



AntiRansomware Tools Thoroughly Tested Part 4

Information Security Inc.

Contents

- What is Ransomware?
- Rise of Ransomware
- Ransomware Testing Environment
- WebRoot Secure Anywhere
- 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

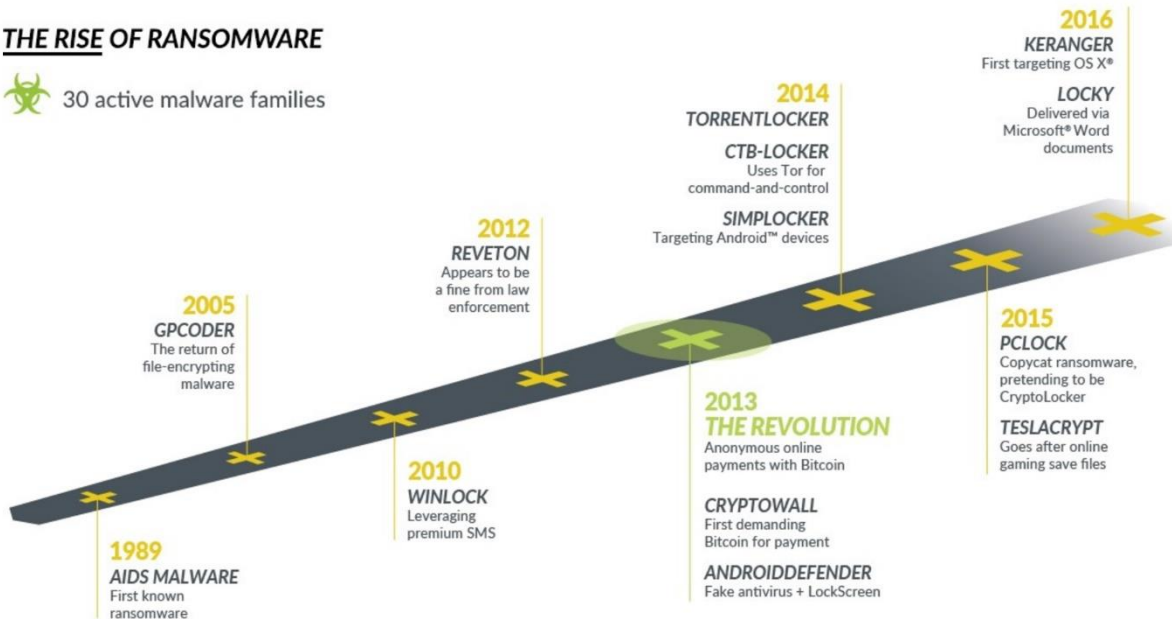


Rise of Ransomware

THE RISE OF RANSOMWARE



30 active malware families



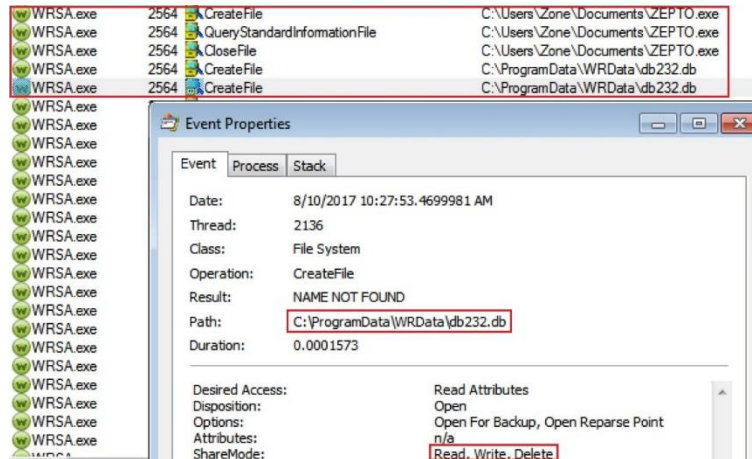
Ransomware Testing Environment

- 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/>)

WebRoot Secure anywhere

- Information link: <https://www.webroot.com/jp/ja/home/products/av>
- How does WebRoot Security Anywhere work?

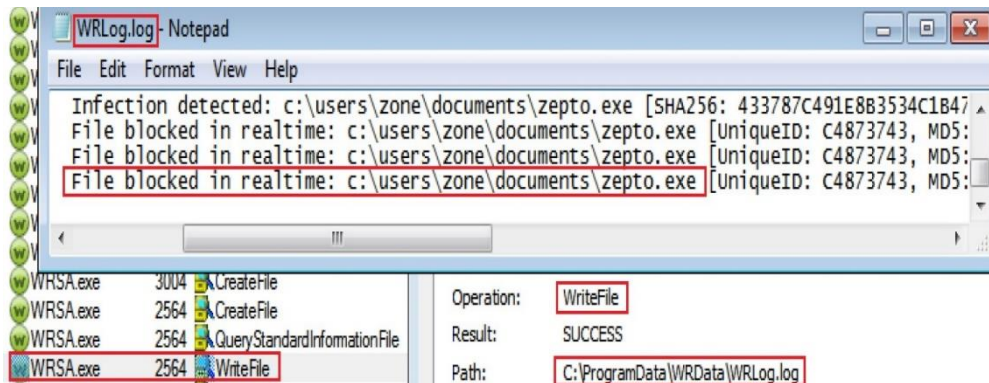
© WebRoot Security Anywhere identifies the ransomware file (from database) and blocks it in real time before creating a process



WebRoot Secure anywhere

- Information link: <https://www.webroot.com/jp/ja/home/products/av>
- How does WebRoot Security Anywhere work?

© After blocking the ransomware WebRoot Security Anywhere writes the result to the log file



References

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