AntiRansomware Tools Thoroughly Tested Part 5

Information Security Inc.

Contents

- What is Ransomware?
- Rise of Ransomware
- Ransomware Testing Environment
- Malwarebytes Anti-Ransomware
- References

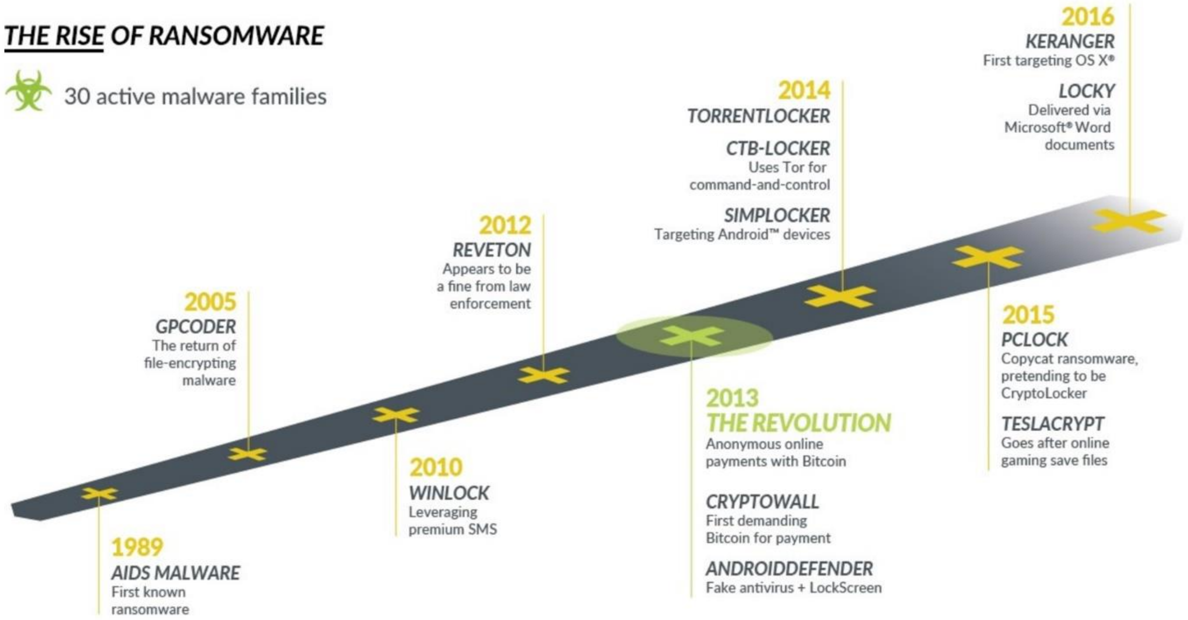
What is Ransomware?

- **Ransomware** is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid
- Ransomware is malicious code that is used by cybercriminals to launch data kidnapping and lockscreen attacks
- The motive for ransomware attacks is monetary

What is RANSOMWARE?

A type of malware that can stop you from using your PC, rename, or encrypt your files so you can't use them. You may be warned that you need to pay money, Bit-Coins, complete surveys, or perform other actions before you can use your PC again.

Rise of Ransomware



THE RISE OF RANSOMWARE

30 active malware families

1989
AIDS MALWARE
First known ransomware

2005
GPCODER
The return of file-encrypting malware

2010
WINLOCK
Leveraging premium SMS

2012
REVETON
Appears to be a fine from law enforcement

2013
THE REVOLUTION
Anonymous online payments with Bitcoin

CRYPTOWALL
First demanding Bitcoin for payment

ANDROIDDEFENDER
Fake antivirus + LockScreen

2014
TORRENTLOCKER

CTB-LOCKER
Uses Tor for command-and-control

SIMPLOCKER
Targeting Android™ devices

2015
PCLOCK
Copycat ransomware, pretending to be CryptoLocker

TESLACRYPT
Goes after online gaming save files

2016
KERANGER
First targeting OS X®

LOCKY
Delivered via Microsoft® Word documents

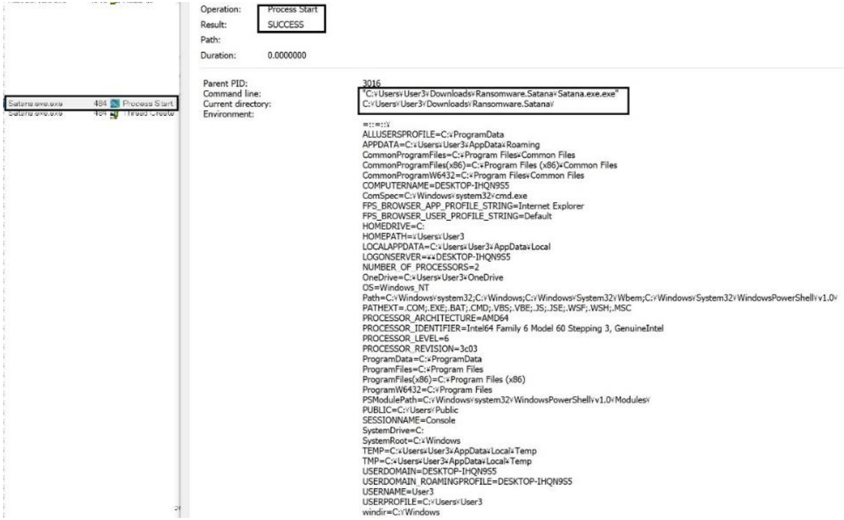
Ransomware Testing Environment

- Victim machine: Windows 10 x64
- Ransomware: Satana Ransomware (https://www.kaspersky.com/blog/satana-ransomware/12558/)

Malwarebytes Anti-Ransomware

- Information link: https://malwarebytes.app.box.com/s/6vqfgzs9ci86fbga4nt95yq5uytppg1b
- How does Malwarebytes Anti-Ransomware work?

◎ Ransomware process starts

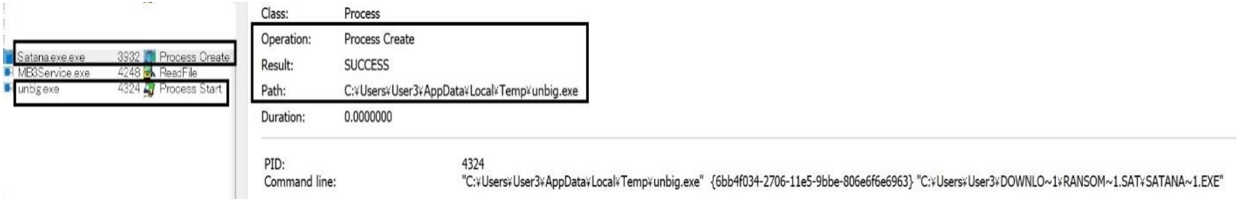


```
Satana.exe.exe    484  Process Start
Satana.exe.exe    484  Thread Create

Operation:    Process Start
Result:       SUCCESS
Path:
Duration:     0.0000000

Parent PID:          3016
Command line:        "C:¥Users¥User3¥Downloads¥Ransomware.Satana¥Satana.exe.exe"
Current directory:   C:¥Users¥User3¥Downloads¥Ransomware.Satana¥
Environment:
                     =::=::¥
                     ALLUSERSPROFILE=C:¥ProgramData
                     APPDATA=C:¥Users¥User3¥AppData¥Roaming
                     CommonProgramFiles=C:¥Program Files¥Common Files
                     CommonProgramFiles(x86)=C:¥Program Files (x86)¥Common Files
                     CommonProgramW6432=C:¥Program Files¥Common Files
                     COMPUTERNAME=DESKTOP-IHQN9S5
                     ComSpec=C:¥Windows¥system32¥cmd.exe
                     FPS_BROWSER_APP_PROFILE_STRING=Internet Explorer
                     FPS_BROWSER_USER_PROFILE_STRING=Default
                     HOMEDRIVE=C:
                     HOMEPATH=¥Users¥User3
                     LOCALAPPDATA=C:¥Users¥User3¥AppData¥Local
                     LOGONSERVER=¥¥DESKTOP-IHQN9S5
                     NUMBER_OF_PROCESSORS=2
                     OneDrive=C:¥Users¥User3¥OneDrive
                     OS=Windows_NT
                     Path=C:¥Windows¥system32;C:¥Windows;C:¥Windows¥System32¥Wbem;C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥
                     PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
                     PROCESSOR_ARCHITECTURE=AMD64
                     PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel
                     PROCESSOR_LEVEL=6
                     PROCESSOR_REVISION=3c03
                     ProgramData=C:¥ProgramData
                     ProgramFiles=C:¥Program Files
                     ProgramFiles(x86)=C:¥Program Files (x86)
                     ProgramW6432=C:¥Program Files
                     PSModulePath=C:¥Windows¥system32¥WindowsPowerShell¥v1.0¥Modules¥
                     PUBLIC=C:¥Users¥Public
                     SESSIONNAME=Console
                     SystemDrive=C:
                     SystemRoot=C:¥Windows
                     TEMP=C:¥Users¥User3¥AppData¥Local¥Temp
                     TMP=C:¥Users¥User3¥AppData¥Local¥Temp
                     USERDOMAIN=DESKTOP-IHQN9S5
                     USERDOMAIN_ROAMINGPROFILE=DESKTOP-IHQN9S5
                     USERNAME=User3
                     USERPROFILE=C:¥Users¥User3
                     windir=C:¥Windows
```

Malwarebytes Anti-Ransomware

- Information link: https://malwarebytes.app.box.com/s/6vqfgzs9ci86fbga4nt95yq5uytppg1b
- How does Malwarebytes Anti-Ransomware work?

◎ Ransomware main process spawns a child process (unbig.exe)



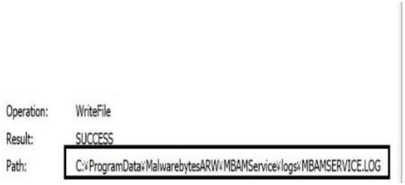
```
Satana.exe.exe   3932  Process Create
MB3Service.exe   4248  ReadFile
unbig.exe        4324  Process Start
```

```
Class:       Process
Operation:   Process Create
Result:      SUCCESS
Path:        C:¥Users¥User3¥AppData¥Local¥Temp¥unbig.exe
Duration:    0.0000000

PID:                   4324
Command line:          "C:¥Users¥User3¥AppData¥Local¥Temp¥unbig.exe"  {6bb4f034-2706-11e5-9bbe-806e6f6e6963} "C:¥Users¥User3¥DOWNLO~1¥RANSOM~1.SAT¥SATANA~1.EXE"
```

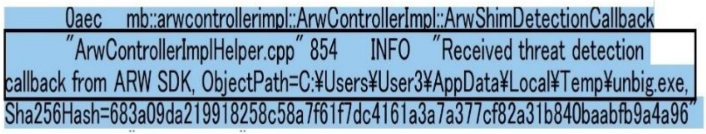
Malwarebytes Anti-Ransomware

- Information link: https://malwarebytes.app.box.com/s/6vqfgzs9ci86fbga4nt95yq5uytppg1b
- How does Malwarebytes Anti-Ransomware work?

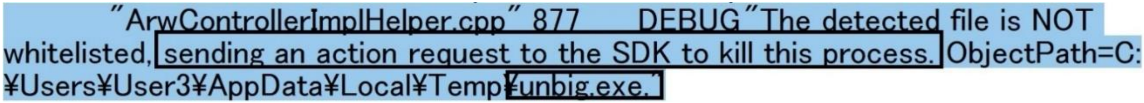
◎ Ransomware process is identified and killed by Malwarebytes Anti-Ransomware



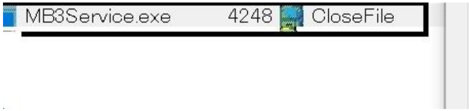
```
Operation:   WriteFile
Result:      SUCCESS
Path:        C:¥ProgramData¥MalwarebytesARW¥MBAMService¥logs¥MBAMSERVICE.LOG
```



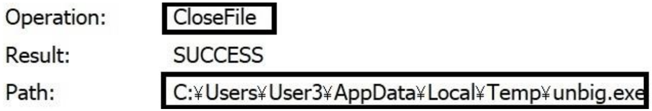
```
0aec    mb::arwcontrollerimpl::ArwControllerImpl::ArwShimDetectionCallback
 "ArwControllerImplHelper.cpp" 854    INFO   "Received threat detection
callback from ARW SDK, ObjectPath=C:¥Users¥User3¥AppData¥Local¥Temp¥unbig.exe,
Sha256Hash=683a09da219918258c58a7f61f7dc4161a3a7a377cf82a31b840baabfb9a4a96"
```



```
      "ArwControllerImplHelper.cpp" 877      DEBUG "The detected file is NOT
whitelisted, sending an action request to the SDK to kill this process. ObjectPath=C:
¥Users¥User3¥AppData¥Local¥Temp¥unbig.exe."
```



```
MB3Service.exe       4248   CloseFile
```



```
Operation:   CloseFile
Result:      SUCCESS
Path:        C:¥Users¥User3¥AppData¥Local¥Temp¥unbig.exe
```

References

- Wikipedia

https://en.wikipedia.org/wiki/Ransomware

- Knowbe

https://www.knowbe4.com/ransomware

- Heimdal security

https://heimdalsecurity.com/blog/what-is-ransomware-protection