McAfee Ransomware Interceptor

Introduction

McAfee Ransomware Interceptor[1] is an Anti-Ransomware tool. Ransomware malware has evolved to be a tremendous threat over the last few years. Such malware will install on your system, encrypt or damage data on your system in a way, which in many cases is irrecoverable unless you have a decryption key. Consumers may have to pay the malware authors hefty amounts of money (varies from a few 100 to a 1000 USD) for to obtain the key. Failure to do so typically results in permanent loss of data.

Interceptor, is an early detection tool that tries to prevent file encryption attempts by ransomware malware.

Installer Details

Interceptor comes with 2 installers:

1.) x86 or 32 bit version for installing MRI on 32 bit OSes.
2.) x64 or 64 bit version for installing MRI on 64 bit OSes.

Please utilize the appropriate installer for your target OS.

NOTE: Please review KB87658 If HIPS 8.0 Patch 5, 6, or 7 are installed in your environment. It is advised not to install this product until you have read and understood this Knowledge Base Article.

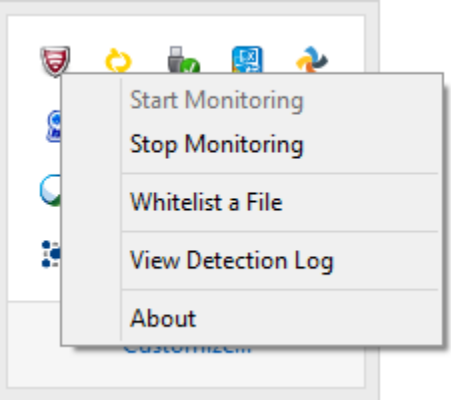
Once the install process is complete, a reboot is recommended. MRI will be visible via a TaskBar Icon  . The *Interceptor* process is named "McAfeeRansomwareInterceptorWin32.exe".

The installer also includes a built-in Uninstaller. The same installer when run again post installation, gives the user the option to uninstall the software. Additionally, users can navigate through Windows Uninstallation menu to remove this tool.

[1] McAfee Ransomware Interceptor will hereon be referred to as *Interceptor* or MRI for short, throughout the document.

The Interceptor TaskBar Menu

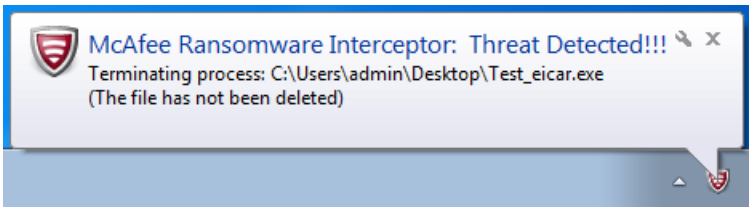
Menu items exist when the user right clicks on the Task Bar icon

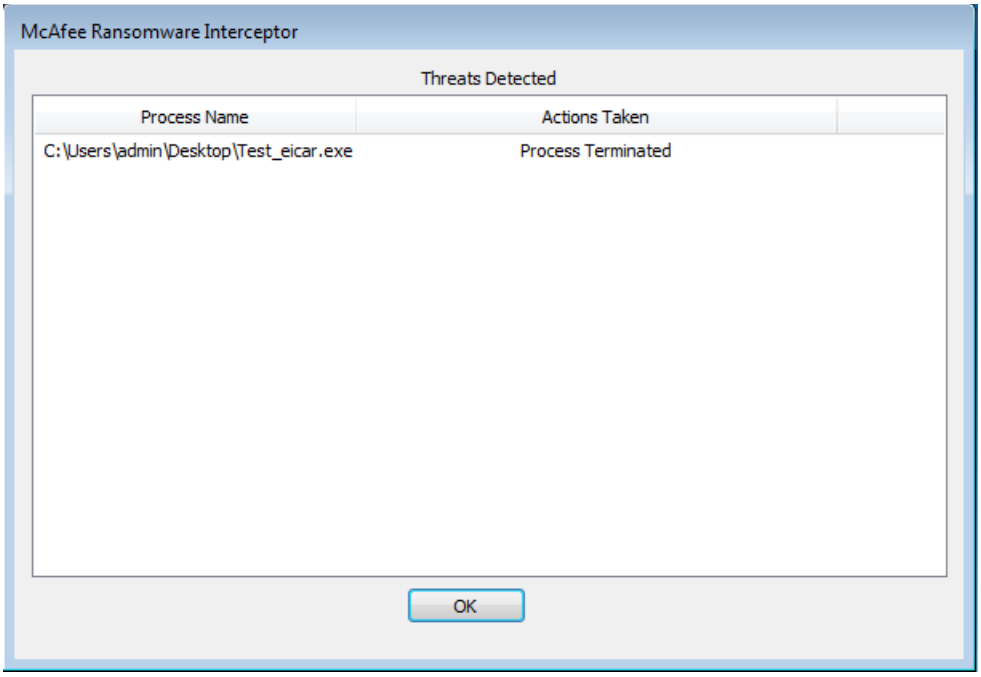


1.) **Start/Stop Monitoring:** This gives the user control to enable/disable monitoring of the entire system by this tool
2.) **Whitelist a File:** This option allows users to add files to a whitelist. This option gives users control to disable monitoring of specific files/processes.
NOTE: Once a file is whitelisted, it cannot be removed from the whitelist. Please use this cautiously such as in cases of misdetection. *Interceptor* is usually smart enough to identify clean processes automatically.
3.) **View Detection Log:** This option allows a user to view the log containing prior detections.
4.) **About:** Provides details about this tool

Detection & Logging

Detections are made visible via a Balloon pop up and a detection window as shown below:





Additionally, detections are logged in "MRIProtectionLog.txt". This file can be viewed at any time via the Taskbar menu, "View Detection Log".

On detection, we only terminate the offending process. We do not delete them. This provides customers more control of their environment.

Supported Operating Systems

Interceptor is recommended to be run on any Windows Operating systems Windows 7 and later.

Disclaimer

1. *Interceptor* is currently in pilot. It is always advisable to try any new tool on non-critical end points first, to ensure it does not cause any unanticipated negative issues in your specific environment.
2. Unlike some of our other free tools such as Real Protect and Stinger, this is not expected to be an exhaustive generic malware tool. The tool however has features to assist our customers detect more than just ransomware.
3. Like most tools, there may be certain limitation in our tool and its ability to detect. We are aware of these and continually strive to improve our tools and their detection. If you have any recommendations for our tool, please feel free to post them to our community page.
4. We have consciously tried to ensure that this product is usable, performant and has no quality issues, however this is a pilot, and we expect occasional issues.
5. This is not a static detection tool.
6. This tool does generate some network traffic. We however, do not gather any user or system specific information. Internet connectivity is recommended for added protection.
7. From time to time, you may need to update the tool. It is recommended that you uninstall the previous version prior to installing any new build.

Ransomware Specific Information

McAfee regularly publishes documentation around various Ransomware families providing detailed Threat Advisories containing behavioral information, Indicators of Compromise (IOC), mitigation techniques etc. This information can be leveraged by end users for identification and remediation of different ransomware infections. The following are some useful links for end-users:

1.) Users can access McAfee's documentation related to Ransomware by visiting the McAfee Service Portal.
    a. Search for advisories by searching, "Threat Advisories". Examples are:
        i. Ransomware-Locky
        ii. TeslaCrypt
        iii. Combatting Ransomware
    b. Select "Knowledge Center" for Knowledge Base Articles
2.) McAfee Ransomware Interceptor related feedback can be provided via our Community Page