CRYPTOLOCKER

“The bleepingest virus of 2013” —Reddit user bluesoul

Andrew Tarrh
Ashley Hansberry
Allan Lasser

CS558
Network Security
2/20/14
CryptoLocker Ransomware Being Described As 'The Perfect Crime'

By Chief Correspondent Joe Shortsleeve, WBZ-TV

December 18, 2013 5:34 PM

Related Tags: CBS Boston, CryptoLocker ransomware, Joe Shortsleeve, WBZ

Joe Shortsleeve
Joe Shortsleeve is chief correspondent for WBZ-TV News weekdays a... Read More
Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. [here] is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
HOW CRYPTOLOCKER WORKS

1. Affects Windows versions XP through 8
2. Encrypts data files using RSA and AES encryption
3. Once encryption is finished, a pop-up asking for $100 or $300 in Moneypack or 2 bitcoins (BTC)
4. User must pay in time in order to decrypt their files
5. If not paid within 72 hours, you pay much more
A TYPICAL CRYPTOLOCKER ATTACK

1. Infection
2. Encryption
3. Decryption

“I know this thing sucks and all, but it is really well done”
—Reddit user olithraz
# Common email subjects

<table>
<thead>
<tr>
<th>Subject</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>USPS – Your package is available for pickup (Parcel 173145820507)</td>
<td>USPS – Missed package delivery (&quot;USPS Express Services&quot; <a href="mailto:service-notification@usps.com">service-notification@usps.com</a>)</td>
</tr>
<tr>
<td>USPS – Missed package delivery</td>
<td>FW: Invoice &lt;random number&gt;</td>
</tr>
<tr>
<td>ADP payroll: Account Charge Alert</td>
<td>ACH Notification (&quot;ADP Payroll&quot; <a href="mailto:*@adp.com">*@adp.com</a>)</td>
</tr>
<tr>
<td>ADP Reference #09903824430</td>
<td>Payroll Received by Intuit</td>
</tr>
<tr>
<td>Important – attached form</td>
<td>FW: Last Month Remit</td>
</tr>
<tr>
<td>McAfee Always On Protection Reactivation</td>
<td>Scanned Image from a Xerox WorkCentre</td>
</tr>
<tr>
<td>Scan from a Xerox WorkCentre</td>
<td>scanned from Xerox</td>
</tr>
<tr>
<td>Annual Form – Authorization to Use Privately Owned Vehicle on State Business</td>
<td>Fwd: IMG01041_6706015_m.zip</td>
</tr>
</tbody>
</table>
How Cryptolocker ruins your life:

1. Domain generation algorithm used to connect to server
2. Server communication encrypted with 2048-bit RSA
3. Files encrypted with 256-bit AES and RSA
Malware

\[ R = \text{Enc}_{PK_s}(\text{request}) \]

\[ SK_M \]

\[ PK_U = \text{Dec}_{SK_M}(U) \]

\[ SK_S \]

\[ PK_M \]

Request for Unique Public Key

Initial communication with server

After infection

\[ U = \text{Enc}_{PK_M}(\text{key}) \]

\[ \text{request} = \text{Dec}_{SK_S}(r) \]
CryptoLocker encrypts each file

File

File Contents

File Specific AES Key

$A$

RSA Encryption

Encrypted AES Key

$X = \text{Enc } PK_U (A)$

AES Encryption

Enc (File)

Enc A (contents)

$X || \text{Encrypted Contents}$
Decrypting modern ransomware:

1. Brute force is impossible
2. With a cold storage backup, just delete the malware and restore the files
3. Otherwise, pay ransom of ~2 bitcoins before the timer expires
A = Dec $SK_U(X)$

File = Dec A (Contents)

$X \|\| \text{Encrypted Contents}$

$A \|\| \text{Encrypted Contents}$

Original File Contents
WHAT ARE THE BENEFITS CONSEQUENCES?

- Funding criminals
- Bitcoin theft and inflation
- Temporary, perhaps permanent, loss of files
- Worm-like infection of subsequent machines
- Computer takeover! 250,000 computers infected.
  - DDoS
  - Bitcoin mining
WHAT CAN WE DO ABOUT IT?

- Once active, cannot be stopped besides payment
- **Prevention** (backups) and caution are key
- Deleting the malware will not remove the encryption and will hinder your ability to pay up—you’ll have to reinfect your computer
- By creating a honeypot (large volume of garbage data) on hard drives, sysadmins have caught the malware in action
• Krebs on Security
• Malware Bytes
• overview on ransomware from Symantec
• Nakedsecurity on Cryptolocker
• Cryptolocker technical analysis by kernelmode
• Cryptolocker FAQ by bleeping computer
• Reddit, and a followup post
• Analysis of ransomware software from Journal of Computer Virology
• differences from CL 1.0 to 2.0
• Kapersky - 2048 bit key(s)
• Police station falls victim, boston.com
• ABC news producer falls victim
• BBC infection statistics
Thanks for listening!

Any questions?