



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

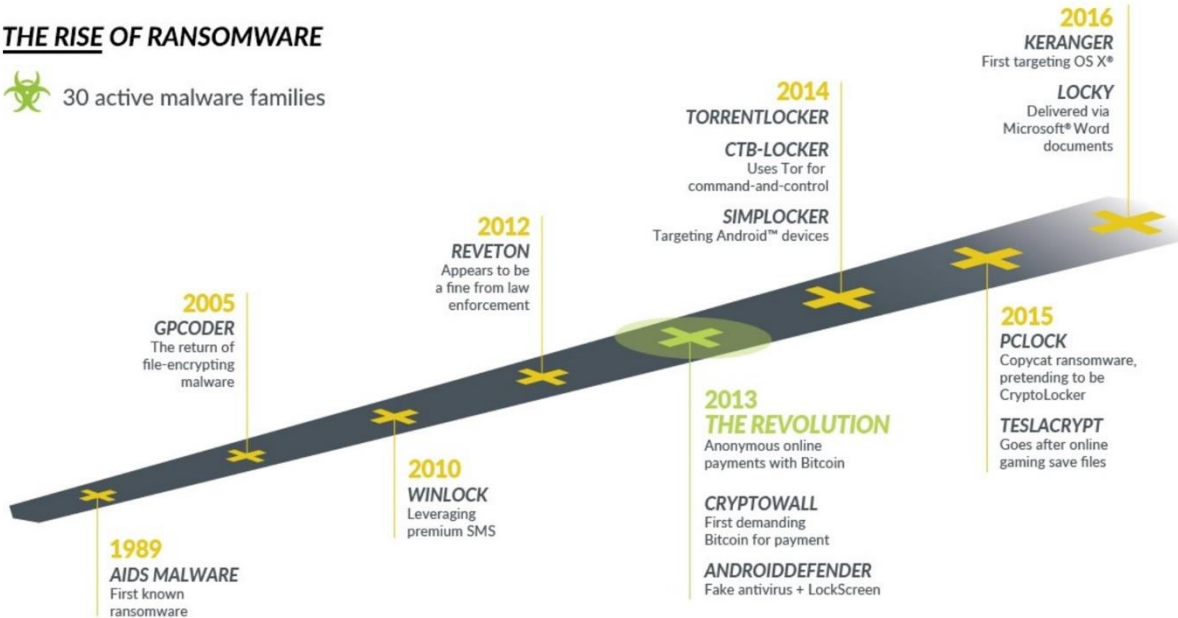


Rise of Ransomware

THE RISE OF RANSOMWARE



30 active malware families



Ransomware Testing Environment

- 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	Date:	8/10/2017 2:38:46.5453879 AM
2:35:4...	McAfeeRanso...	1872	Thread Exit	Thread:	2968
2:35:4...	McAfeeRanso...	1872	Thread Exit	Class:	Process
2:38:1...	McAfeeRanso...	1872	Thread Exit	Operation:	Process Start
2:38:4...	ZEPITO.exe	2532	Process Start	Result:	SUCCESS
2:38:4...	ZEPITO.exe	2532	Thread Create	Path:	
2:38:4...	ZEPITO.exe	2532	Load Image	Duration:	0.0000000
2:38:4...	ZEPITO.exe	2532	Load Image		
2:38:4...	ZEPITO.exe	2532	Load Image		
2:38:4...	ZEPITO.exe	2532	CreateFile		
2:38:4...	ZEPITO.exe	2532	CreateFile	Parent PID:	1364
2:38:4...	ZEPITO.exe	2532	CreateFile	Command line:	"C:\Users\Zone\Documents\ZEPITO.exe"
2:38:4...	ZEPITO.exe	2532	QueryBasicInfo	Current directory:	C:\Users\Zone\Documents\
2:38:4...	ZEPITO.exe	2532	CloseFile	Environment:	
2:38:4...	ZEPITO.exe	2532	CreateFile		=::=:\
2:38:4...	ZEPITO.exe	2532	CreateFile Mapp		ALLUSERSPROFILE=C:\ProgramData
2:38:4...	ZEPITO.exe	2532	CreateFile Mapp		%APPDATA%=C:\Users\Zone\AppData\Roaming
2:38:4...	ZEPITO.exe	2532	Load Image		CommonProgramFiles=C:\Program Files\Com
2:38:4...	ZEPITO.exe	2532	CloseFile		CommonProgramFiles(x86)=C:\Program Files\Com
2:38:4...	ZEPITO.exe	2532	CreateFile		CommonProgramW6432=C:\Program Files\Com
2:38:4...	ZEPITO.exe	2532			COMPUTERNAME=ZONE-PC
2:38:4...	ZEPITO.exe	2532			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

2:39:4...	McAfeeRanso...	1872	ReadFile	Class:	File System
2:39:4...	McAfeeRanso...	1872	QueryStandardInformationFile	Operation:	ReadFile
2:39:4...	McAfeeRanso...	1872	CreateFile	Result:	SUCCESS
2:39:4...	McAfeeRanso...	1872	QueryStandardInformationFile	Path:	C:\Program Files\McAfee Ransomware Interceptor\McAfeeRI.db
2:39:4...	McAfeeRanso...	1872	ReadFile	Duration:	0.0000499
2:39:4...	McAfeeRanso...	1872	UnlockFileSingle		
2:39:4...	McAfeeRanso...	1872	CreateFile		

◎ McAfee RI writes the log file

2:39:4...	McAfeeRanso...	1872	WriteFile	Path:	C:\Program Files\McAfee Ransomware Interceptor\MRIProtectionLog.txt
2:39:4...	McAfeeRanso...	1872	QueryNameInformationFile	Duration:	0.0002972

◎ McAfee RI Identifies the ransomware threat and terminates the process

2:39:4...	McAfeeRanso...	1872	CreateFile	6	rtoskml.exe	NtQueryInformationProcess + 0x3b
2:39:4...	McAfeeRanso...	1872	QueryNetworkOpenInformationFile	K 7	rtoskml.exe	KeSynchronizeExecution + 0x3a4
2:39:4...	McAfeeRanso...	1872	CloseFile	U 8	ntdll.dll	ZwQueryInformationProcess + 0xa
2:39:4...	McAfeeRanso...	1872	WriteFile	U 9	ntdll.dll	RtlCreateUmsCompletionList + 0x3
2:39:4...	McAfeeRanso...	1872	QueryNameInformationFile	U 10	ntdll.dll	MD5Final + 0xbbf6
2:39:4...	ZEPTO.exe	2532	Thread Exit	U 11	KERNELBASE.dll	TerminateProcess + 0x24
2:39:4...	ZEPTO.exe	2532	Thread Exit			

References

- Wikipedia
<https://en.wikipedia.org/wiki/Ransomware>
- Knowbe
<https://www.knowbe4.com/ransomware>
- Heimdal security
<https://heimdalsecurity.com/blog/what-is-ransomware-protection>