FORTINET

How to catch your hacker: practical stories

Artem Semenchenko -

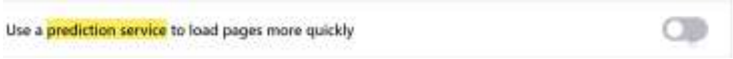
FortiGuard Labs SG

asemenchenko@fortinet.com

How to start your investigation

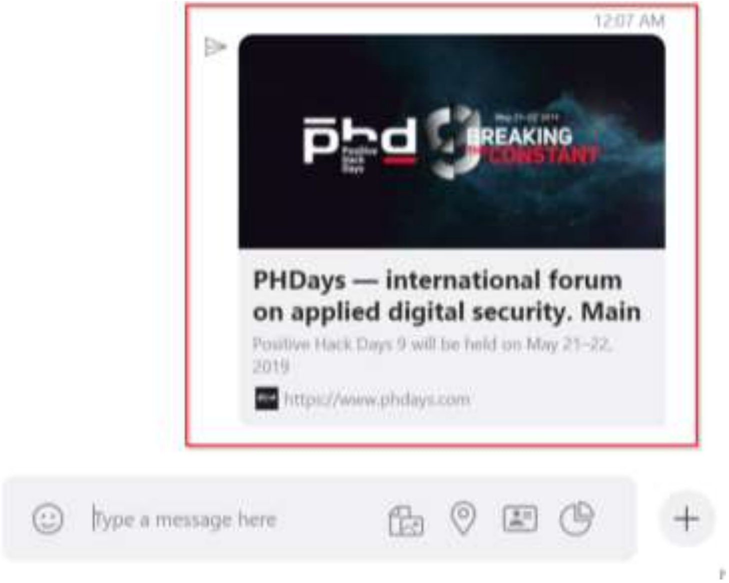
Step 0: Operation Security

Hide IP



Use a prediction service to load pages more quickly

Disable a “prediction service”



12:07 AM

PHDays — international forum on applied digital security. Main

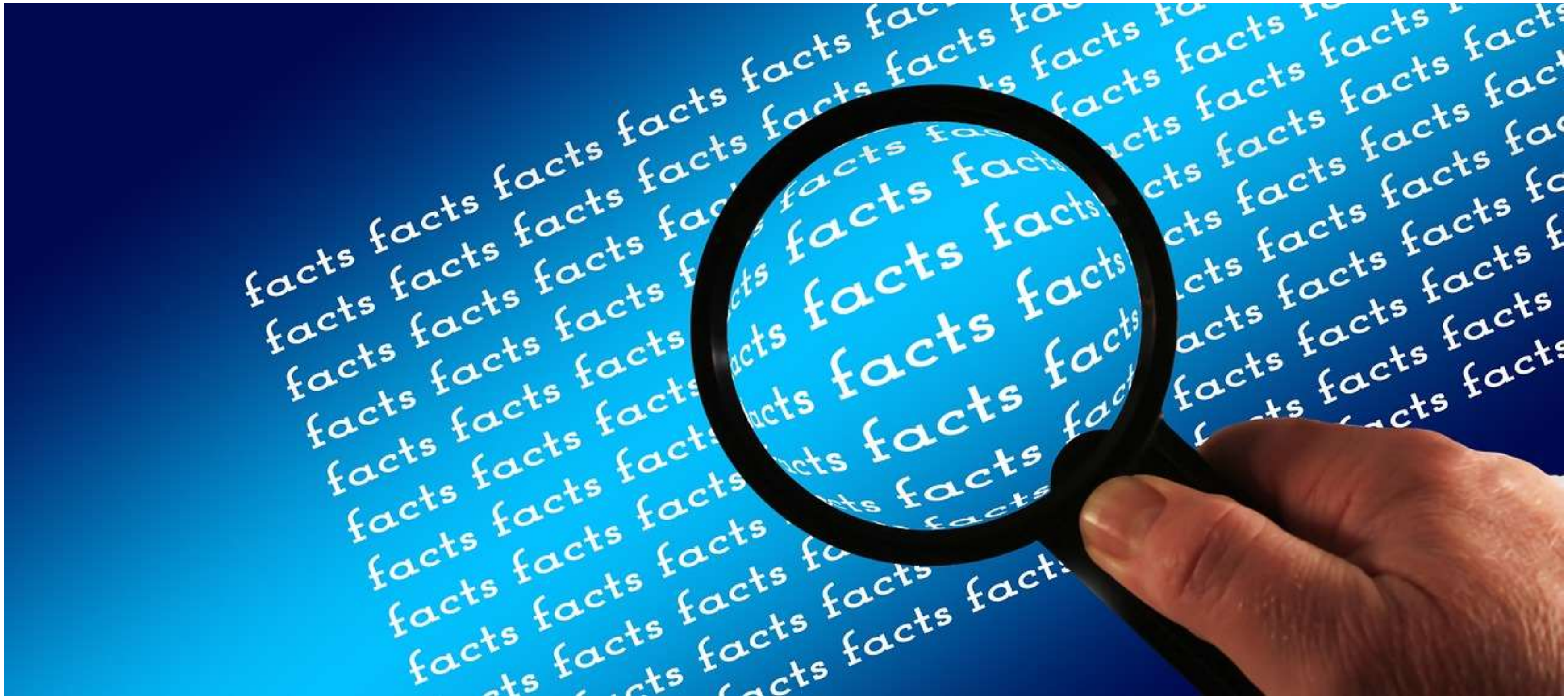
Positive Hack Days 9 will be held on May 21–22, 2019

https://www.phdays.com

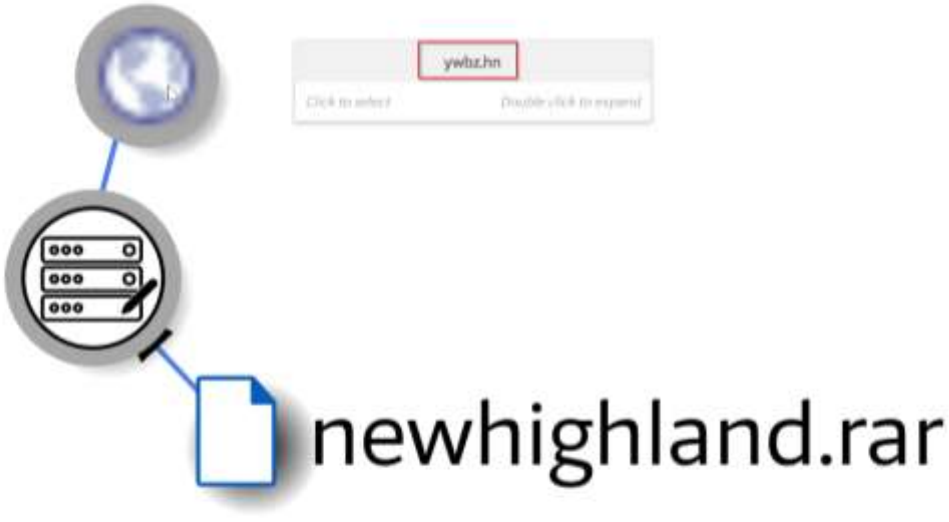
Type a message here

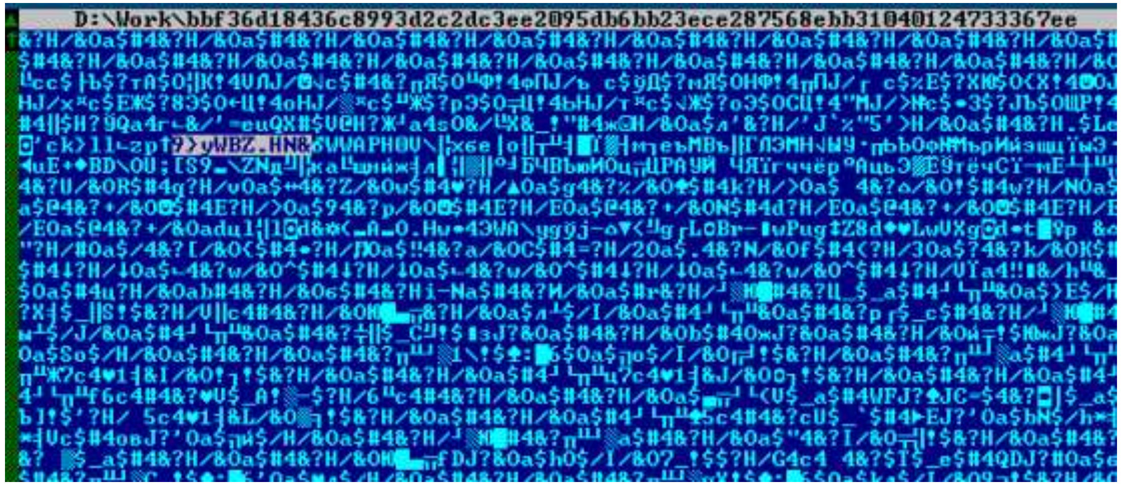
Store and share URLs in a “safe mode”

Step 1&2: Get facts and check facts



Practical story: VT and URL’s





```
D:\Work\bbf36d18436c8993d2c2dc3ee2095db6bb23ece287568ebb3104012473336 7ee
9>yWBZ.HN&
```

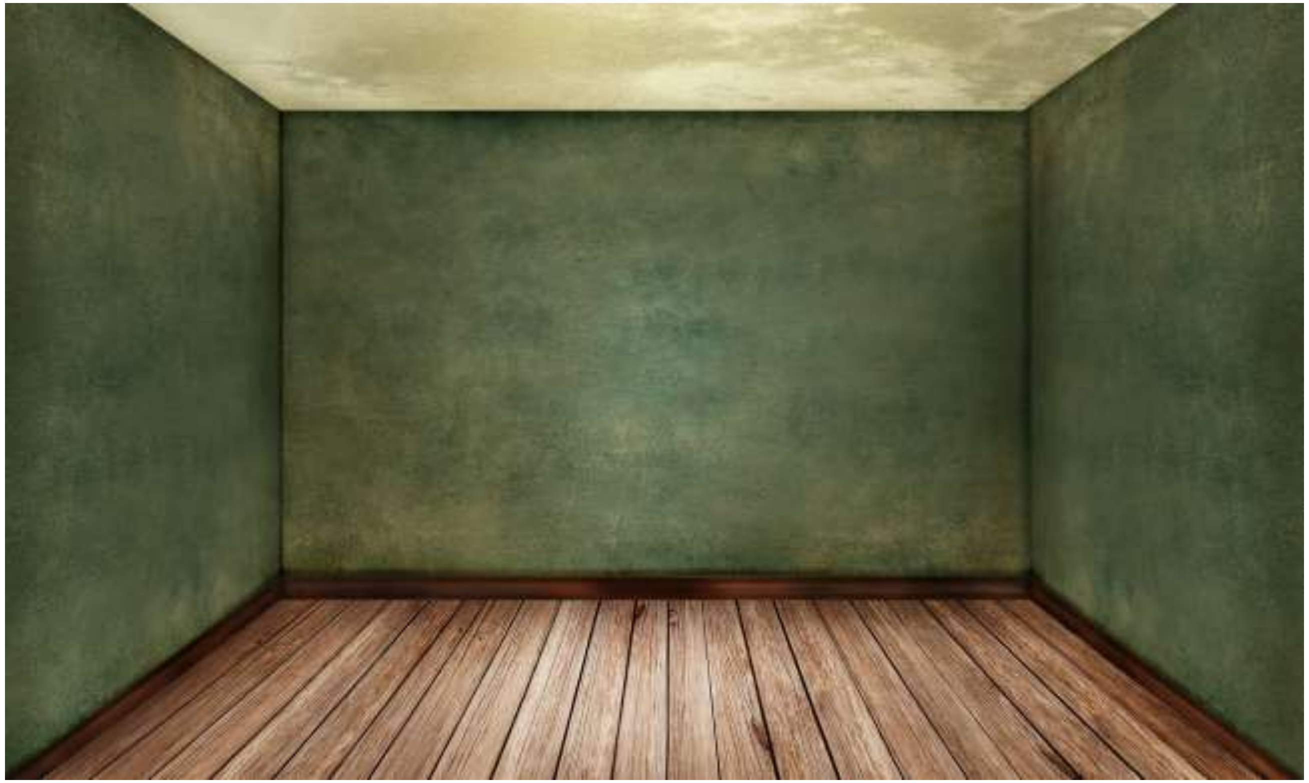
VT shows a connection between a *newhighland.rar* sample and a domain *ywbz.hn*

ywbz.hn substring inside the *newhighland.rar*

When DHS/FBI "GRIZZLY STEPPE" report… goes terribly wrong

Note: Russian authorities reports can be hilarious too ☺

Here are all the people you can fully trust in your investigations:

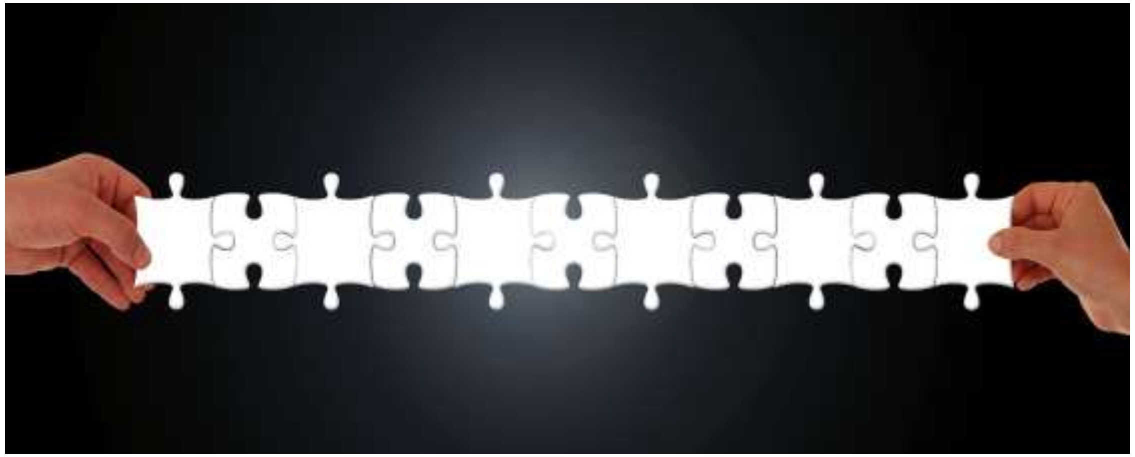


Following the footprints

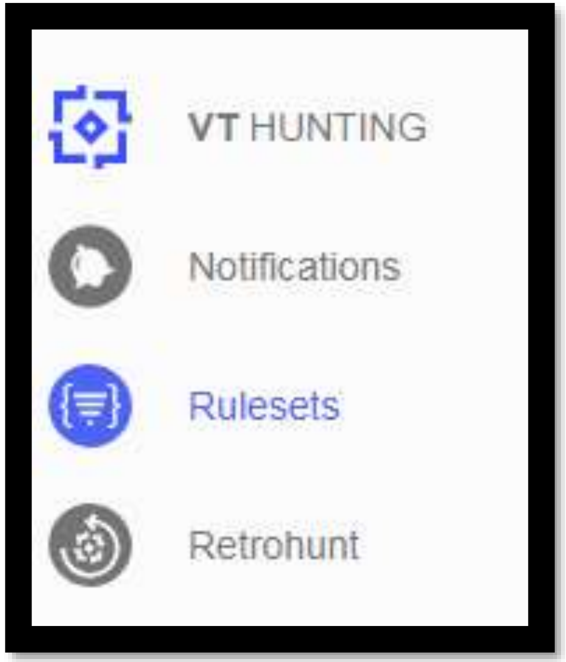
Related samples search

Related samples search:

- Create a detection and check stats.
- Search in your samples library:
  - Heavily vendor dependent;
- Search on the external platforms:
  - Non-strict hashes
  - Strings
  - **YARA**



YARA samples search life-hacks:


VT HUNTING

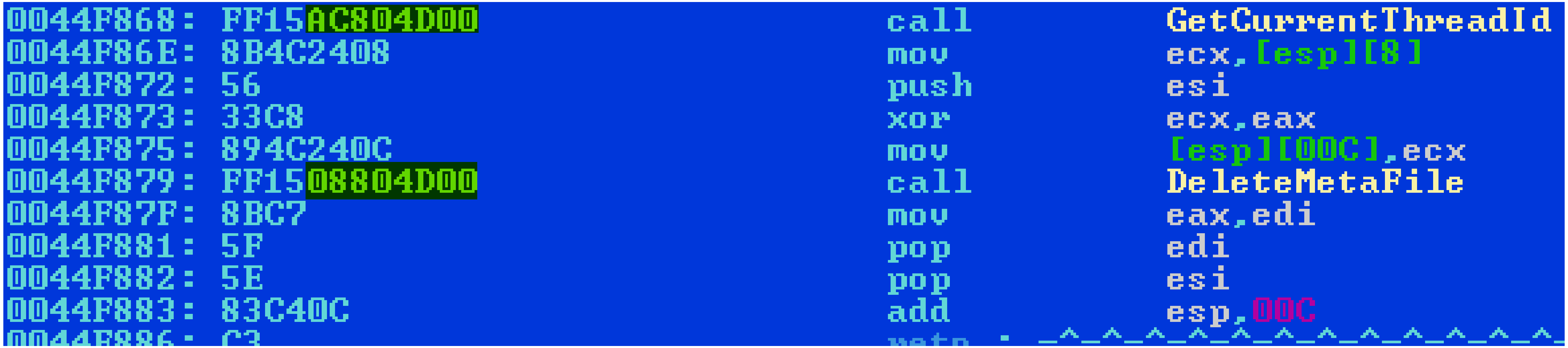
Notifications

Rulesets

Retrohunt

- YARA search is FP friendly ☺
- String search:
  - do not restrict to executables only
- Code search:
  - avoid absolute and long relative addresses

Screenshots code hunting



```
0044F868: FF15AC804D00                          call        GetCurrentThreadId
0044F86E: 8B4C2408                              mov         ecx,[esp][8]
0044F872: 56                                    push        esi
0044F873: 33C8                                  xor         ecx,eax
0044F875: 894C240C                              mov         [esp][00C],ecx
0044F879: FF1508804D00                          call        DeleteMetaFile
0044F87F: 8BC7                                  mov         eax,edi
0044F881: 5F                                    pop         edi
0044F882: 5E                                    pop         esi
0044F883: 83C40C                                add         esp,00C
0044F886: C3                                    retn  ; -^-^-^-^-^-^-^-^-^-^-^-^-
```

Following the footprints

Hunt for Clues

JPEG: not only EXIF

- Size does matter ☺
- Upload time
- Information ON the picture

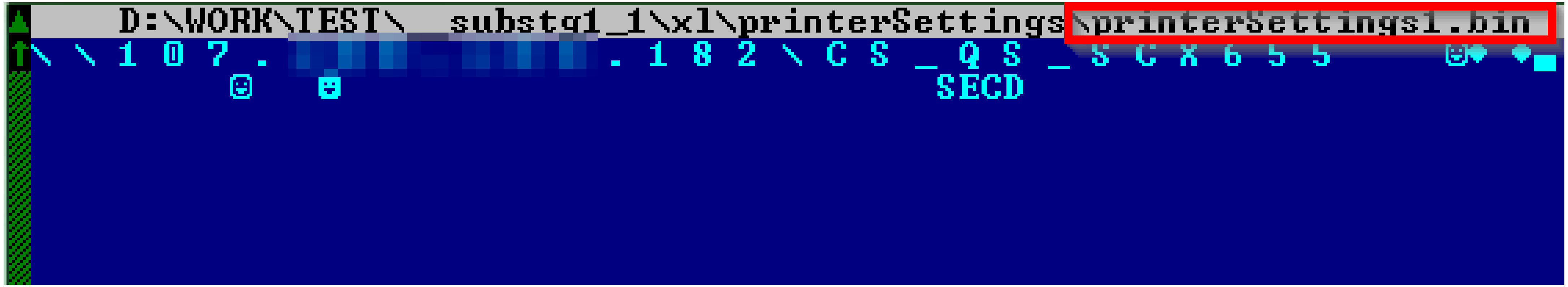
Credits: CabinCr3w ☺

PE: not just a PDB Path and a Resources Locale

- Unique strings
  - Mutexes
  - Reg-keys
  - Dropped files names
- VT upload time
- VT upload name

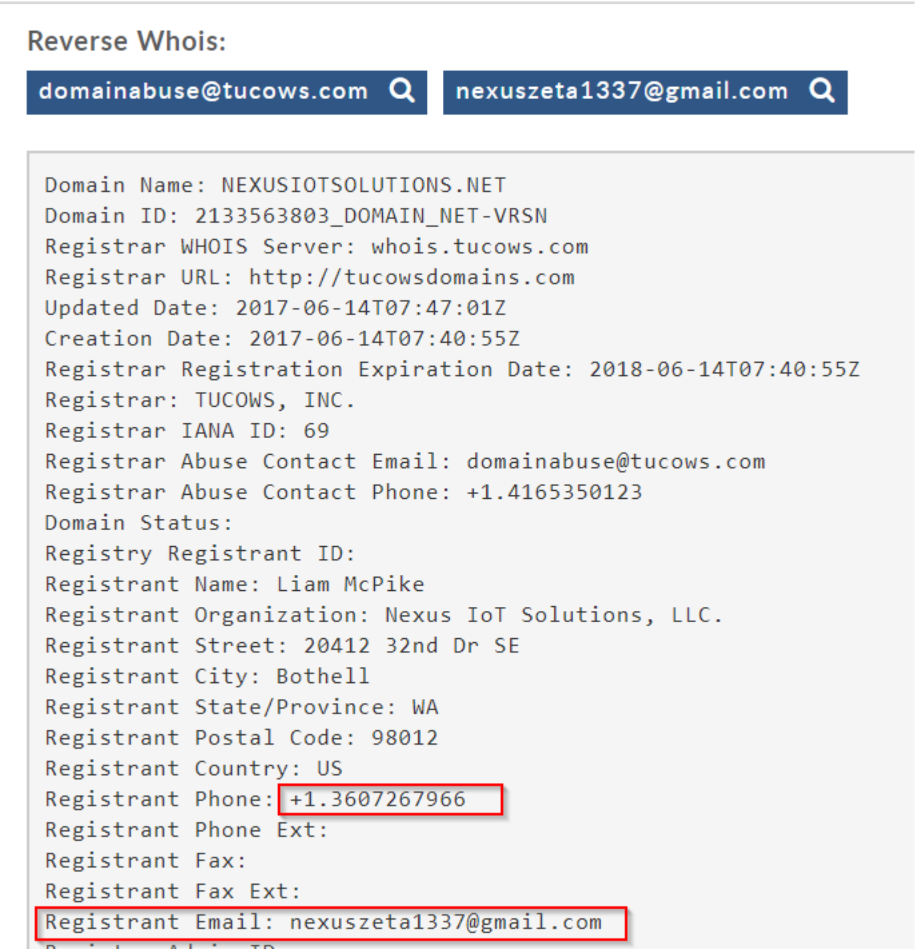
MS office: not only "the dodgy dossier"

- PrinterSettings*.bin:



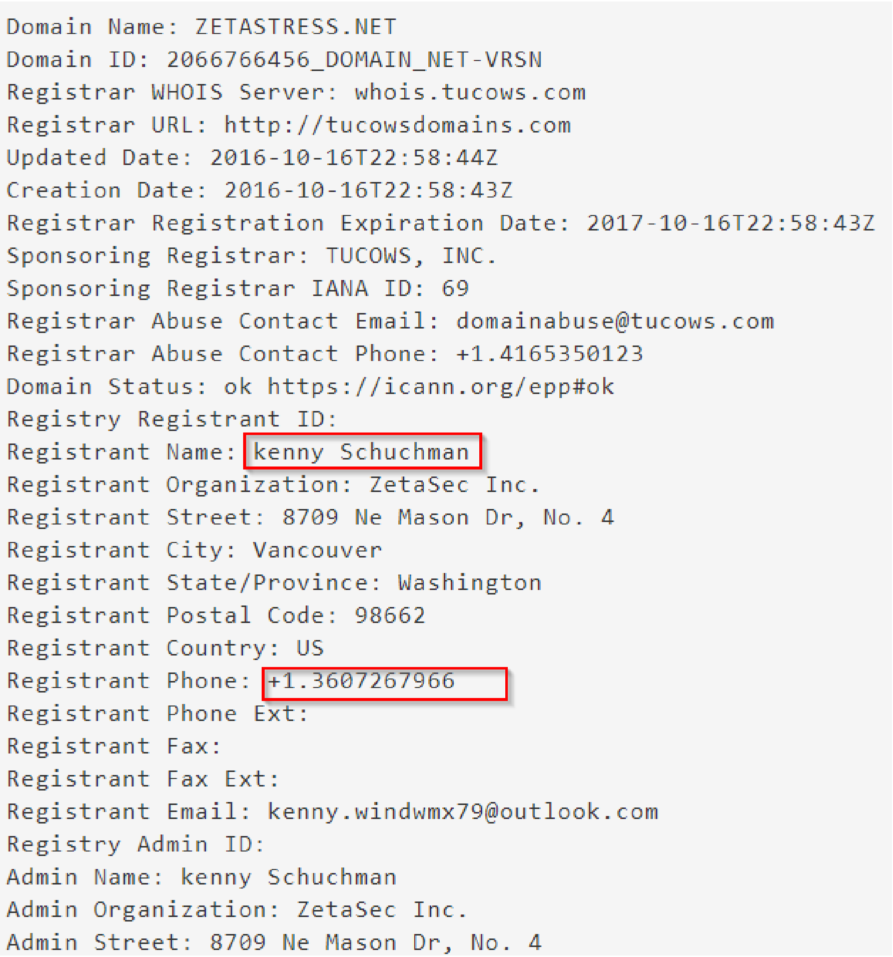
```
D:\WORK\TEST\   substg1_1\xl\printerSettings\printerSettings1.bin
\\107.[redacted].182\CS_QS_SCX655
              ☺    ☻                      SECD
```

Reverse Who-is: not only email - any custom field



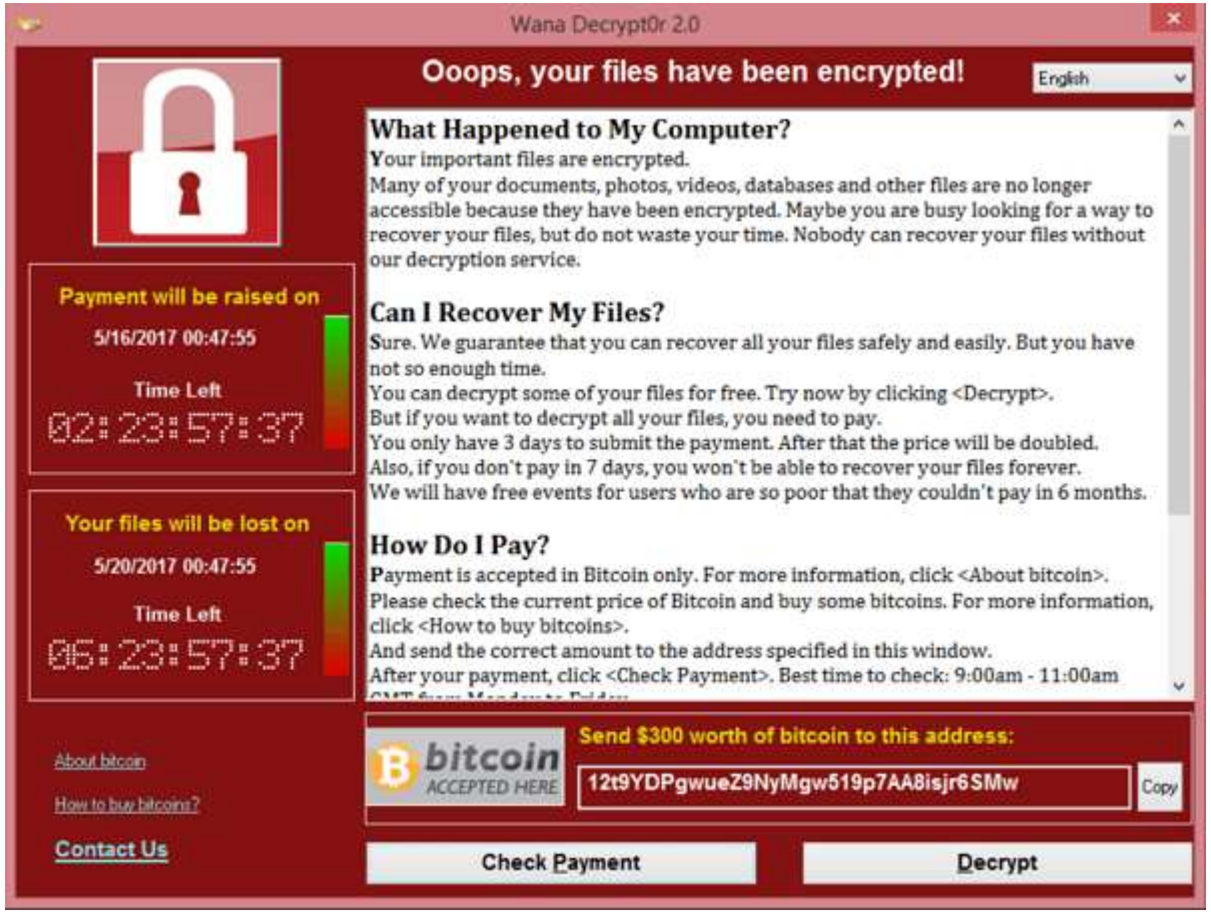
Reverse Whois:

```
Domain Name: NEXUSIOTSOLUTIONS.NET
Domain ID: 2133563803_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2017-06-14T07:47:01Z
Creation Date: 2017-06-14T07:40:55Z
Registrar Registration Expiration Date: 2018-06-14T07:40:55Z
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Domain Status:
Registry Registrant ID:
Registrant Name: Liam McPike
Registrant Organization: Nexus IoT Solutions, LLC.
Registrant Street: 20412 32nd Dr SE
Registrant City: Bothell
Registrant State/Province: WA
Registrant Postal Code: 98012
Registrant Country: US
Registrant Phone: +1.3607267966
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: nexuszeta1337@gmail.com
```



```
Domain Name: ZETASTRESS.NET
Domain ID: 2066766456_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2016-10-16T22:58:44Z
Creation Date: 2016-10-16T22:58:43Z
Registrar Registration Expiration Date: 2017-10-16T22:58:43Z
Sponsoring Registrar: TUCOWS, INC.
Sponsoring Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID:
Registrant Name: kenny Schuchman
Registrant Organization: ZetaSec Inc.
Registrant Street: 8709 Ne Mason Dr, No. 4
Registrant City: Vancouver
Registrant State/Province: Washington
Registrant Postal Code: 98662
Registrant Country: US
Registrant Phone: +1.3607267966
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kenny.windwmx79@outlook.com
Registry Admin ID:
Admin Name: kenny Schuchman
Admin Organization: ZetaSec Inc.
Admin Street: 8709 Ne Mason Dr, No. 4
```

Text: ransom notes language analysis



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>.

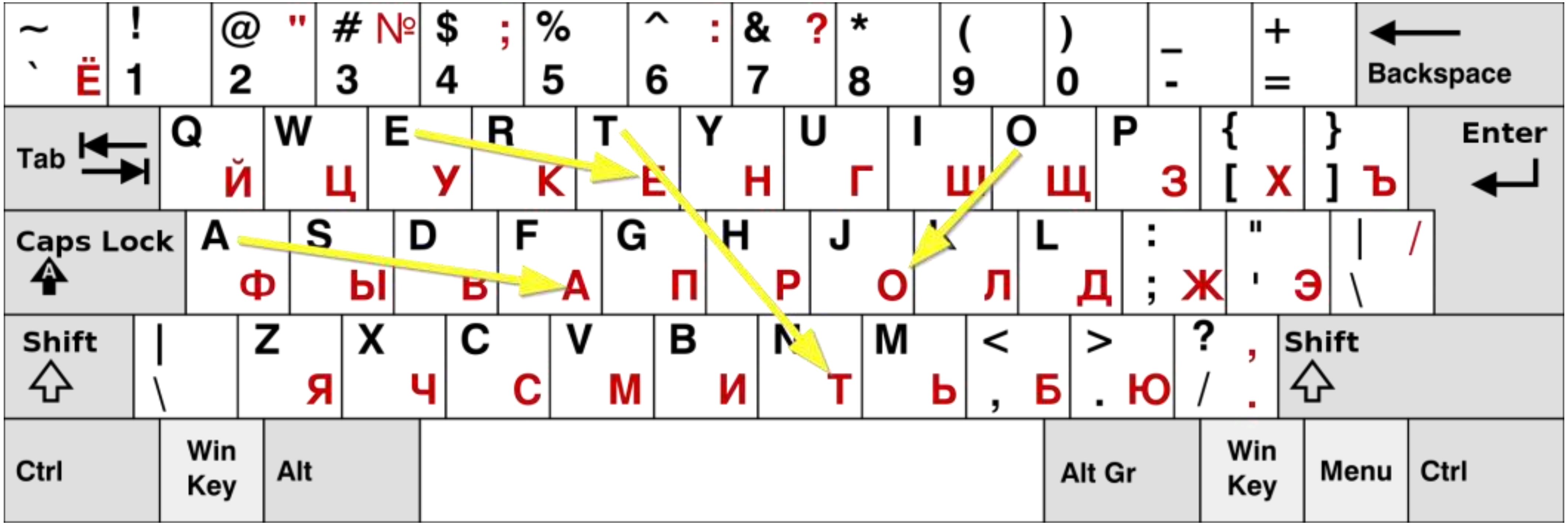
And send the correct amount to the address specified in this window.

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

Text typos: Russian keyboard layout traces

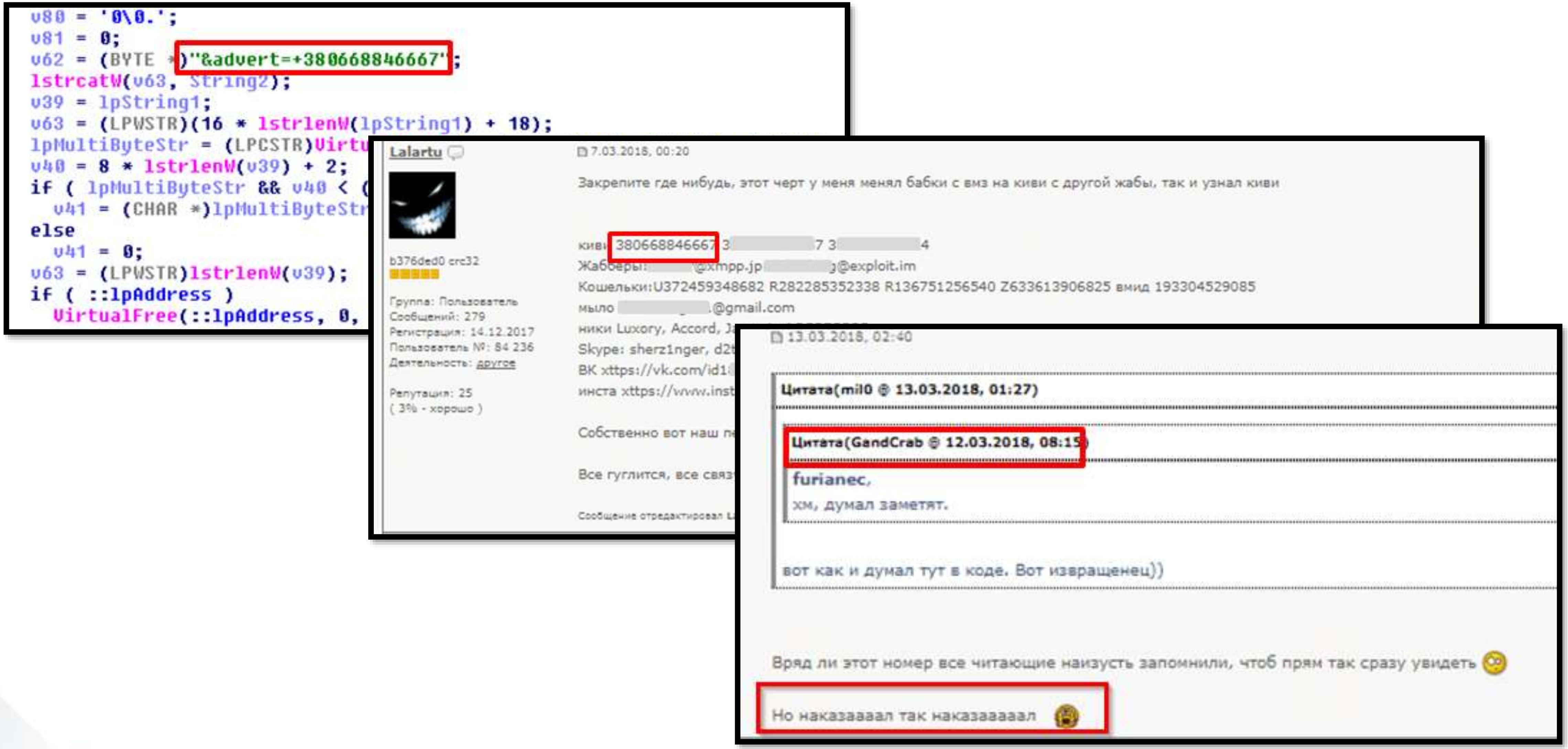


FORTINET

False Flags:

check twice

False Flags: GangCrab and a “sick children scam”



```
v80 = '0\0.';
v81 = 0;
v62 = (BYTE *)"&advert=+380668846667";
lstrcatW(v63, String2);
v39 = lpString1;
v63 = (LPWSTR)(16 * lstrlenW(lpString1) + 18);
lpMultiByteStr = (LPCSTR)Virtu
v40 = 8 * lstrlenW(v39) + 2;
if ( lpMultiByteStr && v40 < (
  v41 = (CHAR *)lpMultiByteStr
else
  v41 = 0;
v63 = (LPWSTR)lstrlenW(v39);
if ( ::lpAddress )
  VirtualFree(::lpAddress, 0,
```

Lalartu

b376ded0 crc32

Группа: Пользователь
Сообщений: 279
Регистрация: 14.12.2017
Пользователь №: 84 236
Деятельность: другое

Репутация: 25
(3% - хорошо)

7.03.2018, 00:20

Закрепите где нибудь, этот черт у меня менял бабки с вмз на киви с другой жабы, так и узнал киви

киви 380668846667 3[redacted]7 3[redacted]4
Жабберы: [redacted]@xmpp.jp [redacted]g@exploit.im
Кошельки:U372459348682 R282285352338 R136751256540 Z633613906825 вмид 193304529085
мыло [redacted].@gmail.com
ники Luxory, Accord, J
Skype: sherz1nger, d2
ВК xttps://vk.com/id1
инста xttps://www.inst

Собственно вот наш п

Все гуглится, все свя

Сообщение отредактировал L

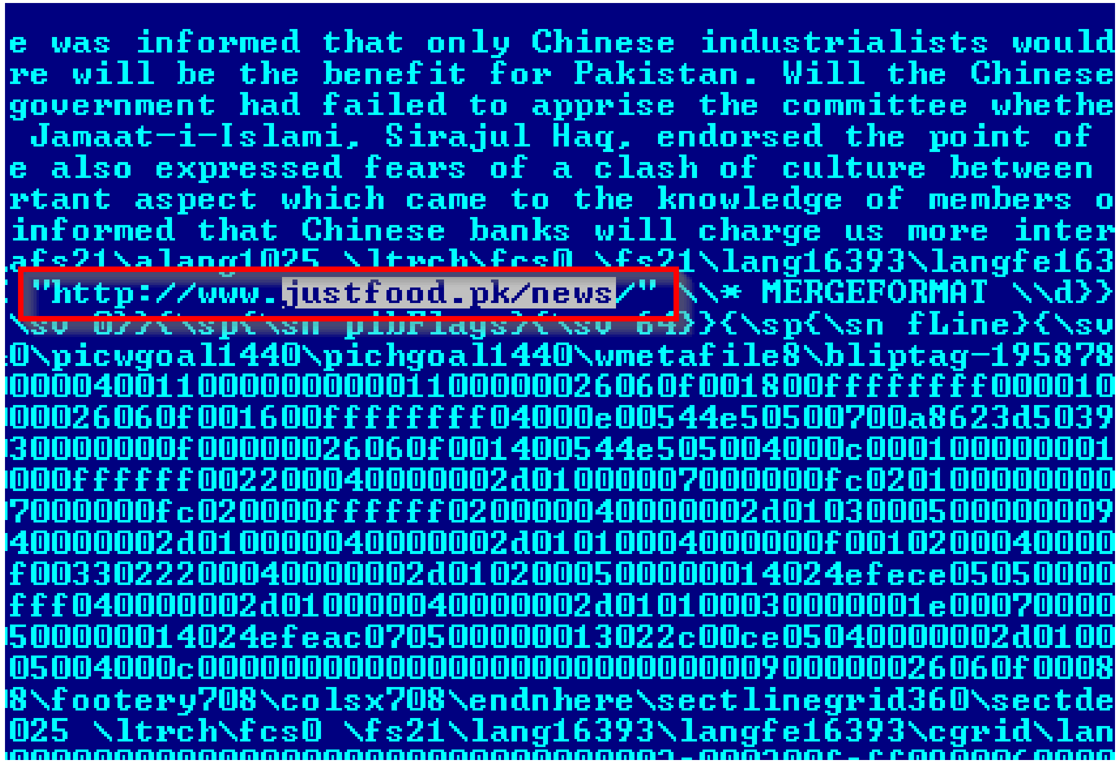
13.03.2018, 02:40

> **Цитата(mil0 @ 13.03.2018, 01:27)**
>
> > **Цитата(GandCrab @ 12.03.2018, 08:15)**
> >
> > furianec,
> >
> > хм, думал заметят.
>
> вот как и думал тут в коде. Вот извращенец))

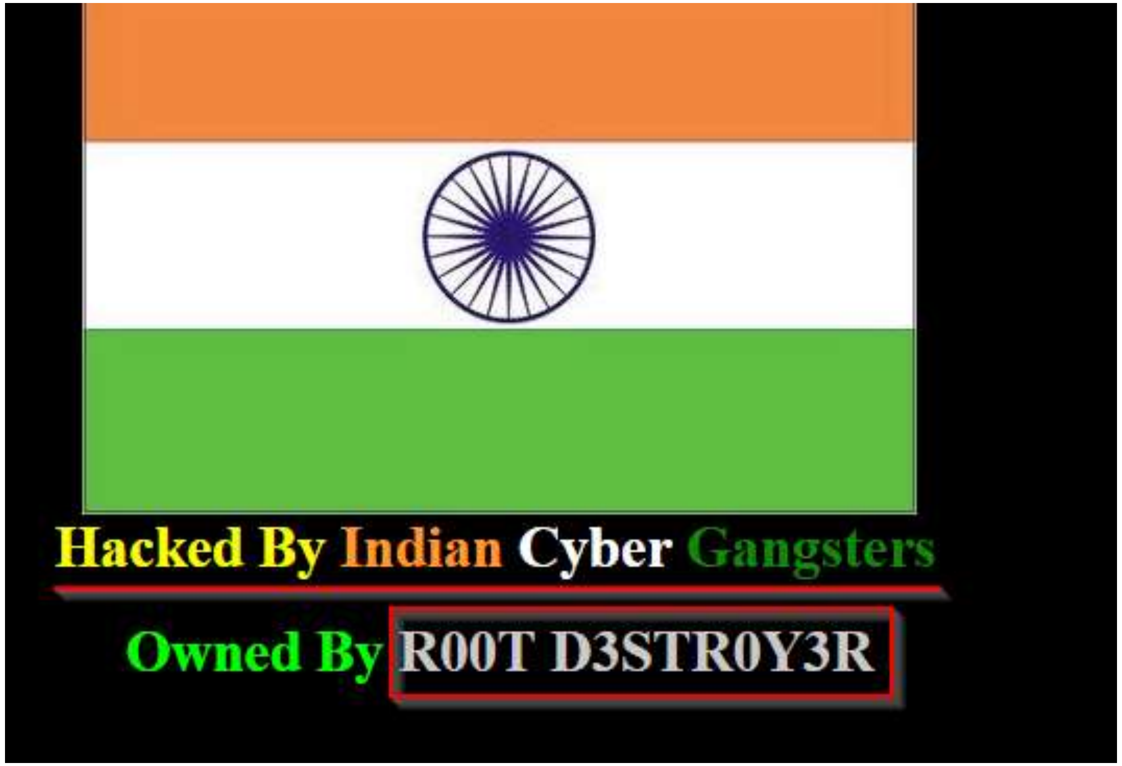
Вряд ли этот номер все читающие наизусть запомнили, чтоб прям так сразу увидеть

Но наказаааал так наказаааал

False Flags: web server can be exploited by multiple groups:

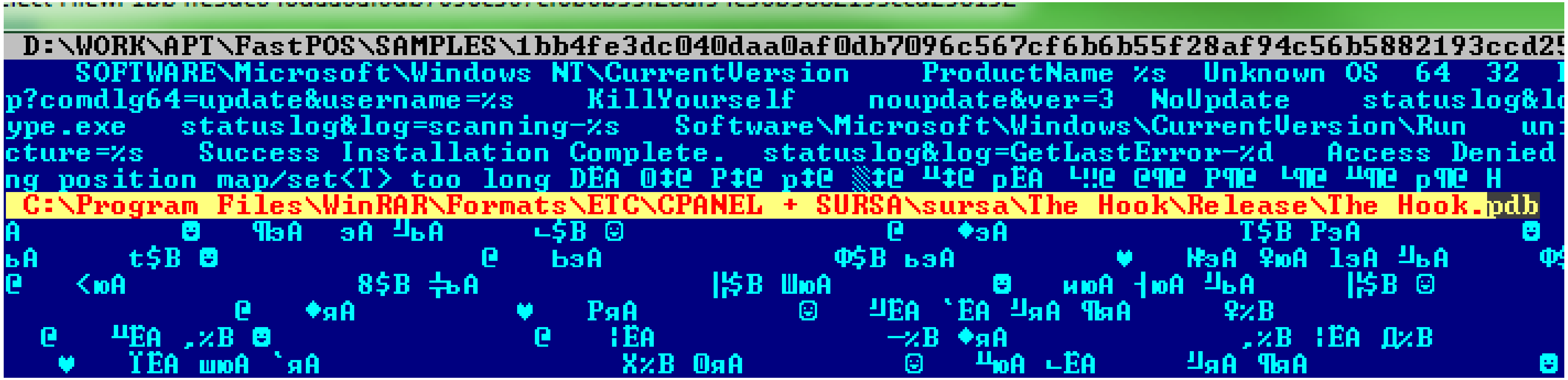


```
e was informed that only Chinese industrialists would
re will be the benefit for Pakistan. Will the Chinese
government had failed to apprise the committee whethe
 Jamaat-i-Islami, Sirajul Haq, endorsed the point of
e also expressed fears of a clash of culture between
rtant aspect which came to the knowledge of members o
informed that Chinese banks will charge us more inter
afs21\alang1025 \ltrch\fcs0 \fs21\lang16393\langfe163
 "http://www.justfood.pk/news/" \\* MERGEFORMAT \\d}}
\sv 0}}{\sp{\sn pibFlags}{\sv 64}}{\sp{\sn fLine}{\sv
0\picwgoal1440\pichgoal1440\wmetafile8\bliptag-195878
0000400110000000000001100000002606 0f001800ffffffff000010
00002606 0f001600ffffffff04000e00544e50500700a8623d5039
30000000f000000026060f001400544e505004000c00010000000001
000ffffff002200040000002d01000007000000fc020100000000
7000000fc020000ffffff020000040000002d010300050000009
40000002d010000040000002d0101000400000f0010200040000
f003302220004000000002d0102000500000014024efece0505000
fff04000000 2d010000040000002d01010003000001e00070000
500000014024efeac07050000000013022c00ce050400000002d0100
05004000c00000000000000000000000000009000000026060f0008
8\footery708\colsx708\endnhere\sectlinegrid360\sectde
025 \ltrch\fcs0 \fs21\lang16393\langfe16393\cgrid\lan
```



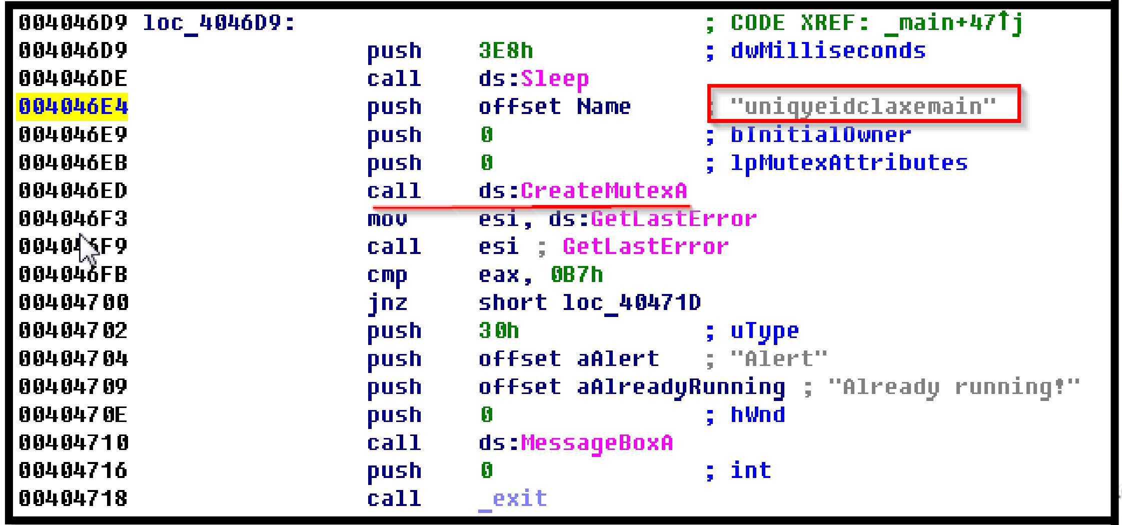
Real Investigation:
a POS malware

POS malware: PDB path

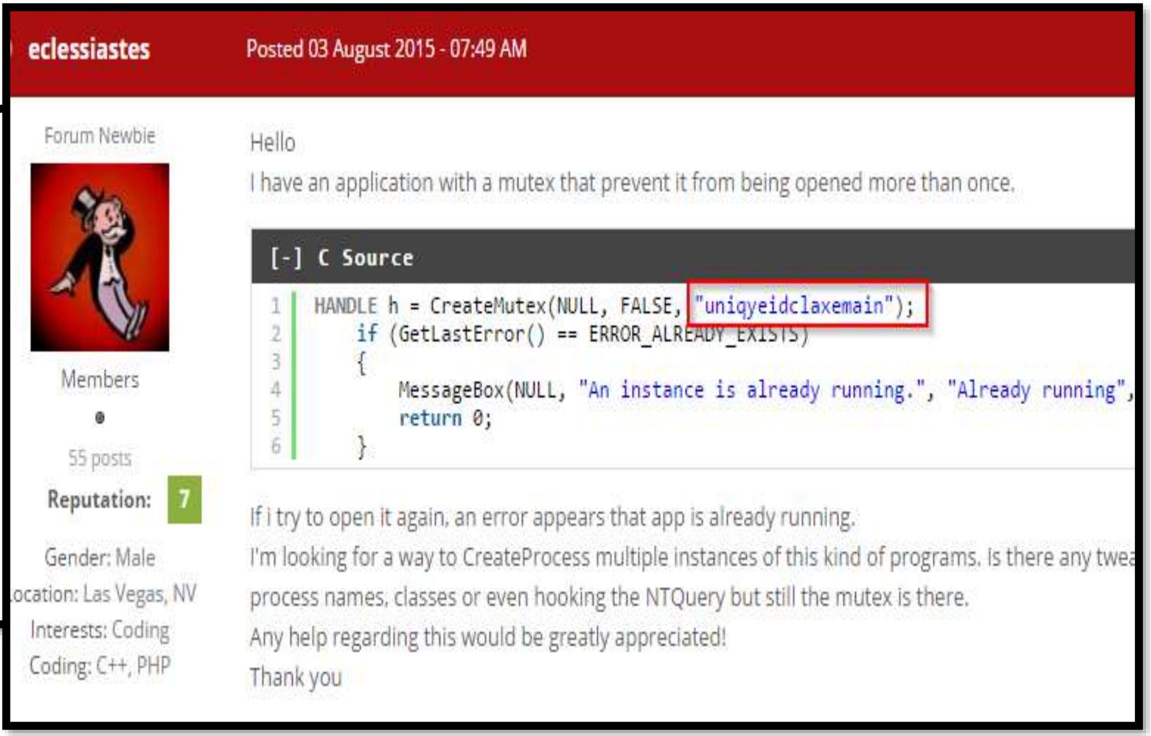


```
 D:\WORK\APT\FastPOS\SAMPLES\1bb4fe3dc040daa0af0db7096c567cf6b6b55f28af94c56b5882193ccd25
    SOFTWARE\Microsoft\Windows NT\CurrentVersion    ProductName %s  Unknown OS  64  32  I
p?comdlg64=update&username=%s    KillYourself    noupdate&ver=3  NoUpdate    statuslog&lo
ype.exe   statuslog&log=scanning-%s   Software\Microsoft\Windows\CurrentVersion\Run   uni
cture=%s   Success Installation Complete.  statuslog&log=GetLastError-%d   Access Denied
ng position map/set<T> too long DÈA 0‡@ P‡@ p‡@ ▒‡@ ╩‡@ pÈA ╚‼@ @¶@ P¶@ ╚¶@ ╩¶@ p¶@ H
 C:\Program Files\WinRAR\Formats\ETC\CPANEL + SURSA\sursa\The Hook\Release\The Hook.pdb
A          ☻   ¶ЬA  эA ╝ьA      ╘$B ☺                 @   ♦эA              T$B PэA         ☻
ьA      t$B ☻                 @    ьэA              Φ$B ьэA          ♥    ЊэA ♀юA lэA ╝ьA      Φ$
@    <юA              8$B ╪ьA                ╟$B ШюA          ☻    ыюA ┤юA ╝ьA      ╟$B ☺
             @    ♦яA          ♥    PяA           ☺   ╝ÈA `ÈA ╝яA ¶яA        ♀%B
  @    ╙ÈA ,%B ☻                @    ¦ÈA                -%B ♦яA              ,%B ¦ÈA Д%B
   ♥    ÏÈA шюA `яA                 X%B 0яA             ☺    ╙юA ╘ÈA       ╝яA ¶яA               ☻
```

POS malware: mutex



```
004046D9 loc_4046D9:                                    ; CODE XREF: _main+47↑j
004046D9                 push    3E8h                   ; dwMilliseconds
004046DE                 call    ds:Sleep
004046E4                 push    offset Name            ; "uniqyeidclaxemain"
004046E9                 push    0                      ; bInitialOwner
004046EB                 push    0                      ; lpMutexAttributes
004046ED                 call    ds:CreateMutexA
004046F3                 mov     esi, ds:GetLastError
004046F9                 call    esi ; GetLastError
004046FB                 cmp     eax, 0B7h
00404700                 jnz     short loc_40471D
00404702                 push    30h                    ; uType
00404704                 push    offset aAlert          ; "Alert"
00404709                 push    offset aAlreadyRunning ; "Already running!"
0040470E                 push    0                      ; hWnd
00404710                 call    ds:MessageBoxA
00404716                 push    0                      ; int
00404718                 call    _exit
```



eclessiastes Posted 03 August 2015 - 07:49 AM

Forum Newbie

Members

55 posts

Reputation: 7

Gender: Male

Location: Las Vegas, NV

Interests: Coding

Coding: C++, PHP

Hello

I have an application with a mutex that prevent it from being opened more than once.

[-] C Source

```
HANDLE h = CreateMutex(NULL, FALSE, "uniqyeidclaxemain");
    if (GetLastError() == ERROR_ALREADY_EXISTS)
    {
        MessageBox(NULL, "An instance is already running.", "Already running",
        return 0;
    }
```

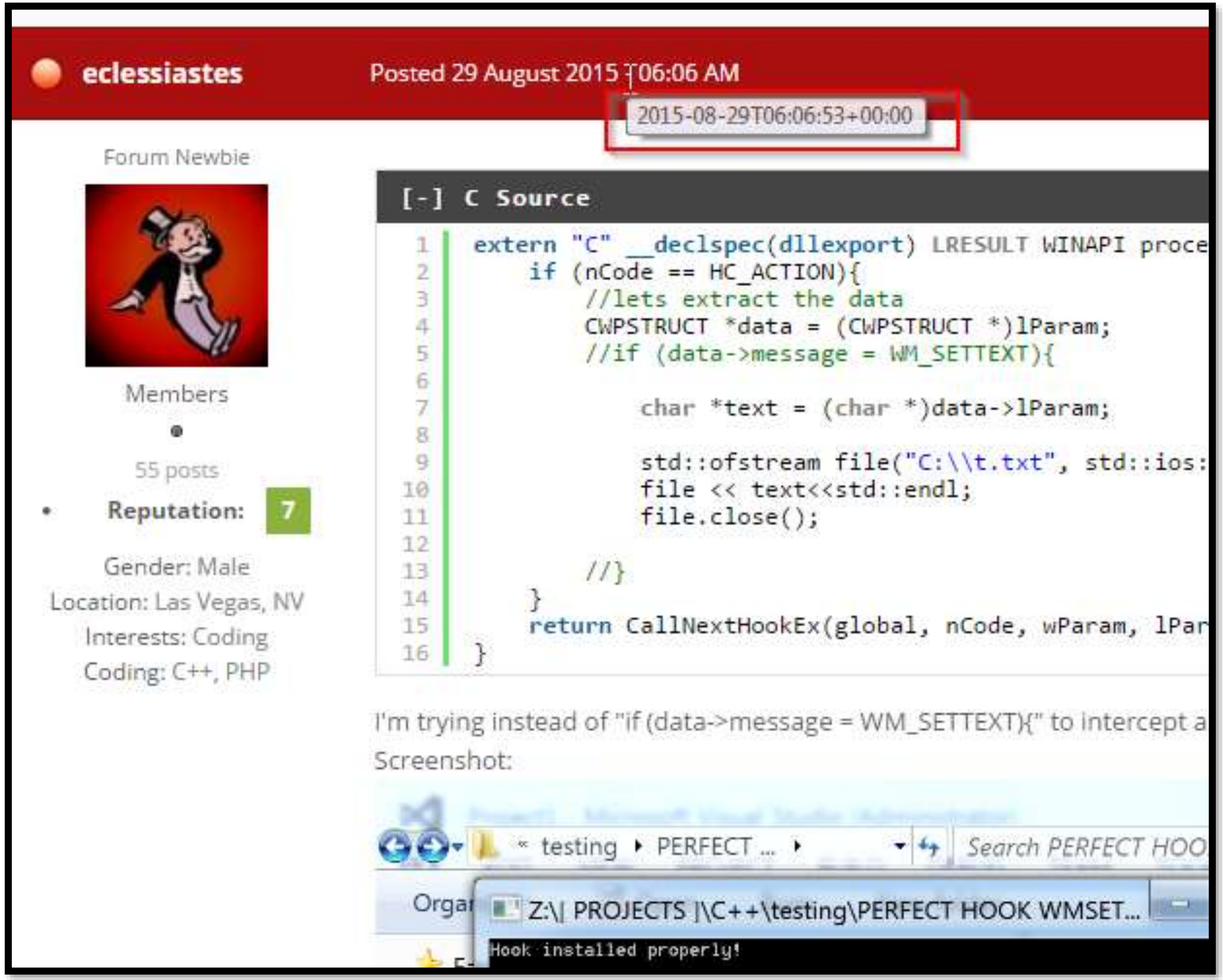
If i try to open it again, an error appears that app is already running.

I'm looking for a way to CreateProcess multiple instances of this kind of programs. Is there any twea process names, classes or even hooking the NTQuery but still the mutex is there.

Any help regarding this would be greatly appreciated!

Thank you

POS malware: the time zone



eclessiastes Posted 29 August 2015 - 06:06 AM

2015-08-29T06:06:53+00:00

Forum Newbie

Members

55 posts

- Reputation: 7

Gender: Male
Location: Las Vegas, NV
Interests: Coding
Coding: C++, PHP

[-] C Source

```
extern "C" __declspec(dllexport) LRESULT WINAPI proce
    if (nCode == HC_ACTION){
        //lets extract the data
        CWPSTRUCT *data = (CWPSTRUCT *)lParam;
        //if (data->message = WM_SETTEXT){

            char *text = (char *)data->lParam;

            std::ofstream file("C:\\t.txt", std::ios:
            file << text<<std::endl;
            file.close();

        //}
    }
    return CallNextHookEx(global, nCode, wParam, lPar
}
```

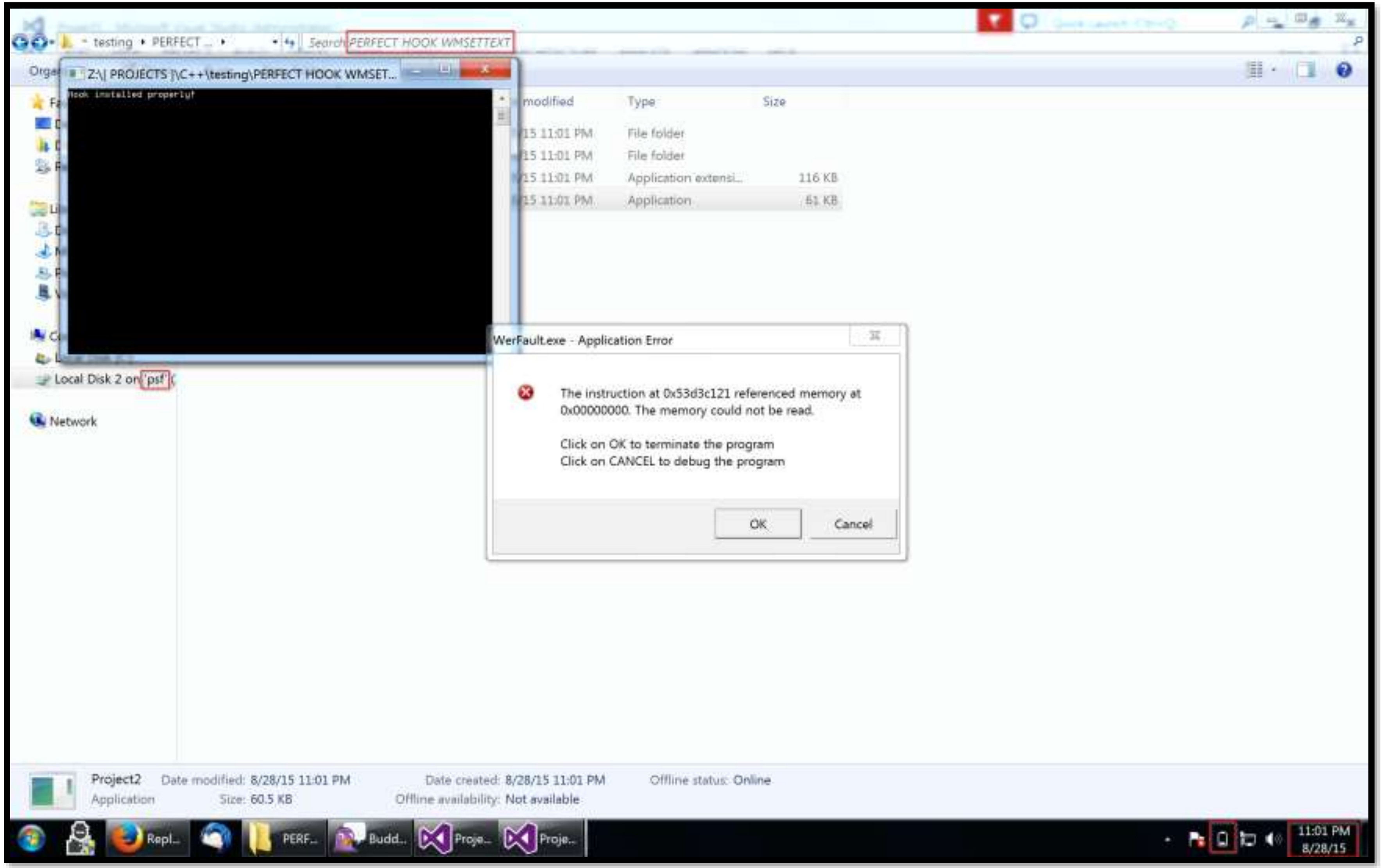
I'm trying instead of "if (data->message = WM_SETTEXT){" to intercept a

Screenshot:

Z:\[PROJECTS]\C++\testing\PERFECT HOOK WMSET...

```
Hook installed properly!
```

POS malware: the screenshot



testing ▸ PERFECT ... ▸
Search PERFECT HOOK WMSETTEXT
Z:\| PROJECTS |\C++\testing\PERFECT HOOK WMSET...

```
Hook installed properly!
```

15 11:01 PM File folder
15 11:01 PM File folder
15 11:01 PM Application extensi... 116 KB
15 11:01 PM Application 61 KB

Local Disk 2 on 'psf'
Network

WerFault.exe - Application Error

The instruction at 0x53d3c121 referenced memory at 0x00000000. The memory could not be read.

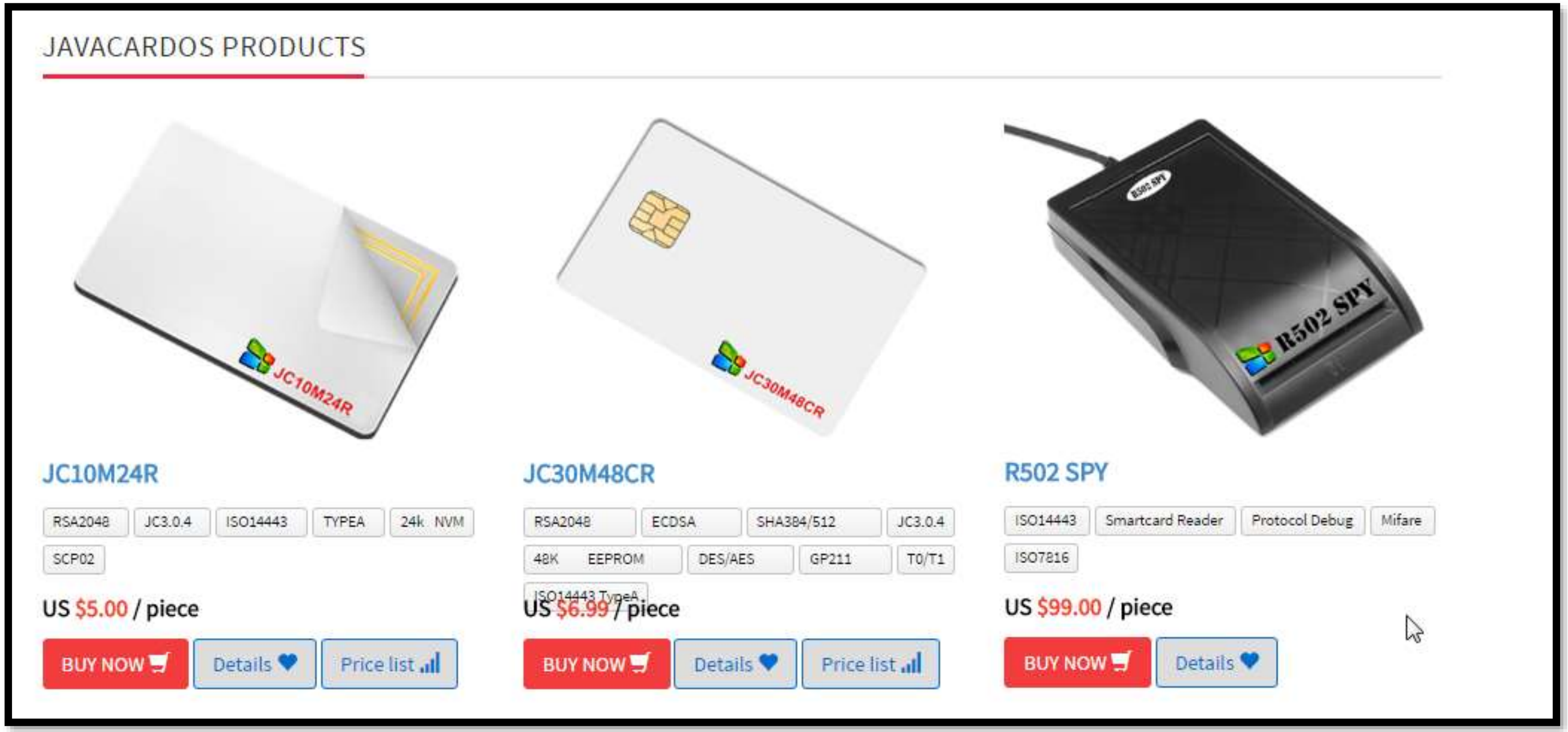
Click on OK to terminate the program
Click on CANCEL to debug the program

Project2 Date modified: 8/28/15 11:01 PM Date created: 8/28/15 11:01 PM Offline status: Online
Application Size: 60.5 KB Offline availability: Not available

POS malware: the screenshot “data”

- 2560x1600
- Laptop
- PSF (Parallels)
- “Perfect Hook” project
- Time Zone: GMT-7

POS malware: Javacardos forum



JAVACARDOS PRODUCTS

JC10M24R

RSA2048 | JC3.0.4 | ISO14443 | TYPEA | 24k NVM | SCP02

US $5.00 / piece

JC30M48CR

RSA2048 | ECDSA | SHA384/512 | JC3.0.4 | 48K EEPROM | DES/AES | GP211 | T0/T1 | ISO14443 TypeA

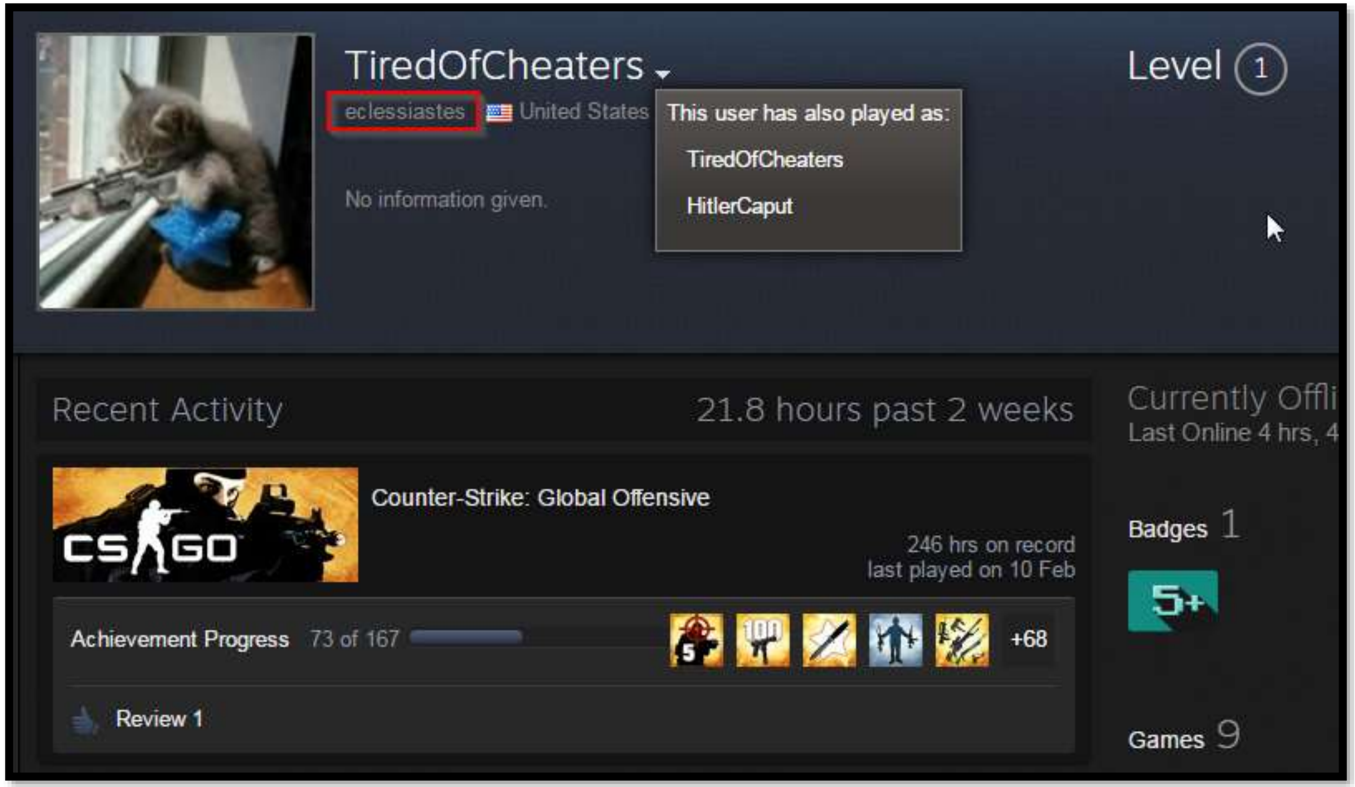
US $6.99 / piece

R502 SPY

ISO14443 | Smartcard Reader | Protocol Debug | Mifare | ISO7816

US $99.00 / piece

POS malware: Steam profile



TiredOfCheaters

eclessiastes United States

No information given.

This user has also played as:

TiredOfCheaters

HitlerCaput

Level 1

Recent Activity 21.8 hours past 2 weeks

Counter-Strike: Global Offensive

246 hrs on record
last played on 10 Feb

Achievement Progress 73 of 167 +68

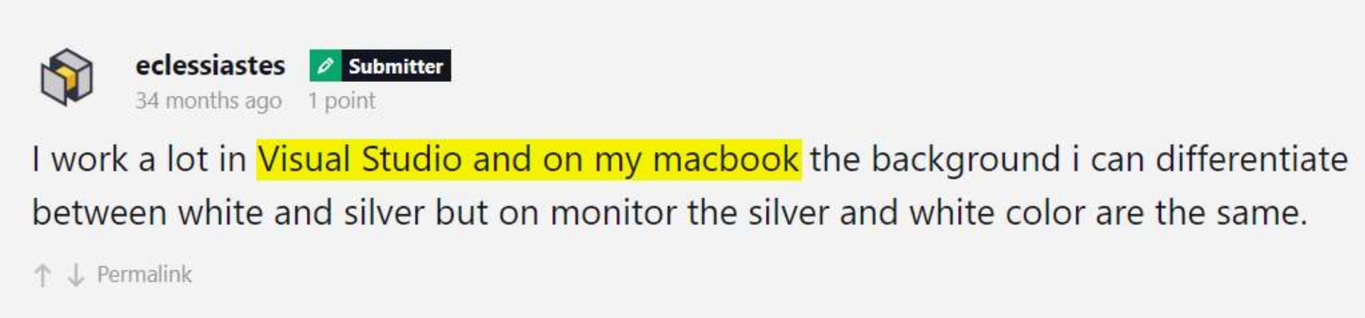
Review 1

Currently Offli
Last Online 4 hrs, 4

Badges 1

Games 9

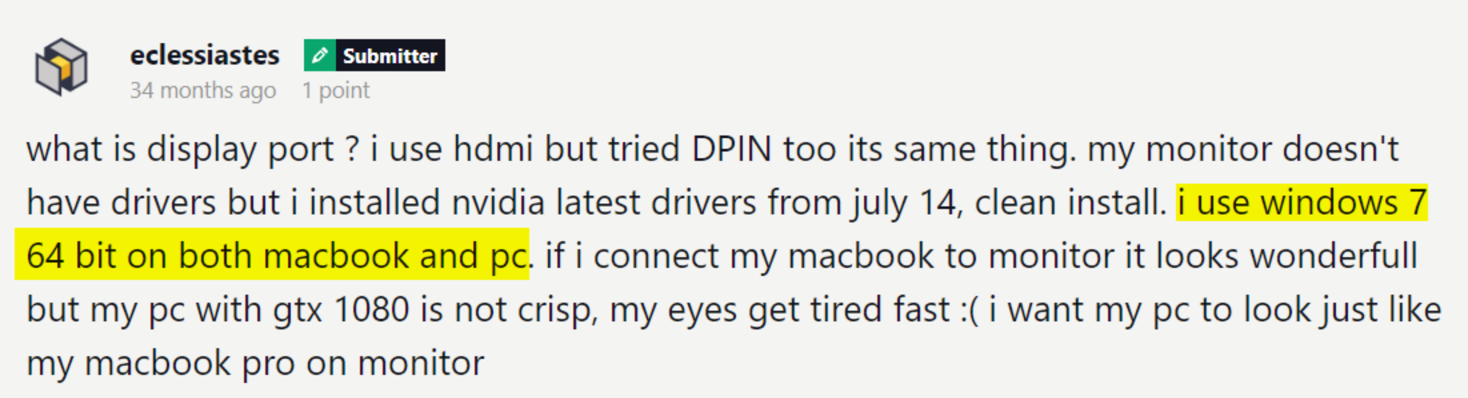
POS malware: pcpartpicker



eclessiastes Submitter
34 months ago 1 point

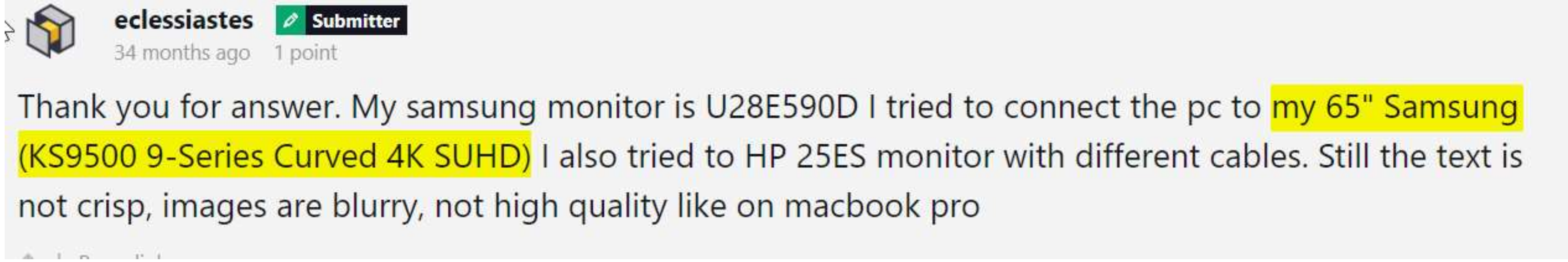
I work a lot in Visual Studio and on my macbook the background i can differentiate between white and silver but on monitor the silver and white color are the same.

↑ ↓ Permalink



eclessiastes Submitter
34 months ago 1 point

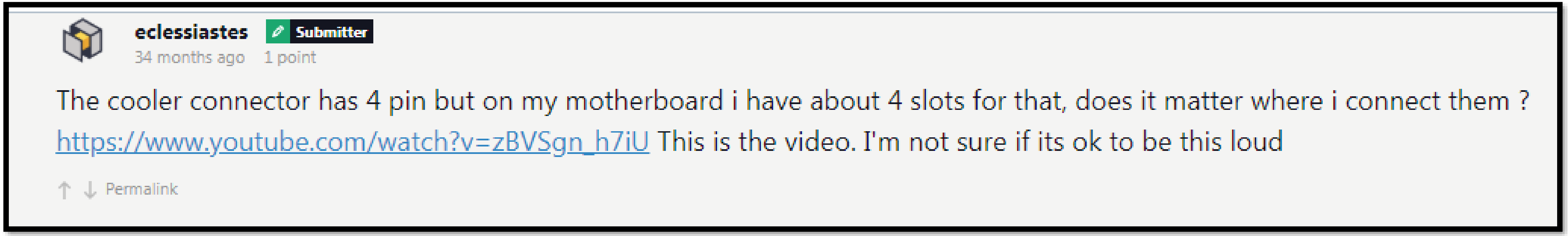
what is display port ? i use hdmi but tried DPIN too its same thing. my monitor doesn't have drivers but i installed nvidia latest drivers from july 14, clean install. i use windows 7 64 bit on both macbook and pc. if i connect my macbook to monitor it looks wonderfull but my pc with gtx 1080 is not crisp, my eyes get tired fast :(i want my pc to look just like my macbook pro on monitor



eclessiastes Submitter
34 months ago 1 point

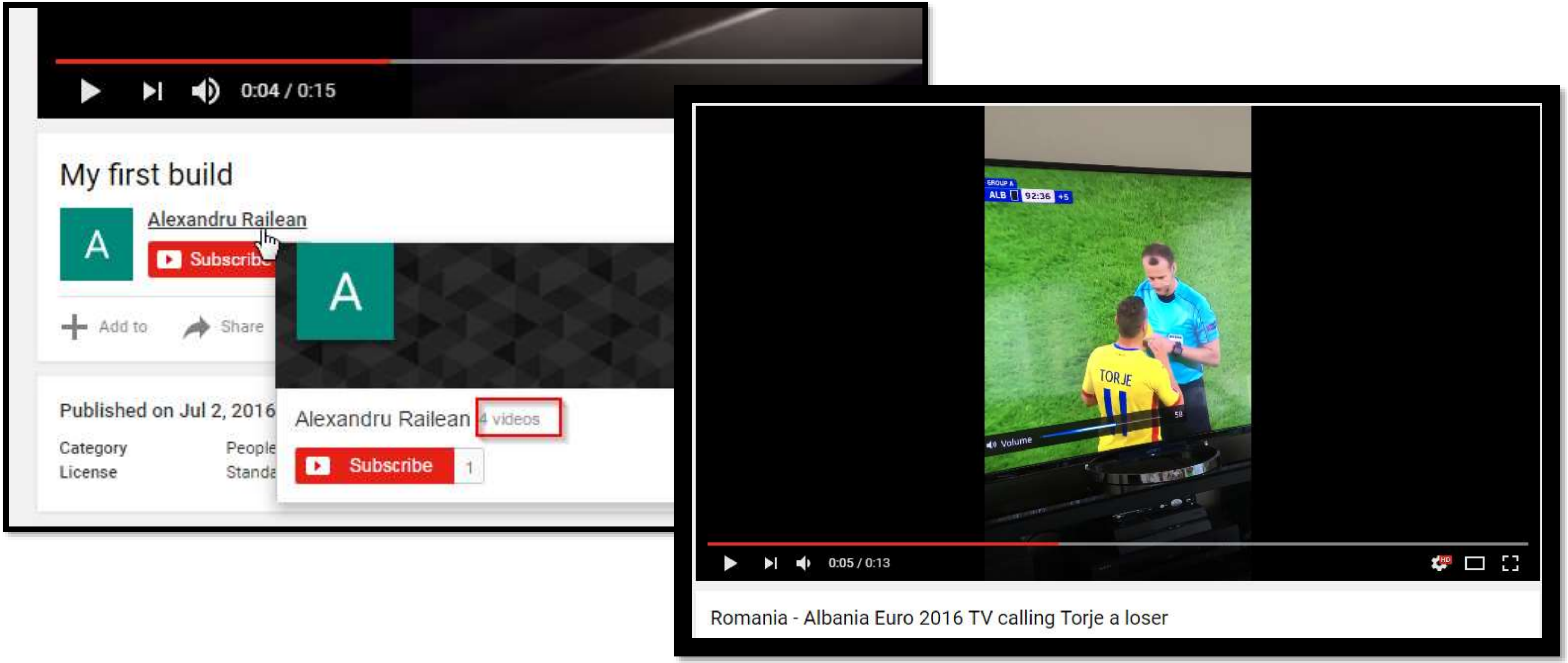
Thank you for answer. My samsung monitor is U28E590D I tried to connect the pc to my 65" Samsung (KS9500 9-Series Curved 4K SUHD) I also tried to HP 25ES monitor with different cables. Still the text is not crisp, images are blurry, not high quality like on macbook pro

POS malware: pcpartpicker



The cooler connector has 4 pin but on my motherboard i have about 4 slots for that, does it matter where i connect them ? https://www.youtube.com/watch?v=zBVSgn_h7iU This is the video. I'm not sure if its ok to be this loud

POS malware: YouTube profile



My first build

Alexandru Railean

Published on Jul 2, 2016

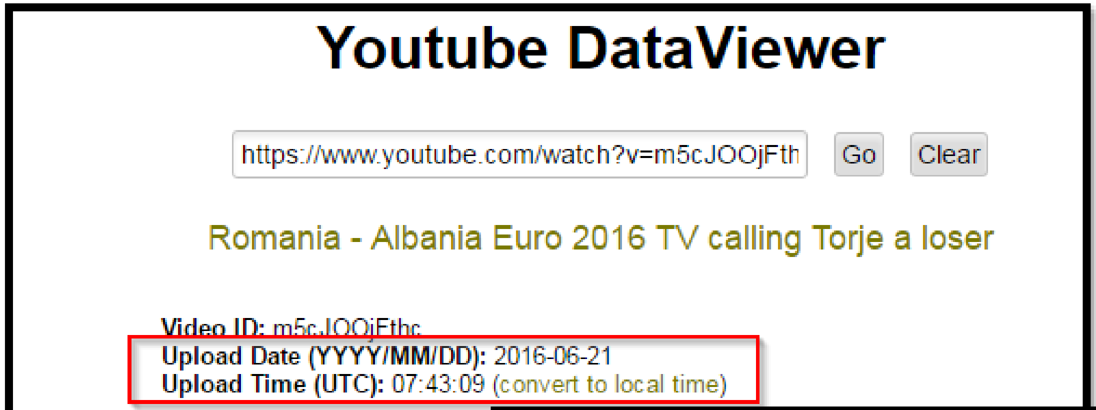
Category People

License Standa

Alexandru Railean 4 videos

Romania - Albania Euro 2016 TV calling Torje a loser

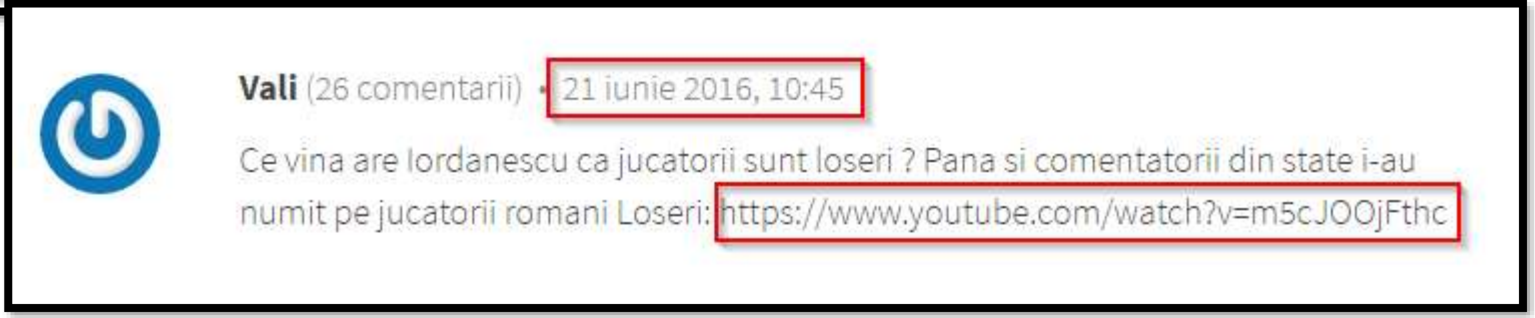
POS malware: YouTube Videos time and links



Youtube DataViewer

Romania - Albania Euro 2016 TV calling Torje a loser

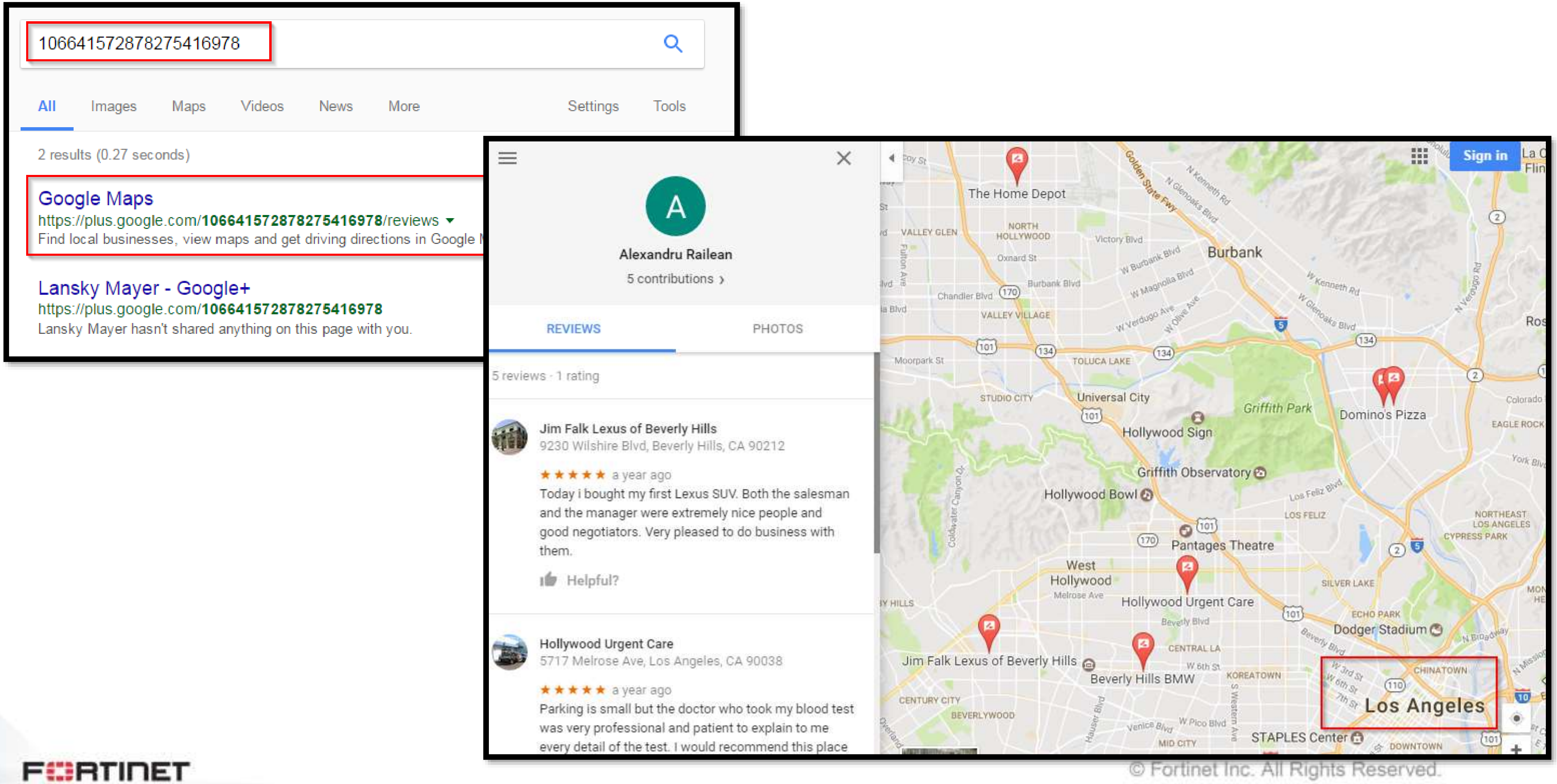
Video ID: m5cJOOjFthc
Upload Date (YYYY/MM/DD): 2016-06-21
Upload Time (UTC): 07:43:09 (convert to local time)



Vali (26 comentarii) • 21 iunie 2016, 10:45

Ce vina are Iordanescu ca jucatorii sunt loseri ? Pana si comentatorii din state i-au numit pe jucatorii romani Loseri: https://www.youtube.com/watch?v=m5cJOOjFthc

POS malware: Google ID



106641572878275416978

All Images Maps Videos News More Settings Tools

2 results (0.27 seconds)

Google Maps
https://plus.google.com/106641572878275416978/reviews
Find local businesses, view maps and get driving directions in Google M

Lansky Mayer - Google+
https://plus.google.com/106641572878275416978
Lansky Mayer hasn't shared anything on this page with you.

A
Alexandru Railean
5 contributions ›

REVIEWS PHOTOS

5 reviews · 1 rating

Jim Falk Lexus of Beverly Hills
9230 Wilshire Blvd, Beverly Hills, CA 90212
★★★★★ a year ago
Today i bought my first Lexus SUV. Both the salesman and the manager were extremely nice people and good negotiators. Very pleased to do business with them.
Helpful?

Hollywood Urgent Care
5717 Melrose Ave, Los Angeles, CA 90038
★★★★★ a year ago
Parking is small but the doctor who took my blood test was very professional and patient to explain to me every detail of the test. I would recommend this place

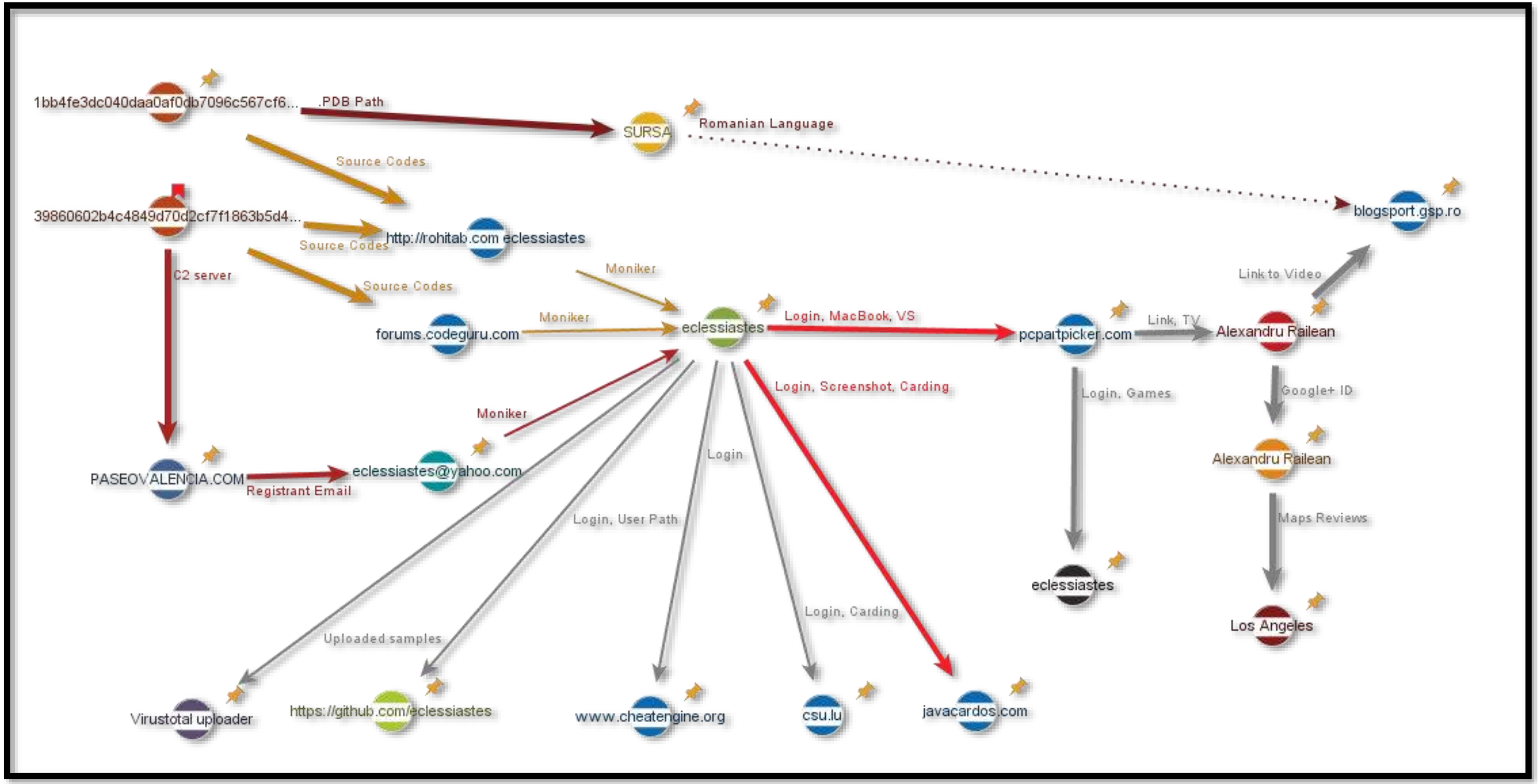
Interaction with Interpol: a researcher perspective

Interaction with Interpol: preparation

Backup all the clues

Write a comprehensive report

POS malware: investigation overview



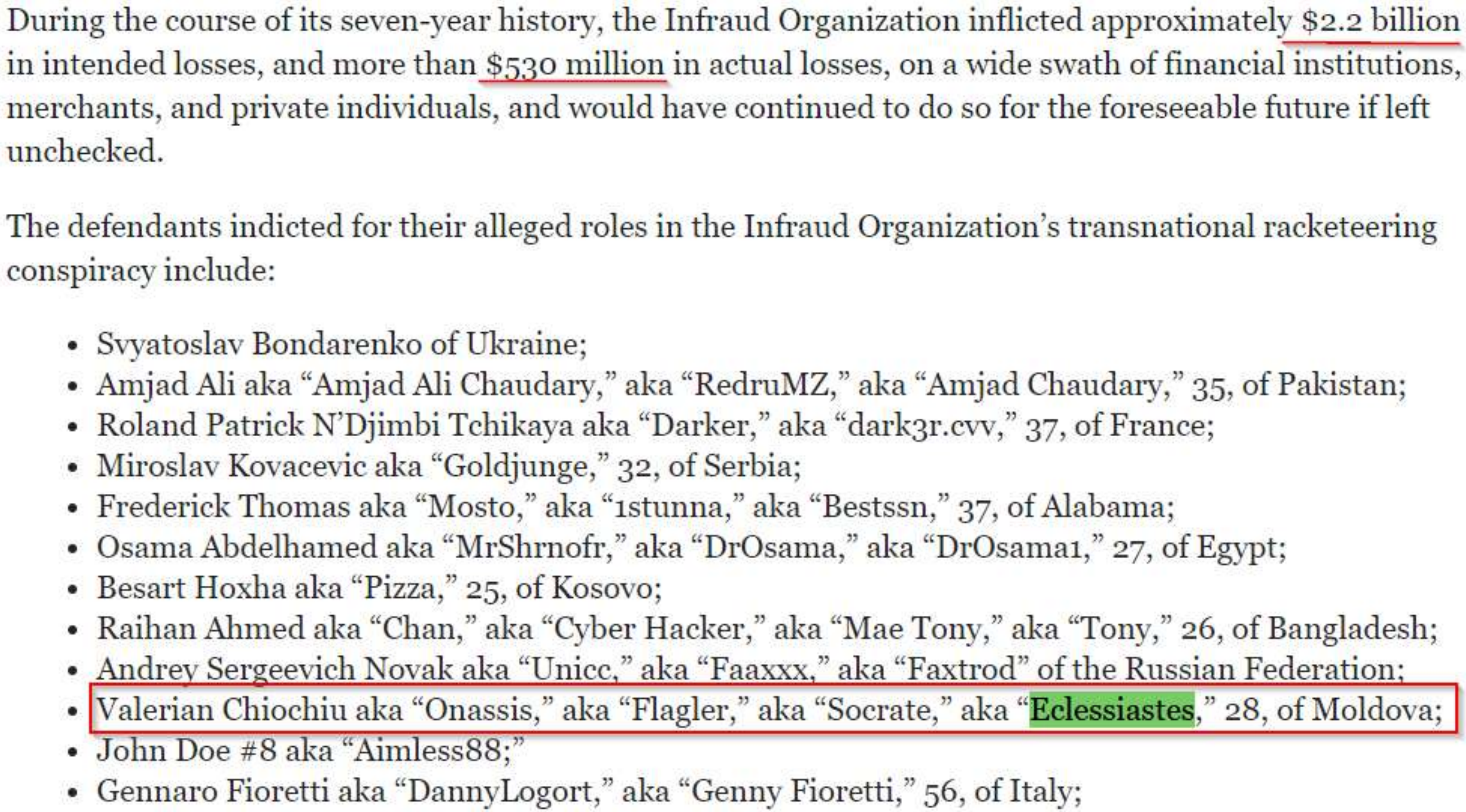
Interview with CFC officers

CFC Interpol building in SG

Waiting…

…and more waiting…

Bingo!



During the course of its seven-year history, the Infraud Organization inflicted approximately $2.2 billion in intended losses, and more than $530 million in actual losses, on a wide swath of financial institutions, merchants, and private individuals, and would have continued to do so for the foreseeable future if left unchecked.

The defendants indicted for their alleged roles in the Infraud Organization's transnational racketeering conspiracy include:

- Svyatoslav Bondarenko of Ukraine;
- Amjad Ali aka "Amjad Ali Chaudary," aka "RedruMZ," aka "Amjad Chaudary," 35, of Pakistan;
- Roland Patrick N'Djimbi Tchikaya aka "Darker," aka "dark3r.cvv," 37, of France;
- Miroslav Kovacevic aka "Goldjunge," 32, of Serbia;
- Frederick Thomas aka "Mosto," aka "1stunna," aka "Bestssn," 37, of Alabama;
- Osama Abdelhamed aka "MrShrnofr," aka "DrOsama," aka "DrOsama1," 27, of Egypt;
- Besart Hoxha aka "Pizza," 25, of Kosovo;
- Raihan Ahmed aka "Chan," aka "Cyber Hacker," aka "Mae Tony," aka "Tony," 26, of Bangladesh;
- Andrey Sergeevich Novak aka "Unicc," aka "Faaxxx," aka "Faxtrod" of the Russian Federation;
- Valerian Chiochiu aka "Onassis," aka "Flagler," aka "Socrate," aka "Eclessiastes," 28, of Moldova;
- John Doe #8 aka "Aimless88;"
- Gennaro Fioretti aka "DannyLogort," aka "Genny Fioretti," 56, of Italy;

Summary:

How to start your investigation
Following the footprints
False Flags
Interaction with Interpol
Investigation example

Let’s Talk?

FORTINET®