AntiRansomware Tools Thoroughly Tested Part 2

Information Security Inc.

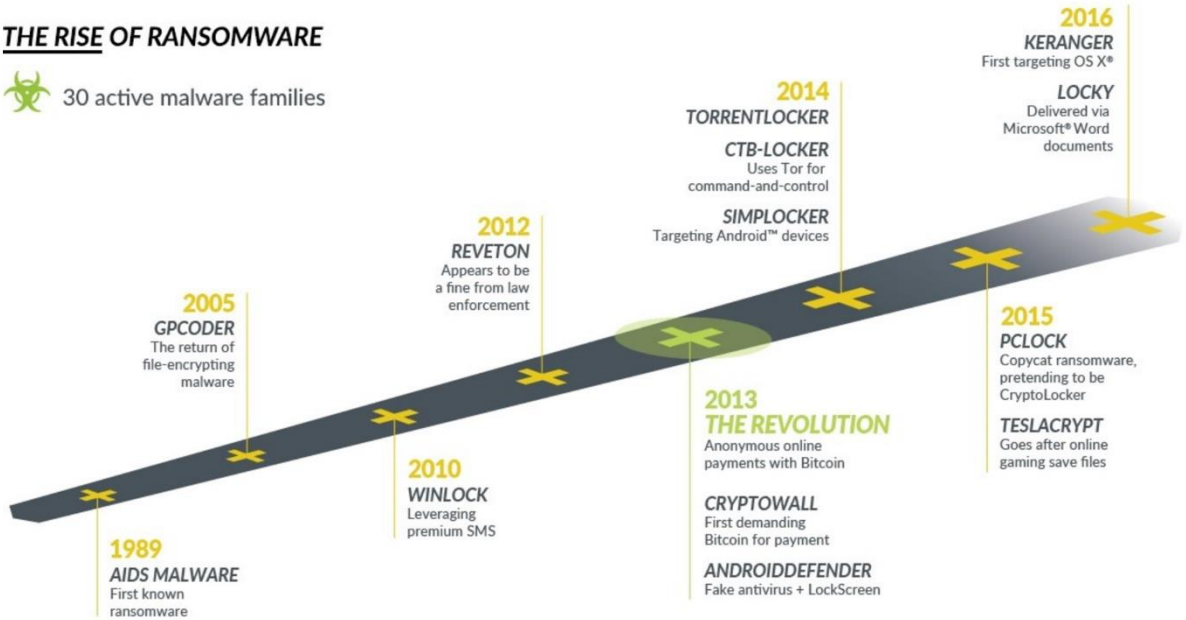
Contents

- 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

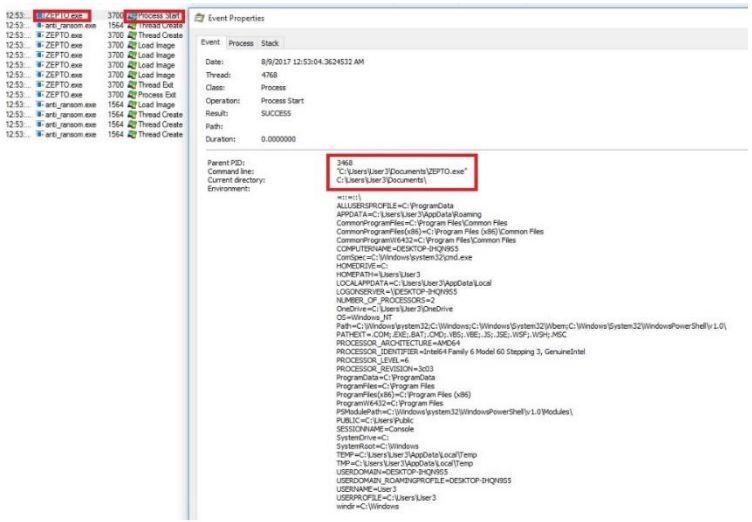


Ransomware Testing Envinronment

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

Anti-Ransomware Kaspersky

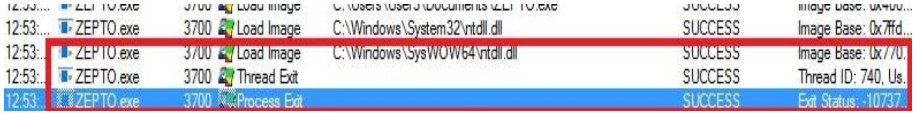
- Information link: https://goo.gl/zYdqYJ
- How does Anti-ransomware Kaspersky work?
-
  ◎ Ransomware process starts



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



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