

AntiRansomware Tools Thoroughly Tested Part 2

Information Security Inc.



Contents

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



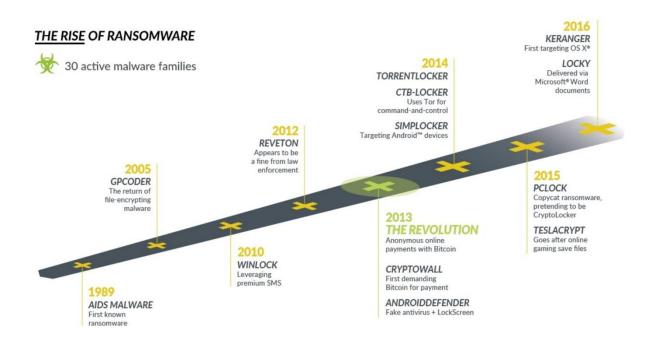
What is Ransomware?

- **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





Ransomware Testing Envinronment

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



Anti-Ransomware Kaspersky

- Information link: <u>https://goo.gl/zYdqYJ</u>
- · How does Anti-ransomware Kaspersky work?
- ◎ Ransomware process starts

ZERIO exe						
	3700 apprincess Start	2 Event Properties				
arti_ransom.exe	1564 🕰 Thread Create					
EPTO exe	3700 Thread Create 3700 Thread Create	Event Process	· Chark			
EPTO exe	3700 Load mage	Process	a utanin			
EPTO exe	3700 At Load Image	Date:	8/9/2017 12:53:04.3624532 AM			
EPTO.exe	3700 R Load Image	Thread:	4768			
EPTO.exe	3700 RThread Ext	Class:	Process			
EPTO exe	3700 Process Ext	Operation:	Process Start			
nti_ransom.exe	1564 RLoad Image 1564 RThread Create	Result:	SUCCESS			
ti_ransom.exe	1564 Thread Create	Path:	SUCCESS			
nti_ransom.exe	1564 Thread Create					
• aujasun.ee		Duration:	0.000000			
		Parent PID:	3468			
		Command line:	"C:\Users\User3\Documents\ZEPTO.exe"			
		Current directo	bry: C: (Lisers)(Jser3)(Documents)			
		Environment:				
			ALLUSERSPROFILE =C-\ProgramData			
			APPDATA=C: Users/User3/AppData/Roaming CommonProgramFiles=C: Program Files/Common Files			
			Common Fogram Field (168) = C (19 fogram Field (168) Common Field			
			CommonProgramW6432=C:\Program Files\Common Files			
			COMPUTERNAME = DESKTOP-IHQN955			
			ComSpec=C:\/Vindows\system32\pmd.exe HOMEDRIVE=C:			
			HOMEPATH# Users User 3			
			LOCALAPPDATA =C: [Users]User3[AppData]Local			
			LOGONSERVER=\/DESKTOP-IHQN955			
			NUMBER_OF_PROCESSORS=2 OveDrive=Ciluters/User3/DoeDrive			
			OneDrive =C: Users User 3 OneDrive OS=Windows JIT			
			OneDrive=ClUsters[Usters](DeeDrive OS=Windows IN Path=C: [Windows]vestens32;C: [Windows;C: [Windows]System32[Wberr;C: [Windows]System32[WindowsPowerShell y 1.0]			
			Ombiner-C, Lises User 2/Dealbine Oshvitokau JI Path-C, Ulindow Hana 22-C, Wondow C, Window S (Haters 22)/Menu C, Window Spaten 22/WindowsPowerShell y 1.0/ Path-C, Ulindow Hate, Barl, Color, Vido, Vido, Vido, Xiao, Xiao, Vidor, Mort, PROSESSE, ALCONTECTUBEL-Mort, Color, Vido, Vido, Xiao, Xiao, Vidor, Mort, PROSESSE, ALCONTECTUBEL-Mort, Color, Vido, Vido, Xiao, Xiao, Vidor, Mort, PROSESSE, ALCONTECTUBEL-Mort, Color, Vido, Vido, Xiao, Xi			
			Overbringen Larger States (2) setted bei Fahr-Cill Varier States 2) Coll Workson CC (Windows (System 32) Workson (System 32) Windows (System 32)			
			OneDine-Cill Jami Kara (Donibine Os-Windows) (7 Part-Cill Windows) bystem 32 Cill Windows (System 32)(Mony, Cill Windows (System 32)(WindowsPower Shelly L.O. Partell's Coll West, 2013, Collon, 188), 1892, 1932, 1934, 1934, 1935, Partell's Coll West, 2013, Collando S, Santo			
			Conditive-CL June 3 June 7 Databline Det 10 - 2010 Det 10 - 2010			
			Ombine-Ci, ben Uker 20mbine Od Windows (F Pain-Ci Windows Ci Windows 20 Windo			
			Conchine-Ci, Barri Jane Zondovie Osrvitolina, JT Particular 2012, Ultridovis (Visidovi Straten 22) (Madovi			
			Ondon-e-C [Lever3uer 20 http:// Open.com/ 20 http://www.action.com/ 20			
			Conditioned, Elever Subar 20 Andrew (Windows Stratem 22) Money C. Windows Stratem 32) Money C. Windows Stratem 32) Money and Stratem			
			Conditioned (Lear Star 20 Addite Conditioned (Lear Star 20 Addite) Conditioned (Lear Star 20 Addite) Additioned (Lear Star 20 Addite) Additioned (Lear Star 20 Addite) Additioned (Lear Star 20 Addite) Records (Le			
			Condition-City Bank Star 20 https:// Pather: University Star 20 https:// Pather: University Star 20 https:// University.20 https:// 20 https:// Pather: Conditional Star 20 https:// 20 https:// 20 https:// 20 https:// Pather: Conditional Star 20 https:// 20 https:// 20 https:// Pather: Conditional Star 20 https:// 20 https:// 20 https:// Pather: Conditional Star 20 https:// Pathe			
			Condition-CL June 3 June 7 Detabline Condition-CL June 3 June 7 Detabline Condition-CL June 3 June 7 Detabline A HTTERT CONE (2016) 2016 (1916) 375, 3261, 3271, 3271, 32755, 3275, 3275, 3275, 3275, 327			
			Condition-City June 1997 2016/114 Condition-City June 1997 2016 2014 2014 2014 2014 2014 2014 2014 2014			
			Conditioned, Team State 20 Additione Openational and the second			
			Condition-City June 1997 2016/114 Condition-City June 1997 2016 2014 2014 2014 2014 2014 2014 2014 2014			
			OneDrive-C [Lever June 70 And/one OneDrive-C [Verification 20 (Verification 20 (Verificatio			



.

Anti-Ransomware Kaspersky

- Information link: <u>https://goo.gl/zYdqYJ</u>
- · How does Anti-ransomware Kaspersky work?
- ◎ Ransomware process is identified and killed by the Kaspersky product

	ZEPTO.exe	3700 🛶 Load Image 3700 🎝 Load Image	C. (Users (Users (Documents (ZL)) 10.exe C:\Windows\System32\ntdll.dll	SUCCESS	Image base: 0x400 Image Base: 0x7ffd
10 10 10 10 10 10 10 10 10 10 10 10 10 1	ZEP10.exe	3700 💐 Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	lmage Base: 0x//0.
12:53:	E 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: <u>https://goo.gl/zYdqYJ</u>
- · 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

