SHI – CUSTOMER ASSISTANCE

# Ransomware Response Guide

May 27, 2016

*** NOTE ** SHI makes no guarantees or warranties regarding the use of any of the procedures or approaches linked below. They are provided solely as possible approaches to helping organizations deal with the challenges of ransomware. Any of the following steps should be tested and confirmed viable prior to deployment.*

## 1. Purpose

With the continued impact of ransomware variations throughout the world, SHI has created the following list of recommendations and reference links to assist our customers in completing many of the stages of IT incident response:

## d. If you can obtain a malware file, use Virustotal to identify security vendors that detect it

https://www.virustotal.com/

Additionally, if you identify any files associated with the malware, submit them to your endpoint protection vendor for inclusion in the next signature update.

http://www.bitdefender.com/submit/
https://newvirus.kaspersky.com/
http://www.mcafee.com/us/threat-center/resources/how-to-submit-sample.aspx
https://www.sophos.com/en-us/support/knowledgebase/11490.aspx
https://ers.trendmicro.com/guide/en_us/AG/Help/Sending_Suspicious_Files_to_Trend_Micro.htm
https://www.symantec.com/security_response/submitsamples.jsp

Any vendor who sees it as a piece of malware may have a free system scan/cleanup tool that you can use.

http://www.bleepingcomputer.com/download/malwarebytes-anti-ransomware/
https://www.f-secure.com/en/web/labs_global/rescue-cd
https://support.kaspersky.com/viruses/utility?CID=acq-freekasp-USA&_ga=1.28634549.802189490.1459266584
https://www.malwarebytes.org/antimalware/
http://www.mcafee.com/us/downloads/free-tools/stinger.aspx
https://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx
https://www.trendmicro.com/vinfo/us/security/definition/Ransomware

## e. Executable may exist in %appdata% or other locations. Some typical locations include

C:\Users\USERNAME\AppData\
C:\Users\USERNAME\AppData\Local\Temp\

## f. Block programs from running in appdata. There is generally a limited requirement for this.

http://www.fatdex.net/php/2014/06/01/disable-exes-from-running-inside-any-user-appdata-directory-gpo/

Computer Configuration > Policies > Windows Settings > Security Settings > Software Restriction Policies

Set the security level to Disallowed, Allow these in "Additional Rules" then add any application paths outside of Program Files that employees will require (network locations, etc.).

If you just want to blacklist, set the default level to Unrestricted and disallow %USERPROFILE%\Appdata

Whitelist *.lnk or start menu shortcuts will not work.

Define Software Restriction Policies that keep executable files from running when they are in specific locations in the system.

The directories most heavily used for hosting malicious processes include ProgramData, AppData, Temp and Windows\SysWow.

## g. Consider the use of AppLocker to restrict applications and permitted locations

https://4sysops.com/archives/applocker-tutorial-part-1-planning/

## h. Consider disabling vssadmin.exe

This service built into Windows to administer Volume Shadow Copy Service is normally used for restoring previous versions of files. In the framework of rapidly evolving file-encrypting malware, vssadmin.exe can be a problem rather than a useful service.

If it is disabled on a computer at the time of a compromise, ransomware will fail to use it for deleting the shadow volume snapshots. This means you can use VSS to restore the encrypted files after an incident.

## i. Consider the use of file and critical server event auditing

http://www.eventsentry.com/blog/2016/03/defeating-ransomware-with-eventsentry-auditing.html

## j. Restrict elevated privileges

Delegation of elevated privileges such as local administrator or domain administrator should be restricted. Additionally, common IT administrators should use a standard user as well as administrative account in the performance of their responsibilities.

## k. Disallow regedit.exe and runas.exe

Where possible, regedit and runas executables can be restricted to prevent those users with administrative privileges from modifying their systems during an infection event.

## l. Enable geo-blocking

Next generation firewalls enable you to block communications with countries that your organization generally should not be interacting with. This should be done carefully to prevent accidentally blocking channels to systems like software update servers.

## m. Examine web and email content filters

Ensure that perimeter gateway filters are configured to block common attachment types that lead to infection by default such as PDF, EXE and other types except when a defined business case has been defined. This is a challenging control to have in place as malware distributors can use file types as common as Microsoft Word documents to distribute malware.

## n. Enable perimeter and cloud sandbox controls

Examine your existing perimeter and cloud controls to see if they have functionality for performing sandboxing – a process by which files are examined for malware content prior to their delivery to a user.

## o. DNS Blackholes

Organizations should also consider the use of DNS blackholes to stop communication with command and control servers or malicious payload distribution points.

https://zeltser.com/malicious-ip-blocklists/

## p. Operating system and third-party patching

Every endpoint should be patched with the latest updates – particularly third-party software packages such as Oracle Java, Adobe Flash, Adobe Acrobat, etc.

## q. Canary indicators using File Server Resource Manager or Microsoft SCCM assistance

Create canary systems by identifying the key indicators you have identified on infected systems and use existing infrastructure such as Microsoft SCCM to search these systems for file types that are indicative of ransomware such as:

| | | | |
|---|---|---|---|
| .ecc | .micro | .pzdc | .0x0 |
| .ezz | .encrypted | .good | .bleep |
| .exx | .locked | .LOL! | 0.1999 |
| .zzz | .crypto | .OMG! | .vault |
| .xyz | _crypt | .RDM | .HA3 |
| .aaa | .crinf | .RRK | .toxcrypt |
| .abc | .r5a | .encryptedRSA | .magic |
| .ccc | .XRNT | .crjoker | .SUPERCRYPT |
| .vvv | .XTBL | .EnCiPhErEd | .CTBL |
| .xxx | .crypt | .LeChiffre | .CTB2 |
| .ttt | .R16M01D05 | | .locky |

- 6-7 length extension consisting of random characters

https://community.spiceworks.com/how_to/100368-cryptolocker-canary-detect-it-early

http://blogs.technet.com/b/scotts-it-blog/archive/2015/01/03/the-basics-of-client-inventory-in-system-center-configuration-manager-2012.aspx

https://social.technet.microsoft.com/Forums/systemcenter/en-US/a63befd9-4df5-4cf5-9576-68fa3796cc6c/search-for-video-pics-music-files-on-sccm-via-reporting?forum=configmgrgeneral

## r. Powershell assistance

Powershell can be used to rapidly search your network for either the above files or registry entries that indicate infection even if you endpoint protection control has not triggered.

https://blogs.technet.microsoft.com/heyscriptingguy/2012/03/18/use-powershell-to-find-and-remove-remote-registry-entries/

http://robwillis.info/2012/03/powershell-remote-file-query/