Most Ransomware Isn’t As Complex As You Might Think

Yes, we should be able to detect most of it

Engin Kirda

Co-Founder and Chief Architect, Lastline Labs

Professor @ Northeastern University
My Background

• Professor at Northeastern University, Boston
  – Started malware research in about 2004
  – Helped build and release popular malware analysis and detection systems (Anubis, EXPOSURE, Wepawet, ...)

• Co-founder of Lastline and Lastline Labs
  – Lastline offers protection against zero-day threats and advanced malware
  – Commercialization of many years of advanced research
  – Lastline Labs is the research and development arm of Lastline
Acknowledgements

• This work is partially based on a study that my Ph.D. student Amin Kharraz worked on
  – We recently published it at DIMVA 2015
  – “Cutting the Gordion Knot: A Look Under the Hood of Ransomware Attacks”
Key Takeaways

• The majority of ransomware launches relatively straightforward attack payloads
  – Using bad cryptography, or standard cryptography libraries
  – Deleting files, but not wiping them off disk

• Compared to other malware, ransomware has very distinct, predictable behavior
  – Ransom notes with background behavior, change in entropy of files, iterating over large numbers of files, etc.
What We Will Discuss

• Significance of the ransomware threat
• Complexity and sophistication of attacks
• Attack mechanisms
• Main ransomware weaknesses
• Better mitigation
The Anatomy of An Attack

• A victim machine is compromised
  – Ransomware is installed
  – Once the attack payload is executed (if there is one), ransomware informs victim of the attack
  – The victim needs to pay -- otherwise, his/her data is kept hostage or destroyed
Your computer has been locked due to suspicion of illegal content downloading and distribution.

The illegal content (414 Mb of photo and video files) was automatically classified as child pornographic materials.

The downloading and distribution of illegal content, in whole or in part, violates following U.S. Federal Laws:

18 U.S.C. § 2251 Sexual exploitation of children (Production of child pornography)
18 U.S.C. § 2252C Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A Certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 6 months to 10 years and shall be fined up to $250,000.

Your case can be classified as occasional/unmotivated, according to 17 (U.S. Code) 5512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300

Exchange your cash for a MoneyPak voucher and use your voucher code in the form below:

Status: Waiting for payment

Where can I buy MoneyPak

---

Collected technical data:
Your IP address: [Redacted]
Your host name: [Redacted]
Source or intermediary sites: [Redacted]
Location: [Redacted]
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]. To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
Ransomware Evolution

• The ransomware concept dates back to 1989
• Clearly, ransomware attacks have increased in numbers over the last 5 years
  – Many security reports talk about the sophistication and complexity of individual attacks
  – The general public is left with the impression that we are faced with a new threat that is very difficult or impossible to prevent
CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES

Data from the FBI's Internet Crime Complaint Center (IC3) shows ransomware continues to spread and is infecting devices around the globe. Recent IC3 reporting identifies CryptoWall as the most current and significant ransomware threat targeting U.S. individuals and businesses.¹ CryptoWall and its variants have been used actively to target U.S. victims since April 2014. The financial impact to victims goes beyond the ransom fee itself, which is typically between $200 and $10,000. Many victims incur additional costs associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers. Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.
“Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.”

Police pay ransom after cyberterror attack on network

By Jayne W. Miller News Editor
Jayne@YourTownCrier.com | 1 comment

Chief: “Paying ransom was the last resort”

TEWKSBURY – Last December Tewksbury Police confronted a new, and growing, frontier in cyberterrorism when the CryptoLocker ransomware virus infected the department’s network, encrypting essential department files until the town paid a $500 bitcoin ransom. In total, police systems were down between four and five days as the department worked with the FBI, Homeland Security, Massachusetts State Police, as well as private firms in an effort to restore their data without paying the ransom.

Thomas Murphy, Daniel Sawicki and Lt. Scott Keddie
Complexity and Sophistication

• Typical way of measuring ransomware sophistication
  – Looking at evasion (e.g., packing, dynamic checks, encryption, etc.)

<table>
<thead>
<tr>
<th>Evasion</th>
<th>Possibly stalling against analysis environment (loop)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evasion</td>
<td>Self-modifying code at runtime</td>
</tr>
</tbody>
</table>

– In this work, we are looking at the sophistication of the attack after compromise
A Closer Look at Ransomware

- 2006-2014
- 1359 samples
- 15 families
  (incl. Cryptolocker and Cryptowall)
Methodology

• Automated, dynamic analysis for all samples
• Manual analysis in some cases
• Verification of samples and cross-checking with VirusTotal
  – Ransomware if three or more scanners agree
• All samples showed ransomware behavior
Ransomware Attack Payloads
Encryption Mechanisms

• About 5% of the samples use some encryption
  – Earlier samples often have custom encryption (which leads to mistakes)
  – Current popular families like Cryptolocker and Cryptowall use Windows crypto libraries
    • Is this sophistication, or just good software engineering?
  – Using strong crypto libraries is a double-edged sword for the attackers
    • Dynamic analysis can catch the use of these libraries
Deletion Mechanisms

• About 36% of the five common ransomware families in data set delete files
  – Most deletion is straight-forward
  – Master File Table (MFT) entries are manipulated, but the data remains on disk
  – Hence, recovery is possible in many cases
  – The MFT is an effective venue for detecting ransomware during analysis
Locking Mechanisms

• Classic ransomware behavior: Lock the desktop of computer
  – More than 60% of the samples simply use `CreateDesktop` to create a persistent new desktop
  – Another approach is to display HTML page and disable components

• In all cases: A message is displayed to the victim

• Locking mechanisms are a nuisance, but the data is typically not harmed
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.) Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
Better Mitigation
Achilles’ Heel of Ransomware

• Ransomware has to inform victim that attack has taken place
  – Behavior inherent in its nature

• Ransomware has certain behaviors that are predictable
  – e.g., entropy changes, modal dialogs and background activity, accessing “honey” files
Example: Dissecting Cryptolocker

- Analysis Overview

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evasion</td>
<td>Checking for specific image filename</td>
</tr>
<tr>
<td>Evasion</td>
<td>Trying to detect analysis virtual environment (guest mode)</td>
</tr>
<tr>
<td>Evasion</td>
<td>Trying to detect analysis virtual environment (malware sandbox)</td>
</tr>
<tr>
<td>File</td>
<td>Modifying executable in Windows directory</td>
</tr>
<tr>
<td>File</td>
<td>Searching for files across mounted drives</td>
</tr>
<tr>
<td>File</td>
<td>Searching for files across mounted drives</td>
</tr>
<tr>
<td>Memory</td>
<td>Search for API functions in memory (possible shellcode)</td>
</tr>
<tr>
<td>Network</td>
<td>Hide network activity through code injection</td>
</tr>
<tr>
<td>Packer</td>
<td>Loading an embedded PE image (potential unpacking)</td>
</tr>
</tbody>
</table>
Example: Dissecting Cryptolocker

• Loaded libraries...

```c:\windows\syswow64\msvort.dll
\c:\windows\syswow64\msctf.dll
\c:\windows\syswow64\lpk.dll
\c:\windows\syswow64\kernelbase.dll
\c:\windows\syswow64\kernel32.dll
\c:\windows\syswow64\advapi32.dll
\c:\windows\syswow64\cryptbase.dll
\c:\windows\system32\wow64win.dll
\c:\windows\system32\wow64cpu.dll
\c:\windows\system32\wow64.dll
\c:\windows\system32\ntdll.dll
\c:\windows\system32\imm32.dll```
Key Takeaways

• The majority of ransomware launches relatively straightforward attack payloads
  – Using bad cryptography, or standard cryptography libraries
  – Deleting files, but not wiping them off disk

• Compared to other malware, ransomware has very distinct, predictable behavior
  – Ransom notes with background behavior, change in entropy of files, iterating over large numbers of files, etc.
THANK YOU!