

AntiRansomware Tools Tested Part 6

Information Security Inc.

Contents

- What is Ransomware?
- Rise of Ransomware
- Ransomware Testing Environment
- Bitdefender 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

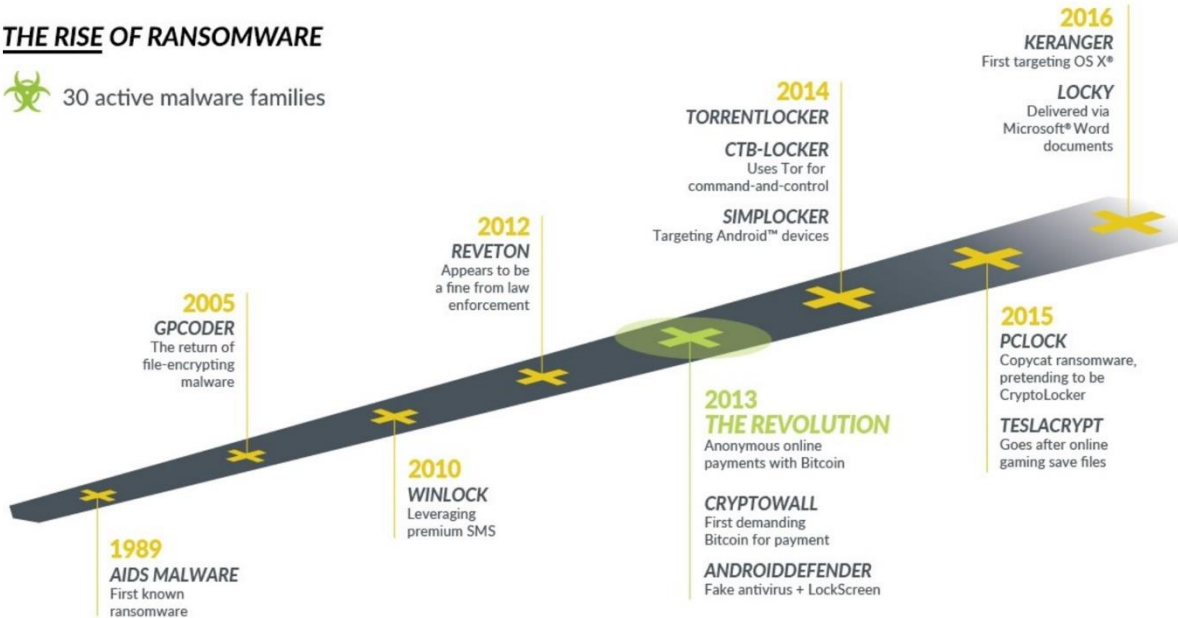


Rise of Ransomware

THE RISE OF RANSOMWARE



30 active malware families



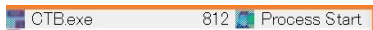
Ransomware Testing Environment

- Victim machine: Windows 10 x64
- Ransomware: CTB-Locker
(<https://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomware-information>)

Bitdefender Anti-Ransomware

- Information link: <https://www.bitdefender.com/solutions/anti-ransomware-tool.html>
- How does Bitdefender Anti-Ransomware work?

© Ransomware process starts



Class:	Process
Operation:	Process Start
Result:	SUCCESS

Path:
Duration: 0.000000

Parent PID: 3472
Command line: "C:\Users\User3\Documents\CTB2014Works\CTB.exe"
Current directory: C:\Users\User3\Documents\CTB2014Works\
Environment:
=::=::
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\User3\AppData\Roaming

Malwarebytes Anti-Ransomware

- Information link: <https://www.bitdefender.com/solutions/anti-ransomware-tool.html>
- How does Bitdefender Anti-Ransomware work?

© Bitdefender Anti-Ransomware injects <InjectionDll.dll> DLL into the ransomware's process address space

CTB.exe 812 Load Image C:\Program Files\Bitdefender\Tools\BDAntiRansomware\InjectionDll.dll

Event Properties

Event	Process	Stack
-------	---------	-------

Date: 2017/08/21 14:28:46.2040928

Thread: 1532

Class: Process

Operation: Load Image

Result: SUCCESS

Path: C:\Program Files\Bitdefender\Tools\BDAntiRansomware\InjectionDll.dll

Malwarebytes Anti-Ransomware

- Information link: <https://www.bitdefender.com/solutions/anti-ransomware-tool.htmls>
- How does Bitdefender Anti-Ransomware work?

© Ransomware process is identified and killed by Bitdefender Anti-Ransomware

OTB.exe	812	Thread Exit
---------	-----	-------------

Class:	Process
Operation:	Thread Exit
Result:	SUCCESS
Path:	
Duration:	0.0000000

References

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