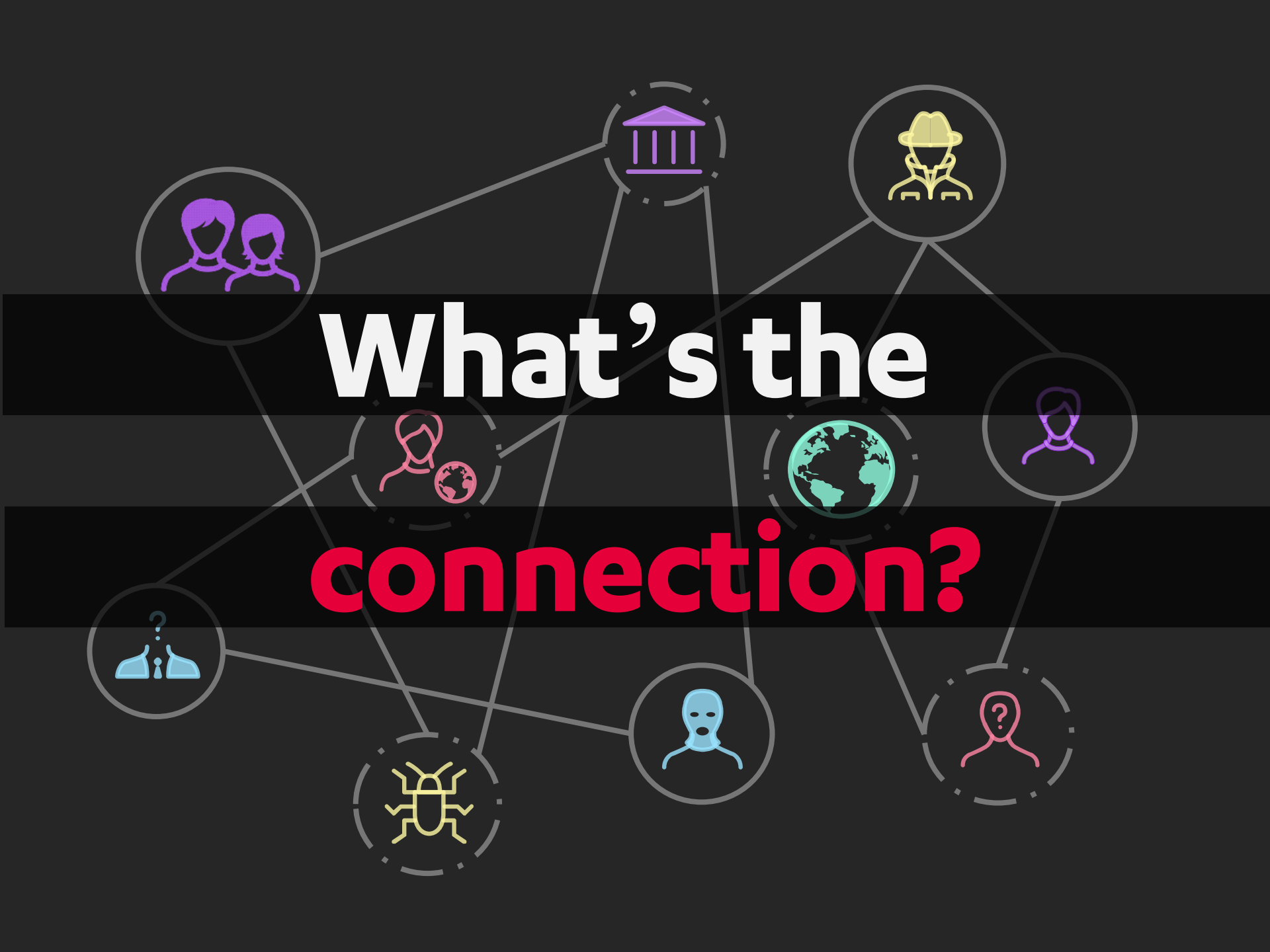

What's the
connection?

#totalhash

MALTEGO

CryptoLocker

Your personal files are encrypted!

Private key will be destroyed on
1/12/2014
4:59 PM

Time left
71 : 49 : 16

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

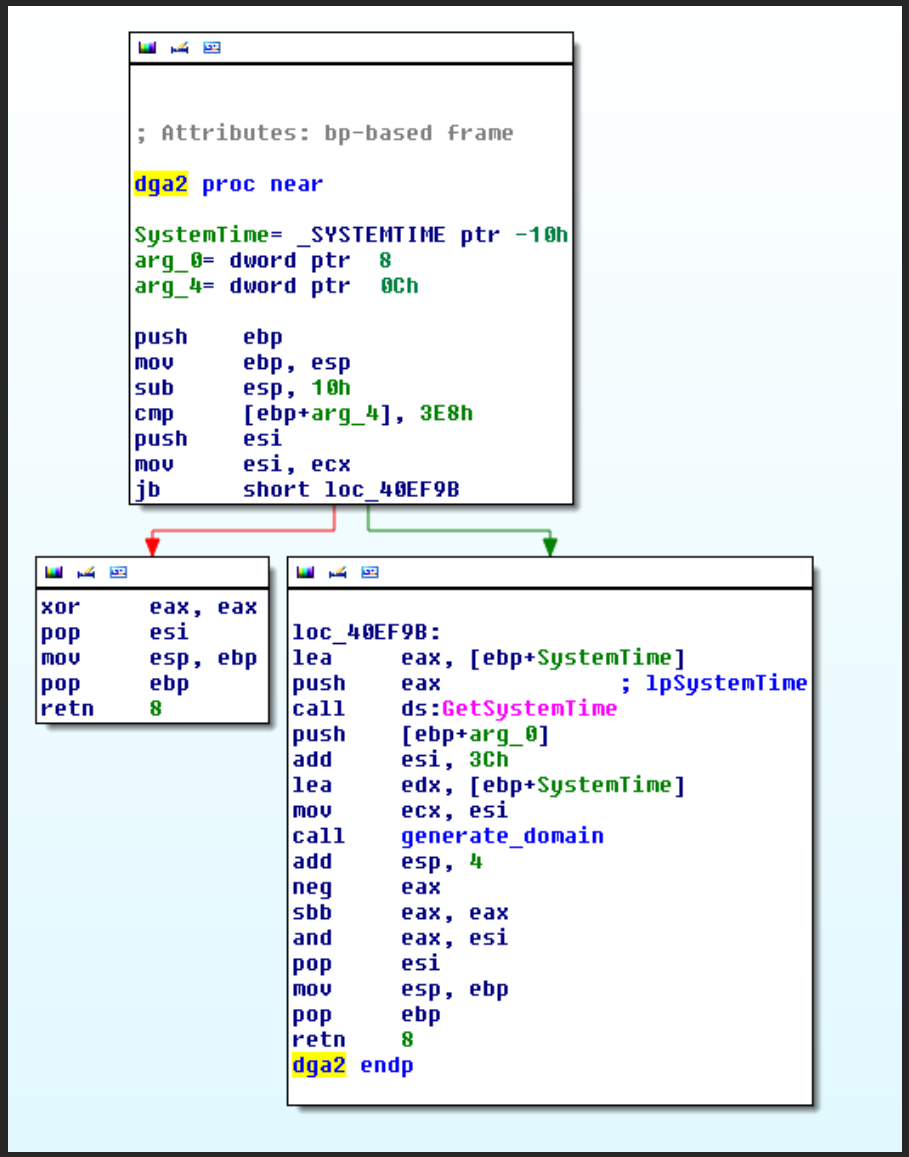
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>

nqhnqhprthtccs.com
kmhihraypajohj.net
xoggeanmiyebpn.biz
lqjbabroghmbja.ru
ysiywjfcyghnin.org
mummfmqkrdgmhx.co.uk
awlkcuexkcbypu.info
nyofxviaikjyqn.com
bbnduevnbjelpt.net
ofpyygqpuscisk.biz
psoleogunlkqsb.ru
pjrrrpiflafuum.org
qwqewxxkesndlp.co.uk
qnudwbhbwvyghs.info
rbtpcjwgpohohc.com
rrwvpkyqndcsqt.net
sfviusovgvkbhp.biz
ymofbgcueknust.ru
mondxlgctpedrn.org
bnqjdptwsjitll.co.uk
opphauxeioycts.info
butjybsggnkssl.com
owshvgwnvsbbrx.net
dvvnbkkiumfrsv.biz
qxulxpopkrvabv.ru
dfwvsuswjdckbi.org
esvixayyycowro.co.uk
fgyauekyxcwjtl.info
gtxmajqbnbjvti.com



URL	Detection	SHA-1	Referer	Last seen
http://www.youtube.com /setup.exe	Trojan.Agent.BHYK	87081f14985a765ba9f1310a534b328744919234	http://www.youtube.com//	2015-02-25 06:43:25.910000
http://www.facebook.com /setup.exe	Trojan-psw:W32/Fariet.0076bc9a22!Online	0076bc9a220dc47e5edf248ff6316eb605c826f0	http://www.facebook.com/	2015-02-24 01:02:39.857000
http://earth.google.com /setup.exe	Trojan.Agent.BHYK	87081f14985a765ba9f1310a534b328744919234	http://earth.google.com/	2015-02-24 16:34:02.813000
http://allegro.pl/setup.exe	Trojan.GenericKD.2069696	b3de3e293710f530fbf74522e507d500c6697708	http://allegro.pl/	2015-01-11 08:52:10.764000
http://it.it.facebook.com /setup.exe	Trojan.GenericKD.2186102	2e0841e058135438		
http://www.o2.pl/setup.exe	Suspicious:W32/Malware.b3de3e2937!Online	b3de3e293710f530		
	BHYK	87081f14985a765ba		

IP Information for 188.138.41.85

Quick Stats

IP Location	Germany Hurth Plusserver Ag
ASN	AS8972 PLUSSERVER-AS PlusServer AG (registered Oct 12, 2001)
Resolve Host	loft9237.serverprofi24.com

IP Information for 85.25.213.208

Quick Stats

IP Location	Germany Hurth Plusserver Ag
ASN	AS8972 PLUSSERVER-AS PlusServer AG (registered Oct 12, 2001)
Resolve Host	malta1360.startdedicated.com

IP Information for 31.192.211.50

Quick Stats

IP Location	Turkey Denizli Netinternet Bilgisayar Ve Telekomunikasyon San. Ve Tic. Ltd. Sti.
ASN	AS51559 NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San. ve Tic. Ltd. Sti. (registered Sep 28, 2010)
Resolve Host	server50.net211.intbildns.org

SECURITY

DNS hijacking vulnerability affects D-Link DSL router, possibly other devices

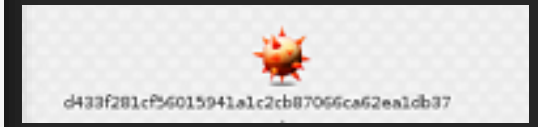
Lucian Constantin
IDG News Service
Jan 27, 2015 10:35 AM

NETWORKING security, routers, wifi, security

Attack campaign compromises 300,000 home routers, alters DNS settings

Lucian Constantin
IDG News Service
Mar 4, 2014 9:50 AM


```
Registration Service Provided By: Rustelekom Limited
Contact: info@rustelekom.biz

Domain name: overpict.com

Registrant Contact:

   John Kasai ()

   Fax:
   Gabelsberger Strasse, 20
   Klagenfurt,  9021
   AT

Administrative Contact:

   John Kasai (postmaster@grouptumbler.com)
   +43.463224501
   Fax: +.
   Gabelsberger Strasse, 20
   Klagenfurt,  9021
   AT

Technical Contact:

   John Kasai (postmaster@grouptumbler.com)
   +43.463224501
   Fax: +.
   Gabelsberger Strasse, 20
   Klagenfurt,  9021
   AT

Status: Locked

Name Servers:
   dns01.gpn.register.com
   dns02.gpn.register.com
   dns03.gpn.register.com
   dns04.gpn.register.com
   dns05.gpn.register.com

Creation date: 29 Jan 2011 13:32:55
Expiration date: 29 Jan 2012 13:32:00
```



DOMAINTOOLS

Whois Lookup

Products Solutions Pricing Support About Account

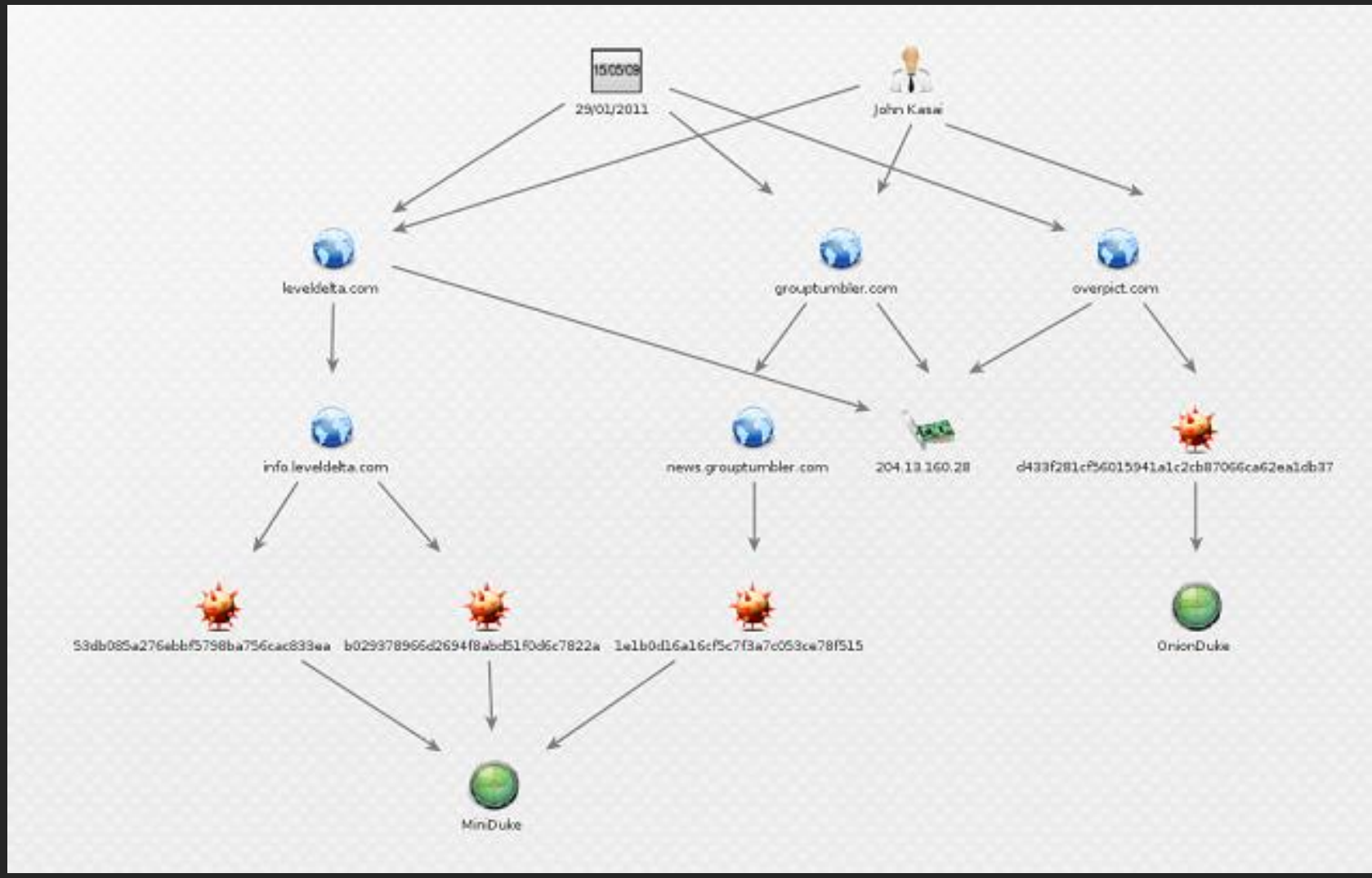
Return to My Reverse Whois Reports

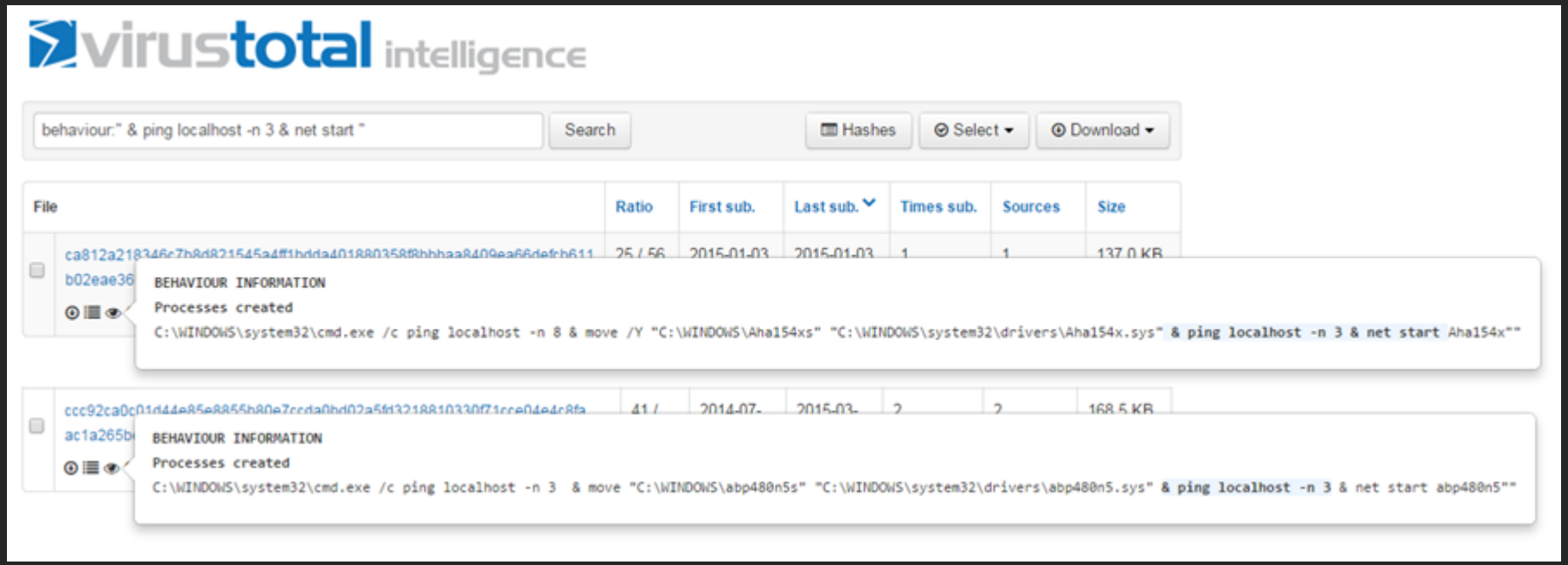
Save as .CSV

Email Address *Exactly Matching* "POSTMASTER@GROUPTUMBLER.COM"

Reverse Whois Report Preview — **Report Compiled: 11/13/2014**

#	Domain	Whois Record
1	AIRTRAVELABROAD.COM	2/14/2011
2	BEIJINGNEWSBLOG.NET	2/14/2011 10/19/2011 12/27/2011 3/11/2012 8/8/2012 2/19/2013 3/25/2013 6/7/2013 11/3/2013 1/10/2014 2/11/2014 4/5/2014 5/29/2014 9/20/2014 9/27/2014 9/29/2014 11/3/2014 11/7/2014
3	GROUPTUMBLER.COM	1/30/2011 3/22/2011 10/7/2011 1/31/2012
4	LEVELDELTA.COM	1/30/2011
5	NASDAQBLOG.NET	2/14/2011 10/19/2011 12/28/2011 3/12/2012 8/8/2012 1/4/2013 3/4/2013 6/5/2013 10/11/2013 12/22/2013 2/11/2014 4/5/2014 7/3/2014 9/25/2014 10/3/2014 11/3/2014 11/5/2014 11/7/2014
6	NATUREINHOME.COM	2/14/2011
7	NESTEDMAIL.COM	2/14/2011
8	NOSTRESSJOB.COM	1/30/2011 3/22/2011 10/4/2011 3/14/2012 5/27/2012 1/27/2013 3/4/2013 6/7/2013 11/4/2013 1/10/2014 1/27/2014 4/2/2014 6/14/2014 9/1/2014 9/26/2014 9/29/2014 10/19/2014 11/3/2014
9	NYTUNION.COM	1/30/2011 10/20/2011 12/29/2011 1/31/2012
10	OILNEWSBLOG.COM	2/14/2011 10/8/2011 2/26/2012 7/25/2012 1/22/2013 3/4/2013 6/4/2013 11/18/2013 1/24/2014 2/10/2014 2/26/2014 7/15/2014 9/27/2014 9/29/2014 10/19/2014 10/21/2014 11/3/2014 11/5/2014
11	OVERPICT.COM	1/30/2011 3/25/2011 10/18/2011 12/26/2011 1/31/2012
12	SIXSQUARE.NET	2/14/2011
13	USTRADECOMP.COM	1/30/2011 3/26/2011 10/19/2011 12/28/2011 4/18/2012 6/29/2012 1/27/2013 3/14/2013 6/5/2013 11/3/2013 1/9/2014 1/27/2014 4/1/2014 6/15/2014 9/4/2014 9/27/2014 9/29/2014 10/19/2014 11/3/2014


15/05/08
29/01/2011
John Kasai
leveldelta.com
groupumbler.com
overpict.com
info.leveldelta.com
news.groupumbler.com
204.13.160.28
d433f281cf56015941a1c2cb87066ca62ea1db37
53db085a276ebbf5798ba756cac833ea
b029378966d2694f8abd51f0d6c7822a
1e1b0d16a16cf5c7f3a7c053ca78f515
OnionDuke
MiniDuke



Written files

C:\WINDOWS\Aha154xs (successful)

Moved files

SRC: C:\WINDOWS\Aha154xs
DST: C:\WINDOWS\system32\drivers\Aha154x.sys (successful)

Created processes

C:\WINDOWS\system32\cmd.exe /c ping localhost -n 8 & move /Y "C:\WINDOWS\Aha154xs" "C:\WINDOWS\system32\drivers\Aha154x.sys" & ping localhost -n 3 & net start Aha154x"" (successful)

C:\WINDOWS\system32\cmd.exe /s /c for /L %i in (1 (successful)

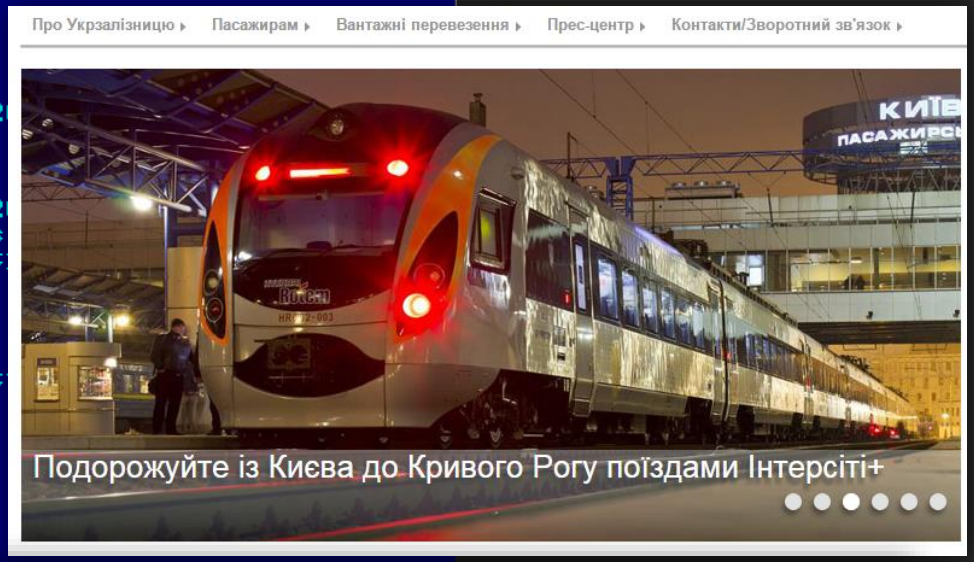
C:\WINDOWS\system32\ping.exe ping localhost -n 3 (successful)

C:\WINDOWS\system32\net.exe net start Aha154x (successful)

BlackEnergy2 version 7.0.9

Posted 1 month ago by [redacted] Useful (0) Not useful (0) Abuse (0)

```
<?xml version="1.0" encoding="UTF-8"?>
<bkernel>
<servers>
<server>
<type>https</type>
<addr>https://95.143.193.182/RnJhbmNlYXZpYXRlbGVjb2
</server>
<server>
<type>https</type>
<addr>https://95.143.193.182/RnJhbmNlYXZpYXRlbGVjb2
https=10.10.255.55:3128,https=10.5.10.11:3128,https
ps=proxy.uz.gov.ua:3128,https=10.5.104.225:9080,htt
.168.1.22:3128</addr>
</server>
<server>
<type>https</type>
<addr>https://5.61.38.31/ZXBzaWxvbmVyaWRhbmkw/setat
</server>
</servers>
<cmds>
</cmds>
<sleepfreq>600</sleepfreq>
<build_id>0D0B15aaa</build_id>
</bkernel>
```


```
<?xml version="1.0" encoding="UTF-8"?>
<bkernel>
<servers>
<server>
<type>https</type>
<addr>https://5.79.80.166/templates/bf0dac805798cc1f633f19ce8ed6382f/getcfg.php
;proxy=https=172.20.124.10:8080,https=aproxy giknpc.intranet:8080,https=proxy.g
iknpc.intranet:8080,https=sproxy.giknpc.intranet:8080,https=nproxy.giknpc.intra
net:8080,https=172.20.124.252:8080</addr>
</server>
</servers>
<cmds>
</cmds>
<sleepfreq>600</sleepfreq>
<build_id>0E0219rku</build_id>
</bkernel>
```

```
https://144.76.119.48/YXJyYWtpczAy/loadvers/paramctrl.php;proxy=https=10.10.255
.55:3128,https=192.168.1.22:3128,https=10.3.10.10:8080,https=172.20.124.10:8080
,https=195.64.190.1:8080
```


Network information

IP address	195.64.190.1
Reverse DNS (PTR record)	relay.giknpc.com.ua
DNS server (NS record)	ns.giknpc.com.ua (195.64.190.1) ns2.giknpc.com.ua (195.24.137.86)

IP Information for 195.64.190.1

– Quick Stats

IP Location	Ukraine Dnipropetrovsk Chief Information-commercial And Scientific-production Regional Centre
ASN	AS41150 GIKNPC-AS GIKNPC AS number (registered Jun 21, 2006)

File pos	Mem pos	ID	Text
A 000000012804	000000412804	0	China in economic crisis 2012.doc
U 0000000122DE	000000436DE	0	VS_VERSION_INFO
U 00000001233A	00000041373A	0	StringFileInfo
U 00000001235E	00000041375E	0	040904B0
U 000000012376	000000413776	0	CompanyName
U 000000012390	000000413790	0	Microsoft Corporation
U 0000000123C2	0000004137C2	0	
U 0000000123E4	0000004137E4	0	
U 00000001241A	00000041381A	0	
U 000000012434	000000413834	0	
U 000000012486	000000413886	0	
U 0000000124A0	0000004138A0	0	
U 0000000124C2	0000004138C2	0	
U 0000000124E2	0000004138E2	0	
U 000000012542	000000413942	0	
U 000000012564	000000413964	0	
U 000000012586	000000413986	0	
U 0000000125C6	0000004139C6	0	
U 0000000125F2	0000004139F2	0	
U 000000012610	000000413A10	0	
U 000000012636	000000413A36	0	VarFileInfo
U 000000012656	000000413A5E		

itw:"china in economic crisis 2012.doc" Search Hashes Select Download

1 files found

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
b1ca89de93a1d9bf17cdbf8a3c61e7f52f275a3bcbbd285d35d6a40c45dde9bd7edc54253563975dd49692bee3bb390a cve-2012-0158 cve-2010-3333 exploit rtf	41 / 55	2012-01-18 06:55:07	2014-10-06 06:54:15	12	10	278.1 KB

China in economic crisis 2012.doc - Microsoft Word

China's collapse 'will bring economic crisis to climax in 2012'

Leading City of London analyst says next 12 months will be one of 'pain and disappointment' if Chinese economy crashes

"China in economic crisis 2012.doc": 4,308 characters (an approximate value).

Prevalence metrics

First seen ITW	2014-08-13T06:08:54.000Z
First submission	2014-08-13 06:14:34
Last submission	2015-03-03 14:24:02
Number of submissions	98
Distinct source submissions	66

Propagation, dissemination and distribution strategies

This file has been spotted in-the-wild travelling as email attachments, some of these emails are later on detailed.

Attached in emails

[+] =?windows-1251?B?w+Xt7/Du6vPw4PLz8OAg4vHy4O3u4ujr4CDn?= =?windows-1251?B?4if... (=?windows-1251?B?

Генпрокуратур
депутатів

Головним слідчим управлінням МВС України внесено відомості до Єдиного реєстру досудо розслідувань про розкрадання посадовими особа України за попередньою змовою грошових ко призначених для АТО.

СБУ України веде перевірку народних депута які підтримують терористів.

1 of 4

Spiski deputatov done

Andrey Krivshenko (1 SlideShare) , Головний редактор at Повінь - зміна системи

+ Follow

in 0 | f 0 | 7 | 8+ 0

Published on Aug 13, 2014

«Повінь – зміна системи» - інформаційно-аналітична студія http://povin.com.ua/

Published in: Mobile

Генпрокуратура встановила зв'язку народних депутатів України з ополченцями. - Cyrillic (Windows)

Message

Junk | Delete | Reply | Reply all | Forward | Instant message | Add to calendar | Move to | Copy to | Flag | Watch | Copy | Find text | Encoding | Previous | Next

Delete | Respond | Actions | Navigate

Генпрокуратура встановила зв'язку народних депутатів України з ополченцями.

Тягн... Add contact 8/13/2014 8:40 AM

To: [redacted]

spiski_deputatov_done.ppsx

Арсеній Яценюк доручив Генпрокурат=F3рі, СБУ, МВС та міністерству=юстиції перевірити всіх народних депутатів, партії =F2а громадські об'єднання на=Україні на причетність до підтримки ополченців півде=EDного сходу країни. Перші ре=E7ультати перевірки показали причетність деяки=F5 партій до підтримки терор=E8стів. Так само були виявлені випадки крадіжки г=F0ошей, призначених для АТО. <=R>У додатку перший список осіб, які підлягають=перевірці на допомогу терористам.

Andrey Sporaw (sporaw) wrote,
@ 2005-03-08 02:26:00

Скачал я фотографии своего ДТП с телефона (как оно произошло и его мат. оценку описывал здесь), теперь можно их посмотреть. Сам заценил их сейчас и думаю... Не много ли я этому деятелю на 9-ке на месте дал - $150? =)

(Машина, кстати, грязной стала за утреннюю поездку длительностью всего минут 10... Подтаяло)

(При нажатии на фотографии можно получить полноразмерный вариант)