CERIAS
The Center for Education and Research in Information Assurance and Security

Finding ransomware encryption keys in volatile memory (Work In Progress)

Joseph Graham; graham78@purdue.edu
Department of Computer And Information Technology
Purdue University

Abstract

Ransomware is malware that encrypts files on the target computer. Ransomware has become more prominent over the years causing problems for both consumers and businesses. Ransomware is extremely hard to recover from on a target computer if there is no backup seeing as how it encrypts most files on the user's computer. The purpose of this poster is to investigate ransomware and see if the encryption key and initialization vector for the ransomware can be found in volatile memory allowing the files to become decrypted and recovered without paying the ransom or needing a backup.

Methodology

- Test file was created and hashed.
- Jigsaw Malware was installed.
- Memory was dumped.
- Memory was Analyzed with Volatility.
- Key and IV were found in memory and extracted.
- File was decrypted using key and IV and rehashed to prove it was the same file.

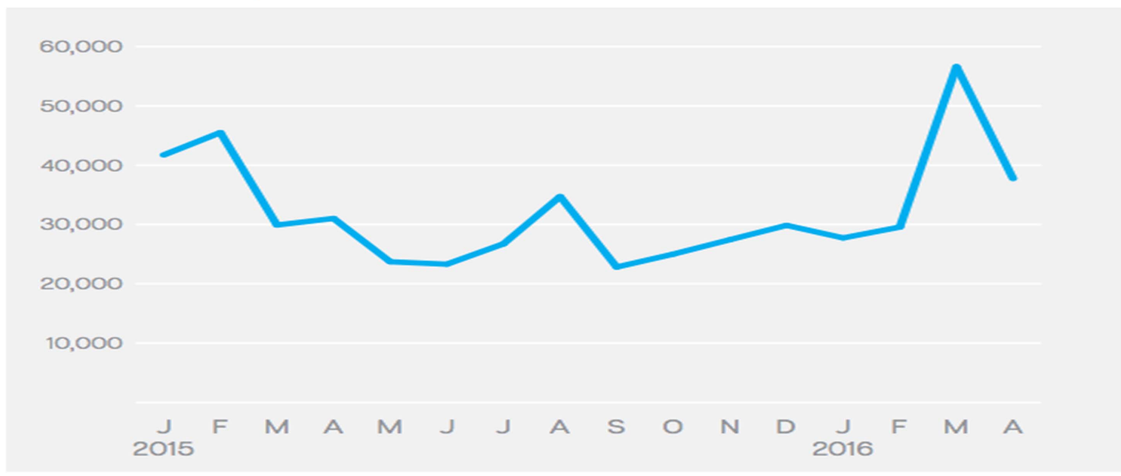
Research Questions

Does the ransomware leave the encryption key and IV in memory?
Can live forensics be done in time before the ransomware cleans itself?
How much of an footprint does the ransomware leave?
Can the ransomware be found in volatile memory using live forensics tools?
How long does it take to find the key in memory?

Significance

As shown by the graphic below the infections caused by ransomware is incredibly high. This causes business to suffer profit losses and users to suffer productivity loss. There needs to be a quick and easy way to be able to recover a system in case all other methods fail and without paying the ransom. Using the new methods of live forensics it may be possible to have another method of recovery from ransomware that may be able to be done at the time of infection.

Figure 1. Overall Ransomware Infections by Month from January 2015 to April 2016



Graph showing the amount of ransomware infections per month from January 2015 to April 2016. [1]

References

[1] Brien, D. O., Power, J. P., & Wallace, S. (2016). *ISTR2016 Ransomware and Businesses* [PDF]. Symantec.