AntiRansomware Tools Thoroughly Tested Part 3

Information Security Inc.

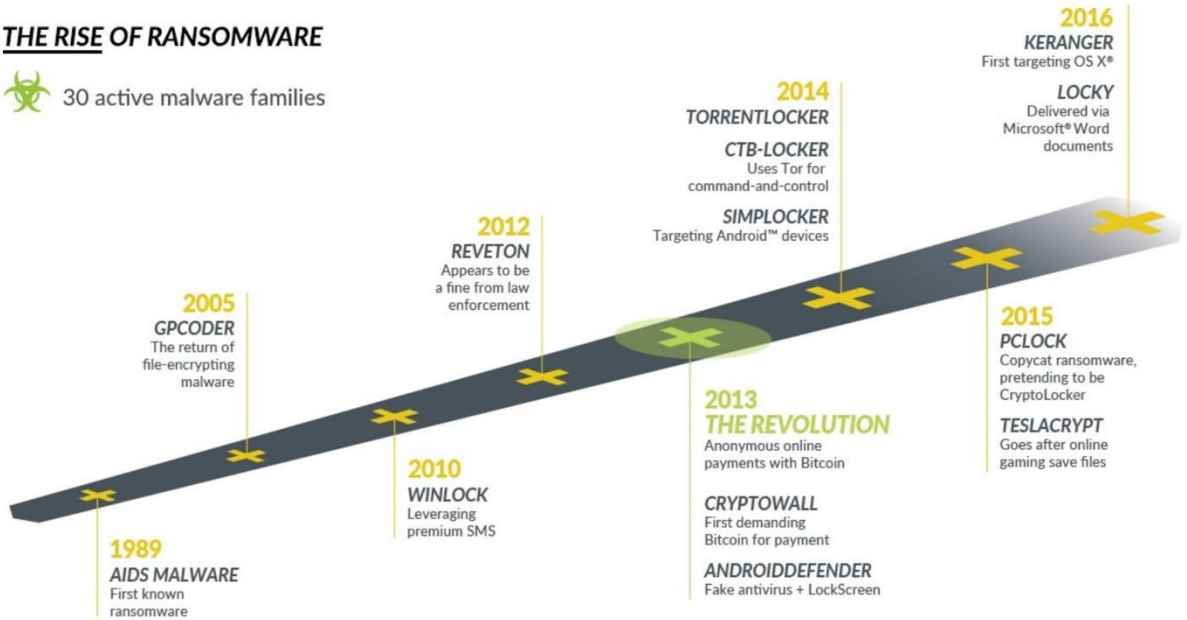
Contents

- What is Ransomware?
- Rise of Ransomware
- Ransomware Testing Environment
- McAfee Ransomware Interceptor
- 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

Rise of Ransomware



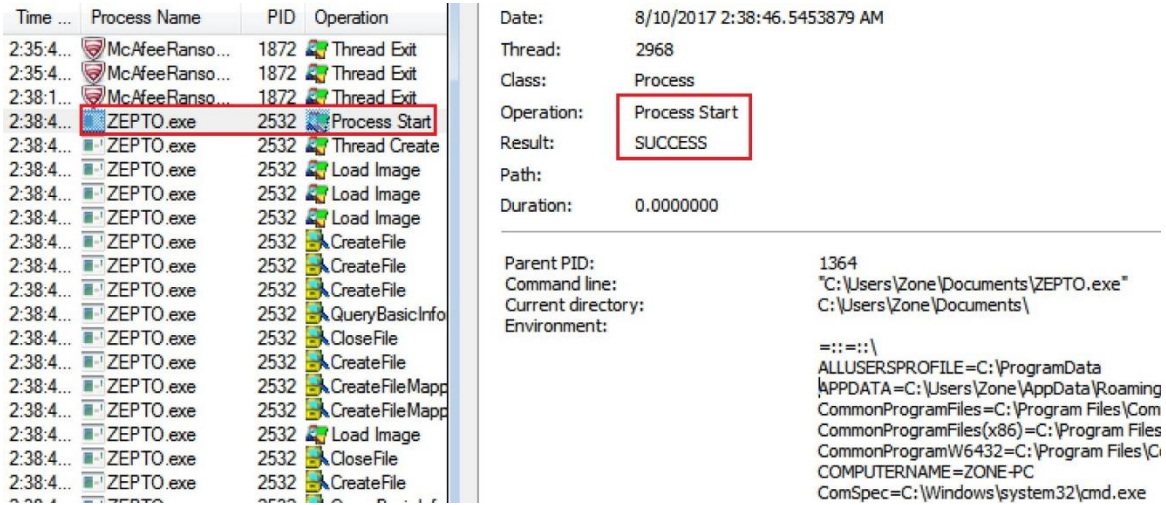
Ransomware Testing Envinronment

- Victim machine: Windows 7 Ultimate SP1 x64
- Ransomware: Zepto ransomware (https://www.tripwire.com/state-of-security/latest-security-news/the-newest-online-threat-zepto-ransomware/)

McAfee Ransomware Interceptor

- Information link: https://www.mcafee.com/jp/downloads/free-tools/interceptor.aspx
- How does McAfeeRansomwareInterceptor work?

◎ Ransomware process starts



Time ...	Process Name	PID	Operation
2:35:4...	McAfeeRanso...	1872	Thread Exit
2:35:4...	McAfeeRanso...	1872	Thread Exit
2:38:1...	McAfeeRanso...	1872	Thread Exit
2:38:4...	ZEPTO.exe	2532	Process Start
2:38:4...	ZEPTO.exe	2532	Thread Create
2:38:4...	ZEPTO.exe	2532	Load Image
2:38:4...	ZEPTO.exe	2532	Load Image
2:38:4...	ZEPTO.exe	2532	Load Image
2:38:4...	ZEPTO.exe	2532	CreateFile
2:38:4...	ZEPTO.exe	2532	CreateFile
2:38:4...	ZEPTO.exe	2532	CreateFile
2:38:4...	ZEPTO.exe	2532	QueryBasicInfo
2:38:4...	ZEPTO.exe	2532	CloseFile
2:38:4...	ZEPTO.exe	2532	CreateFile
2:38:4...	ZEPTO.exe	2532	CreateFileMapp
2:38:4...	ZEPTO.exe	2532	CreateFileMapp
2:38:4...	ZEPTO.exe	2532	Load Image
2:38:4...	ZEPTO.exe	2532	CloseFile
2:38:4...	ZEPTO.exe	2532	CreateFile

Date:	8/10/2017 2:38:46.5453879 AM
Thread:	2968
Class:	Process
Operation:	Process Start
Result:	SUCCESS
Path:	
Duration:	0.0000000

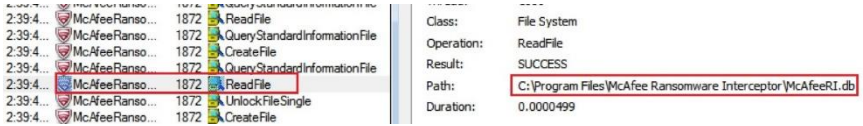
Parent PID:	1364
Command line:	"C:\Users\Zone\Documents\ZEPTO.exe"
Current directory:	C:\Users\Zone\Documents\
Environment:	

```
=::=::\
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\Zone\AppData\Roaming
CommonProgramFiles=C:\Program Files\Com
CommonProgramFiles(x86)=C:\Program Files
CommonProgramW6432=C:\Program Files\C
COMPUTERNAME=ZONE-PC
ComSpec=C:\Windows\system32\cmd.exe
```

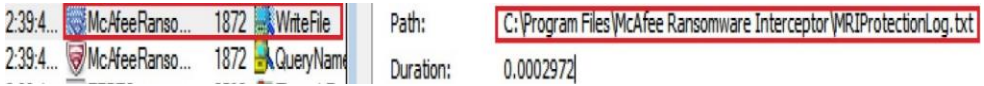
McAfee Ransomware Interceptor

- Information link: https://www.mcafee.com/jp/downloads/free-tools/interceptor.aspx
- How does McAfeeRansomwareInterceptor work?

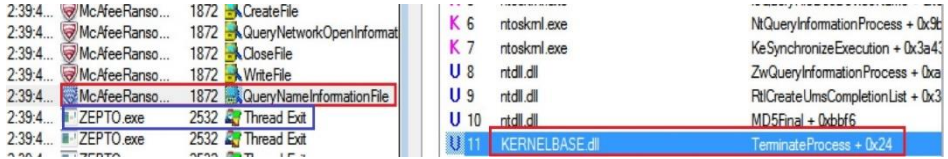
◎ McAfee RI reads McAfeeRI.db file



◎ McAfee RI writes the log file



◎ McAfee RI Identifies the ransomware threat and terminates the process



References

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

- Knowbe
https://www.knowbe4.com/ransomware

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