BLACK ALPS
CYBER SECURITY CONFERENCE

Locky Strike:

Smoking the Locky Ransomware Code

By Rommel Joven & Floser Bacurio Jr

FORTINET®

Overview

I. Prevalence of Locky

II. Timeline of Development

III. Technical Analysis

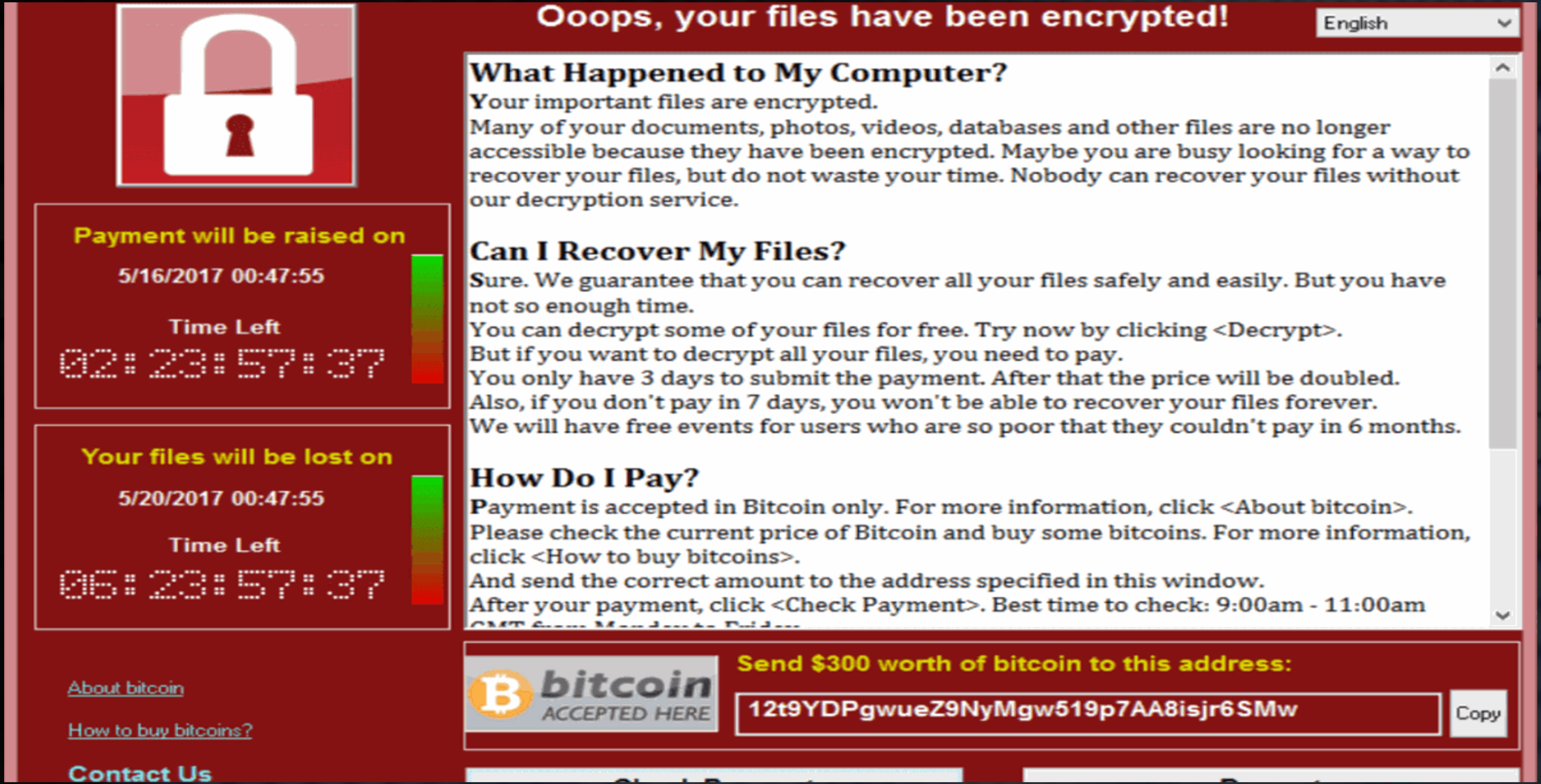
- ❑ Configuration
- ❑ C&C Communication
- ❑ File Encryption

IV. Harvesting Configuration

V. Kill Chain

VI. Interesting Observations

WannaCry



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

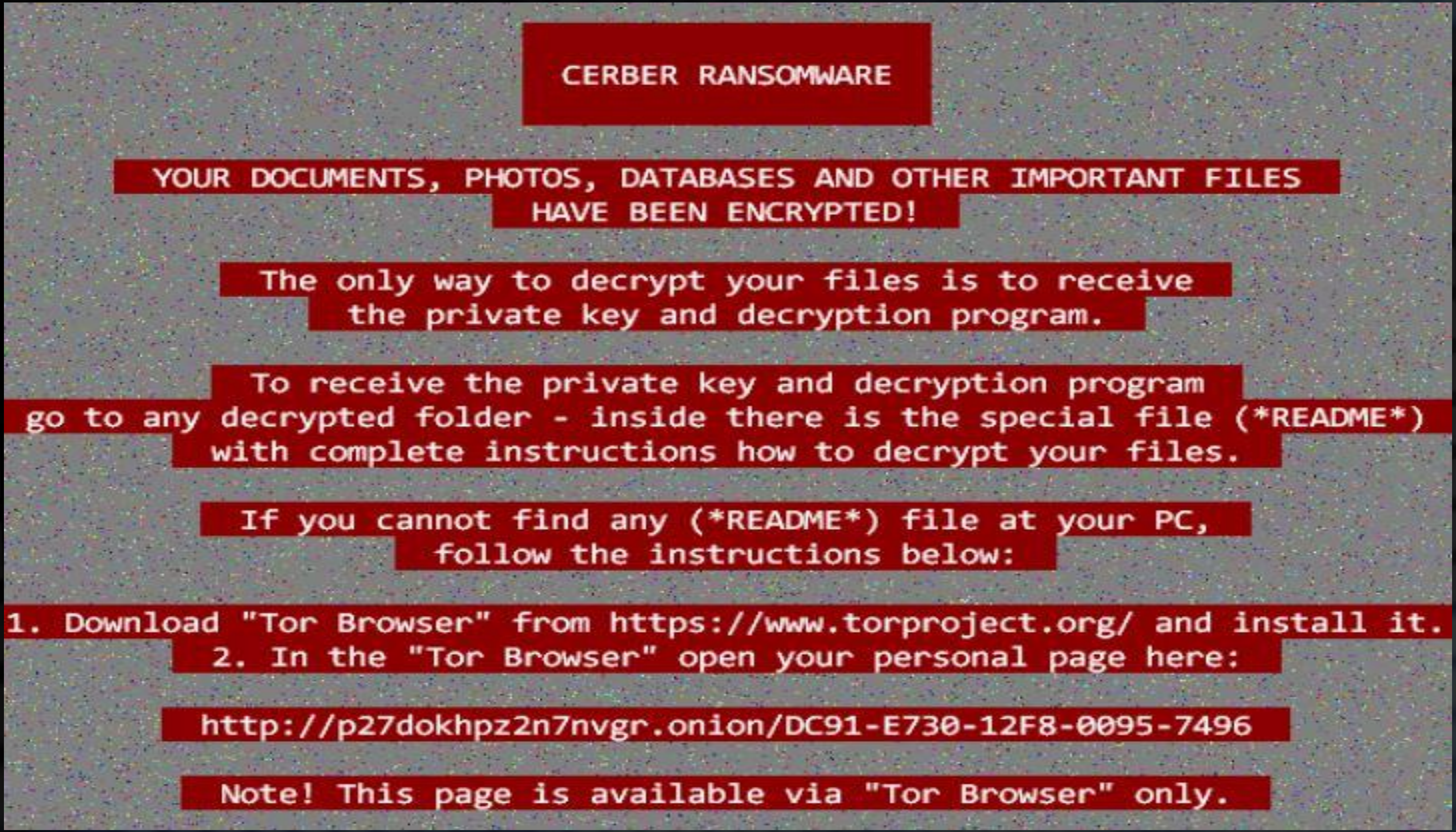
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Cerber



CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive the private key and decryption program.

To receive the private key and decryption program go to any decrypted folder - inside there is the special file (*README*) with complete instructions how to decrypt your files.

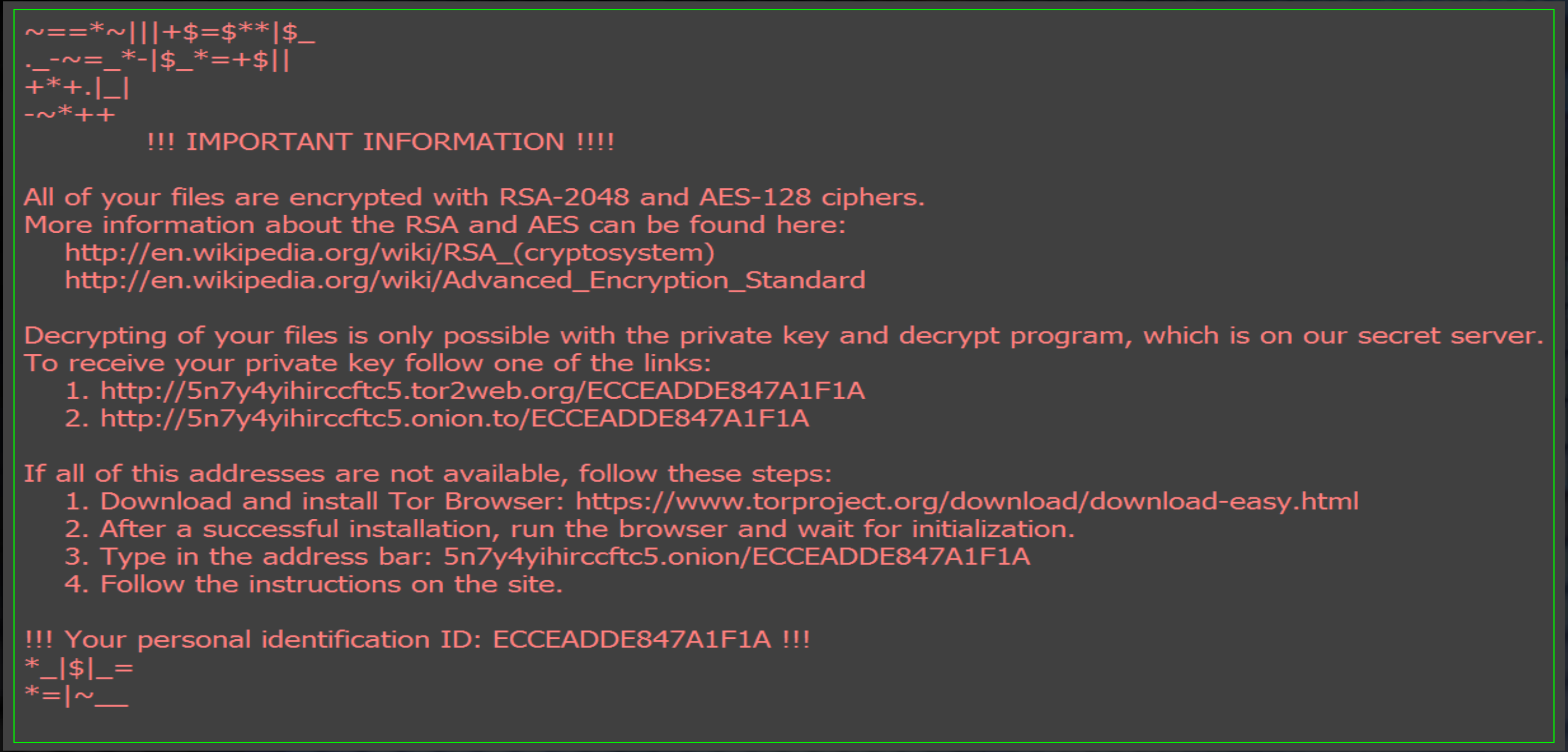
If you cannot find any (*README*) file at your PC, follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://p27dokhpz2n7nvgr.onion/DC91-E730-12F8-0095-7496

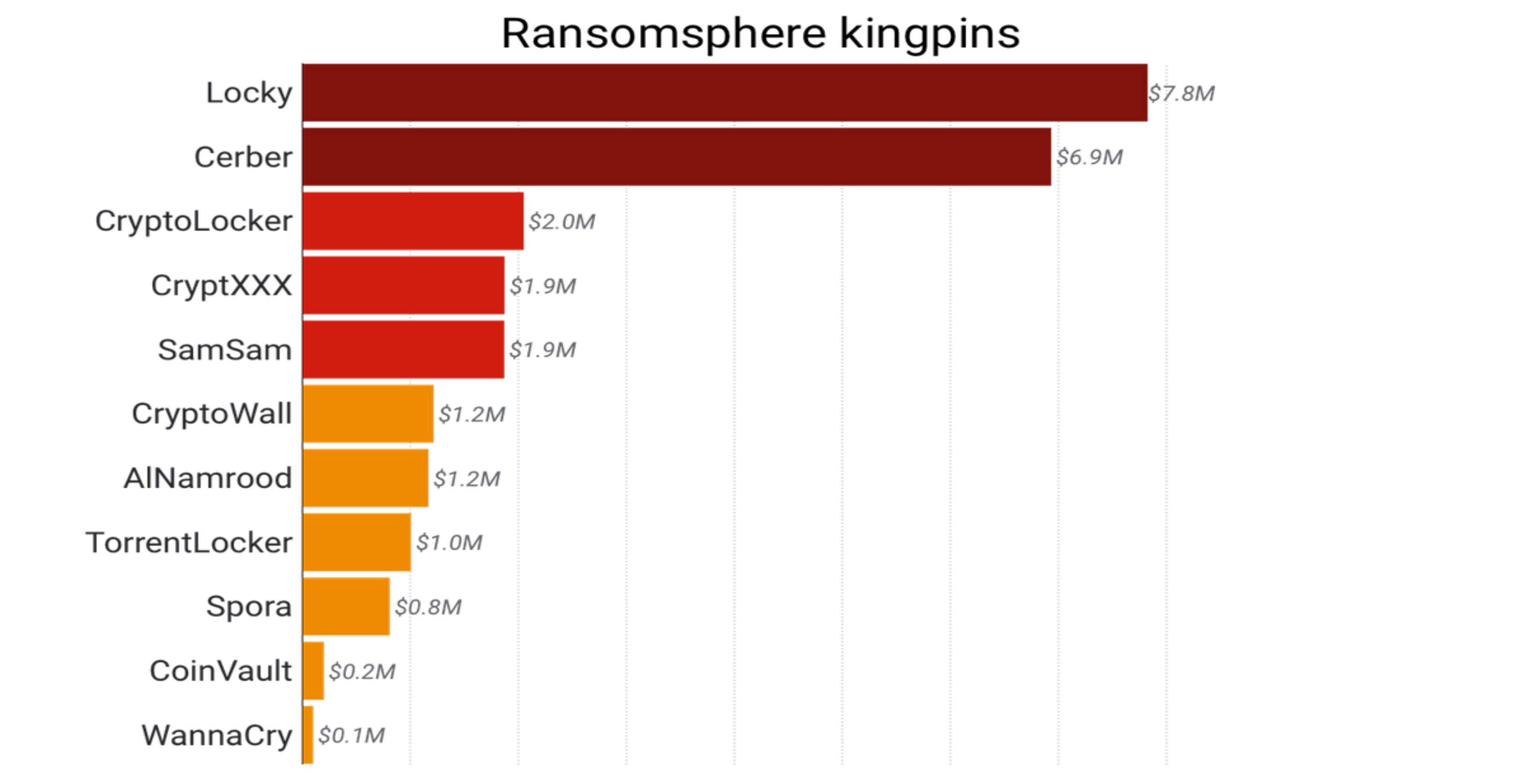
Note! This page is available via "Tor Browser" only.

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://5n7y4yihirccftc5.tor2web.org/ECCEADDE847A1F1A
    2. http://5n7y4yihirccftc5.onion.to/ECCEADDE847A1F1A

If all of this 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: 5n7y4yihirccftc5.onion/ECCEADDE847A1F1A
    4. Follow the instructions on the site.

!!! Your personal identification ID: ECCEADDE847A1F1A !!!
*_|$|_=
*=|~__
```

How Profitable is Ransomware?



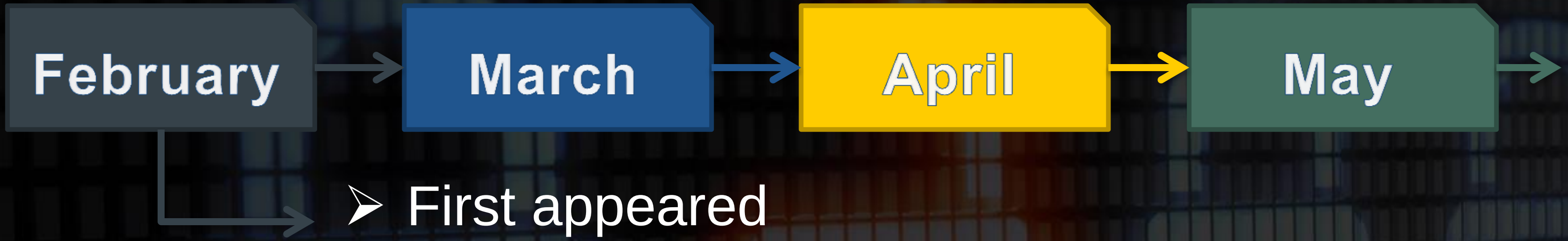
Reference: https://www.elie.net/blog/security/exposing-the-inner-workings-of-the-ransomware-economy

Prevalence: Affiliate Program

Affiliate ID	Method
1, 3, 5, 15, 21	Spam email containing a malicious attachment (e.g. script, MS Office)
13, 24, 1E	Compromised sites that redirects to Nuclear or Neutrino Exploit Kit

Locky Developments

Timeline of Developments: 2016



February

March

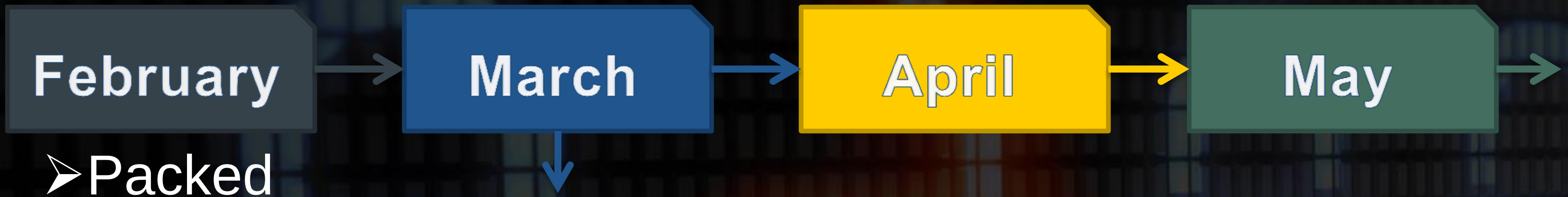
April

May

- First appeared
- No packer
- “Locky” registry key
- Configuration:

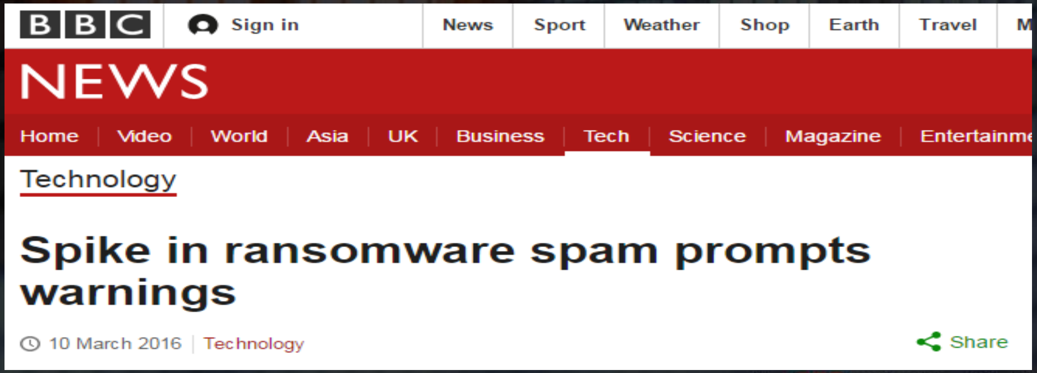
```
{
AffiliateID;
ccservers;
}
```

Timeline of Developments: 2016



- ➢Packed
- ➢Registry key based on VolumeGUID
- ➢Configuration(encrypted):

```
{
AffiliateID;
DGASeed;
delaySeconds;
FakeSvchost;
Persistence;
IgnoreRussian;
ccServers;
}
```

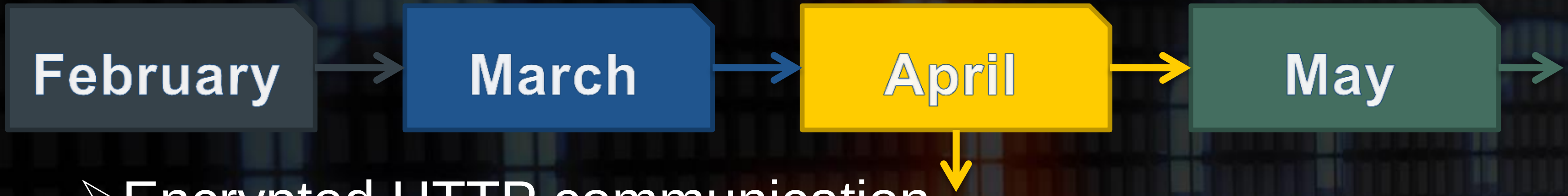


Technology

Spike in ransomware spam prompts warnings

10 March 2016 | Technology

Timeline of Developments: 2016



February

March

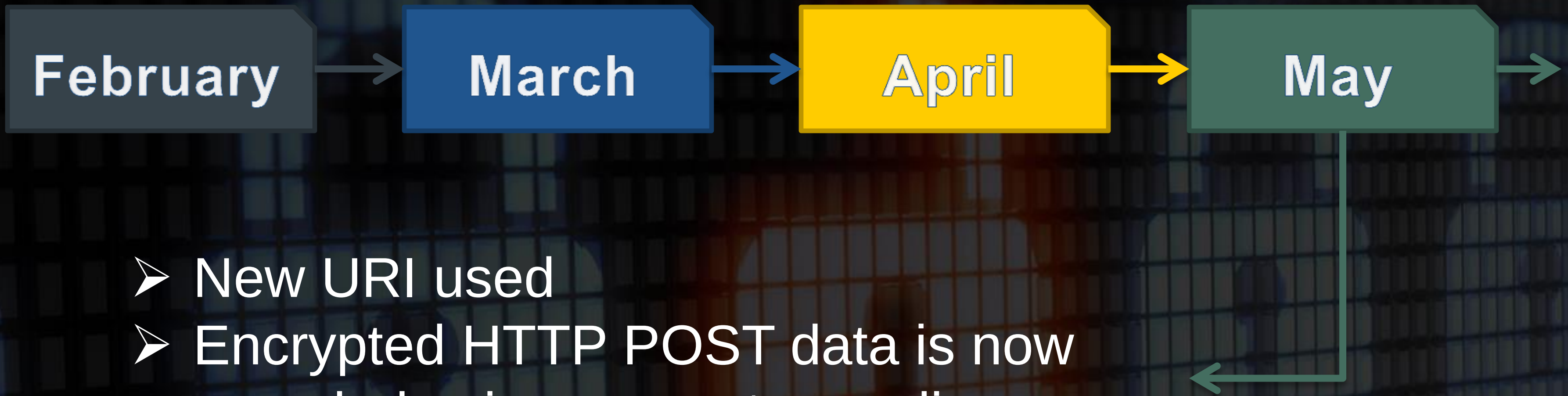
April

May

- Encrypted HTTP communication
- Configuration:

```
{
AffiliateID;
DGASeed;
delaySeconds;
FakeSvchost;
Persistence;
IgnoreRussian;
urlPath;
ccServers;
}
```

Timeline of Developments: 2016

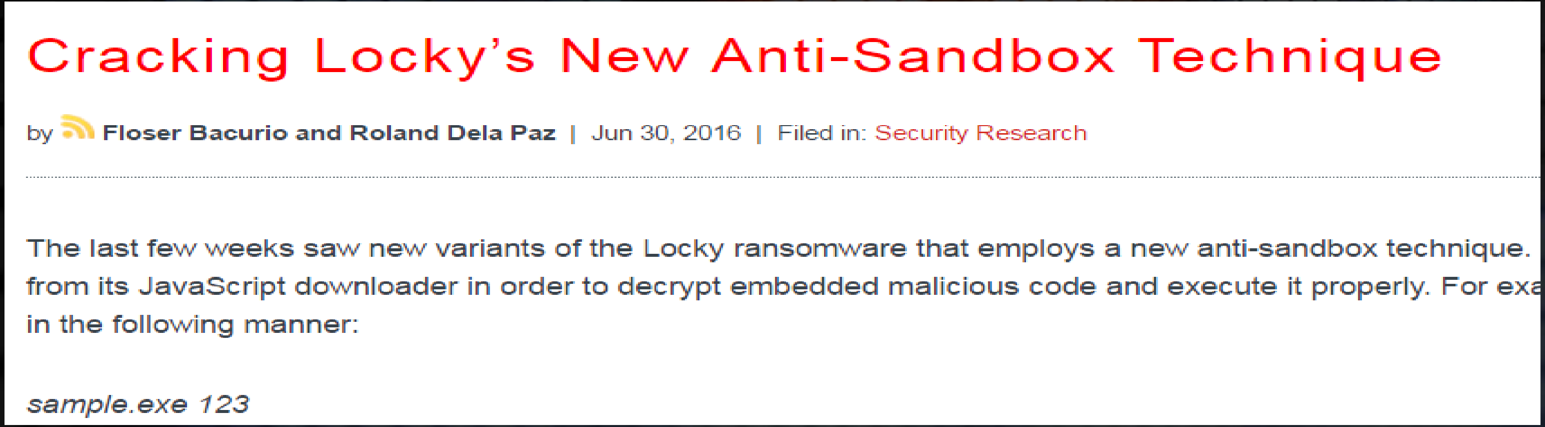


- New URI used
- Encrypted HTTP POST data is now encoded using percent encoding

Timeline of Developments: 2016

June
July
August
September

- Requires argument. (e.g “123”, “321”)



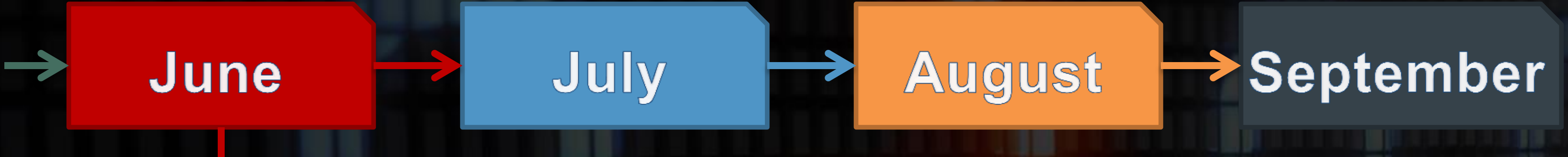
Cracking Locky’s New Anti-Sandbox Technique

by Floser Bacurio and Roland Dela Paz | Jun 30, 2016 | Filed in: Security Research

The last few weeks saw new variants of the Locky ransomware that employs a new anti-sandbox technique. from its JavaScript downloader in order to decrypt embedded malicious code and execute it properly. For exa in the following manner:

sample.exe 123

Timeline of Developments: 2016

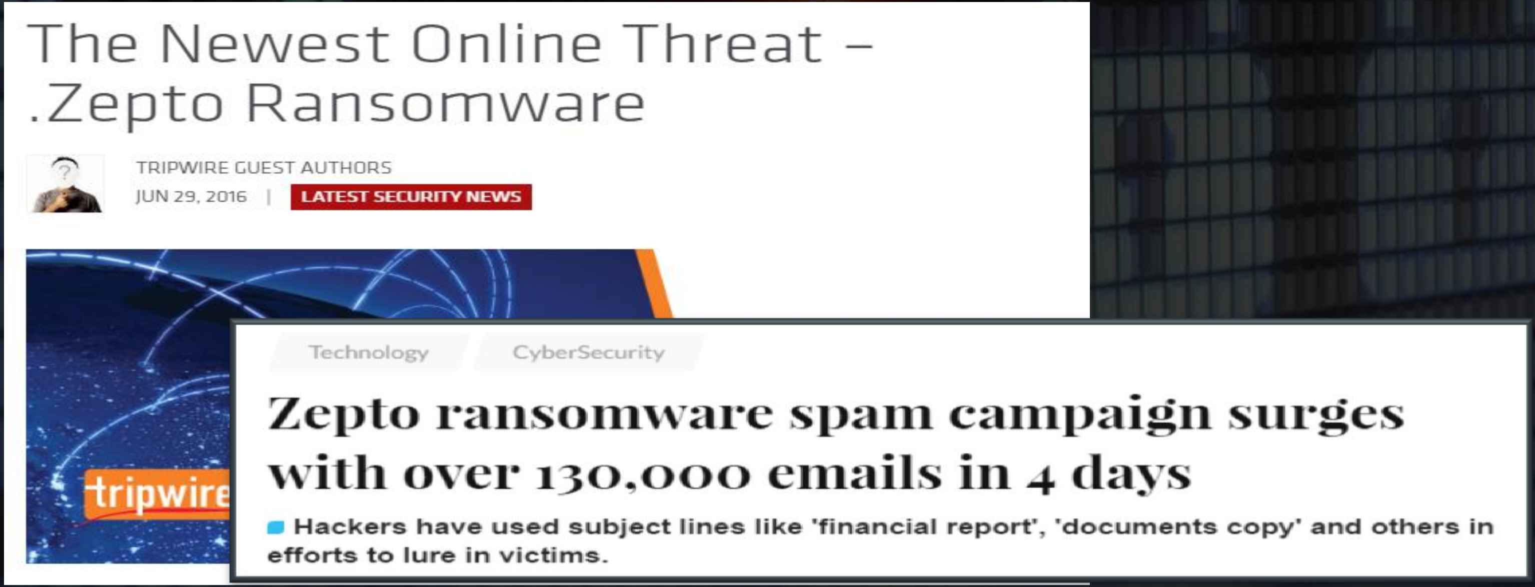


June

July

August

September



The Newest Online Threat – .Zepto Ransomware

TRIPWIRE GUEST AUTHORS

JUN 29, 2016 | LATEST SECURITY NEWS

Technology CyberSecurity

Zepto ransomware spam campaign surges with over 130,000 emails in 4 days

Hackers have used subject lines like 'financial report', 'documents copy' and others in efforts to lure in victims.

Timeline of Developments: 2016

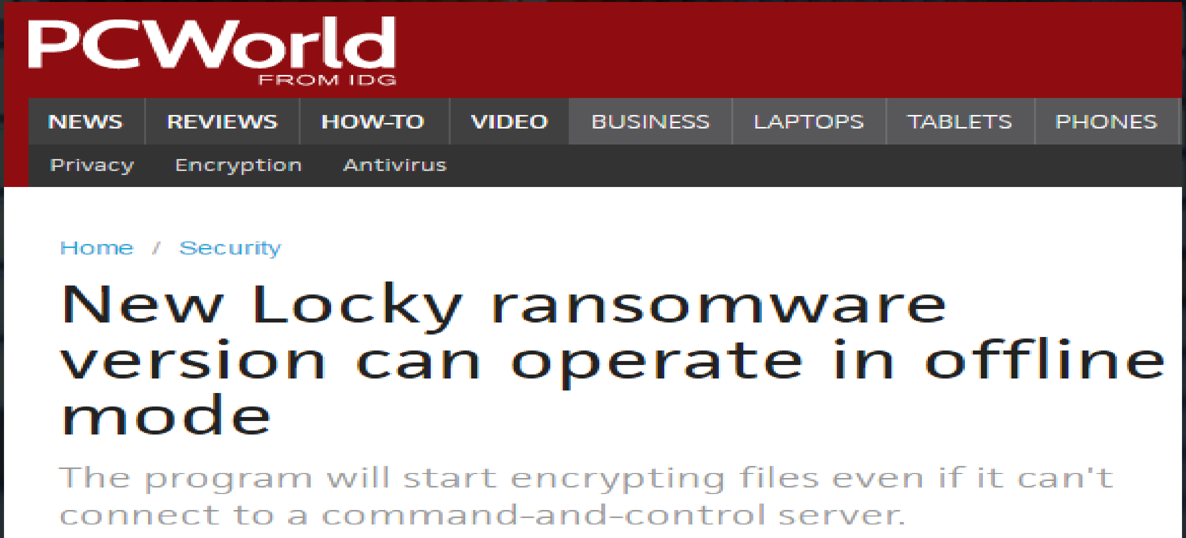
June

July

August

September

- ➢ Offline Mode encryption
- ➢ &v = 2, added to POST request



PCWorld
FROM IDG

NEWS | REVIEWS | HOW-TO | VIDEO | BUSINESS | LAPTOPS | TABLETS | PHONES

Privacy | Encryption | Antivirus

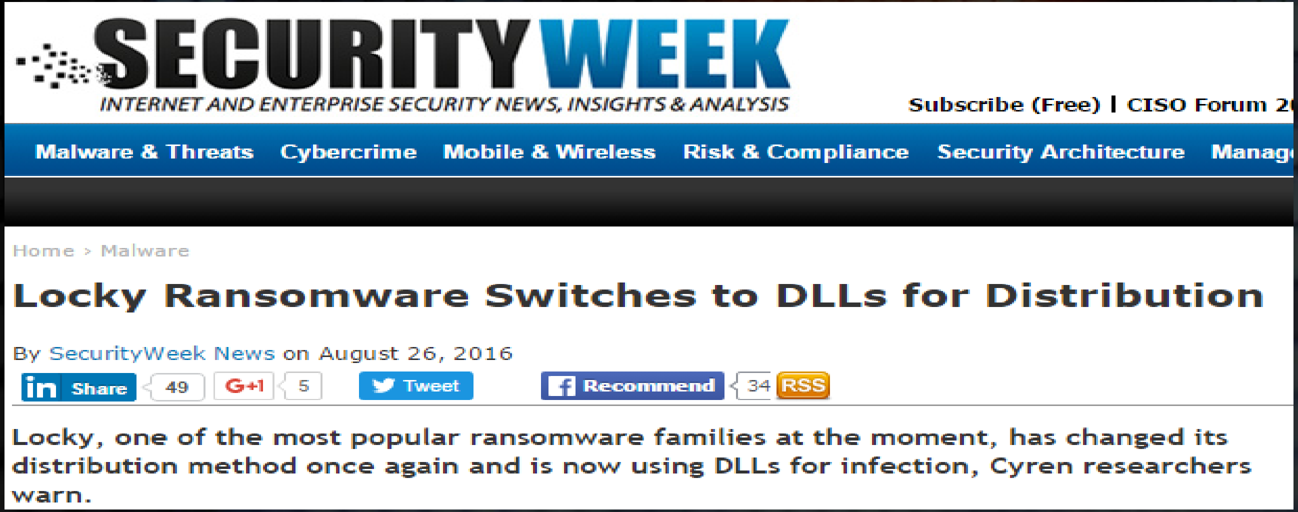
Home / Security

New Locky ransomware version can operate in offline mode

The program will start encrypting files even if it can't connect to a command-and-control server.

Timeline of Developments: 2016

June
July
August
September



SECURITYWEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum 2

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Manag

Home › Malware

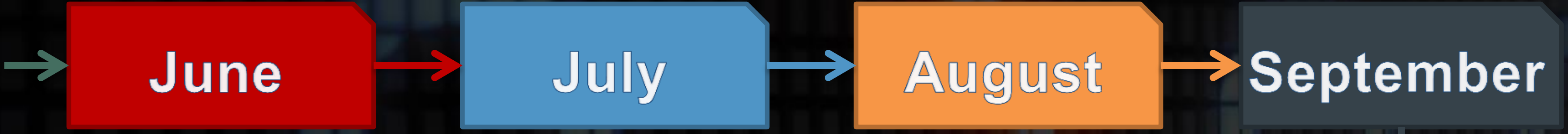
Locky Ransomware Switches to DLLs for Distribution

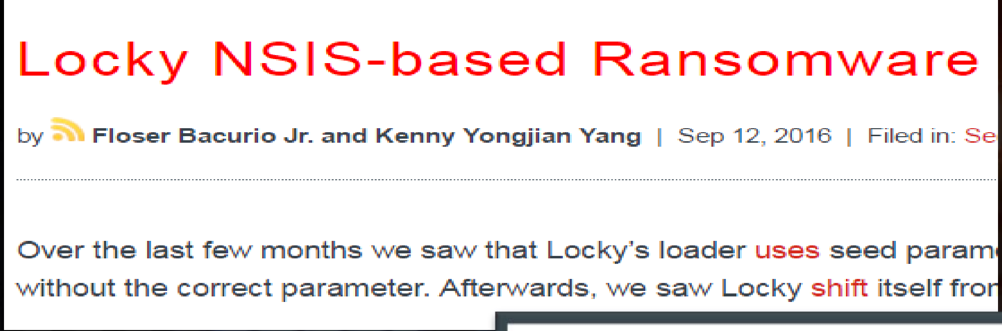
By SecurityWeek News on August 26, 2016

in Share 49 G+1 5 Tweet Recommend 34 RSS

Locky, one of the most popular ransomware families at the moment, has changed its distribution method once again and is now using DLLs for infection, Cyren researchers warn.

Timeline of Developments: 2016

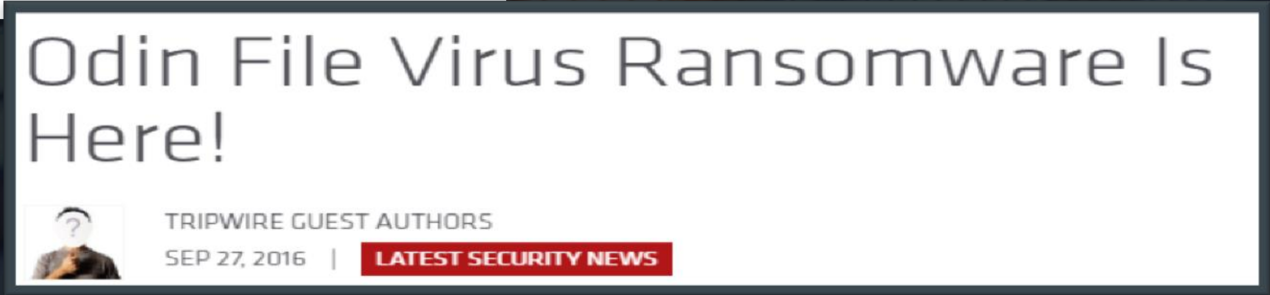




Locky NSIS-based Ransomware

by Floser Bacurio Jr. and Kenny Yongjian Yang | Sep 12, 2016 | Filed in: Se

Over the last few months we saw that Locky's loader uses seed param
without the correct parameter. Afterwards, we saw Locky shift itself fro

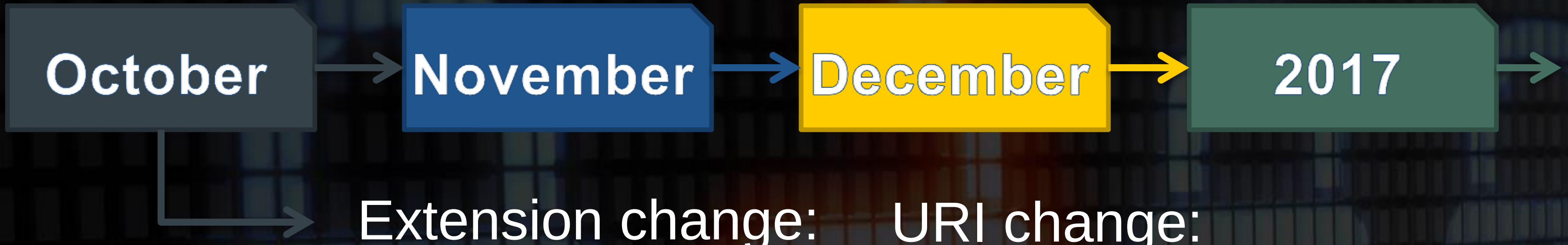


Odin File Virus Ransomware Is Here!

TRIPWIRE GUEST AUTHORS

SEP 27, 2016 | LATEST SECURITY NEWS

Timeline of Developments: 2016



October

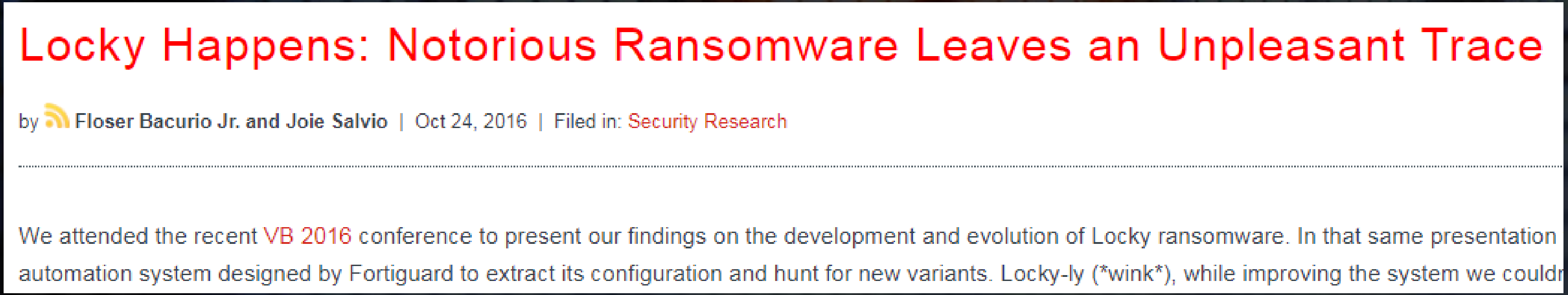
November

December

2017

Extension change:
- .shit
- .thor

URI change:
- /linuxsucks.php

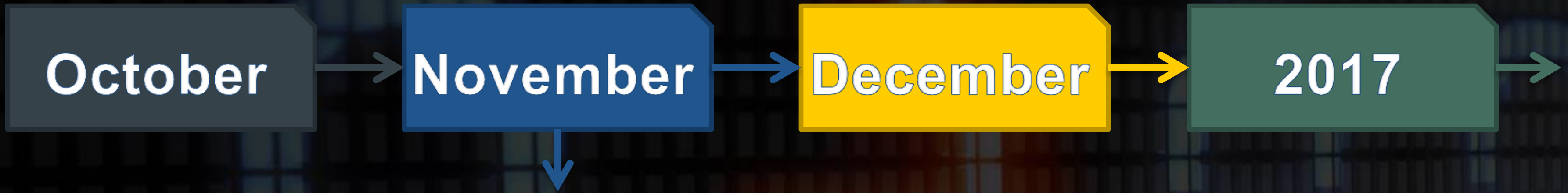


Locky Happens: Notorious Ransomware Leaves an Unpleasant Trace

by Floser Bacurio Jr. and Joie Salvio | Oct 24, 2016 | Filed in: Security Research

We attended the recent VB 2016 conference to present our findings on the development and evolution of Locky ransomware. In that same presentation automation system designed by Fortiguard to extract its configuration and hunt for new variants. Locky-ly (*wink*), while improving the system we couldn

Timeline of Developments: 2016



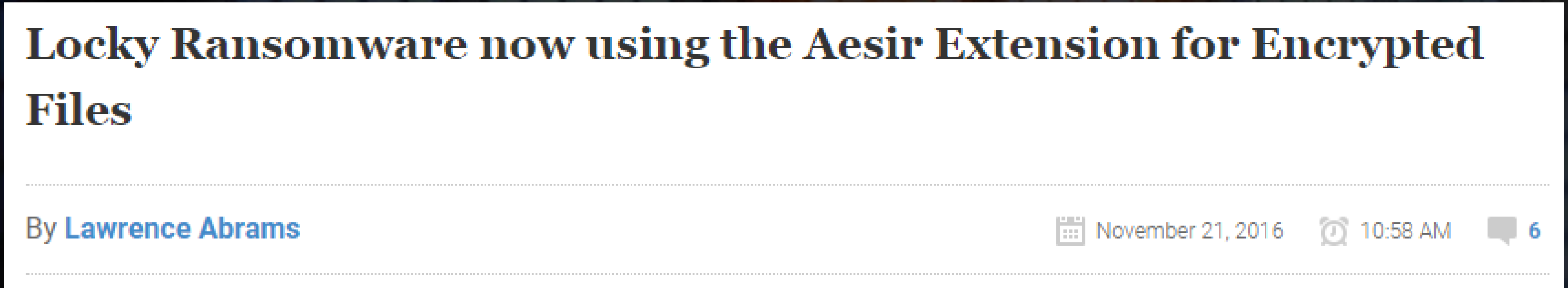
October → November → December → 2017 →

Extension change:

- .aesir
- .zzzzz

URI change:

- /information.cgi



Locky Ransomware now using the Aesir Extension for Encrypted Files

By Lawrence Abrams November 21, 2016 10:58 AM 6

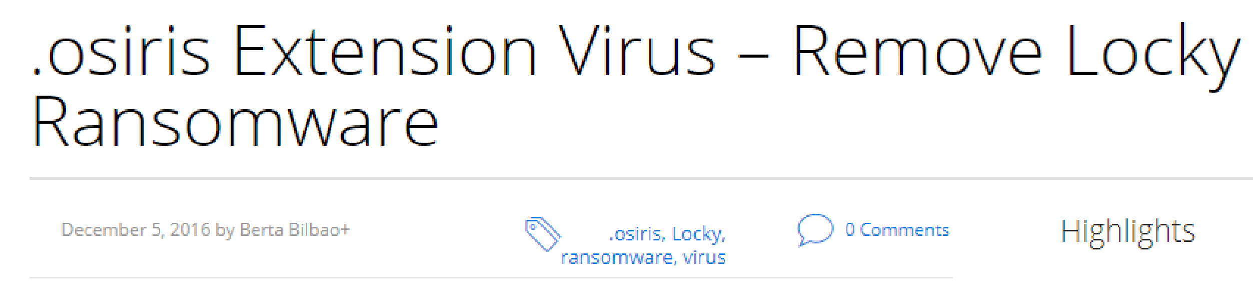
Timeline of Developments: 2016

October

November

December

2017



.osiris Extension Virus – Remove Locky Ransomware

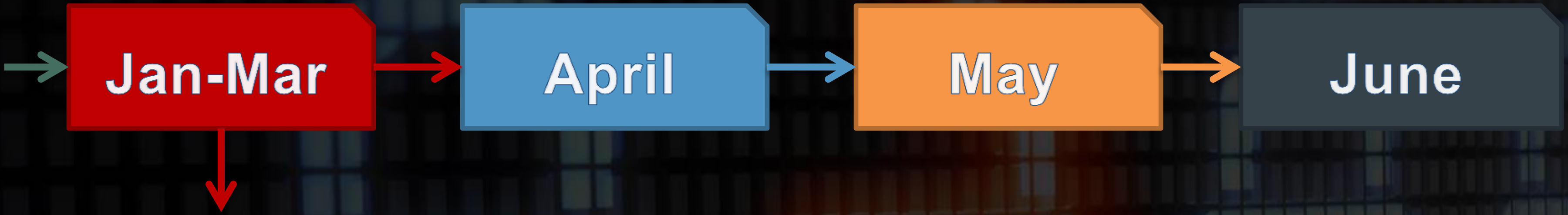
December 5, 2016 by Berta Bilbao+

.osiris, Locky, ransomware, virus

0 Comments

Highlights

Timeline of Developments: 2017



Jan-Mar

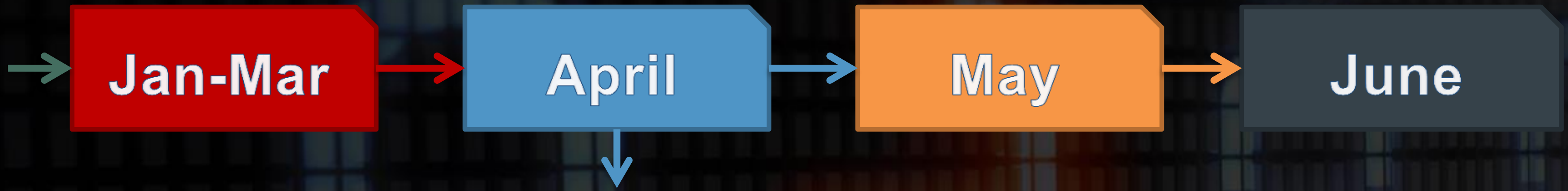
April

May

June

- Locky takes a break

Timeline of Developments: 2017

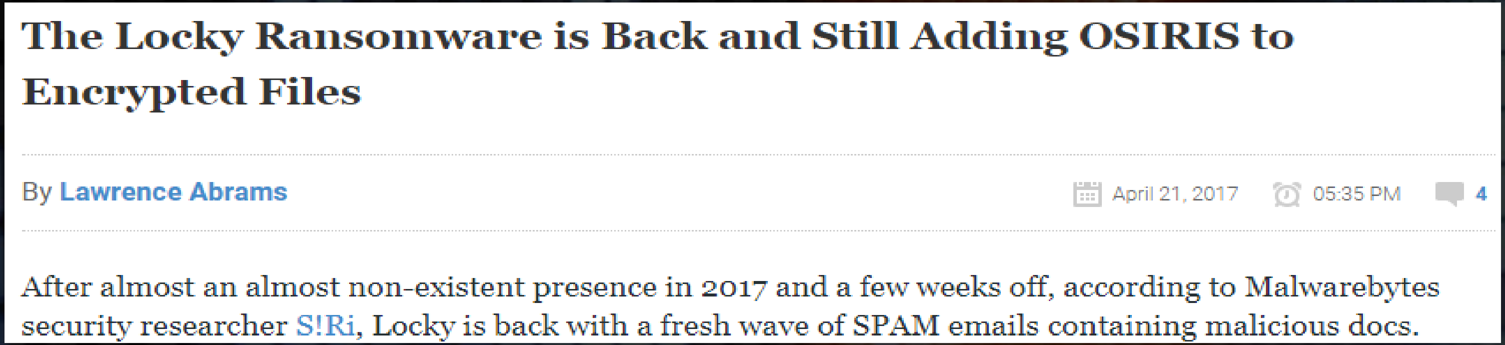


Jan-Mar

April

May

June



The Locky Ransomware is Back and Still Adding OSIRIS to Encrypted Files

By Lawrence Abrams April 21, 2017 05:35 PM 4

After almost an almost non-existent presence in 2017 and a few weeks off, according to Malwarebytes security researcher S!Ri, Locky is back with a fresh wave of SPAM emails containing malicious docs.

Extension change:

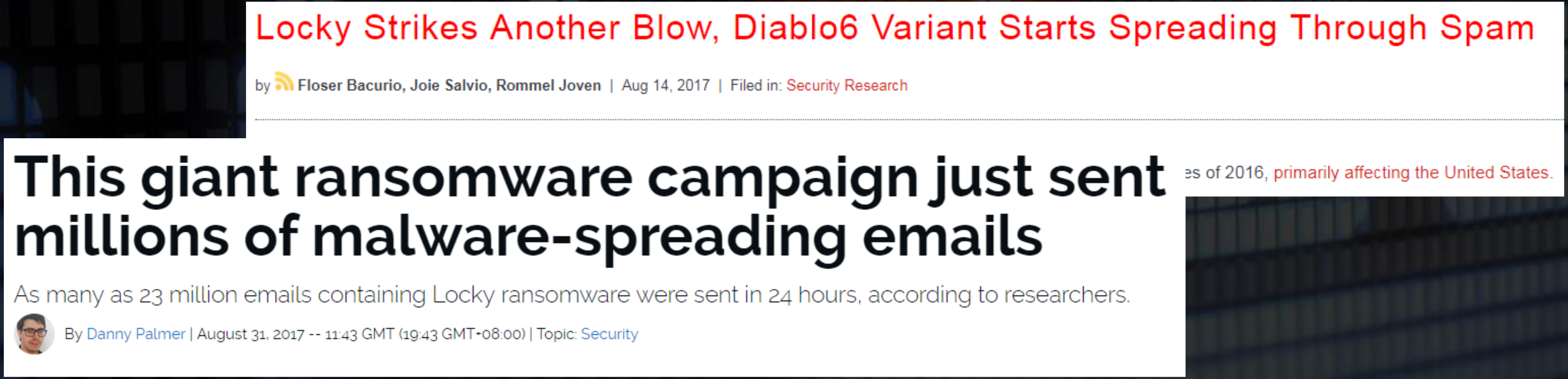
- .loptr

URI change:

- /checkupdate

Timeline of Developments: 2017

July
August
September
October



Locky Strikes Another Blow, Diablo6 Variant Starts Spreading Through Spam

by Floser Bacurio, Joie Salvio, Rommel Joven | Aug 14, 2017 | Filed in: Security Research

es of 2016, primarily affecting the United States.

This giant ransomware campaign just sent millions of malware-spreading emails

As many as 23 million emails containing Locky ransomware were sent in 24 hours, according to researchers.

By Danny Palmer | August 31, 2017 -- 11:43 GMT (19:43 GMT+08:00) | Topic: Security

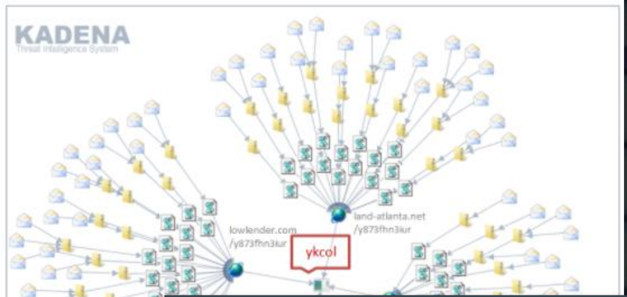
AutoClose() Function start Powershell

Timeline of Developments: 2017

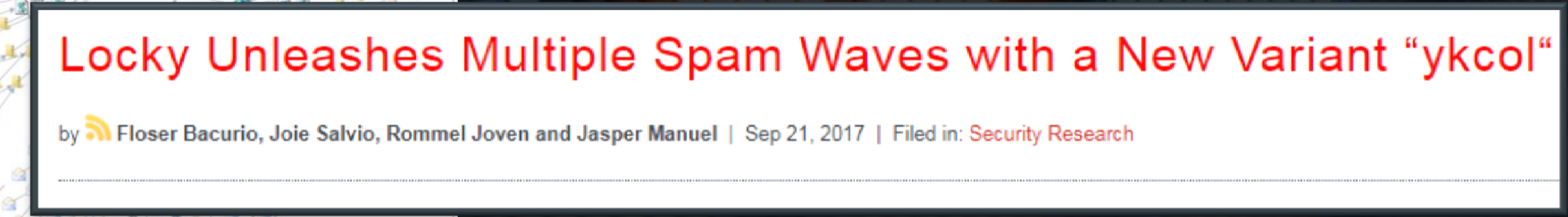
July → August → September → October →

URI change:

- ➢ /imageload.cgi



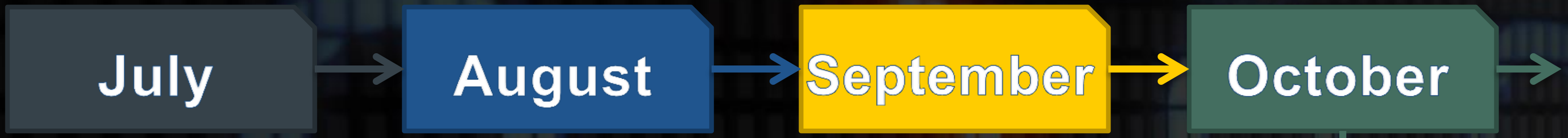
Email Subject:
Emailing – 10008003482 {alphanumeric value}
Attachment: {11 numeric value}.7z (e.g. 10008000958.7z)



Locky Unleashes Multiple Spam Waves with a New Variant "ykcol"

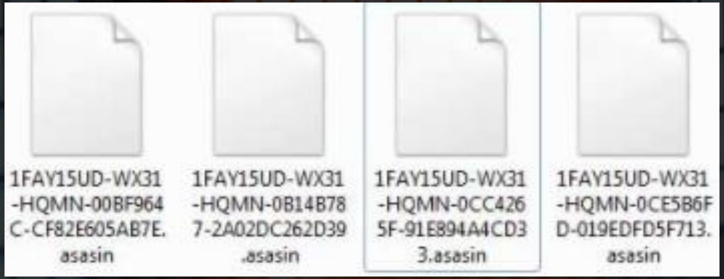
by Floser Bacurio, Joie Salvio, Rommel Joven and Jasper Manuel | Sep 21, 2017 | Filed in: Security Research

Timeline of Developments: 2017



Extension change:

- ➢ .asasin



1FAY15UD-WX31
-HQMN-00BF964
C-CF82E605AB7E.
asasin

1FAY15UD-WX31
-HQMN-0B14B78
7-2A02DC262D39
.asasin

1FAY15UD-WX31
-HQMN-0CC426
5F-91E894A4CD3
3.asasin

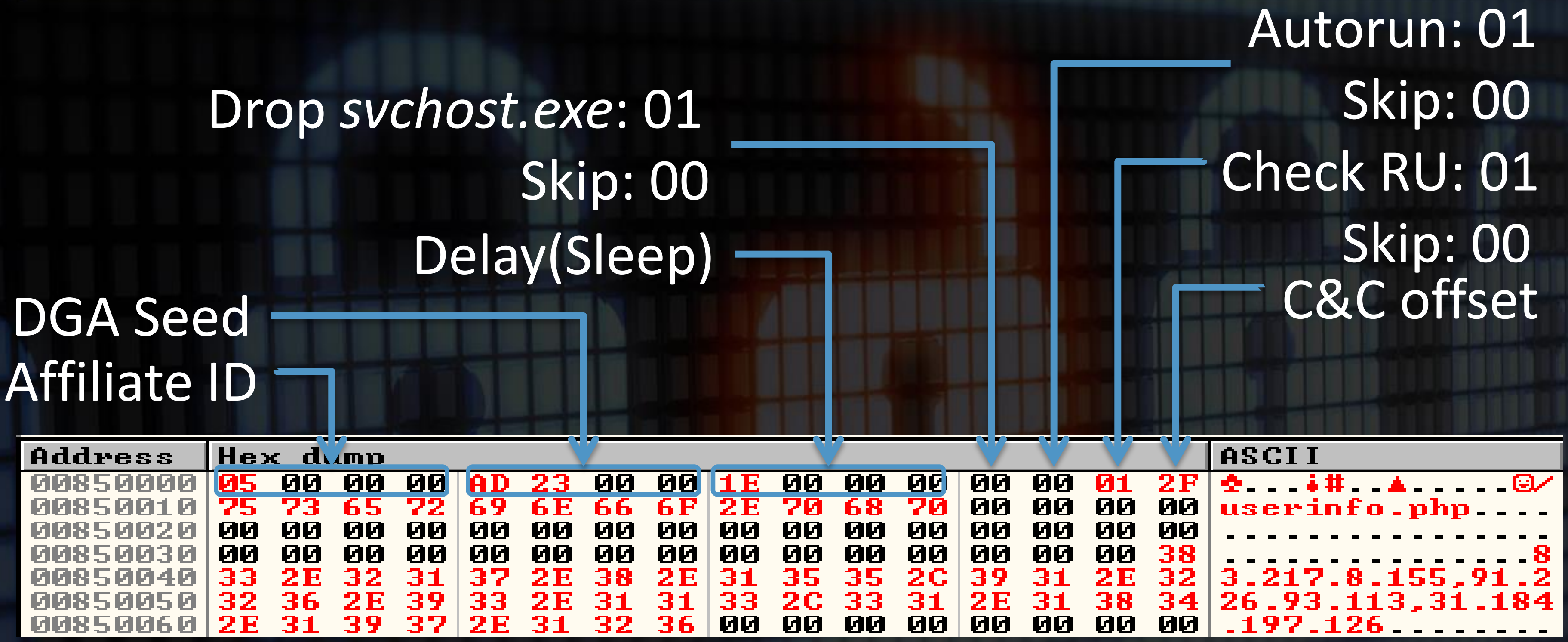
1FAY15UD-WX31
-HQMN-0CE5B6F
D-019EDFD5F713.
asasin

Loader Serves up Locky or Trickbot

Use of DDE Exploit

Technical Analysis

Configuration



Autorun: 01

Skip: 00

Check RU: 01

Skip: 00

C&C offset

Drop *svchost.exe*: 01

Skip: 00

Delay(Sleep)

DGA Seed

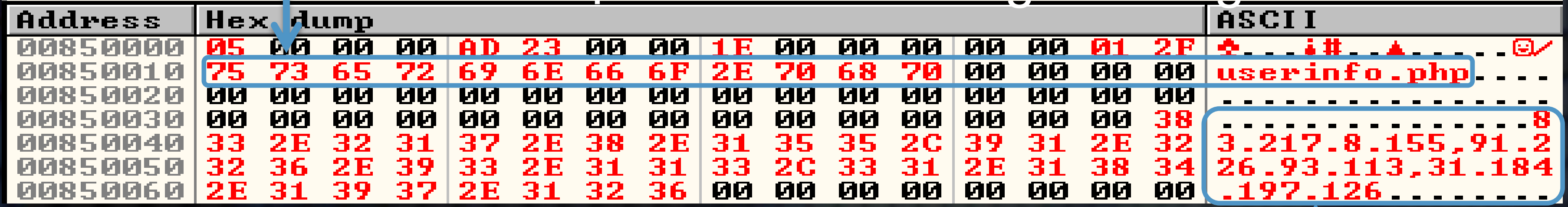
Affiliate ID

```
Address   Hex dump                                         ASCII
00850000  05 00 00 00 AD 23 00 00 1E 00 00 00 00 00 01 2F  ♣...¡#..▲.....☺/
00850010  75 73 65 72 69 6E 66 6F 2E 70 68 70 00 00 00 00  userinfo.php....
00850020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00850030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38  ...............8
00850040  33 2E 32 31 37 2E 38 2E 31 35 35 2C 39 31 2E 32  3.217.8.155,91.2
00850050  32 36 2E 39 33 2E 31 31 33 2C 33 31 2E 31 38 34  26.93.113,31.184
00850060  2E 31 39 37 2E 31 32 36 00 00 00 00 00 00 00 00  .197.126........
```

Configuration

URI for its C&C

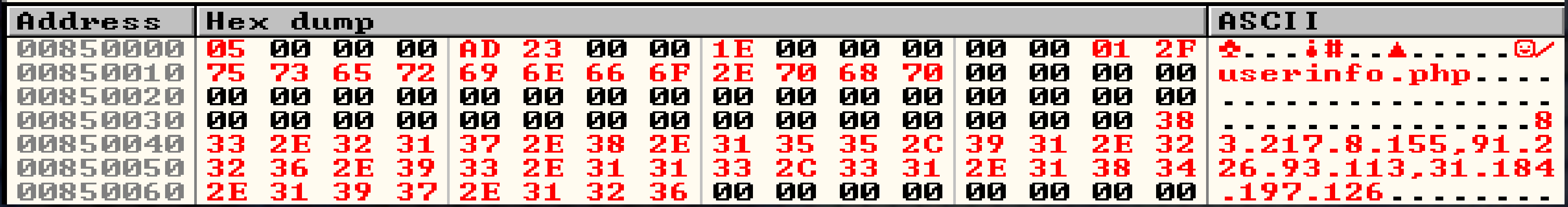
- /main.php
- /submit.php
- /userinfo.php
- /access.cgi
- /linuxsucks.php
- /checkupdate
- /upload/_dispatch.php
- /php/upload.php
- /data/info.php
- /apache_handler.php
- /information.cgi
- /information.asp
- /imageload.cgi



```
Address   Hex dump                                          ASCII
00850000  05 00 00 00 AD 23 00 00 1E 00 00 00 00 00 01 2F  ♣...¡#..▲.....☺/
00850010  75 73 65 72 69 6E 66 6F 2E 70 68 70 00 00 00 00  userinfo.php....
00850020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00850030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38  ...............8
00850040  33 2E 32 31 37 2E 38 2E 31 35 35 2C 39 31 2E 32  3.217.8.155,91.2
00850050  32 36 2E 39 33 2E 31 31 33 2C 33 31 2E 31 38 34  26.93.113,31.184
00850060  2E 31 39 37 2E 31 32 36 00 00 00 00 00 00 00 00  .197.126........
```

C&Cs

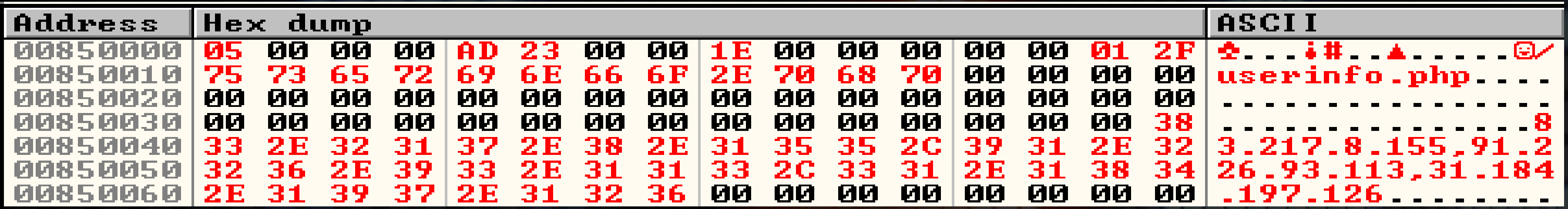
Configuration



```
Address   Hex dump                                          ASCII
00850000  05 00 00 00 AD 23 00 00 1E 00 00 00 00 00 01 2F  ♣...¡#..▲.....☺/
00850010  75 73 65 72 69 6E 66 6F 2E 70 68 70 00 00 00 00  userinfo.php....
00850020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00850030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38  ...............8
00850040  33 2E 32 31 37 2E 38 2E 31 35 35 2C 39 31 2E 32  3.217.8.155,91.2
00850050  32 36 2E 39 33 2E 31 31 33 2C 33 31 2E 31 38 34  26.93.113,31.184
00850060  2E 31 39 37 2E 31 32 36 00 00 00 00 00 00 00 00  .197.126........
```

Configuration: Offline

Online mode

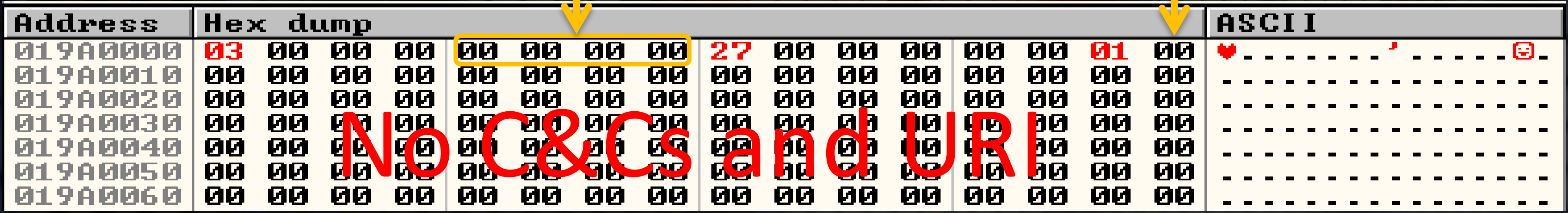


```
Address   Hex dump                                         ASCII
00850000  05 00 00 00 AD 23 00 00 1E 00 00 00 00 00 01 2F  ♣...¡#..▲.....☺/
00850010  75 73 65 72 69 6E 66 6F 2E 70 68 70 00 00 00 00  userinfo.php....
00850020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00850030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38  ...............8
00850040  33 2E 32 31 37 2E 38 2E 31 35 35 2C 39 31 2E 32  3.217.8.155,91.2
00850050  32 36 2E 39 33 2E 31 31 33 2C 33 31 2E 31 38 34  26.93.113,31.184
00850060  2E 31 39 37 2E 31 32 36 00 00 00 00 00 00 00 00  .197.126........
```

No DGA Seed

No C&C offset

Offline mode

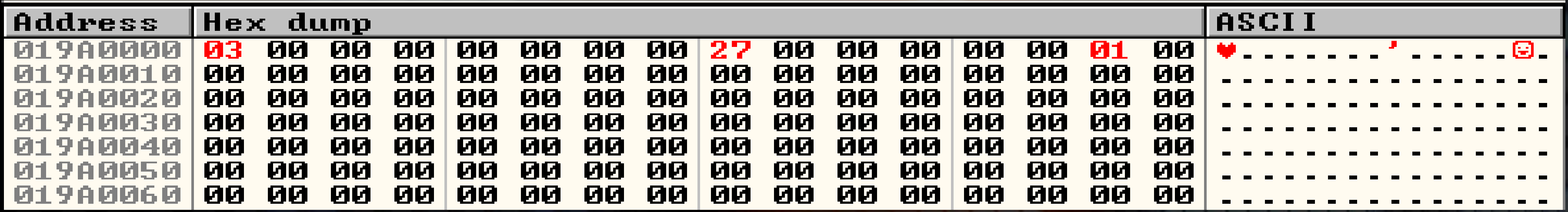


```
Address   Hex dump                                         ASCII
019A0000  03 00 00 00 00 00 00 00 27 00 00 00 00 00 01 00  ♥.......'.....☺.
019A0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

No C&Cs and URI

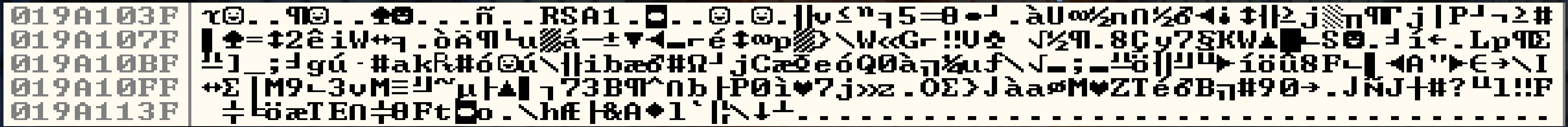
Configuration: Offline

Offline mode



```
Address   Hex dump                                          ASCII
019A0000  03 00 00 00 00 00 00 00 27 00 00 00 00 00 01 00  ♥.......'.....☺.
019A0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
019A0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

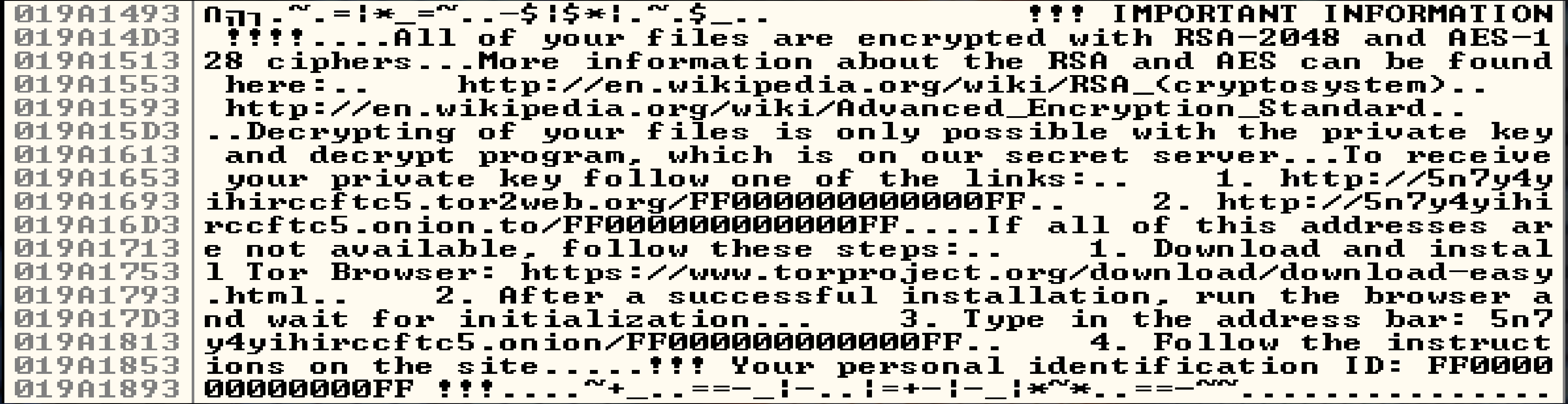
Embedded Public RSA key



```
019A103F  τ☺..¶☺..♠☻...ñ..RSA1.◘..☺.☺.╫╟v≤ⁿ╕5═θ•┘.àU∞½∩∩½δ◄¡‡╟≥j▒╥¶╓j|P┘¬≥#
019A107F  ▌♠=‡2êiW↔╕.òÄ¶└u▓á─±▼◄▬┌é‡∞p▓>\W«G┌‼U♠ √½¶.8Çy7§KW▲█╞─S☻.┤í←.Lp¶E
019A10BF  ╨]_;┤gú-#ak₧#ó☺ú\╫ibæδ#Ω┘jCæ♀eóQ0à╖¼uƒ\√▬;▬╨ö╫╜╙►íöû8F└▌◄A"►€→\I
019A10FF  ↔Σ╘M9└3vM≡╝~µ├▲▌╖73B¶^∩b├P0ì♥7j»z.ÒΣ>JàaσM♥ZTéδB╖#90→.JÑJ┼#?╘1‼F
019A113F   ╪╘öæTEn╪θFt◘o.\hÆ├&A♦1`╟\↓┴.....................................
```

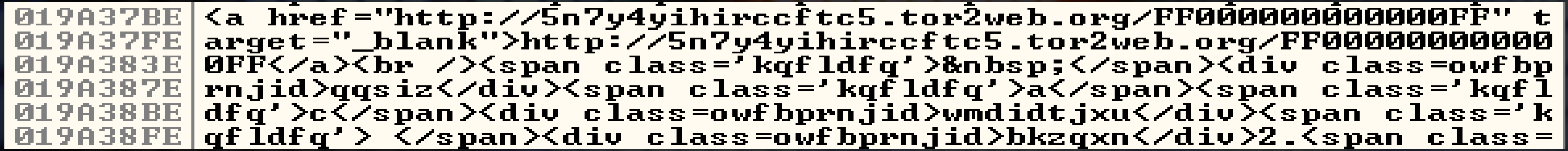
Configuration: Offline

Embedded Ransom Text



```
019A1493 ∩╗┐.~.=¦*_=~..-$¦$*¦.~.$_..           !!! IMPORTANT INFORMATION
019A14D3  !!!!....All of your files are encrypted with RSA-2048 and AES-1
019A1513 28 ciphers...More information about the RSA and AES can be found
019A1553  here:..    http://en.wikipedia.org/wiki/RSA_(cryptosystem)..
019A1593  http://en.wikipedia.org/wiki/Advanced_Encryption_Standard..
019A15D3 ..Decrypting of your files is only possible with the private key
019A1613  and decrypt program, which is on our secret server...To receive
019A1653  your private key follow one of the links:..    1. http://5n7y4y
019A1693 ihirccftc5.tor2web.org/FF000000000000FF..    2. http://5n7y4yihi
019A16D3 rccftc5.onion.to/FF000000000000FF....If all of this addresses ar
019A1713 e not available, follow these steps:..    1. Download and instal
019A1753 l Tor Browser: https://www.torproject.org/download/download-easy
019A1793 .html..    2. After a successful installation, run the browser a
019A17D3 nd wait for initialization...    3. Type in the address bar: 5n7
019A1813 y4yihirccftc5.onion/FF000000000000FF..    4. Follow the instruct
019A1853 ions on the site.....!!! Your personal identification ID: FF0000
019A1893 00000000FF !!!....~+_..==-_¦-..¦=+-¦-_¦*~*..==-~~~...............
```

Embedded HTML Ransom Text



```
019A37BE <a href="http://5n7y4yihirccftc5.tor2web.org/FF000000000000FF" t
019A37FE arget="_blank">http://5n7y4yihirccftc5.tor2web.org/FF00000000000
019A383E 0FF</a><br /><span class='kqfldfq'>&nbsp;</span><div class=owfbp
019A387E rnjid>qqsiz</div><span class='kqfldfq'>a</span><span class='kqfl
019A38BE dfq'>c</span><div class=owfbprnjid>wmdidtjxu</div><span class='k
019A38FE qfldfq'> </span><div class=owfbprnjid>bkzqxn</div>2.<span class=
```

Victim ID: Online

Locky creates a victim ID that needs to identify unique systems.

The victim ID is created from the following information:

- Volume GUID of the *WindowsDirectory*
- *MD5* hash of the GUID value

e.g. ***victim_ID = 4DF383039AB03953***

Victim ID: Offline

The victim ID is created from the following information:

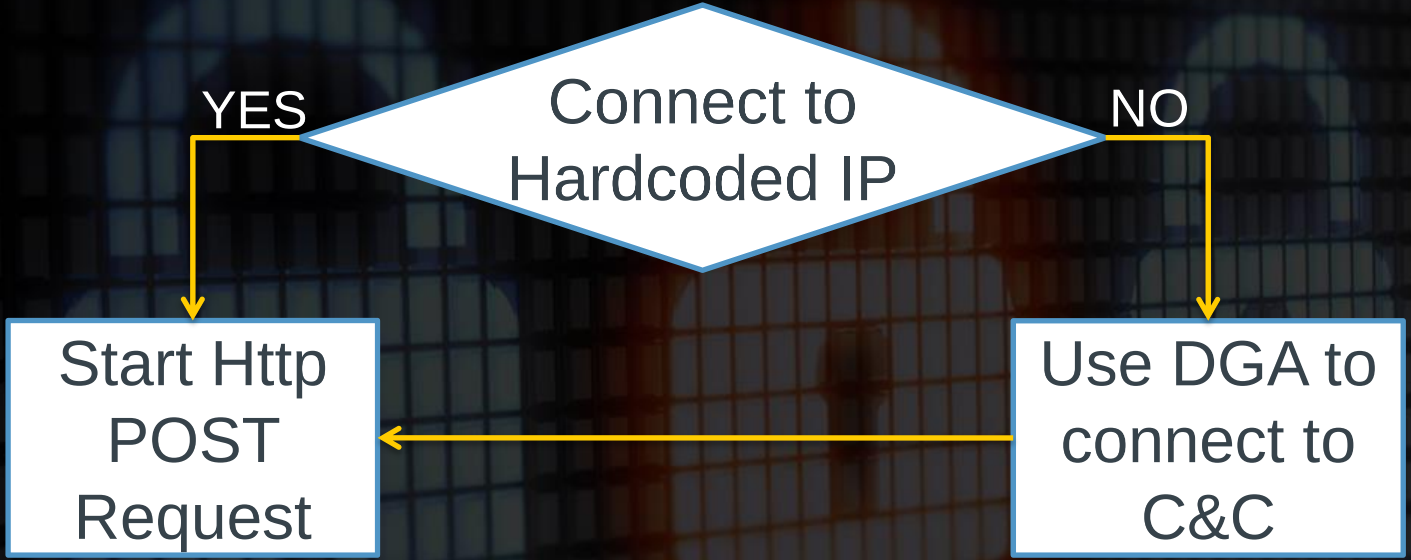
- GUID of the *WindowsDirectory*
- Default UI *Language*
- *OS* version
- Domain Controller
- *Affiliate ID* from the configuration
- *Public key ID* from the configuration

Encodes it using a hard coded 32 character value: “**YBNDRFG8EJKMCPQX0T1UWISZA345H769**”.

e.g. ***victim_ID = IZ8FDGTNEN85I7JZ***

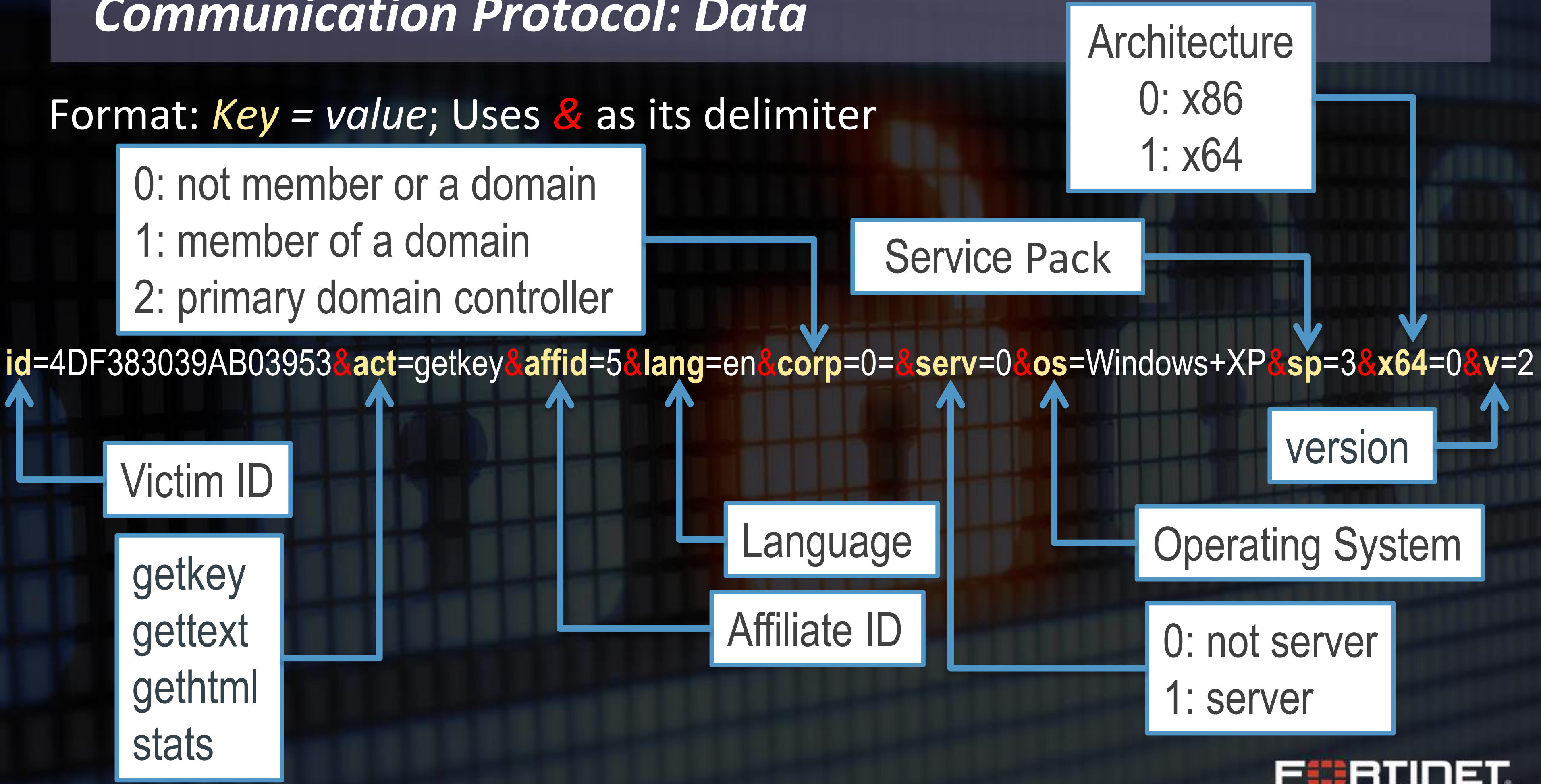
C&C Communication

Communication Protocol: C&C



Communication Protocol: Data

Format: *Key* = *value*; Uses & as its delimiter



```
id=4DF383039AB03953&act=getkey&affid=5&lang=en&corp=0=&serv=0&os=Windows+XP&sp=3&x64=0&v=2
```

Victim ID

getkey
gettext
gethtml
stats

Affiliate ID

Language

0: not member or a domain
1: member of a domain
2: primary domain controller

0: not server
1: server

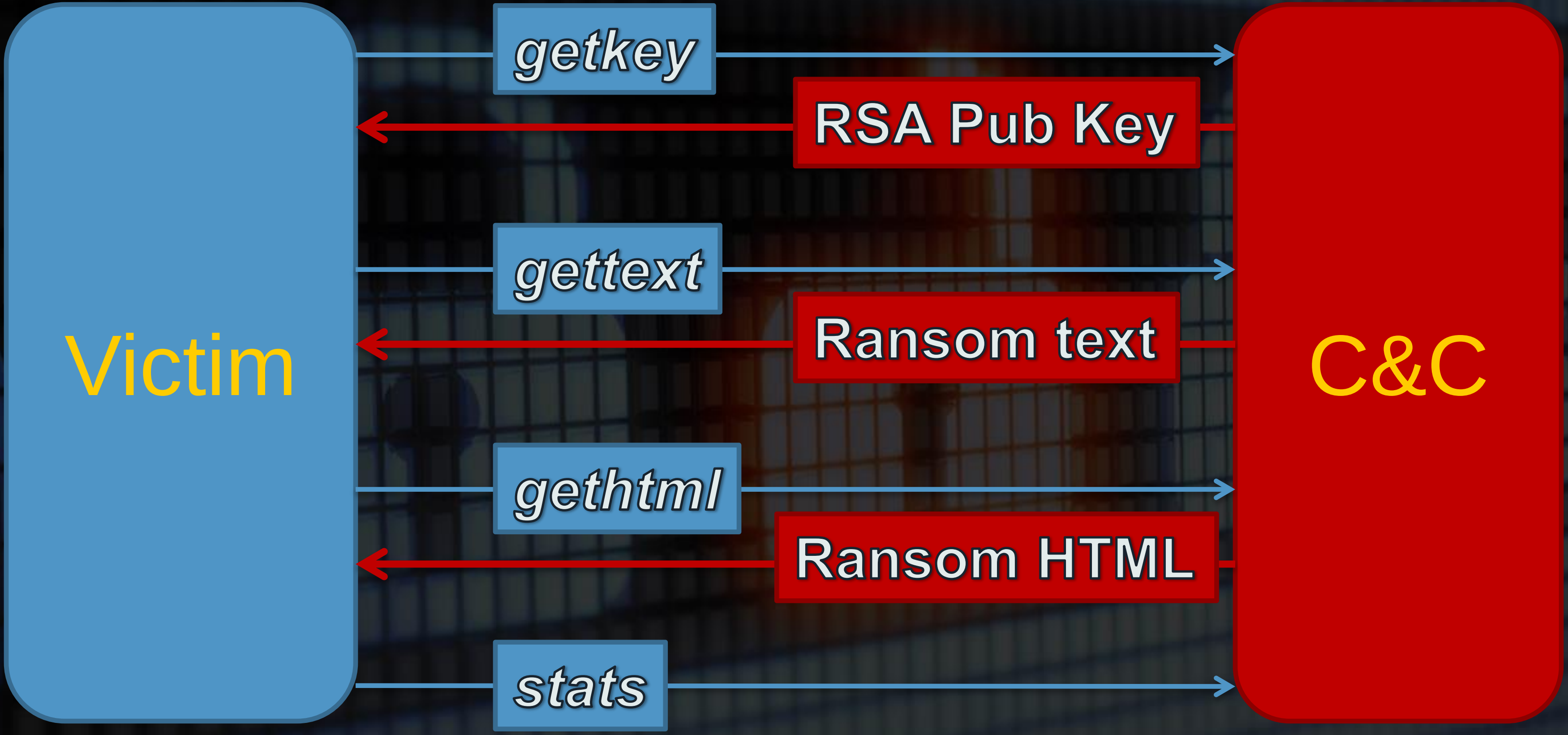
Operating System

Service Pack

Architecture
0: x86
1: x64

version

Communication Protocol: Http request



File Encryption

File Encryption: Targeted drives

- Drive_Removable
- Drive_Fixed
- Drive_Remote
- Drive_Ramdisk

File Encryption: Targeted extensions

File extensions:

*.yuv, .qbx, .ndd, .exf, .cdr4, .vmsd, .dat, .indd, .pspimage, .obj, .ycbcra, .qbw, .mrw, .erf, .cdr3, .vhdx, .cmt, .iif, .ps, .mlb, .xis, .qbr, .**moneywell**, .erbsql, .bpw, .vhd, .bin, .fpx, .pct, .md, .x3f, .qba, .mny, .eml, .bgt, .vbox, .aiff, .fff, .pcd, .mbx, .x11, .py, .mmw, .dxg, .bdb, .stm, .xlk, .fdb, .m4v, .lit, .wpd, .**psafe3**, .mfw, .drf, .bay, .st7, .wad, .dtd, .m, .laccdb, .tex, .plc, .mef, .dng, .bank, .rvt, .tlg, .design, .fxg, .kwm, .sxg, .plus_muhd, .mdc, .dgc, .**backupdb**, .qcow, .st6, .ddd, .flac, .idx, .stx, .pdd, .lua, .des, .backup, .qed, .st4, .dcr, .eps, .html, .st8, .p7c, .kpdx, .der, .back, .pif, .say, .dac, .dxb, .flf, .st5, .p7b, .kdc, .ddrw, .awg, .pdb, .sas7bdat, .cr2, .drw, .dxf, .srw, .oth, .kdbx, .**ddoc**, .apj, .pab, .qbm, .cdx, .**db3**, .dwg, .srf, .orf, .kc2, .dcs, .ait, .ost, .qbb, .cdf, .cpi, .dds, .sr2, .odm, .jpe, .dc2, .agdl, .ogg, .ptx, .blend, .cls, .css, .sqlite, .odf, .incpas, .db_journal, .ads, .nvram, .pfx, .bkp, .cdr, .**config**, .sdf, .nyf, .iiq, .csl, .adb, .ndf, .pef, .al, .arw, .cfg, .sda, .nxl, .ibz, .csh, .acr, .m4p, .pat, .adp, .ai, .cer, .sd0, .nx2, .**ibank**, .crw, .ach, .m2ts, .oil, .act, .aac, .asx, .s3db, .nwb, .hbk, .craw, .accdt, .log, .odc, .xlr, .thm, .aspx, .rwz, .ns4, .gry, .cib, .accdr, .hpp, .nsh, .xlam, .srt, .aoi, .rwl, .ns3, .grey, .ce2, .accde, .hdd, .nsg, .xla, .save, .accdb, .rdb, .ns2, .gray, .ce1, .ab4, .groups, .nsf, .wps, .**safe**, .**7zip**, .rat, .nrw, .fhd, .cdrw, .3pr, .flvv, .nsd, .tga, .rm, .1cd, .raf, .nop, .fh, .cdr6, .3fr, .edb, .nd, .rw2, .pwm, .wab, .qby, .nk2, .ffd, .cdr5, .vmxf, .dit, .mos, .r3d, .pages, .prf, .oab, .msg, .mapimail, .jnt, .dbx, .contact …*

File Encryption: Algorithm

Encryption used:

- Uses both RSA and AES algorithms
- The AES-128 key is randomly generated for each file
- The AES-128 key is used to encrypt the file and it’s filename
- After encryption, the AES-128 key will be encrypted by RSA-2048

File Encryption: Filename

Format of filenames of encrypted files.

4DF383039AB03953D81660EB4CADC28D.locky

Victim ID

File ID

File Encryption: Filename

Format of filenames of encrypted files.

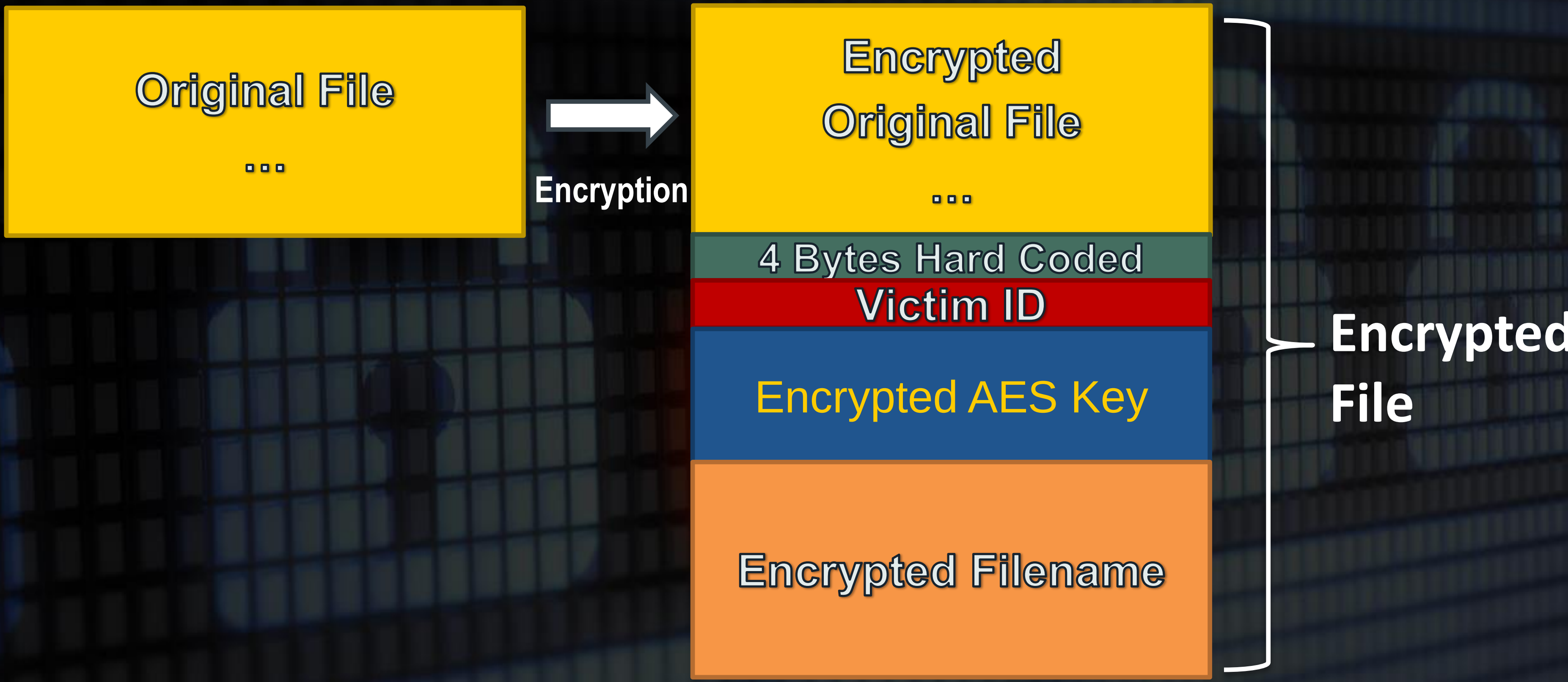
4DF383039AB03953D81660EB4CADC28D.locky

Victim ID File ID

IZ8FDXJD-K685-W9X6-491BC1BE-644CD37731DF.asasin

Victim ID File ID

File Encryption: File layout



Original File

...

Encryption

Encrypted

Original File

...

4 Bytes Hard Coded

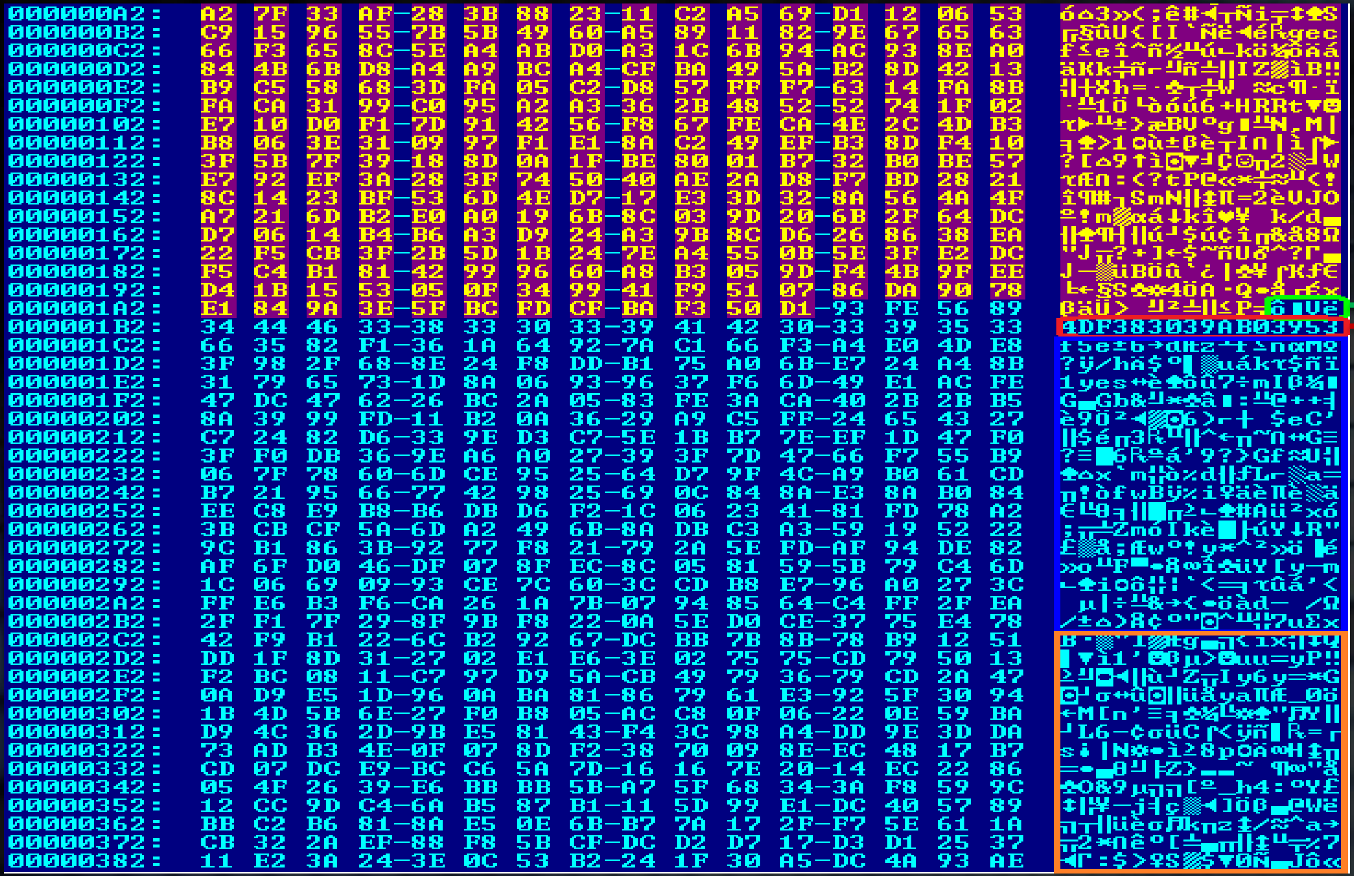
Victim ID

Encrypted AES Key

Encrypted Filename

Encrypted File

File Encryption: File layout



```
000000A2:  A2 7F 33 AF-28 3B 88 23-11 C2 A5 69-D1 12 06 53
000000B2:  C9 15 96 55-7B 5B 49 60-A5 89 11 82-9E 67 65 63
000000C2:  66 F3 65 8C-5E A4 AB D0-A3 1C 6B 94-AC 93 8E A0
000000D2:  84 4B 6B D8-A4 A9 BC A4-CF BA 49 5A-B2 8D 42 13
000000E2:  B9 C5 58 68-3D FA 05 C2-D8 57 FF F7-63 14 FA 8B
000000F2:  FA CA 31 99-C0 95 A2 A3-36 2B 48 52-52 74 1F 02
00000102:  E7 10 D0 F1-7D 91 42 56-F8 67 FE CA-4E 2C 4D B3
00000112:  B8 06 3E 31-09 97 F1 E1-8A C2 49 EF-B3 8D F4 10
00000122:  3F 5B 7F 39-18 8D 0A 1F-BE 80 01 B7-32 B0 BE 57
00000132:  E7 92 EF 3A-28 3F 74 50-40 AE 2A D8-F7 BD 28 21
00000142:  8C 14 23 BF-53 6D 4E D7-17 E3 3D 32-8A 56 4A 4F
00000152:  A7 21 6D B2-E0 A0 19 6B-8C 03 9D 20-6B 2F 64 DC
00000162:  D7 06 14 B4-B6 A3 D9 24-A3 9B 8C D6-26 86 38 EA
00000172:  22 F5 CB 3F-2B 5D 1B 24-7E A4 55 0B-5E 3F E2 DC
00000182:  F5 C4 B1 81-42 99 96 60-A8 B3 05 9D-F4 4B 9F EE
00000192:  D4 1B 15 53-05 0F 34 99-41 F9 51 07-86 DA 90 78
000001A2:  E1 84 9A 3E-5F BC FD CF-BA F3 50 D1-93 FE 56 89
000001B2:  34 44 46 33-38 33 30 33-39 41 42 30-33 39 35 33
000001C2:  66 35 82 F1-36 1A 64 92-7A C1 66 F3-A4 E0 4D E8
000001D2:  3F 98 2F 68-8E 24 F8 DD-B1 75 A0 6B-E7 24 A4 8B
000001E2:  31 79 65 73-1D 8A 06 93-96 37 F6 6D-49 E1 AC FE
000001F2:  47 DC 47 62-26 BC 2A 05-83 FE 3A CA-40 2B 2B B5
00000202:  8A 39 99 FD-11 B2 0A 36-29 A9 C5 FF-24 65 43 27
00000212:  C7 24 82 D6-33 9E D3 C7-5E 1B B7 7E-EF 1D 47 F0
00000222:  3F F0 DB 36-9E A6 A0 27-39 3F 7D 47-66 F7 55 B9
00000232:  06 7F 78 60-6D CE 95 25-64 D7 9F 4C-A9 B0 61 CD
00000242:  B7 21 95 66-77 42 98 25-69 0C 84 8A-E3 8A B0 84
00000252:  EE C8 E9 B8-B6 DB D6 F2-1C 06 23 41-81 FD 78 A2
00000262:  3B CB CF 5A-6D A2 49 6B-8A DB C3 A3-59 19 52 22
00000272:  9C B1 86 3B-92 77 F8 21-79 2A 5E FD-AF 94 DE 82
00000282:  AF 6F D0 46-DF 07 8F EC-8C 05 81 59-5B 79 C4 6D
00000292:  1C 06 69 09-93 CE 7C 60-3C CD B8 E7-96 A0 27 3C
000002A2:  FF E6 B3 F6-CA 26 1A 7B-07 94 85 64-C4 FF 2F EA
000002B2:  2F F1 7F 29-8F 9B F8 22-0A 5E D0 CE-37 75 E4 78
000002C2:  42 F9 B1 22-6C B2 92 67-DC BB 7B 8B-78 B9 12 51
000002D2:  DD 1F 8D 31-27 02 E1 E6-3E 02 75 75-CD 79 50 13
000002E2:  F2 BC 08 11-C7 97 D9 5A-CB 49 79 36-79 CD 2A 47
000002F2:  0A D9 E5 1D-96 0A BA 81-86 79 61 E3-92 5F 30 94
00000302:  1B 4D 5B 6E-27 F0 B8 05-AC C8 0F 06-22 0E 59 BA
00000312:  D9 4C 36 2D-9B E5 81 43-F4 3C 98 A4-DD 9E 3D DA
00000322:  73 AD B3 4E-0F 07 8D F2-38 70 09 8E-EC 48 17 B7
00000332:  CD 07 DC E9-BC C6 5A 7D-16 16 7E 20-14 EC 22 86
00000342:  05 4F 26 39-E6 BB BB 5B-A7 5F 68 34-3A F8 59 9C
00000352:  12 CC 9D C4-6A B5 87 B1-11 5D 99 E1-DC 40 57 89
00000362:  BB C2 B6 81-8A E5 0E 6B-B7 7A 17 2F-F7 5E 61 1A
00000372:  CB 32 2A EF-88 F8 5B CF-DC D2 D7 17-D3 D1 25 37
00000382:  11 E2 3A 24-3E 0C 53 B2-24 1F 30 A5-DC 4A 93 AE
```

Encrypted Data

*Encryption used: AES-128

Hardcoded Value

Victim ID

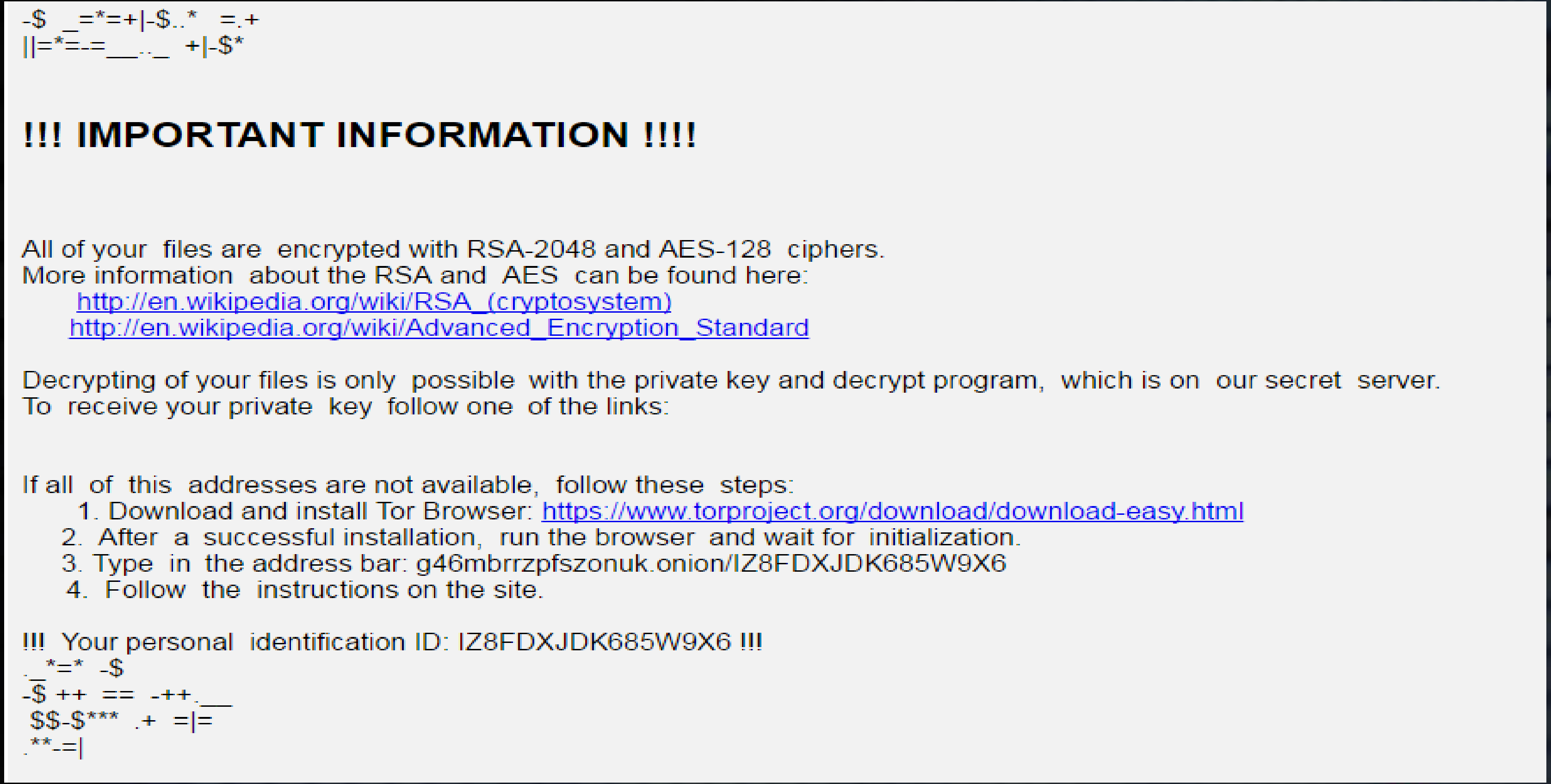
Encrypted AES Key

*Encryption used: RSA-2048

Encrypted Filename

*Encryption used: AES-128

HTML Ransom Note



```
-$ _=*=+|-$..* =.+
||=*=-=___.._ +|-$*
```

!!! 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:

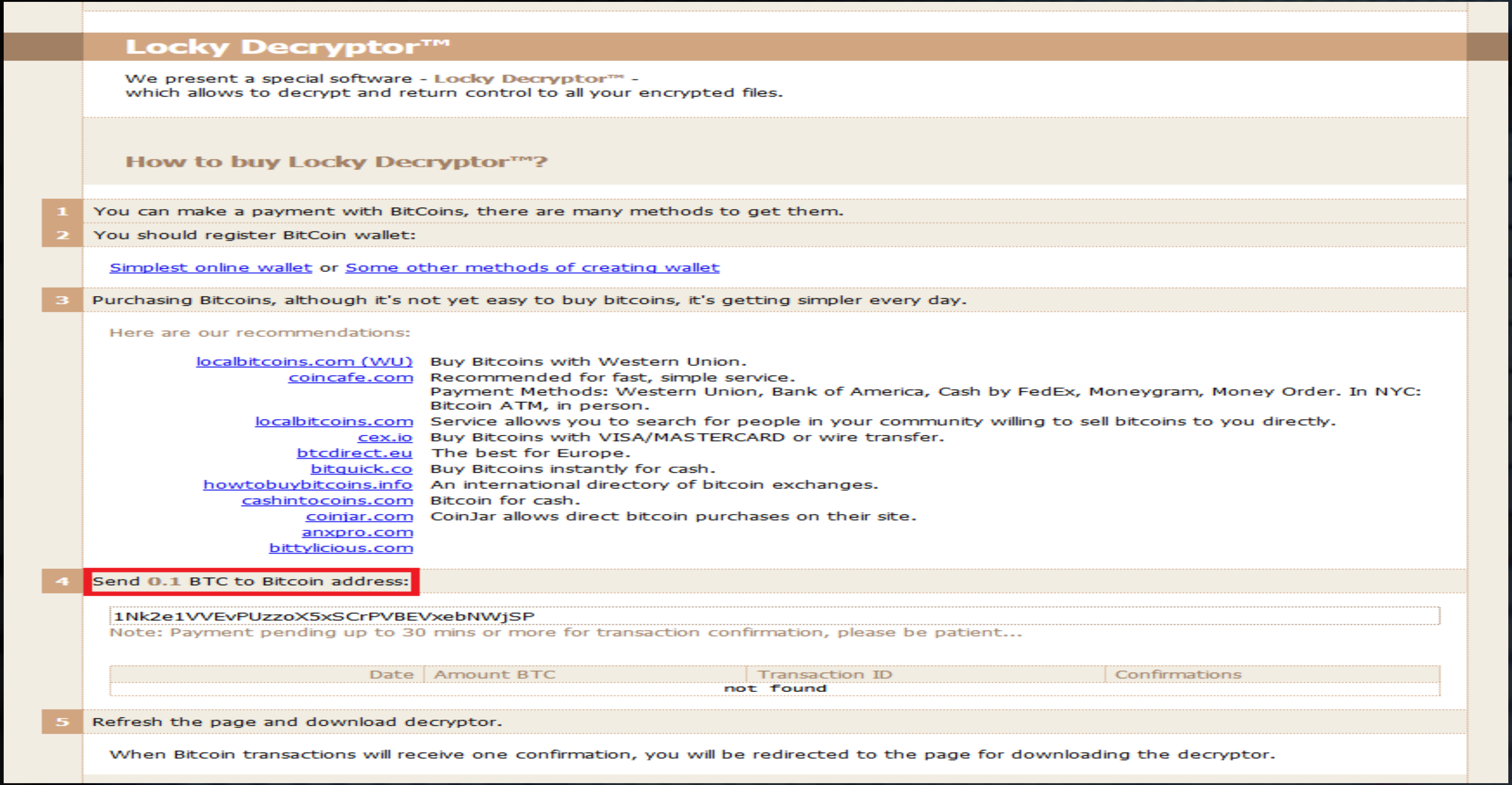
If all of this addresses are not available, follow these steps:

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: g46mbrrzpfszonuk.onion/IZ8FDXJDK685W9X6
4. Follow the instructions on the site.

!!! Your personal identification ID: IZ8FDXJDK685W9X6 !!!

```
._*=* -$
-$ ++ == -++.__
 $$-$*** .+ =|=
.**-=|
```

Decryptor Page



Locky Decryptor™

We present a special software - Locky Decryptor™ -
which allows to decrypt and return control to all your encrypted files.

How to buy Locky Decryptor™?

1 You can make a payment with BitCoins, there are many methods to get them.

2 You should register BitCoin wallet:

Simplest online wallet or Some other methods of creating wallet

3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

localbitcoins.com (WU)	Buy Bitcoins with Western Union.
coincafe.com	Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
localbitcoins.com	Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io	Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu	The best for Europe.
bitquick.co	Buy Bitcoins instantly for cash.
howtobuybitcoins.info	An international directory of bitcoin exchanges.
cashintocoins.com	Bitcoin for cash.
coinjar.com	CoinJar allows direct bitcoin purchases on their site.
anxpro.com	
bittylicious.com	

4 Send 0.1 BTC to Bitcoin address:

1Nk2e1VVEvPUzzoX5xSCrPVBEVxebNWjSP

Note: Payment pending up to 30 mins or more for transaction confirmation, please be patient...

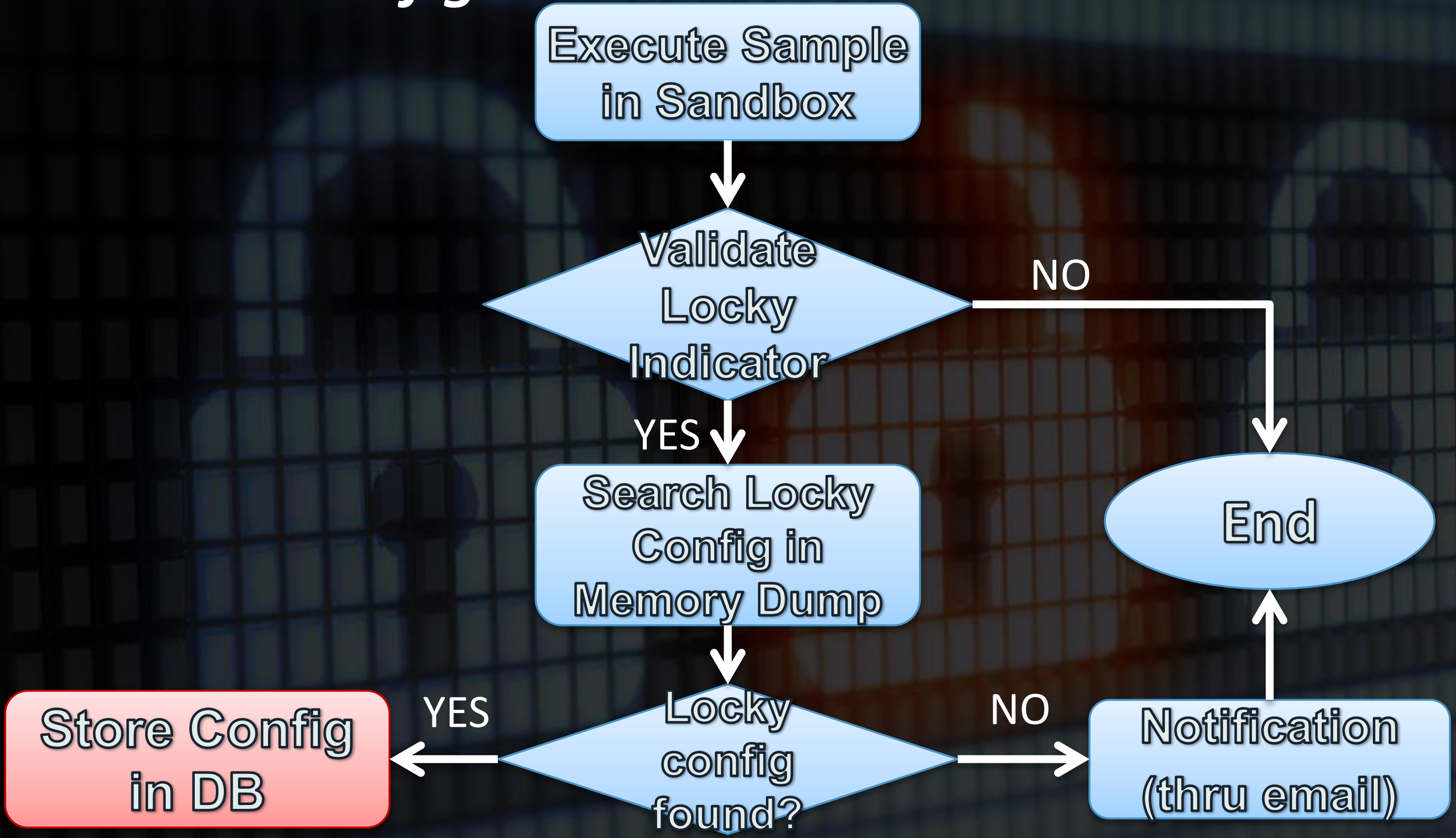
Date	Amount BTC	Transaction ID	Confirmations
		not found	

5 Refresh the page and download decryptor.

When Bitcoin transactions will receive one confirmation, you will be redirected to the page for downloading the decryptor.

Harvest Locky Configuration

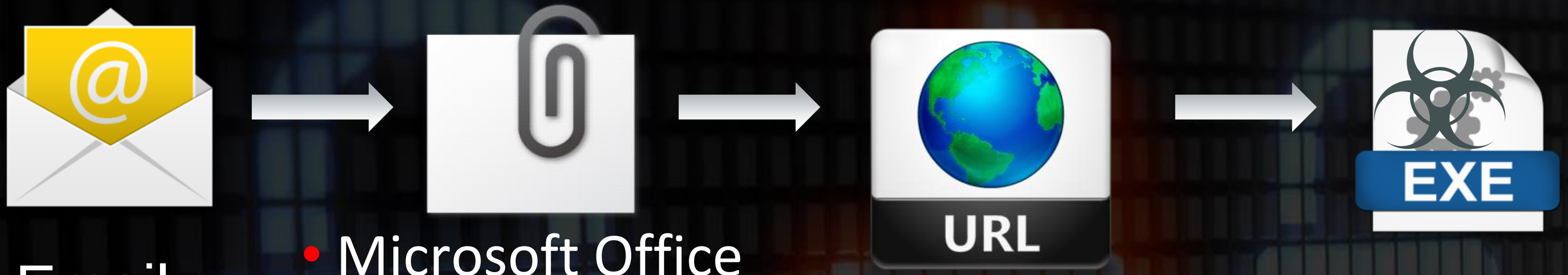
Automate Configuration Extraction: Overview



Execute Sample in Sandbox
Validate Locky Indicator
NO
YES
Search Locky Config in Memory Dump
End
Lucky config found?
YES
Store Config in DB
NO
Notification (thru email)

Kill Chain

Kill Chain: SPAM Campaign

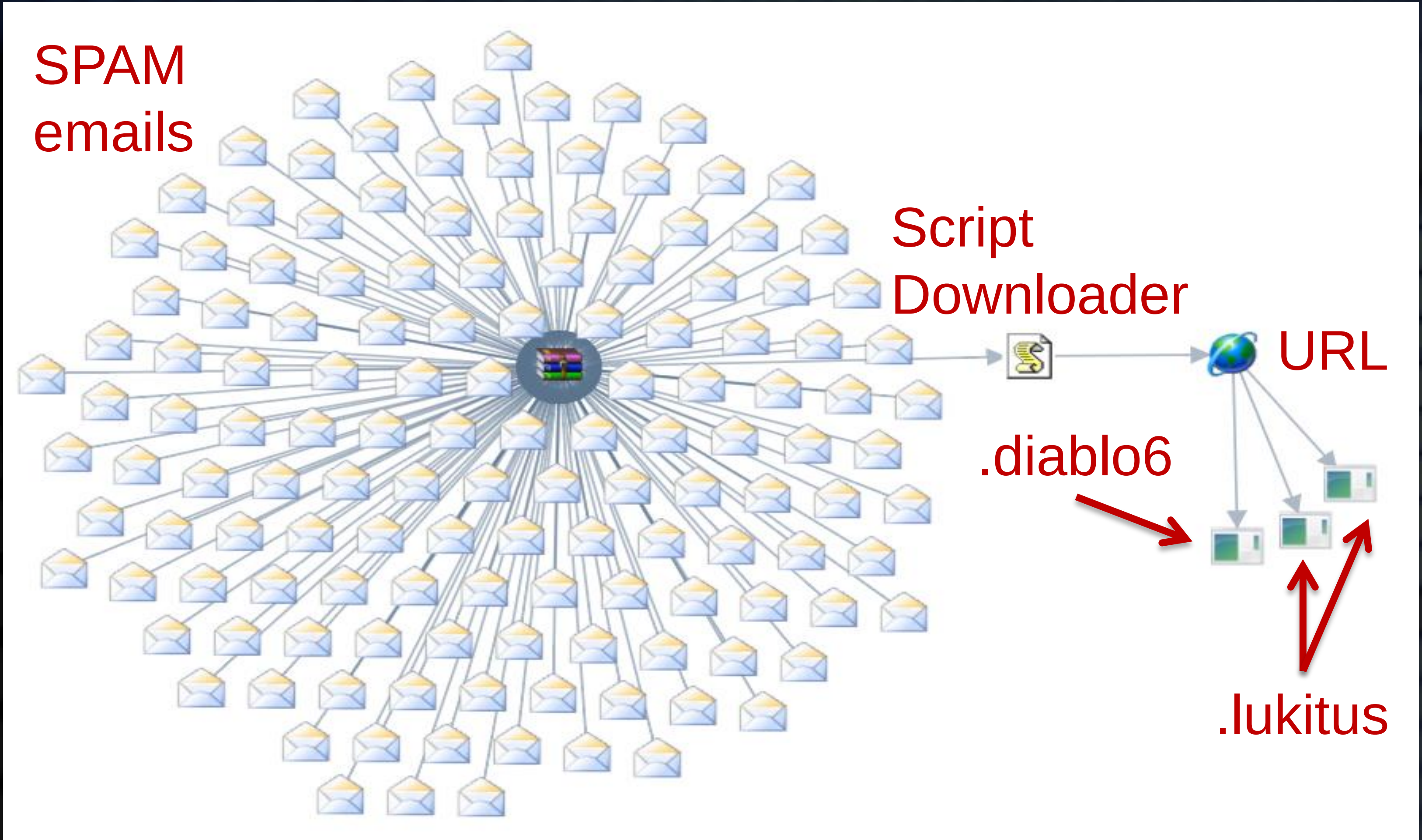


Email

- Microsoft Office
- LNK(.lnk)
- Powershell
- HTML(.hta, .chm)
- Archive(.rar, .zip)
- Script(.js, .jse, .vbs, .wsf)
- Portable Document Format(.pdf)

Download URLs

Payload



SPAM emails

Script Downloader

URL

.diablo6

.lukitus

Date	Email Subject	Attachment	DL URI	Config
1st Wave Monday 09/17/17 08:24 AM	Status of invoice	A2173164-48.7z	/87thiuh3gfDGS	affilID: 3 URI: <yes> C&C: <yes> ***online/offline** encryption
2nd Wave Monday 09/17/17 05:13 PM	Message from km_c224e	20171809_60412473780.7z	/DKndhFG72	affilID: 3 URI: <none> C&C: <none> ***offline** encryption

Interesting Observations

- Email subject (e.g. *“Message from km_c224e”)*
  - *Same spam email subject by Dridex and Jaff Ransomware*
- Qtbot loader serves *Trickbot* and *Locky*
  - *Country codes: UK, IE, AU, GB, LU or BE -> Trickbot*
- Locky ransomware files share the same download servers with Sage ransomware
- Locky ransomware files share the same download servers with Fake Globe ransomware

Conclusion

FortiGuard – Q&A

Thank you

fbacurio@fortinet.com
rjoven@fortinet.com

Follow us on twitter

@fbacurio
@rommeljoven17