



# AntiRansomware Tools Thoroughly Tested Part 2

Information Security Inc.

# Contents

- What is Ransomware?
- Rise of Ransomware
- Ransomware Testing Environment
- Anti-Ransomware Kaspersky
- 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

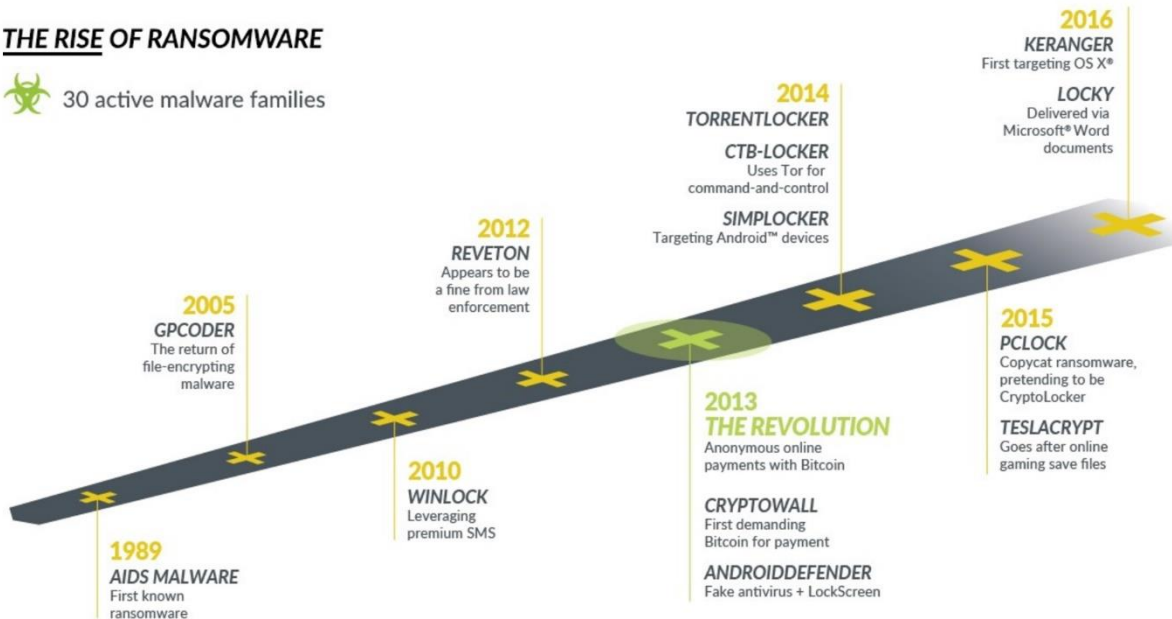


# Rise of Ransomware

## 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/>)

# Anti-Ransomware Kaspersky

- Information link: <https://goo.gl/zYdqYJ>
- How does Anti-ransomware Kaspersky work?
- 

© Ransomware process starts

The image shows a Windows Task Manager window with the 'Processes' tab selected. The 'art\_ransom.exe' process is highlighted in red. To the right, the Windows Event Viewer is open, displaying the 'Event Properties' for the selected process. The 'Command line' field is highlighted in red and contains the path 'C:\Users\User3\Documents\ZEPTO.exe'. The 'Current directory' field also shows 'C:\Users\User3\Documents\'. The 'Environment' field contains a list of system variables.

Time	Process Name	PID	Operation
12:53	art_ransom.exe	1564	Thread Create
12:53	ZEPTO.exe	3700	Thread Create
12:53	ZEPTO.exe	3700	Load Image
12:53	ZEPTO.exe	3700	Load Image
12:53	ZEPTO.exe	3700	Load Image
12:53	ZEPTO.exe	3700	Thread Exit
12:53	art_ransom.exe	1564	Load Image
12:53	art_ransom.exe	1564	Thread Create
12:53	art_ransom.exe	1564	Thread Create

**Event Properties**

Event	Process	Stack
Date:	8/9/2017 12:53:04.3624532 AM	
Thread:	4768	
Client:	Process	
Operator:	Process Start	
Result:	SUCCESS	
Path:		
Duration:	0.000000	

Parent PID: 1568  
Command line: **C:\Users\User3\Documents\ZEPTO.exe\***  
Current directory: C:\Users\User3\Documents\

Environment:  
%ALLUSERSPROFILE% = C:\ProgramData  
APPDATA = C:\Users\User3\AppData\Roaming  
CommonProgramFiles = C:\Program Files\Common Files  
CommonProgramFiles(x86) = C:\Program Files (x86)\Common Files  
CommonProgramFiles(x86) = C:\Program Files (x86)\Common Files  
COMPUTERNAME = DESKTOP-9K2W953  
CSDRIVER = C:\Windows\System32\cmd.exe  
HOMEDRIVE = C:  
HOMEPATH = \Users\User3  
LOCALAPPDATA = C:\Users\User3\AppData\Local  
LOGONSERVERS = \\\*  
NUMBER\_OF\_PROCESSORS = 2  
OneDrive = C:\Users\User3\OneDrive  
OS = Windows 7  
Path = C:\Windows\system32;C:\Windows;C:\Windows\System32;WebC:\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 = 3c33  
ProgramData = C:\ProgramData  
ProgramFiles = C:\Program Files  
ProgramFiles(x86) = C:\Program Files (x86)  
ProgramFiles(x86) = C:\Program Files (x86)  
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-9K2W953  
USERDOMAIN\_FULL = DESKTOP-9K2W953  
USERNAME = User3  
USERPROFILE = C:\Users\User3  
windir = C:\Windows

# Anti-Ransomware Kaspersky

- Information link: <https://goo.gl/zYdqYJ>
- How does Anti-ransomware Kaspersky work?

© Ransomware process is identified and killed by the Kaspersky product

12:53:...	ZEPTO.exe	3700	Load Image	C:\Users\user3\AppData\Local\Temp\ZEPTO.exe	SUCCESS	Image Base: 0x77d...
12:53:...	ZEPTO.exe	3700	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77fd...
12:53:...	ZEPTO.exe	3700	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77fd...
12:53:...	ZEPTO.exe	3700	Thread Exit		SUCCESS	Thread ID: 740, Us...
12:53:...	ZEPTO.exe	3700	Process Exit		SUCCESS	Exit Status: -10737...

# Anti-Ransomware Kaspersky

- Information link: <https://goo.gl/zYdqYJ>
- How does Anti-ransomware Kaspersky work?

© Anti-ransomware Kaspersky process (anti\_ransom.exe) injects its own klhkum.dll into the ransomware 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>