Topics

- What is Ransomware?
- Basic Ransomware Operation
- A Little History
- Ransomware Characteristics
- Actual Compromises
- Some Help With Recovery
- A Plan for Protection

www.bleepingcomputer.com
What is Ransomware?

- Ransomware, such as Cryptolocker and Cryptowall, does not bother to steal your critical files (Office documents, photos, videos) as it is much easier to just encrypt them in-place and give you a ransom note.
- If the ransom is not paid by its due date, you do not get the decryption key needed to decrypt your files.
- Depending on the variant of Ransomware you’ve been infected with, you may be able to recover your files.
Basic Ransomware Operation

- Infect system via email attachment, Angler exploit kit (0-day Flash exploit), or GameOver Zeus Botnet.
- Contact CnC server to generate / receive encryption key.
- Perform a depth first search of all disk folders (including network drives), encrypting files with targeted extensions using with one of several algorithms, such as RSA, ECC, AES.
- Place ransom notes in all folders where files were encrypted.
- Delete malware when encryption is complete and display final ransom note.
Basic Ransomware Operation

- Depending on which variant of Ransomware a system has been infected with, other activities shown here may also take place:
  - Deletion of Shadow Volume copies:
    - "C:\Windows\SYsWOW64\cmd.exe" /C "C:\Windows\Sysnative\vssadmin.exe" Delete Shadows /All /Quiet
  - Secure deletion of original files after they’ve been encrypted.
  - Malware setup as a scheduled task to run whenever system boots.
A Little History

- Cryptolocker arrives in September 2013.
  - Spread via infected email attachments and via the GameOver Zeus botnet until shut down by Operation Tovar.
- CryptorBit / HowDecrypt arrives in December 2013.
- CBT Locker / Critroni arrives in July 2014.
- CryptoWall arrives in September 2014.
  - Followed by CryptoWall 2.0 in October and CryptoWall 3.0 in January 2015.
- TeslaCrypt arrives in February 2015.
  - Files associated with video games also encrypted.
- AlphaCrypt arrives in April 2015.
Ransomware Characteristics

- File types that are targeted for encryption can include the following:

  .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .sc2save, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mcgame, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .001, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .DayZProfile, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, .unity3d, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .pl2, .pxf, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rw1, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbfv, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt
Ransomware Characteristics
Ransomware Characteristics

All your documents, photos, databases and other important files have been encrypted with strongest encryption RSA-2048 key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main encryptor red window, examine it and follow the instructions. Otherwise, it seems that you or your antivirus deleted the encryptor program.

Now you have the last chance to decrypt your files.

Open in your browser one of the links:
http://is6xsojdy4qtgur.xfnwdsy4j37.com
http://is6xsojdy4qtgur.9isernvur33.com
https://is6xsojdy4qtgur.tor2web.blutmagie.de

They are public gates to the secret server.

Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.
12kpuMak91BF5PKr1NdUNyi42fr0Mwa8tB

Follow the instructions on the server.

If you have problems with gates, use direct connection:
1. Download Tor Browser from http://torproject.org
2. In the Tor Browser open the http://is6xsojdy4qtgur.onion/
   * Note that this server is available via Tor Browser only.
   * Retry in 1 hour if site is not reachable.

Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.
12kpDMak91BF5PKr1NdUNyi42fr0Mwa8tB

Follow the instructions on the server.
**Ransomware Characteristics**

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
More information about the encryption keys using RSA-2048 can be found here:

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private. All your files were encrypted with the public key, which has been transferred to your computer via the Internet. Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed. If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1. https://kpai7ycrjxqkilp.toraminer.com/g169
2. https://kpai7ycrjxqkilp.torchen.com/g169
3. https://kpai7ycrjxqkilp.way2tor.com/g169

If for some reasons the addresses are not available, follow these steps:
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: kpai7ycrjxqkilp.onion/g169
4. Follow the instructions on the site.

**IMPORTANT INFORMATION:**
Your personal page: https://kpai7ycrjxqkilp.toraminer.com/g169
Your personal page (using TOR): kpai7ycrjxqkilp.onion/g169
Your personal identification number (if you open the site (or TOR’s) directly): g169
Ransomware Characteristics

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Also, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. [https://kpat7yr7jxzklip.torminator.com/g169](https://kpat7yr7jxzklip.torminator.com/g169)
2. [https://kpat7yr7jxzklip.topchek.com/g169](https://kpat7yr7jxzklip.topchek.com/g169)
3. [https://kpat7yr7jxzklip.way2tor.com/g169](https://kpat7yr7jxzklip.way2tor.com/g169)

If for some reasons the addresses are not available, follow these steps:

2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: kpat7yr7jxzklip.onion@g169
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGE: [https://kpat7yr7jxzklip.torminator.com/g169](https://kpat7yr7jxzklip.torminator.com/g169)
Your Personal PAGE (using TOR): kpat7yr7jxzklip.onion@g169
Your personal code (if you open the site (or TOR’s) directly): g169
Ransomware Characteristics
# Ransomware Characteristics

![File List]

<table>
<thead>
<tr>
<th>Name</th>
<th>Label</th>
<th>Item #</th>
<th>Ext</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>152566</td>
<td>html</td>
<td>9/22/2014 11:19:22 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>152585</td>
<td>html</td>
<td>9/22/2014 11:19:22 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>152630</td>
<td>html</td>
<td>9/22/2014 11:19:22 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158014</td>
<td>html</td>
<td>9/23/2014 4:42:56 PM (2)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158030</td>
<td>html</td>
<td>9/22/2014 11:19:23 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158041</td>
<td>html</td>
<td>9/22/2014 11:19:23 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158061</td>
<td>html</td>
<td>9/22/2014 11:19:23 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158083</td>
<td>html</td>
<td>9/22/2014 11:19:23 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158101</td>
<td>html</td>
<td>9/22/2014 11:19:23 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158130</td>
<td>html</td>
<td>9/23/2014 4:42:30 PM (2)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158209</td>
<td>html</td>
<td>9/22/2014 11:20:07 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158247</td>
<td>html</td>
<td>9/22/2014 11:21:45 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158331</td>
<td>html</td>
<td>9/22/2014 11:21:48 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158354</td>
<td>html</td>
<td>9/22/2014 11:21:53 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158387</td>
<td>html</td>
<td>9/22/2014 11:21:52 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158427</td>
<td>html</td>
<td>9/22/2014 11:22:26 PM (1)</td>
<td></td>
</tr>
<tr>
<td>DECRYPT_INSTRUCTION.HTML</td>
<td>158590</td>
<td>html</td>
<td>9/22/2014 11:22:27 PM (1)</td>
<td></td>
</tr>
</tbody>
</table>
Ransomware Characteristics

- If the ransomware is allowed to finish encrypting files, it deletes itself. Since it was discovered relatively quickly, it still existed on disk:
Ransomware Characteristics

![VirusTotal Analysis](image)

- **SHA256:** 99fc04d82877acea0247286d41186b985ab773b19ce8cefe7866f1fafa50a35a029
- **File name:** k6fbqqw.exe
- **Detection ratio:** 42 / 56
- **Analysis date:** 2015-05-31 14:02:13 UTC (0 minutes ago)

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALYac</td>
<td>Trojan.GenericKD.2382607</td>
<td>20160531</td>
</tr>
<tr>
<td>AVG</td>
<td>FileCryptor.BLZ</td>
<td>20150531</td>
</tr>
<tr>
<td>AVWare</td>
<td>Trojan.Win32.GenericIBT</td>
<td>20150531</td>
</tr>
<tr>
<td>Ad-Aware</td>
<td>Trojan.Generic.2382587</td>
<td>20150531</td>
</tr>
<tr>
<td>AhnLab-V3</td>
<td>Win-Trojan/Mda.275456</td>
<td>20150531</td>
</tr>
<tr>
<td>AntiX-AVL</td>
<td>Trojan/Ransom.Win32.Bitman</td>
<td>20160531</td>
</tr>
<tr>
<td>Avast</td>
<td>Win32-Malware-gen</td>
<td>20160531</td>
</tr>
<tr>
<td>Avira</td>
<td>TR/Dropper.A.38261</td>
<td>20160531</td>
</tr>
<tr>
<td>Baidu-International</td>
<td>Trojan.Win32.Ransom.lq</td>
<td>20150531</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Trojan.GenericKD.2382507</td>
<td>20150531</td>
</tr>
<tr>
<td>CAT-QuickHeal</td>
<td>Ransom.Tescrypt.r3</td>
<td>20150530</td>
</tr>
</tbody>
</table>
Ransomware Characteristics

GetThreadContext
SetThreadContext
LoadLibraryW
CreateProcessA
GetProcAddress
LoadLibraryA
GetModuleFileNameA
KERNEL32.dll
GetLastError
HeapFree
HeapAlloc
GetModuleHandleW
Sleep
ExitProcess
GetStartupInfoW
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
SetUnhandledExceptionFilter
IsDebuggerPresent
HeapCreate
VirtualFree
DeleteCriticalSection
LeaveCriticalSection
EnterCriticalSection
VirtualAlloc
HeapReAlloc
WriteFile

GetStdHandle
TlsGetValue
TlsAlloc
TlsSetValue
TlsFree
InterlockedIncrement
SetLastError
GetCurrentThreadId
InterlockedDecrement
InitializeCriticalSectionAndSpinLock
GetModuleFileNameW
FreeEnvironmentStringsW
GetEnvironmentStringsW
GetCommandLineW
SetHandleCount
GetFileType
GetStartupInfoA
QueryPerformanceCounter
GetTickCount
GetCurrentProcessId
GetSystemTimeAsFileTime
RtlUnwind
GetCPInfo
GetACP
GetOEMCP
IsValidCodePage
HeapSize
GetLocaleInfoA

WideCharToMultiByte
GetStringTypeA
MultiByteToWideChar
GetStringTypeW
LCMapStringA
LCMapStringW
## Ransomware Characteristics

### PE header basic information

<table>
<thead>
<tr>
<th>Target machine</th>
<th>Intel 386 or later processors and compatible processors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Compilation timestamp</strong></td>
<td>2015-05-07 05:59:59</td>
</tr>
<tr>
<td><strong>Link date</strong></td>
<td>6:59 AM 5/7/2015</td>
</tr>
<tr>
<td><strong>Entry Point</strong></td>
<td>0x00023154</td>
</tr>
<tr>
<td><strong>Number of sections</strong></td>
<td>3</td>
</tr>
</tbody>
</table>

### PE sections

<table>
<thead>
<tr>
<th>Name</th>
<th>Virtual address</th>
<th>Virtual size</th>
<th>Raw size</th>
<th>Entropy</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>.rdata</td>
<td>4096</td>
<td>7074</td>
<td>7160</td>
<td>5.49</td>
<td>97a4dc4cc1d5d1b45b5b93bc26733776</td>
</tr>
<tr>
<td>.data</td>
<td>12288</td>
<td>199708</td>
<td>162816</td>
<td>7.70</td>
<td>19cc688e335f2b481917648085b4fb50</td>
</tr>
<tr>
<td>.rsrcc</td>
<td>212992</td>
<td>104448</td>
<td>104448</td>
<td>2.95</td>
<td>3eba9ec081cc6e08f7ca5b6c692526f1</td>
</tr>
</tbody>
</table>

### PE imports

- KERNEL32.dll
- GetLastError
- InitializeCriticalSectionAndSpinCount
- HeapFree
- GetStdHandle
- EnterCriticalSection
- LCMapStringW
Ransomware Characteristics

```
R0034
An application has made an attempt to load the C runtime library incorrectly.
Please contact the application's support team for more information.
R0033
- Attempt to use MSIL code from this assembly during native code initialization
This indicates a bug in your application. It is most likely the result of calling
an MSIL-compiled (/clr) function from a native constructor or from DllMain.
R0032
- not enough space for locale information
R0031
- Attempt to initialize the CRT more than once.
This indicates a bug in your application.
R0030
- CRT not initialized
R0028
- unable to initialize heap
R0027
- not enough space for lowio initialization
R0026
- not enough space for stdio initialization
R0025
- pure virtual function call
R0024
- not enough space for _onexit/atexit table
R0019
- unable to open console device
R0018
- unexpected heap error
R0017
- unexpected multithread lock error
R0016
- not enough space for thread data
This application has requested the Runtime to terminate it in an unusual way.
Please contact the application's support team for more information.
R0009
- not enough space for environment
R0008
- not enough space for arguments
R0002
- floating point support not loaded
Microsoft Visual C++ Runtime Library
...
<program name unknown>
Runtime Error!
Program:
EncodePointer
DecodePointer
FlSFree
FlSSetValue
FlSSetValue
FlSAlloc
GetProcessWindowStation
GetUserObjectInformationA
GetLastError
GetActivePopup
GetActiveWindow
MessageBoxA
```
Actual Compromises

- Company A: Health Care provider
  - Employee computer infected via email attachment.
  - No malware scanning on Exchange server or employee computer.
  - Files on computer and all company network shares mapped to the employee computer were encrypted.
  - Company used Carbonite for real-time backup.
  - All Carbonite files were replaced with (new) encrypted versions.
  - IT staff located offending email on Exchange server and deleted it.
  - The company paid the Bitcoin ransom.
Actual Compromises

- Company B: Educational Institution
  - Remote employee laptop infected via personal email attachment.
  - Files on laptop were encrypted. College policy dictates no files are stored locally…. But this policy is not fully complied with.
  - Husband of employee was security savvy and disconnected computer from VPN connection. This was a good thing!
  - A limited number of files on the schools network shares mapped to the employee computer were encrypted.
  - Spread was limited due to proper permissions in effect.
  - The company reimaged the laptop and restored other encrypted files from a current backup.
  - Endpoint protection did not stop the malware.
Actual Compromises

- **Company C: Town Police**
  - Administrative assistant’s computer infected via email attachment.
  - Files on computer and department file server were encrypted.
  - Files were restored from a recent backup.
  - An IT security audit was suggested but not performed due to budget concerns.
  - Three months later the same employee infected her computer a second time.
  - Many encrypted files were lost due to a failed hardware backup process.
Some Help with Recovery

- Be aware that others have already suffered through ransomware attacks and some tools are available.
- [https://decryptcryptolocker.com/](https://decryptcryptolocker.com/) provides relief for Cryptolocker victims.
Some Help with Recovery

- Varonis provides instructions on detecting and cleaning Cryptolocker infections.

- Bleeping Computer provides the ListCwall tool that will scan the Windows Registry for the Cryptowall key that contains the list of encrypted files. This is helpful for finding out what files were encrypted prior to recovery from backup.
Some Help with Recovery
Some Help with Recovery

- Be aware that others have already suffered through ransomware attacks and some tools are available.
- For TeslaCrypt visit http://blogs.cisco.com/security/talos/teslacrypt for information about what the ransomware does and access to a decryption tool to recover encrypted ECC files.
- AlphaCrypt is a variant of TeslaCrypt, but the Cisco decrypting tool does not work for its EZZ files. However, Bleeping Computer has a decrypting tool that works for ECC and EZZ files, located here: http://www.bleepingcomputer.com/forums/t/574900/teslacrypt-ransomware-changes-its-name-to-alpha-crypt/page-4
Some Help with Recovery
Some Help with Recovery

- Here are the original and decrypted versions of some sample files from an AlphaCrypt infection:
Some Help with Recovery
Some Help with Recovery
A Plan for Protection

- Helping prevent future ransomware infections requires a combination of several things:
  - Maintain current backups.
  - Proper (and limited) access permissions.
  - Use Firewall, IDS / IPS, and anti-virus to assist with real-time detection and mitigation.
  - An Incident Response team in place, ready to quickly respond to an infection.
  - Ongoing security awareness training.
  - Employ Software Restriction Policies.
A Plan for Protection

- Additional suggestions:
  - Check for Shadow Volume copies.
  - Read the blog post located here, which provides interesting insight into the network communications employed by Ransomware and how server event logging may be used to detect an infection:
    - [https://blog.logrhythm.com/tags/cryptolocker/](https://blog.logrhythm.com/tags/cryptolocker/)
  - Keep looking for tools provided by others.
The End

- Thank you for listening.
- Questions?

- Feel free to contact me at jantonakos@excelsior.edu