

Tales From The Crypt

Fighting Ransomware

James L. Antonakos
SUNY Distinguished Teaching Professor
Computer Science, Broome Community College
NCI Fellow

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.



www.wysiwygventures.com

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

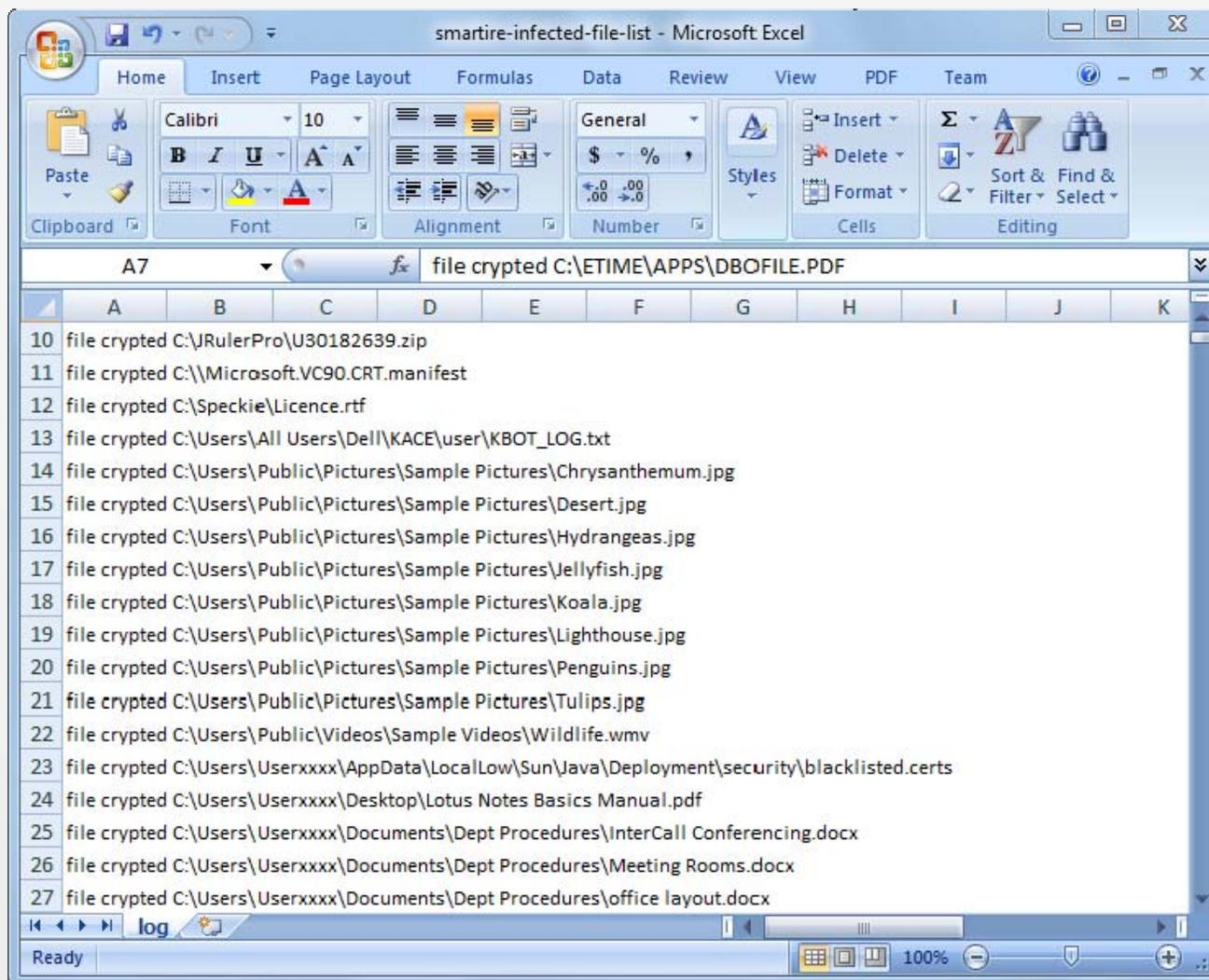
- Cryptolocker arrives in September 2013.
 - Spread via infected email attachments and via the GameOver Zeus botnet until shut down by Operation Tovar.
- CryptorBit / HowDecrypt arrives in December 2013.
- CBT Locker / Critroni arrives in July 2014.
- CryptoWall arrives in September 2014.
 - Followed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

Ransomware Characteristics

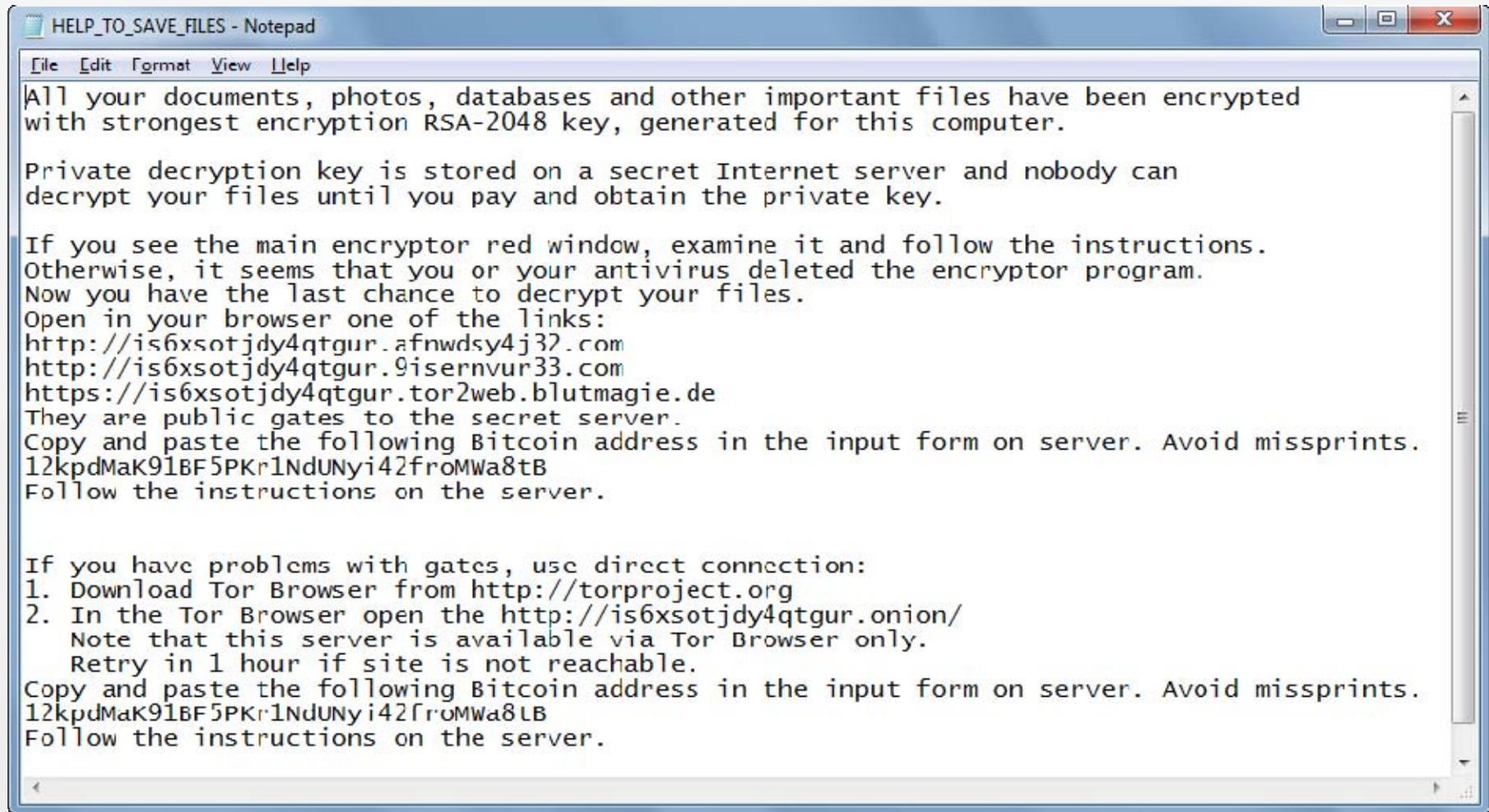
- File types that are targeted for encryption can include the following:

.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, .mpgge, .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, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .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



HELP_TO_SAVE_FILES - Notepad

File Edit Format View Help

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://is6xsotjdy4qtgur.afnwdsy4j32.com>
<http://is6xsotjdy4qtgur.9isernvur33.com>
<https://is6xsotjdy4qtgur.tor2web.blutmagie.de>

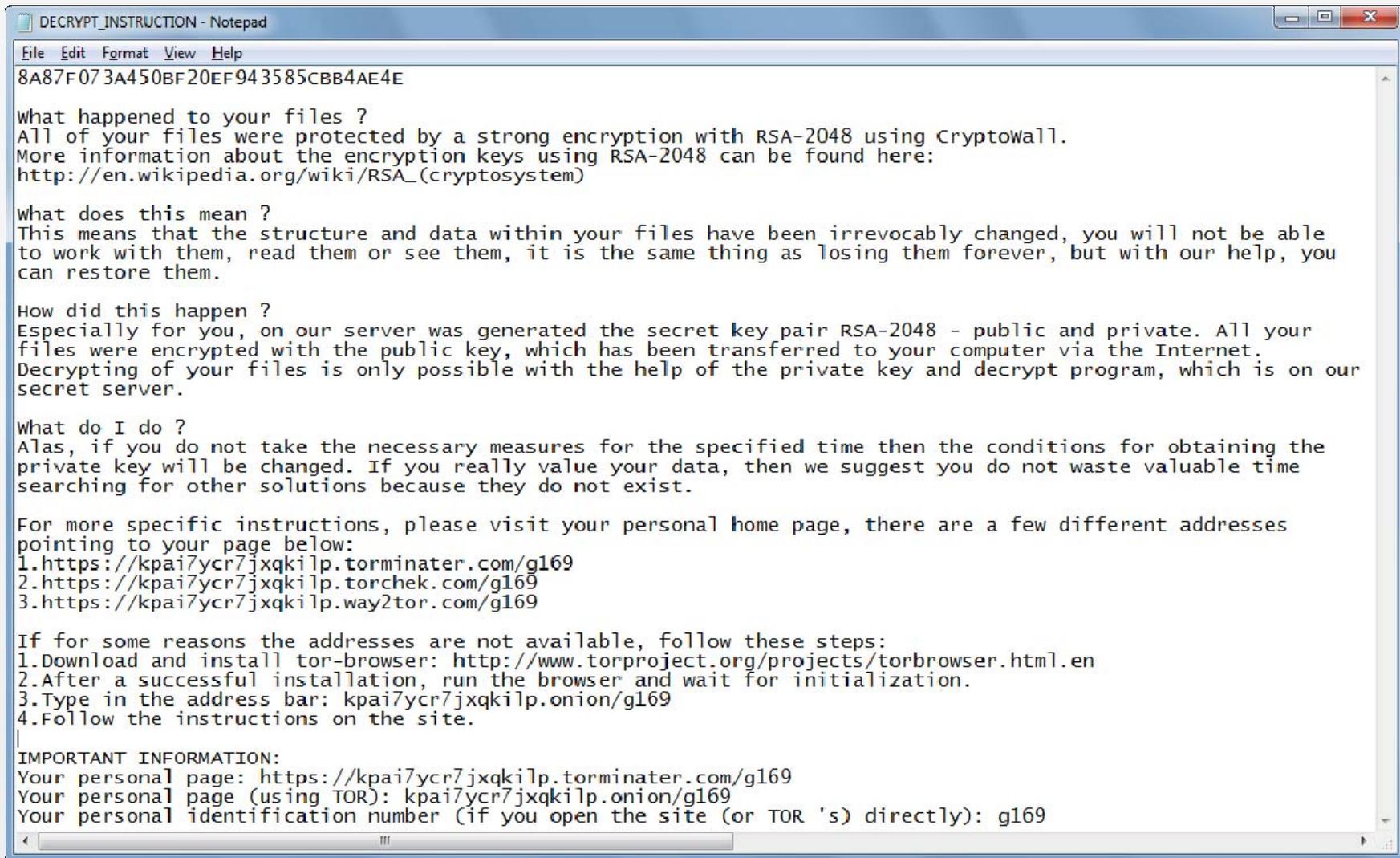
They are public gates to the secret server.
Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.
12kpdMaK91BF5PKr1NdUNyi42fromWa8tB
Follow the instructions on the server.

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://is6xsotjdy4qtgur.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.
12kpdMaK91BF5PKr1NdUNyi42fromWa8tB
Follow the instructions on the server.

Ransomware Characteristics



DECRYPT_INSTRUCTION - Notepad

File Edit Format View Help

8A87F073A450BF20EF943585CBB4AE4E

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:
[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

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://kpai7ycr7jxqkilp.torminater.com/g169>
2. <https://kpai7ycr7jxqkilp.torchek.com/g169>
3. <https://kpai7ycr7jxqkilp.way2tor.com/g169>

If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: kpai7ycr7jxqkilp.onion/g169
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your personal page: <https://kpai7ycr7jxqkilp.torminater.com/g169>
Your personal page (using TOR): kpai7ycr7jxqkilp.onion/g169
Your personal identification number (if you open the site (or TOR 's) directly): g169



Ransomware Characteristics

8A87F073A450BF20EF943585CBB4AE4E

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: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

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://kpai7ycr7jxqkpl.torminater.com/g169>
2. <https://kpai7ycr7jxqkpl.torchek.com/g169>
3. <https://kpai7ycr7jxqkpl.way2tor.com/g169>

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

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: kpai7ycr7jxqkpl.onion/g169
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGE: <https://kpai7ycr7jxqkpl.torminater.com/g169>
Your Personal PAGE(using TOR): kpai7ycr7jxqkpl.onion/g169
Your personal code (if you open the site (or TOR 's) directly): **g169**

Ransomware Characteristics

The screenshot displays the AccessData Forensic Toolkit (ADFT) interface. The top menu includes File, Edit, View, Evidence, Filter, Tools, Manage, and Help. The main window is divided into several panes:

- Evidence Items:** A tree view on the left showing a directory structure including Administrator, All Users, Default, Default User, AppData, Application Data, Contacts, Cookies, Desktop, Documents, Dell WebCam Central, Fax, and My Music.
- File Content:** A pane on the right showing the hex dump of a file. The hex data is as follows:


```

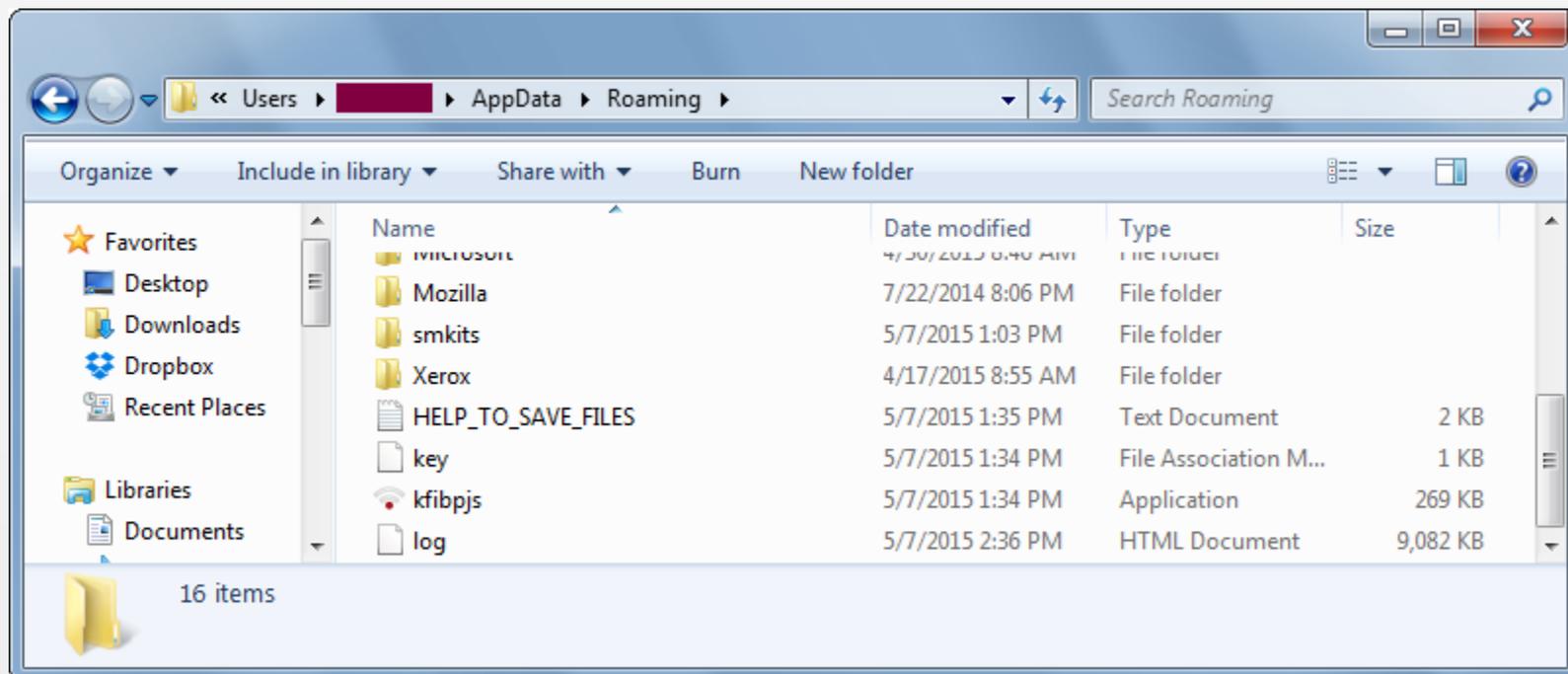
000000 01 FE 42 87 C5 5C AA DE-00 01 00 00 00 2A 08 00 00 |bB`A\*P.....+...
000010 83 E7 1F 00 18 5A 00 00-30 02 CD 8C 0D C0 0D B4 00 00 |c...Z..0.I..A..
000020 30 CA FD 6D 42 5A 98 1F-23 0F 3E DF 9B 17 60 1A 0E ymBZ...#>B...
000030 EE 95 B0 60 B5 52 C5 D3-B5 64 77 E1 E8 85 59 E3 i..`pRÃÓpdwâè..Yâ
000040 B5 C9 C8 6A 9F 54 7B 9E-1F 72 A3 DF CC 41 7C 5D µÈËj-I{..rèSIA|]
000050 74 D4 5F E6 40 DA F0 2A-6C 34 E0 70 6C 1C EE D8 t0_æ@08*14âpl.i0
000060 3F 33 A4 8D 5C 77 8C 38-AC 7B DE C5 AE 75 77 86 ?3x.\w-8-{B&ouw
000070 7E C1 89 65 DB FF 0F B9-84 CF 89 4A 04 3C 60 D2 -Ã.eÛy..I.J.<`0
000080 6C 9A 25 9E BC 44 83 FB-9C 88 30 02 42 E5 CA BF 1-;`kD-â..0.BâÈz
000090 1D 27 7E 88 93 0F B1 8D-46 1E EC 1F 09 B6 B6 62 `..w...±.F.i..ÛÛb
      
```
- File List:** A table at the bottom showing a list of files with columns for Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, Accessed, and Modified. The table contains 20 rows of file entries, including various .jpg and .kc8 files.

Ransomware Characteristics

<input checked="" type="checkbox"/>	▲ Name	Label	Item #	Ext	Created
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		152566	html	9/22/2014 11:19:22 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		152585	html	9/22/2014 11:19:22 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		152630	html	9/22/2014 11:19:22 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158014	html	9/23/2014 4:42:56 PM (2...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158030	html	9/22/2014 11:19:23 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158041	html	9/22/2014 11:19:23 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158061	html	9/22/2014 11:19:23 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158083	html	9/22/2014 11:19:23 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158101	html	9/22/2014 11:22:27 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158130	html	9/23/2014 4:42:30 PM (2...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158209	html	9/22/2014 11:20:07 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158247	html	9/22/2014 11:21:45 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158331	html	9/22/2014 11:21:48 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158354	html	9/22/2014 11:21:53 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158387	html	9/22/2014 11:21:52 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158427	html	9/22/2014 11:22:26 PM (...)
<input type="checkbox"/>	DECRYPT_INSTRUCTION.HTML		158590	html	9/22/2014 11:22:27 PM (...)

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



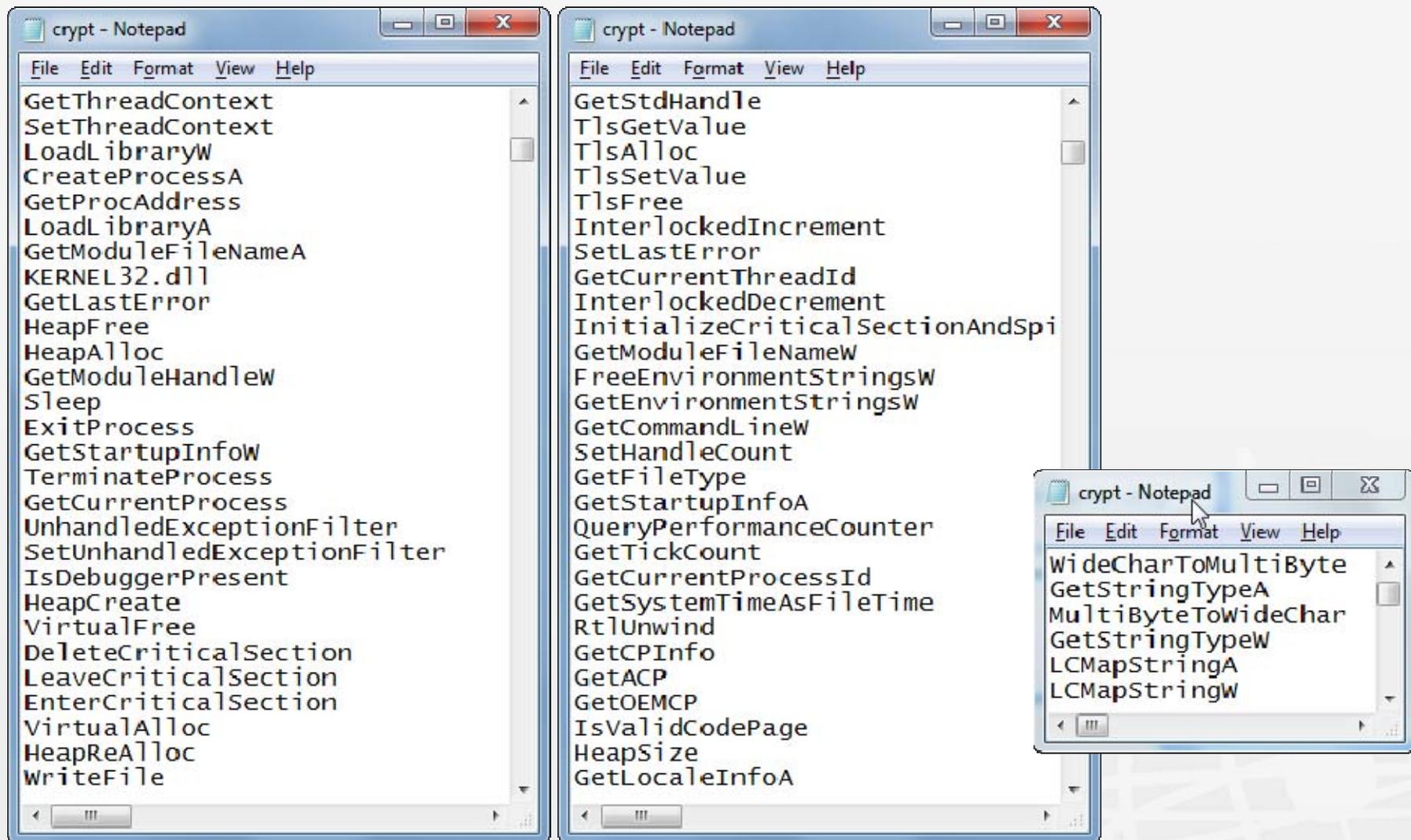
SHA256: 99fc04d82877aea0247286d41186b985ab773b19c8cef8786ffc1fa50e35af29
File name: kfibpjs.exe
Detection ratio: 42 / 56
Analysis date: 2015-05-31 14:02:13 UTC (0 minutes ago)



Analysis File detail Additional information Comments Votes Behavioural information

Antivirus	Result	Update
ALYac	Trojan.GenericKD.2382507	20150531
AVG	FileCryptor.BLZ	20150531
AVware	Trojan.Win32.GenericIBT	20150531
Ad-Aware	Trojan.GenericKD.2382507	20150531
AhnLab-V3	Win-Trojan/Mda.275456	20150531
Antiy-AVL	Trojan[Ransom]/Win32.Bitman	20150531
Avast	Win32:Malware-gen	20150531
Avira	TR/Dropper.A.38261	20150531
Baidu-International	Trojan.Win32.Ransom.lq	20150531
BitDefender	Trojan.GenericKD.2382507	20150531
CAT-QuickHeal	Ransom.Tescrypt.r3	20150530

Ransomware Characteristics



The image shows three Notepad windows, each containing a list of Windows API functions and DLLs. The windows are titled "crypt - Notepad".

Window 1 (Left):

- 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

Window 2 (Middle):

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

Window 3 (Right):

- WideCharToMultiByte
- GetStringTypeA
- MultiByteToWideChar
- GetStringTypeW
- LCMapStringA
- LCMapStringW

Ransomware Characteristics

☰ PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2015-05-07 05:59:59
Link date	6:59 AM 5/7/2015
Entry Point	0x00023154
Number of sections	3

🏗 PE sections

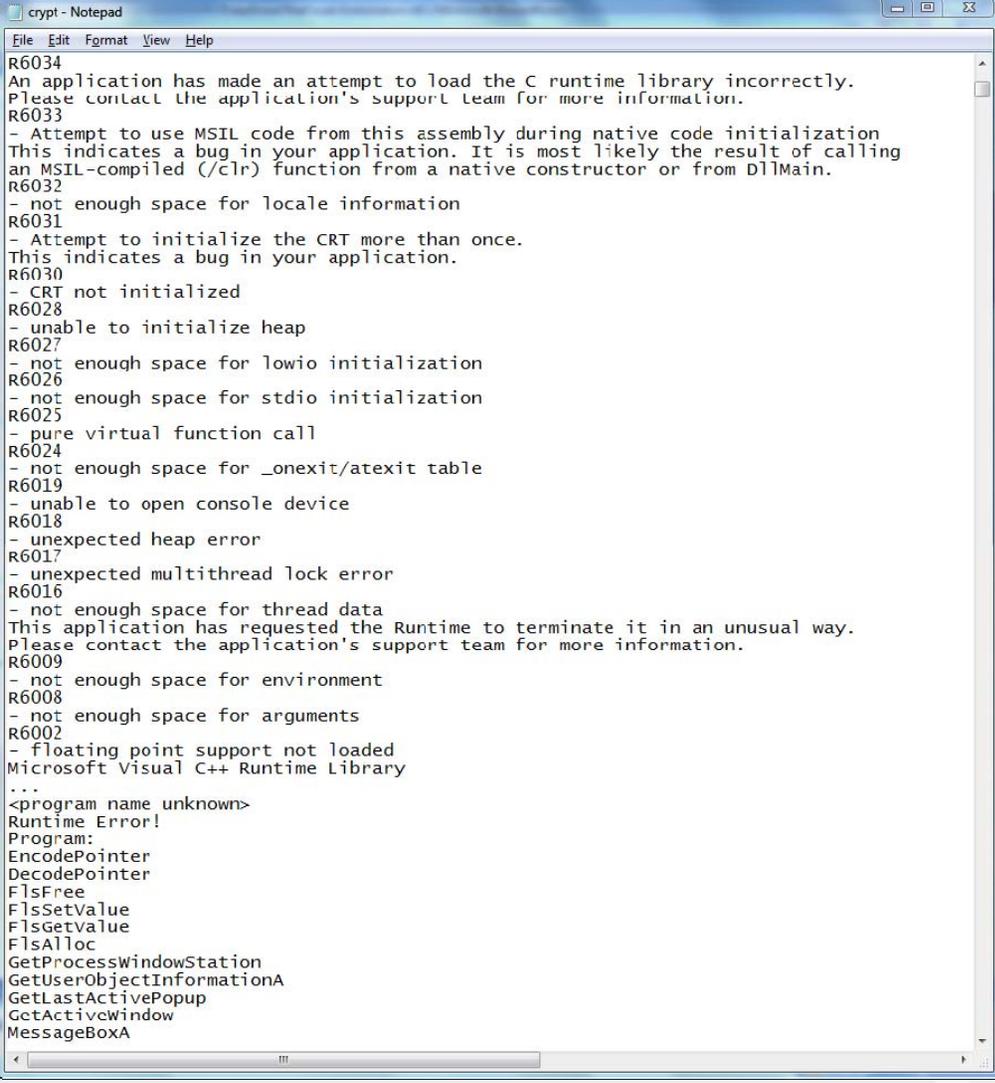
Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.rdata	4096	7074	7168	5.49	97a4dc4cc1d5d1b45b5b93bc28733776
.data	12288	199708	162816	7.70	19cc688e335f2b481917648085b4fb60
.rsrc	212992	104448	104448	2.95	3eba9ec081ccee08f7ca5b6c692526f1

➡ PE imports

[+] KERNEL32.dll

GetLastError
InitializeCriticalSectionAndSpinCount
HeapFree
GetStdHandle
EnterCriticalSection
LCMapStringW

Ransomware Characteristics



```
crypt - Notepad
File Edit Format View Help
R6034
An application has made an attempt to load the C runtime library incorrectly.
Please contact the application's support team for more information.
R6033
- 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.
R6032
- not enough space for locale information
R6031
- Attempt to initialize the CRT more than once.
This indicates a bug in your application.
R6030
- CRT not initialized
R6028
- unable to initialize heap
R6027
- not enough space for lowio initialization
R6026
- not enough space for stdio initialization
R6025
- pure virtual function call
R6024
- not enough space for _onexit/atexit table
R6019
- unable to open console device
R6018
- unexpected heap error
R6017
- unexpected multithread lock error
R6016
- 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.
R6009
- not enough space for environment
R6008
- not enough space for arguments
R6002
- floating point support not loaded
Microsoft Visual C++ Runtime Library
...
<program name unknown>
Runtime Error!
Program:
EncodePointer
DecodePointer
FlsFree
FlsSetValue
FlsGetValue
FlsAlloc
GetProcessWindowStation
GetObjectInformationA
GetLastActivePopup
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

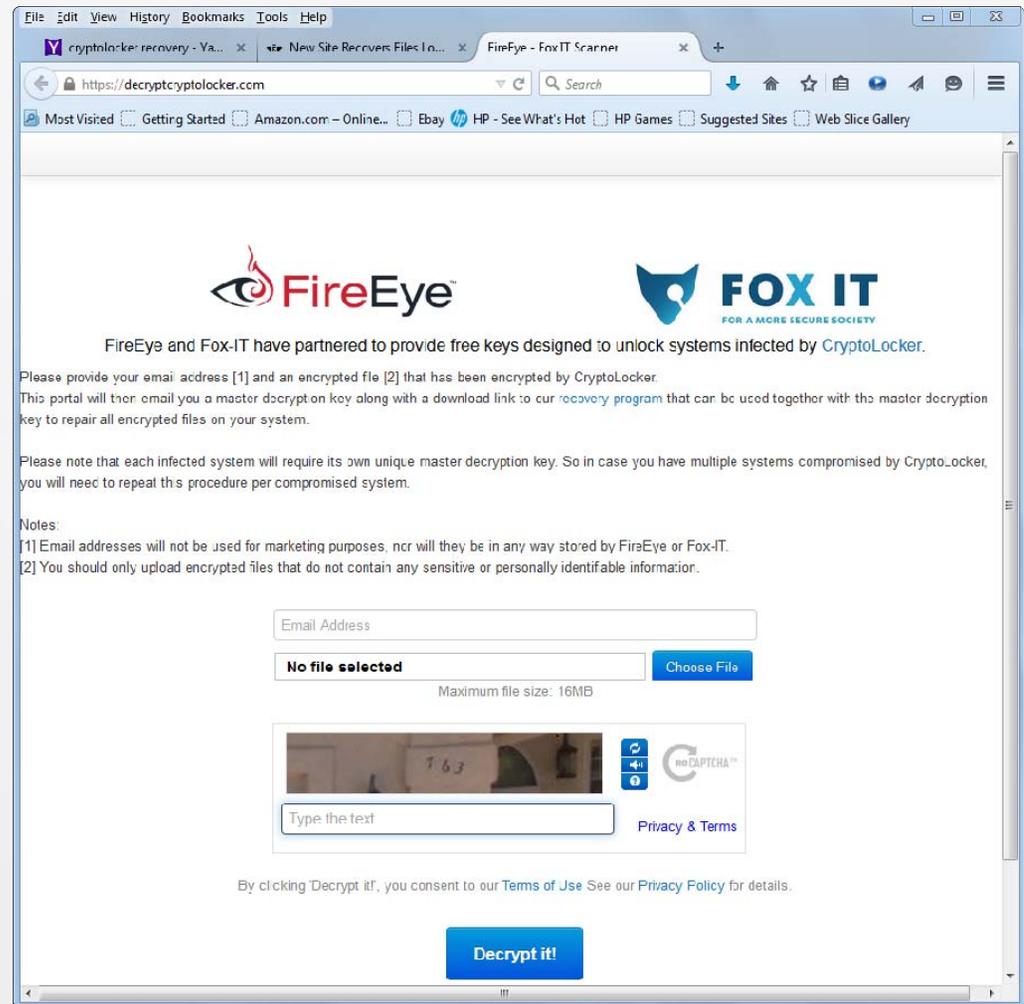
- **Company B: Educational Institution**
 - Remote employee laptop infected via personal email attachment.
 - Files on laptop were encrypted. College policy dictates no files are stored locally.... But this policy is not fully complied with.
 - Husband of employee was security savvy and disconnected 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/> provides relief for Cryptolocker victims.



The screenshot shows a web browser window displaying the website <https://decryptcryptolocker.com/>. The page features logos for FireEye and FOX IT. Below the logos, the text reads: "FireEye and Fox-IT have partnered to provide free keys designed to unlock systems infected by CryptoLocker." The page instructs users to provide an email address and an encrypted file. It also includes a "Choose File" button, a "Maximum file size: 16MB" indicator, a CAPTCHA verification step, and a "Decrypt it!" button at the bottom.

File Edit View History Bookmarks Tools Help

cryptolocker recovery - Ya... New Site Recovers Files In... FireEye - FoxIT Scanner

https://decryptcryptolocker.com

Most Visited Getting Started Amazon.com - Online... Ebay HP - See What's Hot HP Games Suggested Sites Web Slice Gallery

FireEye and Fox-IT have partnered to provide free keys designed to unlock systems infected by CryptoLocker.

Please provide your email address [1] and an encrypted file [2] that has been encrypted by CryptoLocker. This portal will then email you a master decryption key along with a download link to our recovery program that can be used together with the master decryption key to repair all encrypted files on your system.

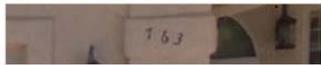
Please note that each infected system will require its own unique master decryption key. So in case you have multiple systems compromised by CryptoLocker, you will need to repeat this procedure per compromised system.

Notes:
[1] Email addresses will not be used for marketing purposes, nor will they be in any way stored by FireEye or Fox-IT.
[2] You should only upload encrypted files that do not contain any sensitive or personally identifiable information.

Email Address

No file selected Choose File

Maximum file size: 16MB

 no CAPTCHA™

Type the text Privacy & Terms

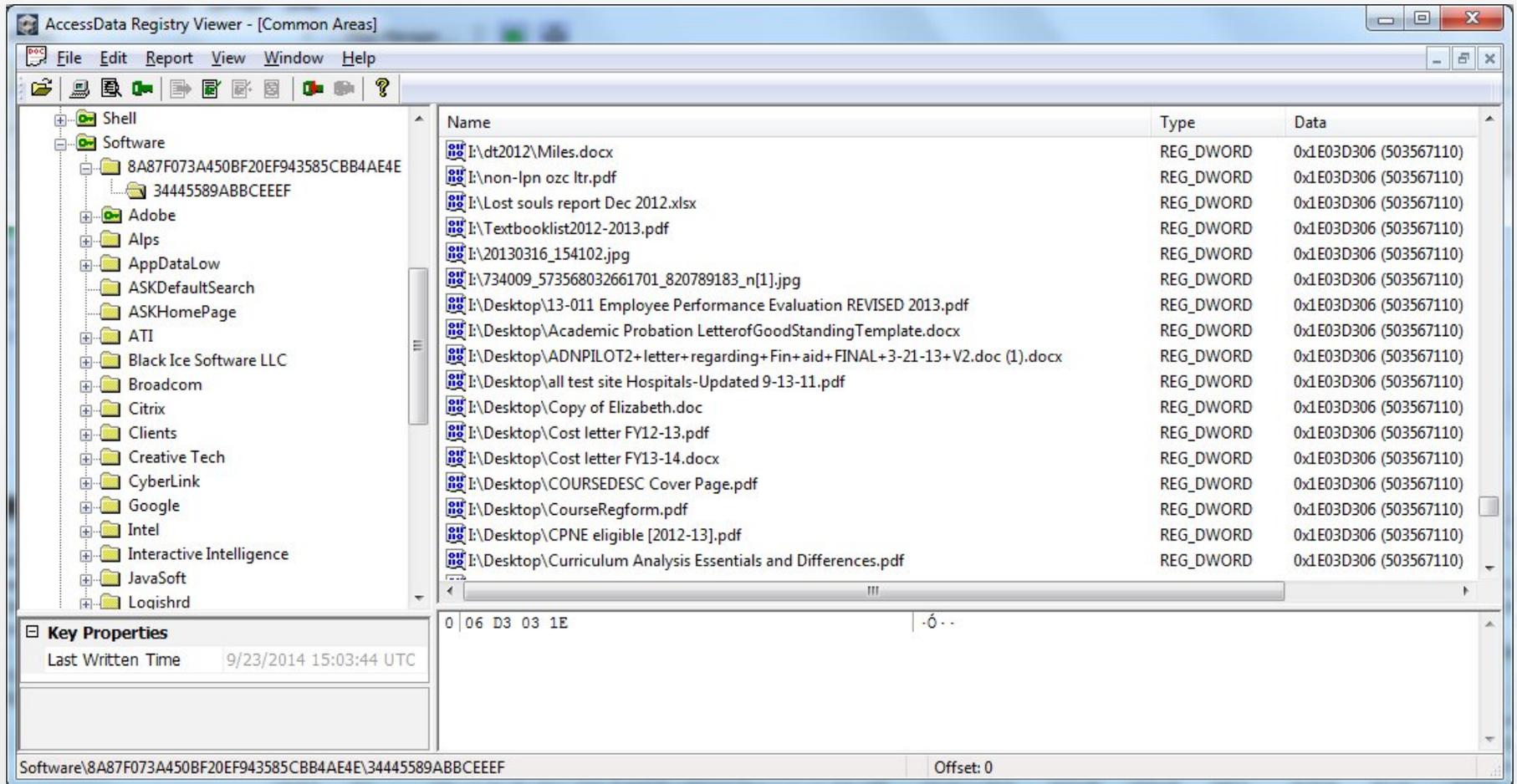
By clicking Decrypt it!, you consent to our Terms of Use See our Privacy Policy for details.

Decrypt it!

Some Help with Recovery

- Varonis provides instructions on detecting and cleaning Cryptolocker infections.
 - <http://blog.varonis.com/detect-clean-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.
 - <http://www.bleepingcomputer.com/download/listcwall/>

Some Help with Recovery



The screenshot shows the AccessData Registry Viewer application. The left pane displays a tree view of registry paths, with the following path selected: `Software\8A87F073A450BF20EF943585CBB4AE4E\34445589ABBCEEEF`. The right pane shows a list of registry values with the following columns: Name, Type, and Data.

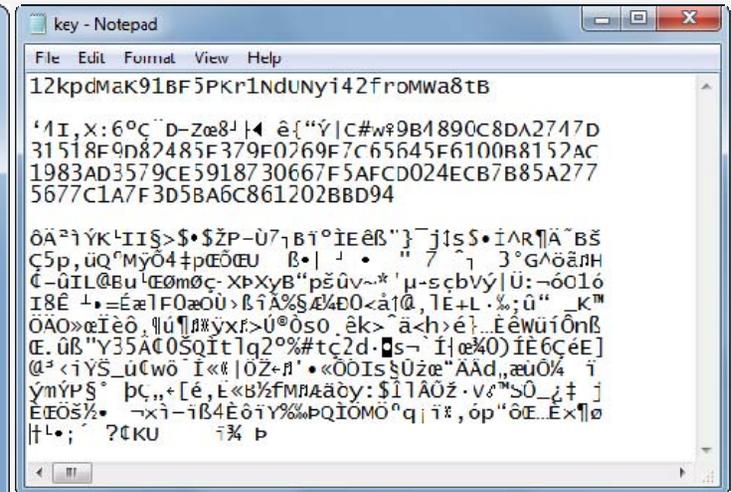
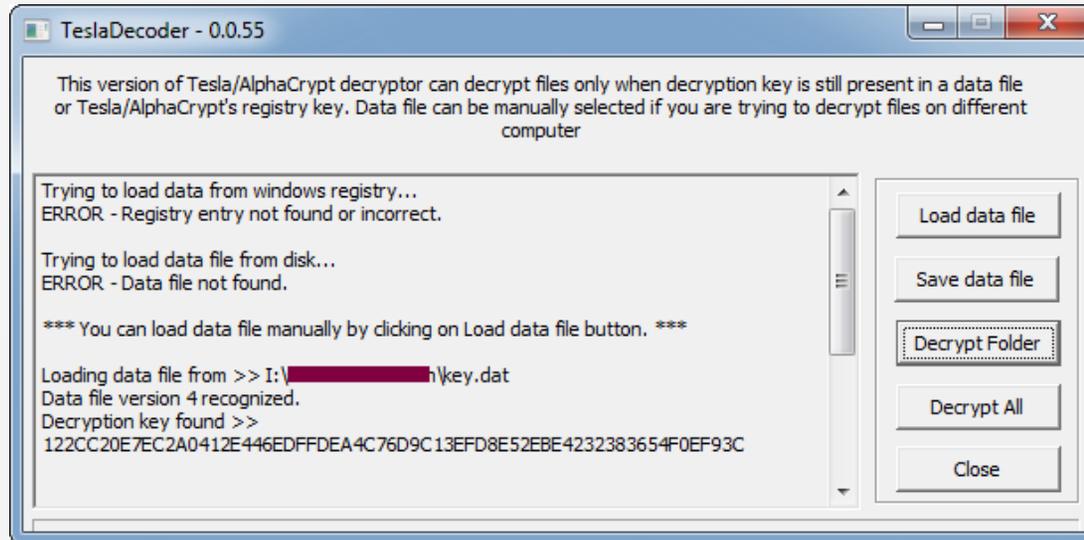
Name	Type	Data
E:\dt2012\Miles.docx	REG_DWORD	0x1E03D306 (503567110)
E:\non-lpn ozc ltr.pdf	REG_DWORD	0x1E03D306 (503567110)
E:\Lost souls report Dec 2012.xlsx	REG_DWORD	0x1E03D306 (503567110)
E:\Textbooklist2012-2013.pdf	REG_DWORD	0x1E03D306 (503567110)
E:\20130316_154102.jpg	REG_DWORD	0x1E03D306 (503567110)
E:\734009_573568032661701_820789183_n[1].jpg	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\13-011 Employee Performance Evaluation REVISED 2013.pdf	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\Academic Probation LetterofGoodStandingTemplate.docx	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\ADNPILOT2+letter+regarding+Fin+aid+FINAL+3-21-13+V2.doc (1).docx	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\all test site Hospitals-Updated 9-13-11.pdf	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\Copy of Elizabeth.doc	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\Cost letter FY12-13.pdf	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\Cost letter FY13-14.docx	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\COURSEDESC Cover Page.pdf	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\CourseRegform.pdf	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\CPNE eligible [2012-13].pdf	REG_DWORD	0x1E03D306 (503567110)
E:\Desktop\Curriculum Analysis Essentials and Differences.pdf	REG_DWORD	0x1E03D306 (503567110)

Below the list, the 'Key Properties' section shows 'Last Written Time' as '9/23/2014 15:03:44 UTC'. The bottom status bar displays the path and 'Offset: 0'.

Some Help with Recovery

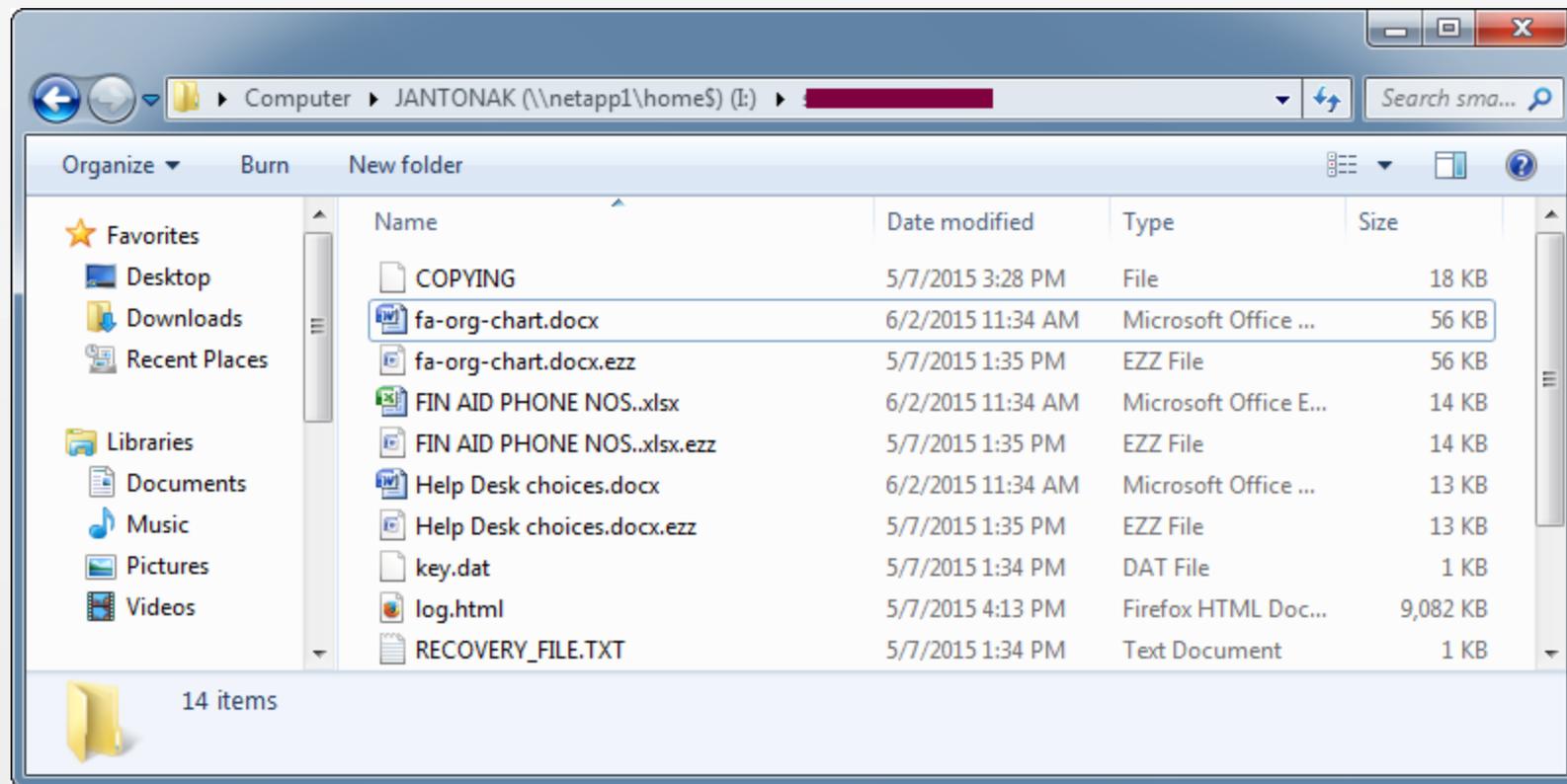
- Be aware that others have already suffered through ransomware attacks and some tools are available.
- For TeslaCrypt visit <http://blogs.cisco.com/security/talos/teslacrypt> for information about what the ransomware does and access to a decryption tool to recover encrypted ECC files.
- AlphaCrypt is 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

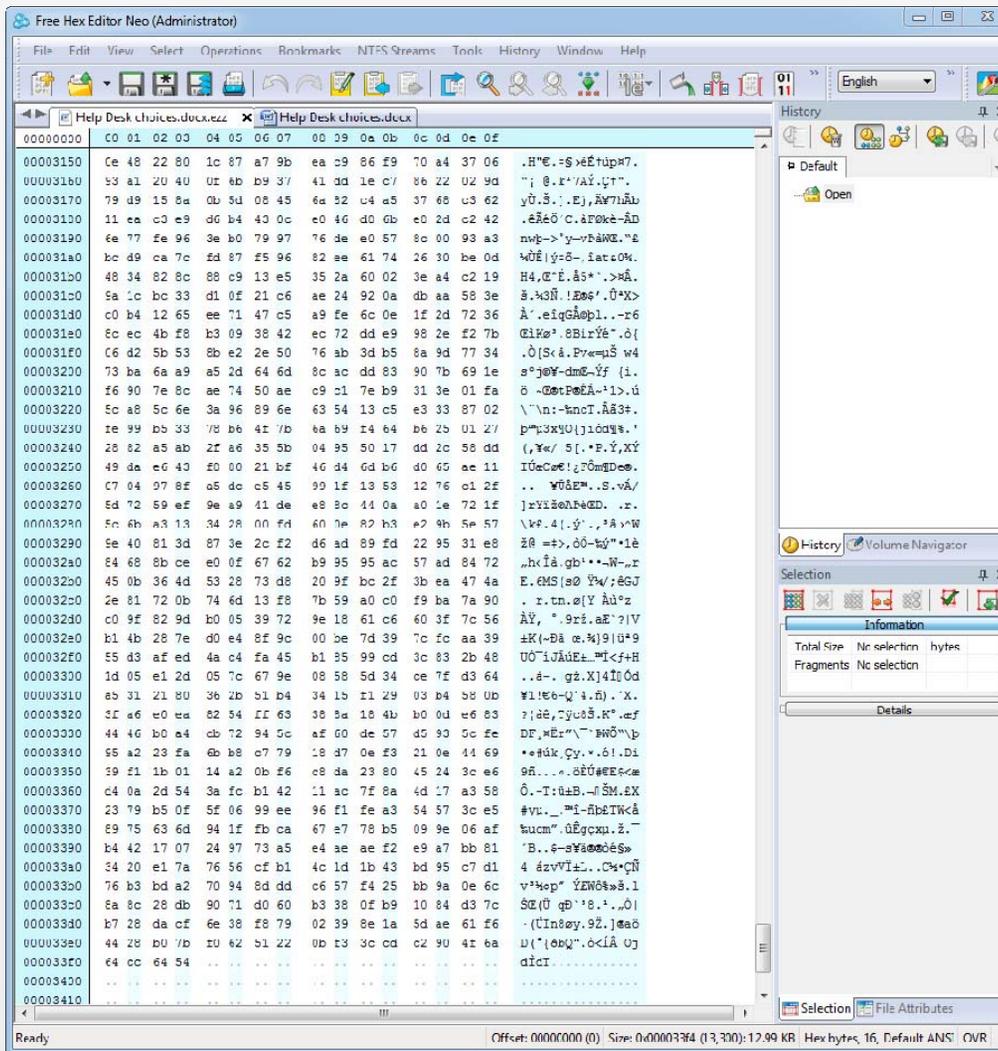


Some Help with Recovery

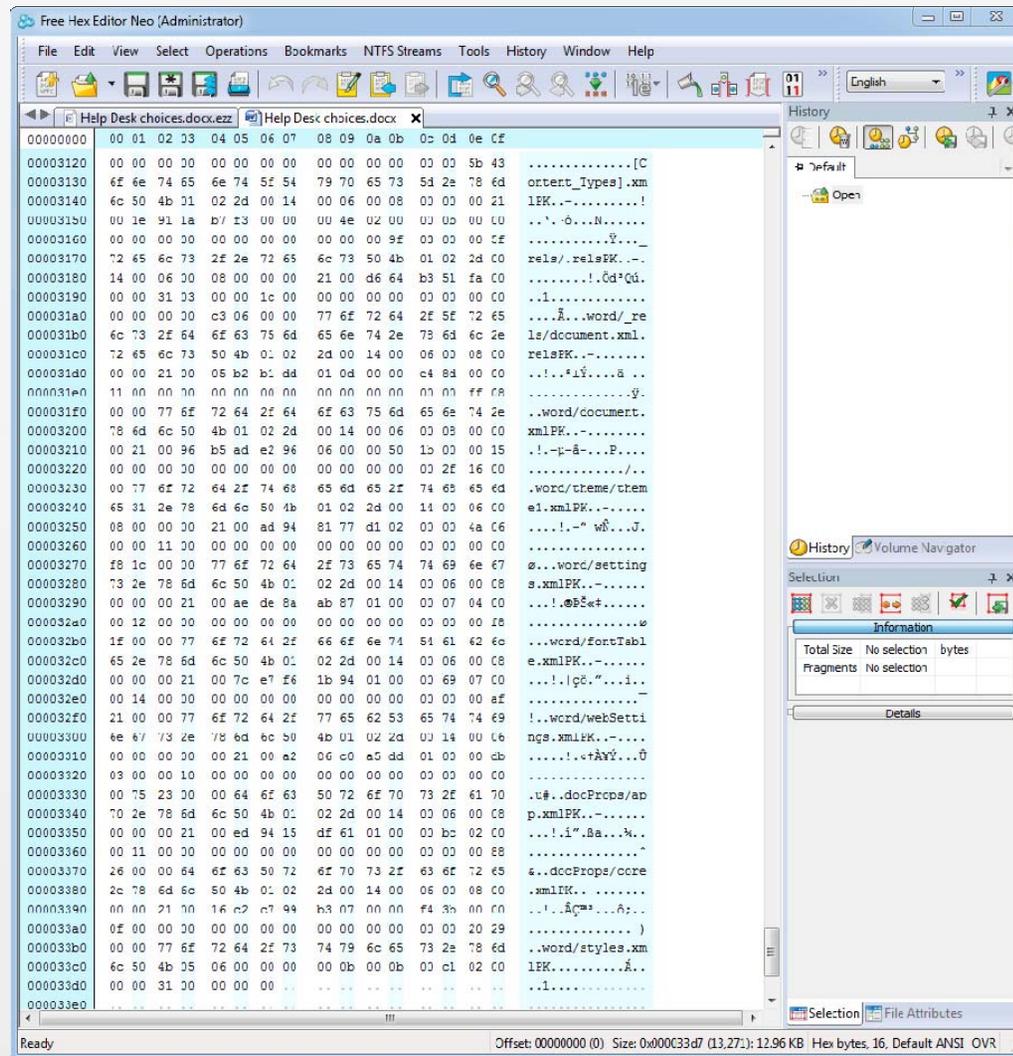
- Here are the original and decrypted versions of some sample files from an AlphaCrypt infection:



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.



www.info-utiles.fr

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/>
 - Keep looking for tools provided by others.



www.info-utiles.fr

The End

- Thank you for listening.
- Questions?
- Feel free to contact me at jantonakos@excelsior.edu