



Inside Technologies

Guide for System Center Management Pack to Detect CryptoLocker

Silvio Di Benedetto

Published: April 3rd, 2015

Modified: January 1st, 2017

Send feedback or suggestions about this document to <http://www.insidetechnologies.eu>

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

Microsoft, Active Directory, Windows, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

Guide History	4
Getting started	4
Supported Configurations	4
Prerequisites	4
Management Pack Scope	5
How Works	5
What kind of Extension?	5
Before Start	5
Deployment	4
Setup	4
Configuration	7
Dashboard	9
Resolution Actions	11
Appendix: Known Issues and Release Notes	12

Guide for System Center Management Pack to Detect CryptoLocker

This guide was written based on version 1.0.0.0 of Inside Technologies - Detect CryptoLocker.

Guide History

Release Date	Changes
April 3 rd , 2015	First release
January 1 st , 2017	Revision 1.1

Getting Started

In this section:

[Supported Configurations](#)

[Prerequisites](#)

[Scope](#)

[How Works](#)

[What Kind of Extension?](#)

[Before Start](#)

Supported Configurations

This Management Pack is designed for the following versions of System Center Operations Manager:

- System Center Operations Manager 2012 R2 UR5
- System Center Operations Manager 2016

Prerequisites

As a best practice, you should import the Windows Server Management Pack for the operating system you are using.

Scope

CryptoLocker is a virus that encrypt all of your files with a hard key locker. Targets are Office docs, images, pdf and videos. The only way to rescue your documents is pay to receive the unlock key but this is not suggested.

When a user run the virus, all files into mapped drive are locked.

With Detect CryptoLocker Management Pack you can prevent this behavior for all Windows Server with File Server role enabled into share folders.

How Works

If your File Server has a file with a potential risk extension, the automatic recovery task will stop three important services of File Server to avoid the total loss of data.

Server: this service manages File & Printing Sharing role. This service will be stopped to block files encryption.

DFS: this service manages DFS Namespace. This service will be stopped to because there's dependencies with Server service.

DFS: this service manage replica between servers. This service will be stopped to avoid the replica of bad files.

What Kind of Extension?

The extension under monitor are: *.cryptolocker, .encrypted, .ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .locked, .crypto_crypt, .crinf, .r5a, .xrnt, .xtbl, .crypt, .r16m01d05, .pzdc, .good, .lol!, .omg!, .rdm, .rrk, .encryptedrsa, .crjoker, .enciphered, .lechiffre, .keybtc@inbox_com, .0x0, .bleep, .1999, .vault, .ha3, .toxencrypt, .magic, .supercrypt, .ctbl, .ctb2.*

These are the most important format. For your information there are many others type of virus that use random extension, this means that is not possible detect all the critical extensions.

Before Start

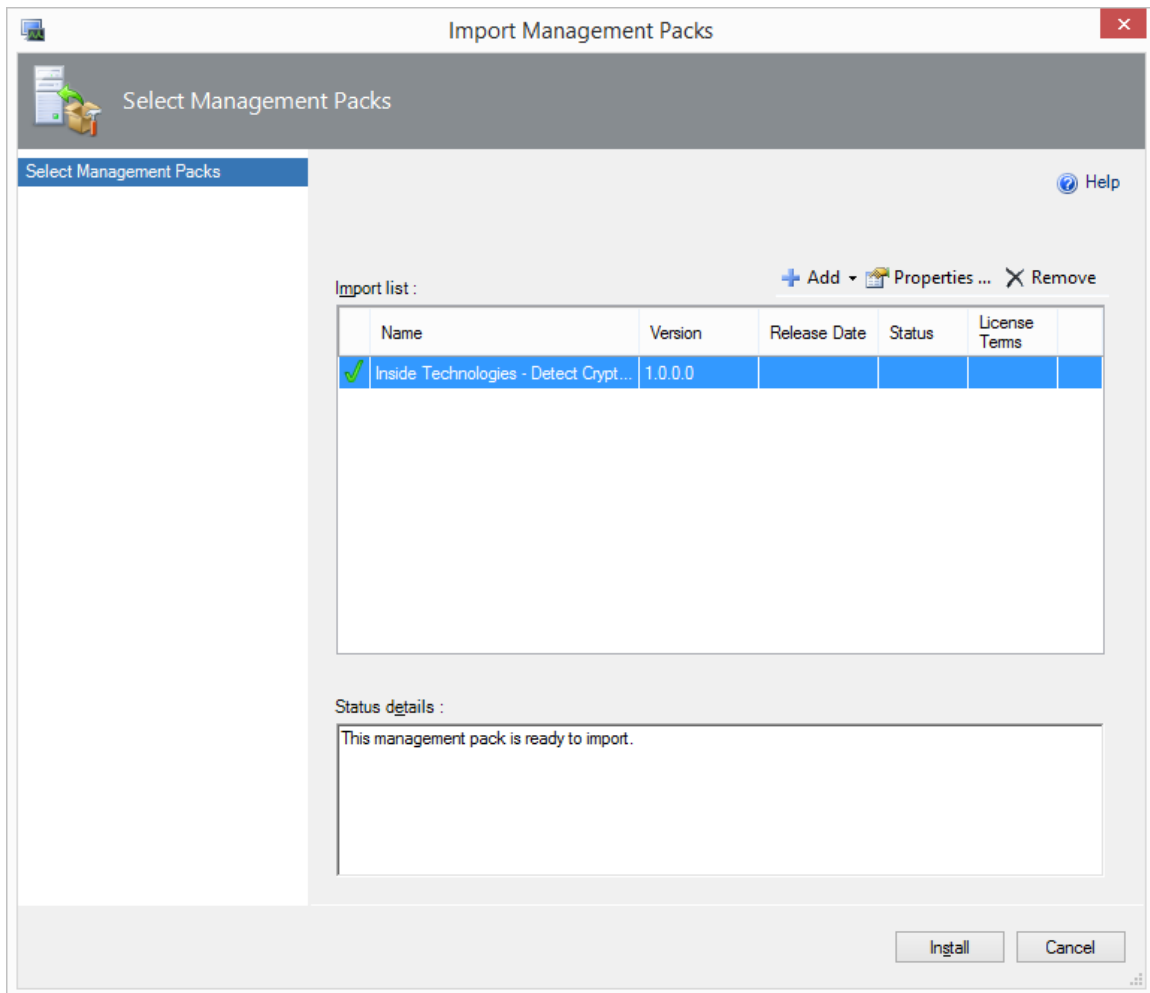
Detect CryptoLocker MP is not an antivirus and cannot delete corrupted files. Cannot be guarantee a faster detect prevention, in particular case if File Server is very large.

The MP owner is not responsible of any kind of data loss or other issues.

Deployment

Setup

Download the MP and import it into your Operations Manager







Configuration

Enable Object Discovery

This Management Pack is disabled by default. To enable server discovery is follow these list, into each servers that you want monitor:

- Open Registry
- Create a new key called **Inside Technologies** into HKLM\Software
- Create a new DWORD32 called **CryptoLockerEnabledMonitor** with value 1 to disable monitoring, change the value to 0 or remove DWORD.

Detection is every 3600 seconds. All the servers are included into a Group called **IT - CryptoLocker Monitoring Server Group**. When the objects are discovered you will see them with the View Group Members.

Managed Objects (2)			
Name	Health State	Path	Types
 SRV-FPD01.insidetechologies.lcl	 Healthy		Windows Server 2012 R2 Full Computer
 Azure-fs01.insidetechologies.lcl	 Healthy		Windows Server 2012 R2 Full Computer

Enable Monitor Rule

When the server is discovered it will be possible enable the Monitor Unit from Monitors view. Find the Detect CryptoLocker monitor into Windows Server scope and override the rule for the group **IT - CryptoLocker Monitoring Server Group**.

Target	Type	Inherited From	Management Pack	Enabled by Default
IT - CryptoLocker Monitoring Server Group				
Entity Health	Aggregate Rollup	Object	Health Library	Yes
Availability	Aggregate Rollup	Object	Health Library	Yes
Configuration	Aggregate Rollup	Object	Health Library	Yes
Performance	Aggregate Rollup	Object	Health Library	Yes
Security	Aggregate Rollup	Object	Health Library	Yes
Detect CryptoLocker	Timed Script Two S...	(Not inherited)	Inside Technologies - Detect CryptoLo...	No

Override Properties

Monitor name:

Detect CryptoLocker

Category:

Custom

Overrides target:

Group: IT - CryptoLocker Monitoring Server Group

Show Monitor Properties...

Override-controlled parameters:

	Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
	<input type="checkbox"/>	Alert severity	Enumeration	Critical	Critical	Critical	[No change]
	<input type="checkbox"/>	Auto-Resolve Alert	Boolean	True	True	True	[No change]
▶	<input checked="" type="checkbox"/>	Enabled	Boolean	False	True	False	[Added]
	<input type="checkbox"/>	Generates Alert	Boolean	True	True	True	[No change]
	<input type="checkbox"/>	Interval in seconds	Integer	300	300	300	[No change]
	<input type="checkbox"/>	Script Arguments	String				[No change]
	<input type="checkbox"/>	Time at which to st...	String				[No change]
	<input type="checkbox"/>	Timeout Seconds	Integer	60	60	60	[No change]

Details:

From here it's also possible change the execution time (by default the script running every 5 minutes).

Dashboard

Management Pack contains a view folder into Monitoring pane, called Inside Technologies – Detect CryptoLocker MP.

Inside Technologies - Detect CryptoLocker

Dashboard

Alerts View

Filter

Severity	Source	Maintenance Mode	Name	Age	Rep
----------	--------	------------------	------	-----	-----

State View (2)

Filter

Health	Display Name	Path
✓	Azure-fs01.insidetechnologies.lcl	
✓	SRV-FPD01.insidetechnologies.lcl	

Alert Details

Select an item to display its details

Dashboard gives you a view about all the critical new alerts of all servers into **IT - CryptoLocker Monitoring Server Group**, with the possibility to see the details of objects.

When a file with a potential extension will be detected, the MP will show a message error.

Alerts View (8)

Filter			
Severity	Source	Maintenance	
	SRV-FPD01 (SMB)		
	Microsoft Windows Server 2012 R2 Datacenter		
	SRV-FPD01		
	Azure-fs01 (SMB)		
	Azure-fs01		
	Microsoft Windows Server 2012 R2 Datacenter		
	Azure-fs01.insidetechnologies.lcl		
	SRV-FPD01.insidetechnologies.lcl		

State View (2)

Filter			
Health	Display Name	Path	
	Azure-fs01.insidetechnologies.lcl		
	SRV-FPD01.insidetechnologies.lcl		

Alert Details

Description	Server with Issue: SRV-FPD01.insidetechnologies.lcl Active Directory OU: OU=Server,OU=Milano,DC=insidetechnologies,DC=lcl Infected Item Detected: 2
Source	SRV-FPD01.insidetechnologies.lcl
Path	
Monitor	Detect CryptoLocker
Created	4/3/2015 9:07:10 AM

Resolution Actions

The Management Pack doesn't remove the infected items so the IT Admin must do it! After cleaning it will allowed restart the services:

- DFS Namespace
- DFS Replica
- Server

Appendix: Known Issues and Release Notes

Extensions

If you discover a new standard extension, send us a feedback from module into my web site.

Performance

Make a test before implement the MP in production. Continuous item's discovery could reduce the performance of File Server. If there are too many files could be better grow the Execution Time.