field of that line.

To **modify the set of honeypot files** in a directory, enter **1** in the **Opt** field of that line. The **Work with Honeypot Files in a Directory** screen appears:

```
Work with Honeypot Files in a Directory

Dir: /tmp/.com_ibm_tools_attach/

Type choices, press Enter.
  1=Work with   3=Copy   4=Remove   7=Rename   8=WRKLNK

Opt Type      Object
-  *STMF      #CLIENT54.docx
-  *STMF      2016.xlsx
-  *STMF      2017.xlsx
-  *STMF      Balance2017.xlsx
-  *STMF      BalanceCapt1.xlsx
-  *STMF      Business2017.xlsx
-  *STMF      Business5y.xlsx
-  *STMF      Bussines2y.xlsx
-  *STMF      Bussines3y.xlsx
-  *STMF      Bussinesy4.xlsx
-  *STMF      CLIENT 1.docx
-  *STMF      CLIENT 2.docx
                                     More...

F3=Exit   F12=Cancel   F22=Full path
```

The body of the screen lists the honeypot files in the directory. For each, after the standard **Opt** field, it shows the **Type** of the file and the file's name. If the name is truncated, to see the full name, place the cursor in the **Opt** field on that line and press the **F22 (Shift+F10)** key.

To **copy** a file, enter **3** in the **Opt** field for that file. The **Copy Object (CPY)** screen appears. The screen shows three fields:

- **Object:** (Read-only) The pathname of the current file
- **To object:** A copy of the pathname, which you can alter to be the pathname of the new object
- **Authority:** One of these options:

***OBJ**

The authority information for copied objects is based on the authority for the object to be copied.

***INDIR**

The authority information for copied objects is based on the authority for the directory to which the file is to be copied.

***INDIROBJ**

The authority information for copied objects is initially based on the authority for the directory to which the file is to be copied. Then authority information from the object to be copied is assigned to the target object.

To **remove** a file, enter **4** in the **Opt** field for that file. The **Remove Link (DEL)** screen appears, in which you can confirm that you want to remove the file.

To **rename** a file, enter **7** in the **Opt** field for that file. The **Rename Object (REN)** screen appears, in which you can enter the new name of the file.

To **perform other operations** on the file, enter **1** in the **Opt** field for that file. The standard IBM **WRKLNK** screen appears.

Managing Default Honeypot Files

Anti-Ransomware uses a standard set of honeypot files, which are kept in the honeypot template directory, **/iSecurity/ATP/HoneyPot-Default/**. New honeypot sets, when created in other directories, are copied from there.

To manage the default set of honeypot files, select **5. Setup Honeypot Template** from the **Malware Honeybots** screen (**STRAR > 5**) as shown in "Starting Anti-Ransomware" on page 15. The **Setup Honeypot Template** screen appears:

```
Setup Honeypot Template

Dir: /iSecurity/ATP/HoneyPot-Default/

Type choices, press Enter.
  1=Work with   3=Copy   4=Remove   7=Rename

Opt Type      Object
-  *DIR       subdir/
-  *STMF      #CLIENT54.docx
-  *STMF      2016.xlsx
-  *STMF      2017.xlsx
-  *STMF      Balance2017.xlsx
-  *STMF      BalanceCapt1.xlsx
-  *STMF      Business2017.xlsx
-  *STMF      Business5y.xlsx
-  *STMF      Bussines2y.xlsx
-  *STMF      Bussines3y.xlsx
-  *STMF      Bussinesy4.xlsx
-  *STMF      CLIENT 1.docx
-
More...

F3=Exit   F6=New   F10=Restore Default   F22=Full path
```

The body of the screen lists the honeypot files in the directory. For each, after the standard **Opt** field, it shows the **Type** of the file and the file's name. If the name is truncated, to see the full name, place the cursor in the **Opt** field on that line and press the **F22 (Shift+F10)** key.

To copy a honeypot file from another directory, press the **F6** key. The **Copy to Default H-P Dir (TPHPNEW)** screen appears. Enter values in the screen's fields:

From Object

The pathname of the original file.

Object is from Default H-P

YES if the object was originally from the honeypot template directory.

NO if it originated elsewhere.

New object

The name of the new file, or ***SAME*** if it will have the same name as the **From Object**.

To **copy a honeypot file**, enter **3** in the **Opt** field for that file. The **Copy Honey-Pot Object (TPHPCPY)** screen appears. The name of the original file appears in the **Object** and **New object** fields. Change the value in the **New object** field to the name of the new file.

To **remove a honeypot file**, enter **4** in the **Opt** field for that file. The **Remove Link (DEL)** screen appears, in which you can confirm that you want to remove the file.

To **rename a honeypot file**, enter **7** in the **Opt** field for that file. The **Rename Honey-Pot Object (TPHPREN)** screen appears. The original name of the file appears in the **Object** and **New object** fields. Change the value in the **New object** field to the new name of the file.

To **perform other operations on a honeypot file**, enter **1** in the **Opt** field for that file. The standard IBM **WRKLNK** screen appears.

To **restore the set of honeypot files** to the default, press the **F10** key. The **Restore Factory Setting** window appears, confirming that you want to restore the original files.

Updating Anti-Ransomware Definitions

To refresh threat information on demand, select **1. Refresh** from the Threat Information Refresh screen (*STRAR*> **52**).

The Update ATP Definitions (*UPDATPDFN*) screen appears:

```
Update ATP Definitions (UPDATPDFN)

Type choices, press Enter.

Refresh source . . . . . *WEB          *WEB, *DIR
For *WEB: . . . . . *RAZLEE
-----
For *DIR: '/dir/' . . . . . '/SMZVDTA/tmp/'
-----
-----
-----

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

To refresh definitions **from the web**, set the **Refresh source** field to ***WEB** and the **For *WEB** field to the source from which you are refreshing the definitions. Possible choices are ***RAZLEE** to refresh from Raz-Lee's definitions and ***BACKUP** to refresh from a backup.

To refresh definitions **from a directory** on the same system, set the **Refresh source** field to ***DIR** and the **For *DIR** field to the pathname of the directory, between single quotation marks.

1. Download *BADEXTA.TXT* (the Anti Ransomware database file) from <http://av.razlee.com/BADEXTA.TXT> to a PC.
2. Transfer the *BADEXTA.TXT* file from the PC to the directory */SMZVDTA/tmp* in IFS.
3. On the **Update ATP Definitions (UPDATPDFN)** screen, set the **Refresh source** field to ***DIR** and the **For *DIR** field to **' /SMZVDTA/tmp '** (including the single quotation marks).

- To update the definitions immediately, enter the command **SMZV/UPDATPDFN SOURCE(*DIR) DIR('/SMZVDTA/tmp/')**

To schedule updates, as either a one-time or recurring event, select **2 . Schedule Refresh** from the **Threat Information Refresh** main menu (**STRAR > 52**). The standard **Work with Job Schedule Entries (WRKJOBSCDE)** screen appears, with an entry for virus scanning.

```

Work with Job Schedule Entries                                RLDEV
                                                           18/10/20 15:52:48 UTC

Type options, press Enter.
  2=Change   3=Hold   4=Remove   5=Display details   6=Release
  8=Work with last submission   10=Submit immediately

-----Schedule-----
Opt  Job          Status  Date      Time      Frequency  Action  Recovery  Next
---  AV$UPDATP    SCD     *ALL      03:00:00  *WEEKLY    *SBMRLS  *SBMRLS  19/10/20

Parameters or command
===> _____
F3=Exit   F4=Prompt   F5=Refresh  F6=Add     F9=Retrieve
F11=Display job queue data  F12=Cancel  F17=Top     F18=Bottom

```

To see and change the parameters for a scheduled job, type **2** in the **Opt** field for that line and press **Enter**. The **Change Job Schedule Entry (CHGJOBSCDE)** screen for that command appears, showing the values for the job.

```

Change Job Schedule Entry (CHGJOBSCDE)

Type choices, press Enter.

Job name . . . . . > AV$UPDATP      Name
Entry number . . . . . > 001232      000001-999999, *ONLY
Command to run . . . . . SMZV/UPDATPDFN
_____
_____
_____
_____
_____
_____
Frequency . . . . . *WEEKLY      *SAME, *ONCE, *WEEKLY...
Schedule date . . . . . *NONE      Date, *SAME, *CURRENT...
Schedule day . . . . . *ALL      *SAME, *NONE, *ALL, *MON...
      + for more values
Schedule time . . . . . '03:00:00'  Time, *SAME, *CURRENT

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys

```

To add a scheduled job, press the **F6** key from the **Work with Job Schedule Entries (WRKJOBSCDE)** screen. The **Add Job Schedule Entry (ADDJOBSCDE)** screen for that command appears, showing the values for the job.

```

Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name . . . . . _____  Name, *JOB
Command to run . . . . . _____
_____
_____
_____
_____
_____
Frequency . . . . . _____  *ONCE, *WEEKLY, *MONTHLY
Schedule date . . . . . *CURRENT  Date, *CURRENT, *MONTHSTR...
Schedule day . . . . . *NONE      *NONE, *ALL, *MON, *TUE...
      + for more values
Schedule time . . . . . *CURRENT  Time, *CURRENT

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys

```


Set the **Command to run** field to **SMZV/UPDATPDFN**.

Simulating a Ransomware Attack

To **simulate a ransomware attack** on your system, select **9. Simulate Attack** from the main **Anti-Ransomware** screen. The **Simulate Attack** screen appears, with instructions showing how to simulate an attack.

The procedure creates a test folder and simulates an attack on it. The simulated attack does not involve real malware. The attack is limited to the test folder and cannot infect or harm any other folders or files.

At the end of the simulation, everything returns to its state from before the simulation.

Examining and Recovering Files in the Recycle Bin

Raz-Lee has implemented a recycle bin for the IBM i. Files that are to be deleted are copied first to another location on your system where they are temporarily preserved. This provides an added layer of protection against some (but not all) ransomware variants that delete files before replacing them with encrypted versions.

Anti-Ransomware must be active for the Recycle Bin to work.

Enabling the Recycle Bin

To use the recycle bin, enter **25** from the **AntiVirus & AntiRansomware (ATP) Configuration** screen (**STRAR > 81**). The **Anti-Ransomware Protection Setting** screen appears.

```
Anti-Ransomware Protection Setting      20/08/20 18:11:42
RLDEV
Recycle bin active . . . . . Y          Y=Yes, N=No
Anti-Ransomware must be active for this operation.

Keep data in Recycle bin for.  7          Days, 9999=*NOMAX

The Recycle bin may not help against Ransomware. Ransomware often use methods
to prevent this.
It is strongly recommended that you always keep good backups.

F3=Exit  F12=Cancel
```

To **activate** the recycle bin, set the **Recycle bin active** field to **Y**.

To **deactivate** the recycle bin, set the **Recycle bin active** field to **N**.

The **Keep data in Recycle bin** field determines the number of days for which files are kept in the bin. To keep them indefinitely, set the field to **9999**.

NOTE: Keeping too many files in the bin for too long a time can consume a large amount of disc space.

Viewing the Recycle Bin

To **view the contents of the recycle bin**, select 12 from the Anti-Ransomware main screen. The Work with Recycle Bin Files screen appears.

```
595 Files, sorted by TIME          Work with Recycle bin files          Subset . . . _____
Type options, press Enter.
  1=Select  2=Restore  4=Delete  5=Display  8=Display attribute

Opt Time      User      Object              Path
- 13/08/20 14:58 SLAVA      2016.xlsx           /atptest/2016.xlsx
- 13/08/20 14:58 SLAVA      Budget.xlsx          /atptest/Budget.xlsx
- 13/08/20 14:58 SLAVA      Business.xlsx        /atptest/Business.xlsx
- 13/08/20 14:58 SLAVA      2016.xlsx.wncry     /atptest/2016.xlsx.wncry
- 13/08/20 14:58 SLAVA      Business.xlsx.wncry /atptest/Business.xlsx.wncry
- 13/08/20 14:58 SLAVA      Budget.xlsx.wncry   /atptest/Budget.xlsx.wncry
- 13/08/20 14:59 SLAVA      CLIENT.docx          /atptest/CLIENT.docx
- 13/08/20 14:59 SLAVA      codes.csv            /atptest/codes.csv
- 13/08/20 14:59 SLAVA      cust.php             /atptest/cust.php
- 13/08/20 15:00 SLAVA      CLIENT.docx.wncry   /atptest/CLIENT.docx.wncry
- 13/08/20 15:00 SLAVA      codes.csv.wncry     /atptest/codes.csv.wncry
- 13/08/20 15:01 SLAVA      cust.php.wncry.WNCRY /atptest/cust.php.wncry.WNCRY
- 13/08/20 15:01 SLAVA      CLIENT.docx.wncry.WNCRY /atptest/CLIENT.docx.wncry.WNCRY
- 13/08/20 15:01 SLAVA      codes.csv.wncry.WNCRY /atptest/codes.csv.wncry.WNCRY
- 13/08/20 15:01 SLAVA      cust.php.wncry      /atptest/cust.php.wncry
- 13/08/20 15:01 SLAVA      c_main.php          /atptest/c_main.php
- 13/08/20 15:02 SLAVA      c_main.php.WNCRI    /atptest/c_main.php.WNCRI
-
More...

Recycle Bin cannot be considered a method to use against Ransomware. Keep backups.
F3=Exit  F13=Repeat  F14=Clear repeat  F16=Resequene (by cursor position)
```

The body of the screen shows information on each file that is currently in the recycle bin.

For each file, it shows:

Time

The date and time that the original file was deleted.

User

The user who deleted the file.

Object

The name of the file.

Path

The path to the original location of the file.

To **sort the list** by a different field, place the cursor in that field on any line and press the **F16 (Shift-F4)** key.

To **restore a deleted file** from the recycle bin, enter **2** in the **Opt** field for that line and press **Enter**. The **Confirm Restore Recycle bin Files** screen appears. Press **Enter** to confirm restoring the file or the **F3** key to exit without restoring it.

To **permanently delete a file** from the recycle bin, enter **4** in the **Opt** field for that line and press **Enter**. The **Confirm Delete Recycle bin Files** screen appears. Press **Enter** to confirm deleting the file or the **F3** key to exit without deleting it.

To **display further information about a file** from the recycle bin, enter **5** in the **Opt** field for that line and press **Enter**. The standard **Work with Object Links** screen appears.

To **display the attributes of a file** from the recycle bin, enter **8** in the **Opt** field for that line and press **Enter**. The standard **Display Attributes** screen appears.

Processing Multiple Files

As with most screens with lists of items preceded by Opt fields, you can select multiple files and work on them as a group. For example, you could enter 2 in the Opt fields for multiple files, then restore them together.

To **select groups of items that appear sequentially** in the list by using the **F13=Repeat** and **F14=Clear Repeat** keys:

1. Sort the list by the field (**Time**, **User**, **Object**, or **Path**) by placing the cursor in that field on any line and pressing the **F16 (Shift-F4)** key.
2. Scroll to the first line where the field by which you sorted is within the range of files that you would like to process together.
3. Enter the number for the command that you would like to perform in the **Opt** field for that line.
4. Press the **F13 (Shift-F1)** key to mark the beginning of the group.
5. Scroll to the last item in that range.
6. Press the **F14 (Shift-F2)** key to mark the end of the range.
7. Press **Enter** to perform the action.

8. The appropriate screen appears, showing all the items.
9. Press **Enter** to confirm the action or the **F3** key to cancel it.

For example, to restore all files that had been deleted by the user **BOB**:

1. Sort the list by the **User** field by placing the cursor in that field on any line and pressing the **F16 (Shift-F4)** key.
2. Scroll to the first line where the **User** field has the value **BOB**.
3. Enter **2** in the **Opt** field for that line.
4. Press the **F13 (Shift-F1)** key to mark the beginning of the group.
5. Scroll to the last line where the **User** field has the value **BOB**.
6. Press the **F14 (Shift-F2)** key to mark the end of the group.
7. Press **Enter** to restore the files.
8. The **Confirm Restore Recycle Bin Files** screen appears, listing all the files deleted by **BOB**.
9. Press **Enter** to confirm restoring them.

Viewing Detected Attacks

To view a list of unresolved attacks, select **11. Work with Detected Attacks** from the **Anti-Ransomware** main menu. The **Work with Detected Attacks** screen appears.

```
Work with Detected Attacks

Type options, press Enter.          Include history  Y  Y=Yes, N=No
4=Remove          █ = Active Attack  Subset . . . .  _____

Opt  Time                User      Mode   IP Address
2020-10-14-14.53.00  VVM      *REAL  1.1.1.129
2020-10-12-15.44.49  YOEL     *REAL  1.1.1.195
2020-10-12-15.44.32  YOEL     *REAL  1.1.1.195
2020-10-12-14.44.50  YOEL     *REAL  1.1.1.195
2020-10-12-14.38.59  YOEL     *REAL  1.1.1.195
2020-10-12-14.37.20  YOEL     *REAL  1.1.1.195
2020-10-12-14.35.18  YOEL     *REAL  1.1.1.195
2020-10-12-14.33.21  YOEL     *REAL  1.1.1.195
2020-10-12-14.31.02  YOEL     *REAL  1.1.1.195
2020-10-12-14.25.54  YOEL     *REAL  1.1.1.195
2020-10-12-12.23.00  VVM      *REAL  1.1.1.129
2020-10-12-12.18.39  VVM      *REAL  1.1.1.129
2020-10-12-12.15.19  VVM      *REAL  1.1.1.129

*** Attacks must be deleted to restore normal activity.
F3=Exit

More...
```

The body of the screen contains lines for each unresolved attack. Each line includes the fields:

Time

The date and time at which the attack occurred.

User

The user under whose login the attack occurred.

Product Status

The mode in which Anti-Ransomware was running at the type.

Possible values are:

- ***REAL**: Fully operational
- ***FYI**: Simulation mode, in which Anti-Ransomware logs events and actions that it would take in response without performing them.

IP Address

The IP address that was the source of the attack.

To **delete an attack listing**, enter **4** in the **Opt** field for that item. Press **Enter** to confirm the deletion or the **F3** key to exit that screen.