Cryptolocker Canary - detect it early!

by JustinCredible on Nov 21, 2014 at 11:32am

Introduction

I thought I'd share with you what steps I've taken to alert me to a likely Cryptolocker infection.

Generally, if someone gets a virus on their computer it's a pain in the ass but it's not threatening to the company on the whole. The computer is isolated and reinstalled or otherwise cleaned up, and you're off again.

With Cryptolocker, 9 times out of 10 the person seems to also have a link to at least one network share. Because it's encrypting everything it can (not -infecting- everything, just encrypting), it will go out to those shares and do it's thing.

Now, if you're familiar with this, hopefully not first hand, you'll know they drop two files in every folder with encrypted files - INSTALL_TOR.txt and DECRYPT_INSTRUCTION.txt. You can use this to your advantage as a sort of 'early warning system'. This works on Server 2008+, don't know what facilities exist for this for earlier or different OS's.

EDIT: I guess I should mention it's a good way to quickly tell who the culprit is, if it's useful for nothing other than that.

DOUBLE EDIT: Updated Jan 7/2015 with clearer instructions and screenshots

EDIT AGAIN: Updated Jan 29/2015 to add help_decrypt*.* to the file screen, thanks go to +blefler for that!

C-C-C-C-C-COMBO EDIT: March 19/2015 With the release of new cryptolocker-like variants, they've taken to dropping randomly named files into the encrypted folders, making this method useless against those variants. Just FYI!

KEEP ON EDITING: August 19/2015 Added additional filenames that a new variant is using (restore_Flies*.*, *djqfu*.*, *.aaa). Thanks to +Mconn for the heads up: http://community.spiceworks.com/topic/1135679-new-trojan-crypto-virus

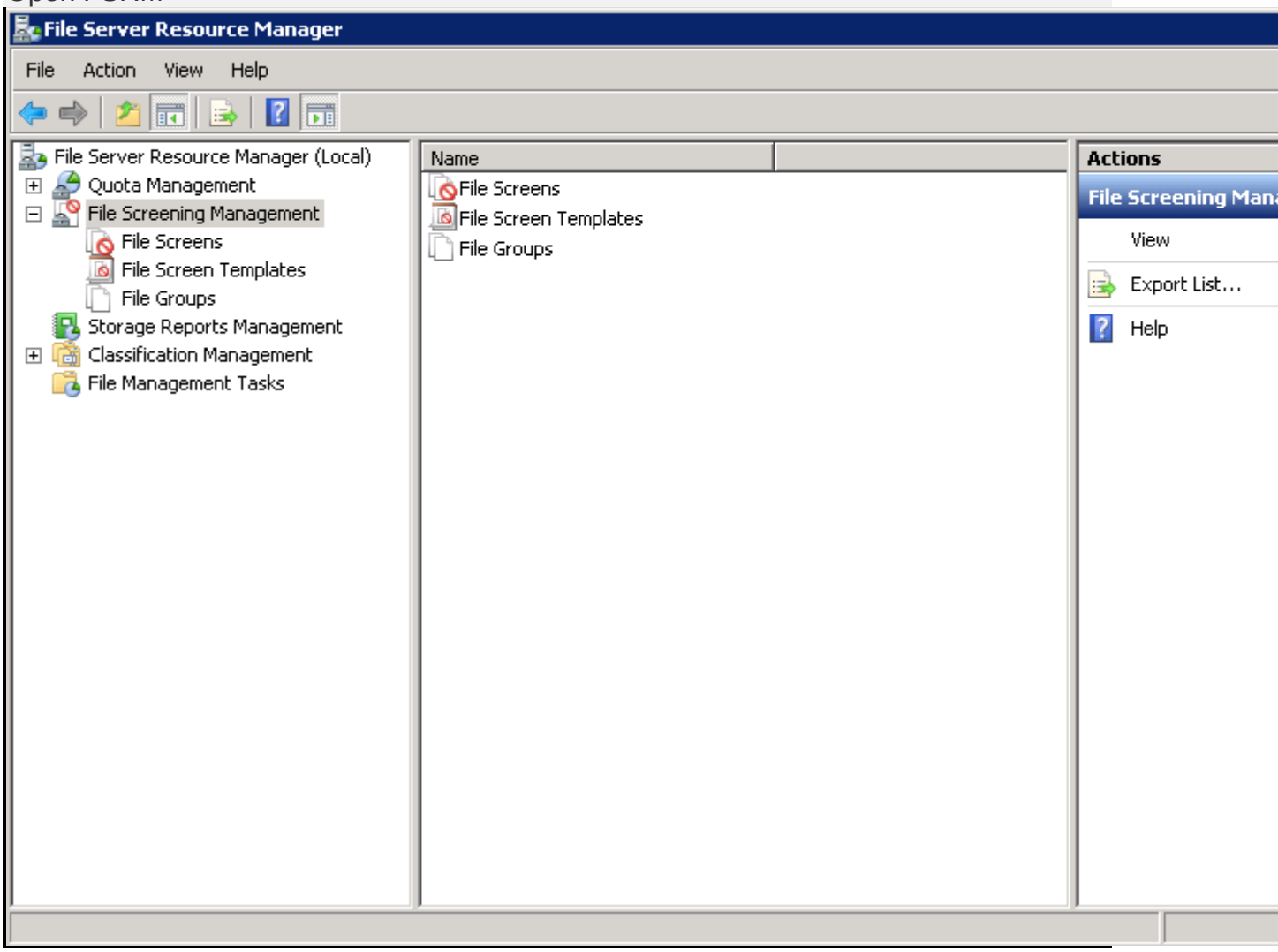
NEVER STOP EDITING: November 5, 2015 Added additional filenames that Cryptowall 4.0 uses (help_your_files*.*) Thanks to +Lawrence Abrams for the heads up: http://community.spiceworks.com/topic/1274312-cryptowall-v4-0-released-now-encrypts-the-file-names-as-well

MORE EDIT!: February 16, 2016 Added additional filenames various crypto infections use. Credit goes to quietman7 at bleepingcomputer and Jaymesned at Reddit.

Steps (8 total)

1

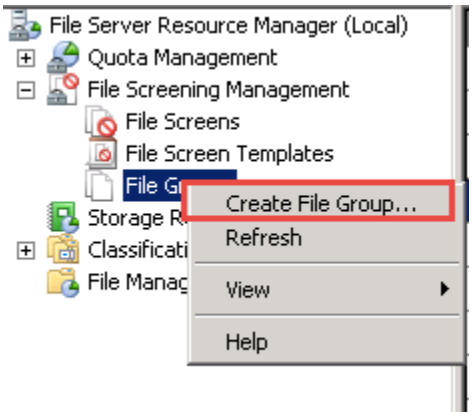
Open FSRM



Open up File Server Resource Manager. (or Win key + R , fsrm.msc)

2

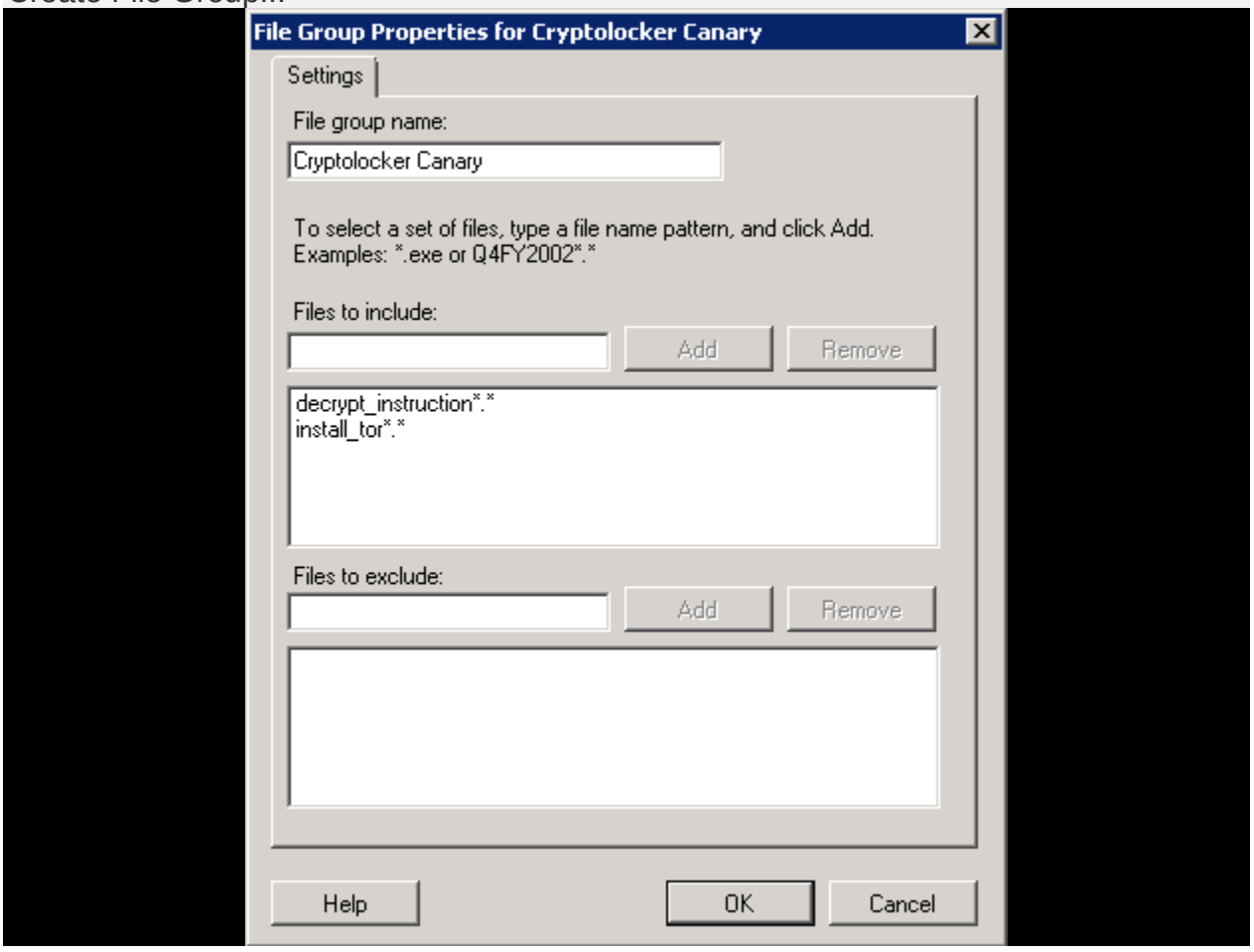
Create File Group



Right click on File Groups under File Screening Management on the left and choose "Create File Group..."

3

Create File Group...



Call it "Cryptolocker Canary"
Under files to include:
*.ecc

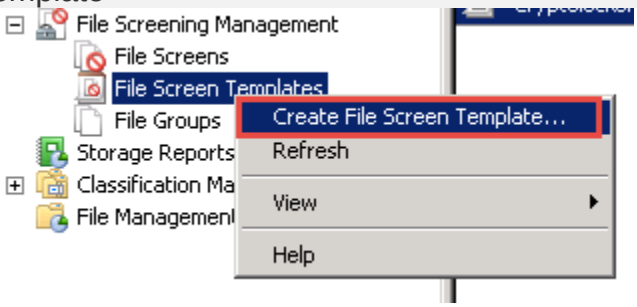
*.ezz
*.exx
*.zzz
*.xyz
*.aaa
*.abc
*.ccc
*.vvv
*.xxx
*.ttt
*.micro
*.encrypted
*.locked
*.crypto
_crypt
*.crinf
*.r5a
*.XRNT
*.XTBL
*.crypt
*.R16M01D05
*.pzdc
*.good
*.LOL!
*.OMG!
*.RDM
*.RRK
*.encryptedRSA
*.crjoker
*.EnCiPhErEd
*.LeChiffre
*.keybtc@inbox_com
*.0x0
*.bleep
*.1999
*.vault
*.HA3
*.toxcrypt
*.magic
*.SUPERCRYPT
*.CTBL
*.CTB2
*.locky
HELPDECRYPT.TXT
HELP_YOUR_FILES.TXT
HELP_TO_DECRYPT_YOUR_FILES.txt
RECOVERY_KEY.txt
HELP_RESTORE_FILES.txt

HELP_RECOVER_FILES.txt
HELP_TO_SAVE_FILES.txt
DecryptAllFiles.txt
DECRYPT_INSTRUCTIONS.TXT
INSTRUCCIONES_DESCIFRADO.TXT
How_To_Recover_Files.txt
YOUR_FILES.HTML
YOUR_FILES.url
encryptor_raas_readme_liesmich.txt
Help_Decrypt.txt
DECRYPT_INSTRUCTION.TXT
HOW_TO_DECRYPT_FILES.TXT
ReadDecryptFilesHere.txt
Coin.Locker.txt
_secret_code.txt
About_Files.txt
Read.txt
ReadMe.txt
DECRYPT_ReadMe.TXT
DecryptAllFiles.txt
FILESAREGONE.TXT
IAMREADYTOPAY.TXT
HELLOTHERE.TXT
READTHISNOW!!!.TXT
SECRETIDHERE.KEY
IHAVEYOURSECRET.KEY
SECRET.KEY
HELPDECYPRT_YOUR_FILES.HTML
help_decrypt_your_files.html
HELP_TO_SAVE_FILES.txt
RECOVERY_FILES.txt
RECOVERY_FILE.TXT
RECOVERY_FILE*.txt
HowtoRESTORE_FILES.txt
HowtoRestore_FILES.txt
howto_recover_file.txt
restorefiles.txt
howrecover+*.txt
_how_recover.txt
recoveryfile*.txt
recoverfile*.txt
recoveryfile*.txt
Howto_Restore_FILES.TXT
help_recover_instructions+*.txt
_Locky_recover_instructions.txt

click OK

4

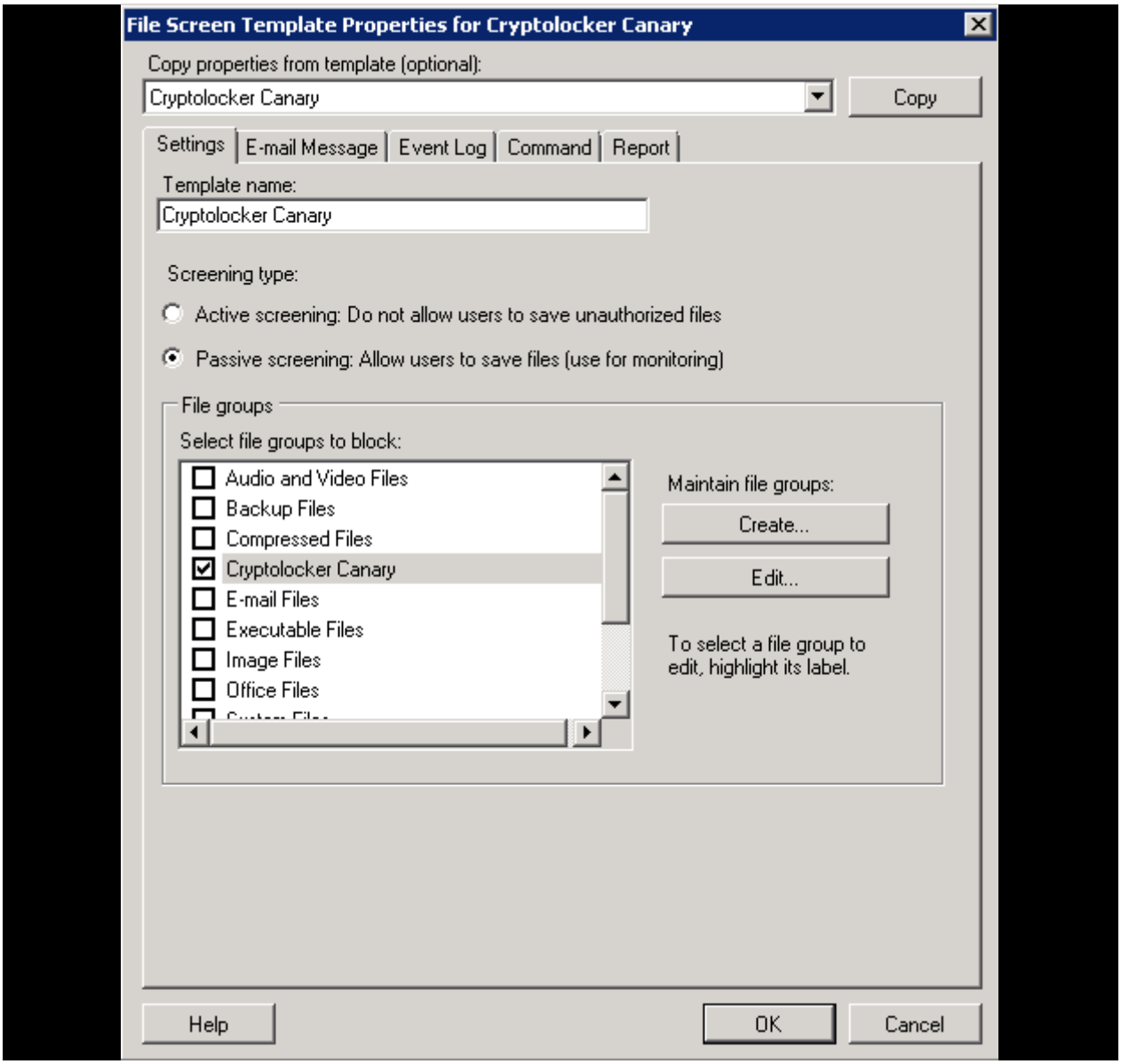
Create File Screen Template



Right click on File Screen Templates on the left and choose "Create File Screen Template..."

5

Create File Screen Template...



Call it "Cryptolocker Canary"

Set it up as PASSIVE screening. You want the file to be saved - it's a harmless txt file, and it allows you to search for all instances of it and know which folders have been affected.

Under File groups, choose Cryptolocker Canary.

Under the E-mail Message tab, check the option to send a message and enter your email. Also check the option to send an email to the user who generated the violation.

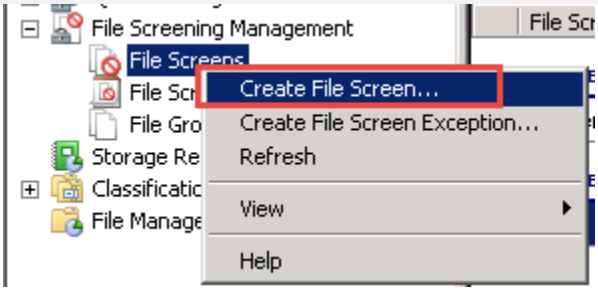
For my Subject, I wrote: "POSSIBLE VIRUS INFECTION DETECTED"
For the body I wrote:

"User [Source Io Owner] attempted to save [Source File Path] to [File Screen Path] on the [Server] server.

This file indicates that the file server is in the process of being encrypted by a virus. If you are [Source Io Owner] please shut down any computers you are using IMMEDIATELY and notify IT at 123-456-7890 orhelpdesk@domain.com"

6

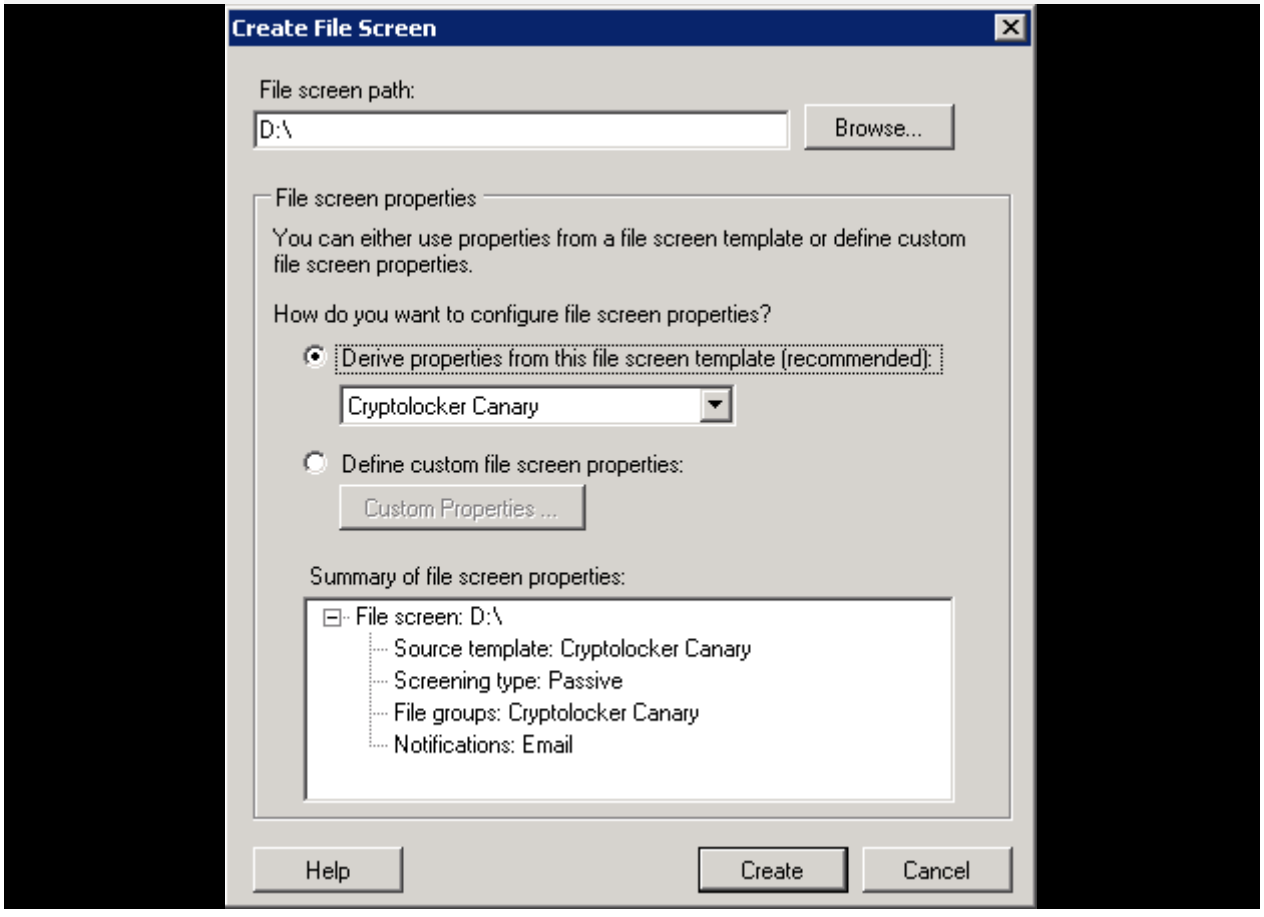
Create File Screen



Right click on File Screens on the left and choose "Create File Screen..."

7

Create File Screen...



Choose the path you want to 'protect', and choose "Derive properties from this file screen template" and select your Cryptolocker Canary template from the list and click Create.

8

Remediation

Once their system is offline it can't harm anything and it's time for remediation.

Wipe the infected machines and reinstall. No two ways about it. You don't want Cryptolocker lingering at all.

To figure out what's encrypted, do a search of your file server for the files and extensions mentioned in Step 3, make note of the resulting folders. You'll want to restore those.

If you have Shadow Copies turned on for your file server (I highly recommend it), it can make restoring your data that much faster - choose the latest point and click Restore.

I should note, we were able to identify the user that was infected because their personal network share was encrypted - nobody else's. That's a dead giveaway.

If you don't have Shadow Copies set up, then it's off to your backups - you do have those, right?

Conclusion

In the end, it's not going to stop the infection, but it will warn you hopefully early enough that you have to restore very little data to your network shares. The infected machine is most likely completely encrypted at this point, but it's a great way to "protect the herd" from one bad apple.

Thanks Ian S for the link to configuring Exchange
Thanks to +Mconn for the heads up on the latest variant at
http://community.spiceworks.com/topic/1135679-new-trojan-crypto-virus

Big thanks to Jaymesned over at reddit for his compilation
https://www.reddit.com/r/sysadmin/comments/46361k/list_of_ransomware_extensions_and_known_ransom/ which was copied from quietman7 at bleepingcomputer
http://www.bleepingcomputer.com/forums/t/605116/im-hit-with-a-cryptolocker-virus/

References

- Reddit
- Bleeping Computer
- New Trojan Crypto Virus
- Configure E-Mail Notifications for FSRM
- Configuring Exchange to accept FSRM E-Mails