



Backdoor.Proxybox

Russian Hackers, Proxy Resellers and Rootkits

Joseph Bingham

Malware Analyst

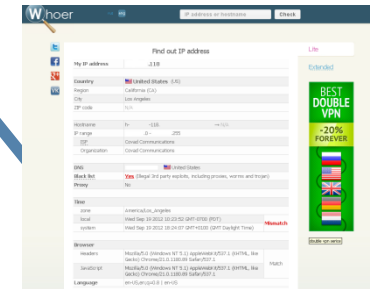
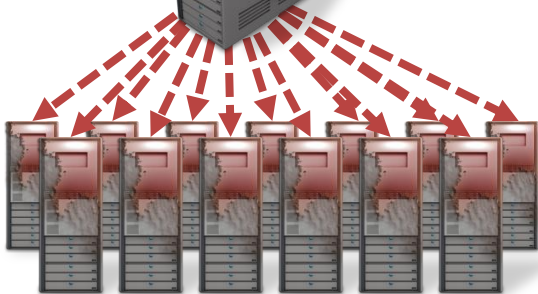
Overview



server IP	Count
95.111.162.3	733
95.111.162.1	734
97.220.96.9	736
95.159.102.21	733
95.149.226.14	694
97.220.96.4	695
97.220.96.3	696
97.220.96.5	695
97.220.96.8	695
95.155.96.41	696
97.220.96.2	693
95.159.102.34	647
97.220.96.5	637
97.220.96.6	626
95.111.162.37	624
97.220.96.15	622
95.111.162.72	623
97.220.96.2	625
95.111.162.11	624
97.220.96.24	624
97.220.96.7	624



Advertising Network



Agenda

1 Sophisticated Malware

2 Reselling proxies

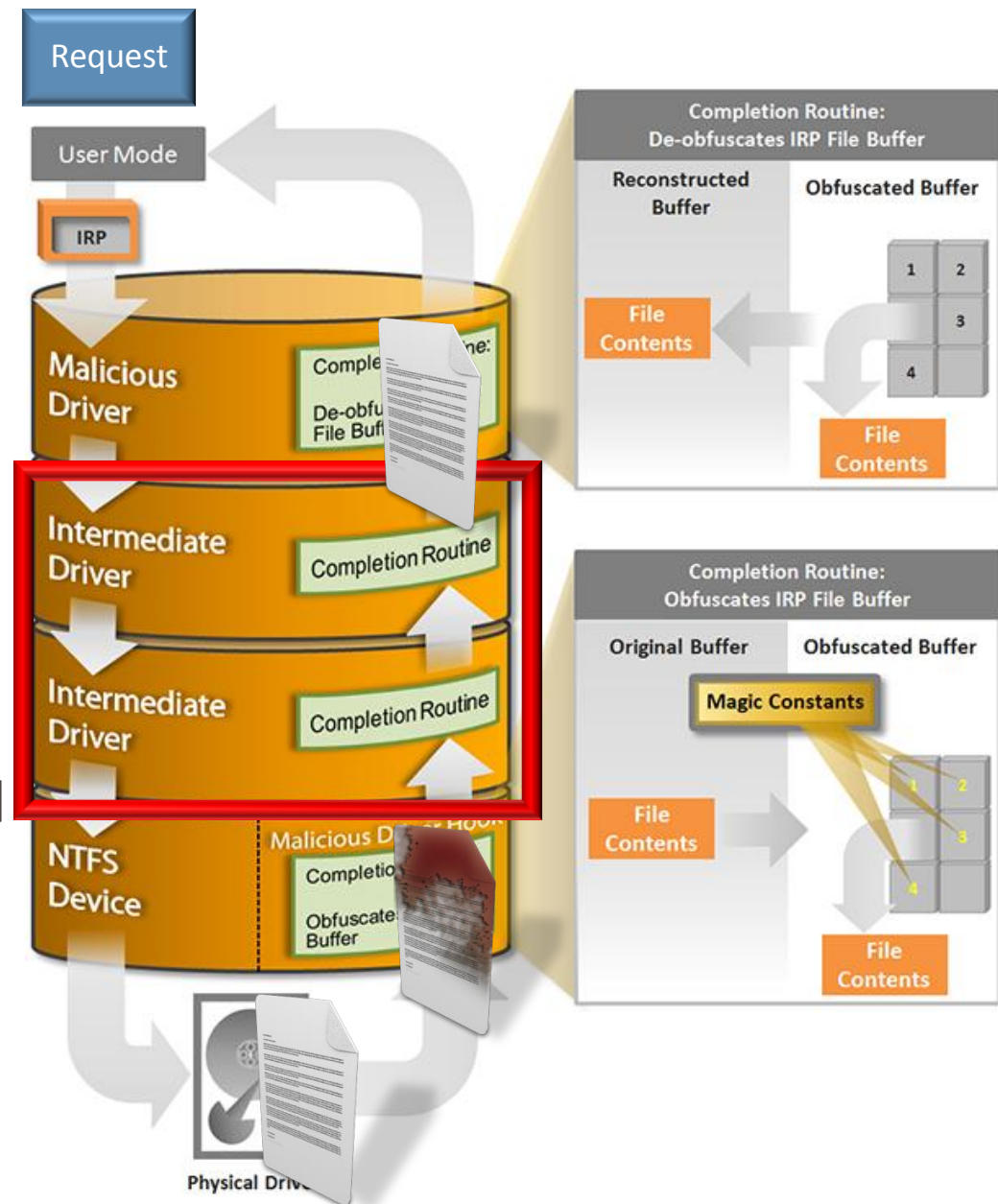
3 Sophisticated Command and Control

4 Money trail

Malware

Kernel Filesystem Filter

- Hooks kernel filesystem device stack
- Obfuscates IRP file buffer for protected files
- Attempts to avoid low level anti-virus scanning
- Author displays a technical understanding of windows internals



Malware

Overview

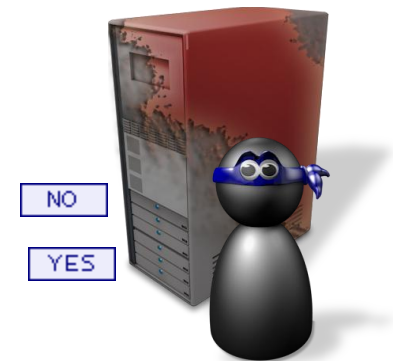
- Unusual Command and Control behavior



```
GET /bn/botinfo.php
```



```
GET /bn/botinfo.php  
guid=cef1ad9b-fc65-4e3c-9b70-368e709be51e  
installtype=service  
version=2.4.6
```



Malware

Overview

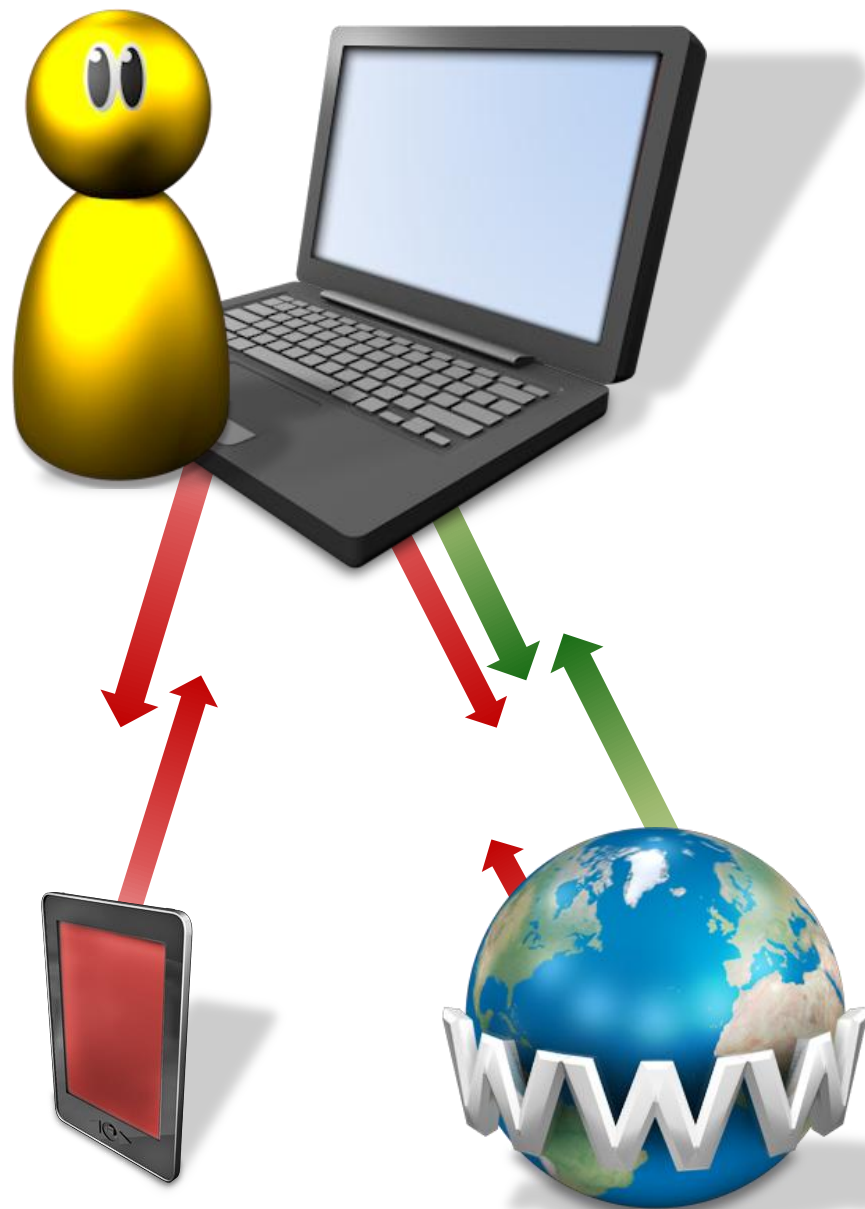
- Proxy authentication
 - English Command Protocol



Malware

Proxy Component

- Deeper Investigation
 - Malware was actually a SOCKS proxy
 - Passing PPC traffic from Command servers
 - Passing traffic for Proxybox.name users



Malware

Botnet

- Proxy bot network spread across several C&Cs
- Total infected users maintaining around 40,000
- High turn over rate
- 6000 unique md5's per month
 - Repackaging malware often

All proxy: 37093
24h proxy: 37093
OnLine: 13594
All by version

version	count
1.0.5	5
1.1.1	4
1.1.2	7
2.2.1	153
2.2.10	4911
2.2.2	2417
2.2.3	4279
2.4.1	2187
2.4.4	1709
2.4.40	4296
2.4.5	3087
2.4.6	1190
2.4.7	2948
2.4.8	5924
5.2.0	3976

Malware

Pay per click fraud

- Proxy controllers commanded bots to forward click fraud traffic
 - Infected client replays the ad “click”
 - Simulates browser activity on target website



```
<html>  
<script src='fivestar.js'></script>  
...  
</html>
```

```
GET /sites/all/modules/contrib/fivestar/js/fivestar.js  
Host: www.movieroomreviews.com
```

```
GET /sites/all/modules/panels/js/panels.js  
Host: www.movieroomreviews.com
```

```
GET /modules/system/system.css has-men-black-role  
Host: cdn3.movieroomreviews.com
```

```
GET /modules/node/node.css  
Host: cdn3.movieroomreviews.com
```

Command and Control

Overview

- Multiple botnet command pages
- Performed load splitting to 15 different IP addresses
- Public server monitoring software installed
- **Unsecured** configuration and statistics pages

Command and Control

Bot Command Pages

- `get_servers.php`
 - Bot asks for a proxy controller server
 - Proxy controller is chosen by the C&C from list of 15-20 servers

```
GET /bn/get_servers.php?version=2.4.6 HTTP/1.0
Host: g000gle.com.tw
Connection: Close

HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Mon, 10 Sep 2012 22:29:59 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.4.0-3
95.211.162.87:22222|
```

- `get_reserved_servers.php`

```
GET /bn/get_reserved_servers.php HTTP/1.0
Host: g000gle.com.tw
Connection: Close

HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Mon, 10 Sep 2012 22:29:39 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.4.0-3
http://proxybox.name/|
```

PROXYBOX

Socks/Proxy Service

[Рус](#) [Eng](#)

Login

[Forgot password?](#)

[Registration](#)

Enter

[Homepage](#)

[Fees](#)

[Features](#)

[Articles](#)

[FAQ](#)

[Contacts](#)

CHECK PROXY

Proxybox

We are glad to inform you that we have fully rewritten the software part of our service, making it more functional, simple and convenient.

Features:

- Convenient division by countries, states, cities, everything is clickable.
- Quality database search and alignment according to your parameters.
- Fully automatic payment and registration system via WebMoney, Liberty Reserve, Robox.
- We expect over 2000 bots online all the time.
- All reviewed proxies are marked with another color.

Based on our experience, we have developed a convenient service, which features all the best options and significantly simplifies the work with a proxy. We hope that cooperating with us you will make your routine work easier, and that our pricing policy will suit you.

News

9.09 New tariff plans!

8.09 The number of proxies online exceeds 2000

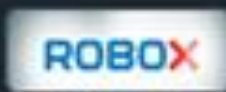
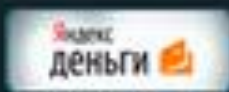
15.06 Payment System Liberty reserve was added

Accepted:



Reseller Frontend – Proxybox.name

Choose payment system: *WebMoney*



Attention! In case if the payments are made via Liberty Reserve system we charge additional fee amounting to 3% of the price plan cost.

Choose tariff plan:

20 proxy for 10 days - 9.90\$
150 proxy for 30 days - 25\$
300 proxy for 30 days - 30\$

400 proxy for 60 days - 45\$
600 proxy for 90 days - 65\$
1200 proxy for 180 days - 120\$

Unlimited 30 days - 40\$
Unlimited 90 days - 110\$
Unlimited 120 days - 130\$

BUY

Reseller Frontend – Proxybox.name

CHECK PROXY

Proxy

Payment

My Proxy

Statistics

Settings

Search proxy



SUBMIT

Country		Region		Address	Hostname	City / Region	UpTime	Speed
All Countries	596	N/A	240	90.84.***.***	90.84.***.***	KINSHASA KINSHASA	00:00:02	10
EGYPT	83	ABUJA CAPITAL TERRITORY	1	186.65.***.***	186.65.***.***	N/A N/A	00:00:02	40
UNITED KINGDOM	53	AL JIZAH	1	37.239.***.***	37.239.***.***	N/A N/A	00:00:02	16
N/A	41	AL KHARTUM	4	41.45.***.***	41.45.***.***	N/A N/A	00:00:02	2
INDONESIA	29	AL KUWAYT	1	84.185.***.***	84.18***.***.***	DUSSELDORF NORDRHEIN-WESTFALEN	00:00:02	58
TURKEY	27	AL QAHIRAH	36	41.188.***.***	4***.***88.***27.***	N/A	00:00:02	3
MEXICO	21	ALBERTA	1					
UNITED STATES	17	ALGERIA						

Reseller Frontend – Proxybox.name

Author

Overview

- Proxybox.name advertisements

24-08-2010, 17:34 ProxyBox.name - comfortable with us! (+ Action!) # 1

antichat

Verified. (Zone)
Newcomer
Joined: 04.01.2008
Posts: 1
Thanks:
9:00 46 minutes 4 seconds
Reputation: 0

ProxyBox.name - comfortable with us! (+ Action!)

Action! The first five customers who purchase any rate the second month in a gift. To receive the bonus payment after knock in ICQ: 536 636. **Dear customers! Introducing you to your new proxy ProxyBox.name , over which we have been working the past six months.** Among the features of the service **Admin:**

- A convenient division of countries, states, cities, all clickable.
- Intelligent database search and alignment of your parameters.
- Fully automatic payment and registration via WebMoney, Liberty Reserve, Robox.
- All viewed the proxy recorded in a different color.
- Ability to rent any socks from the list for a month for just \$ 3. At the same time to use it will be just you.
- Checking Your Socks on Whoer.net
- Statistics of your payments.

Service:

- More than 3,000 boats online.
- Constantly updated GeoIP database.
- Integrity checks every 10 minutes online.
- Self-loading only of our unique software.
- As always, courteous and competent support.
- Net, an exclusive software with the possibility of any changes or additions.




If you are interested in our offer or you have any questions do not hesitate to contact our caliper. Support ICQ: 536 636 Sincerely, Team ProxyBox.name

Last edited by Verified. (Zone), 24.08.2010 at 17:38 .

Author

Overview

- Linked to 3 other shady service websites
 - Whoer.net
 - Proxy verification
 - AVCheck.ru
 - Malware detection
 - VPNlab.ru
 - Encrypted VPN access

Thread /		Last Post	Replies	Views
	ProxyBox.name - comfortable with us! (+ Action!) Verified. (Zone)	02/11/2011 19:05 by infraud	1	3,983
	WHOER.NET - Service check your anonymity (1 2 3 4) Verified. (Zone)	07/15/2010 16:24 by Verified. (zone)	30	4,739
	AVCheck.ru - service antivirus scan files (1 2 3 4) Verified. (Zone)	07/12/2010 18:51 by warwar	33	6,117



News

01/12/2010

We are open! Once again we are here for you .. See section [Tariffs](#)

Home

AV Check.ru - a service test your antivirus files. The main difference from similar is that we do not mail your files for analysis to antivirus companies. We honor your right to property and privacy. AVCheck conceived as a convenient service to check files, including the battery. Advantage of which would be automated testing with detailed reports via email or IM client. Rely on us to check and sleep well!

The technical side AVCheck - is:

- 20 popular [antivirus](#) is updated daily;
- can automatically check your files;
- audit reports on e-mail, in icq and jabber;
- convenient customer control panel;
- flexible tariff plans - guarantee of privacy for you and your files;
- full scan of the file within 30-40 seconds;
- change personal information and passwords;
- courteous and competent support.

In order to familiarize yourself with the control panel to register and login. After payment of the chosen tariff plan will be available to check files. To test the possibilities, you can buy one check.

We appreciate your feedback on our service. All comments, suggestions and comments, please send to icq caliper or e-mail. We will try to take into account all realize.

Login:

Password:

[Register](#) | [Recover](#)

Login

Compatible:



IE



Firefox



Opera



ICQ



Jabber



E-Mail

Accept:



Webmoney



Yandex



Money Mail

Support:



469057748

Other services – AVCheck.ru



Find out IP address

Lite

My IP address	.118		
Country	United States (US)		
Region	California (CA)		
City	Los Angeles		
ZIP code	N/A		
Hostname	h-	-118.	→ N/A
IP range	.0 - .255		
ISP	Covad Communications		
Organization	Covad Communications		
DNS	<input type="text"/>	United States	
Black list	Yes (Illegal 3rd party exploits, including proxies, worms and trojan)		
Proxy	No		
Time			
zone	America/Los_Angeles		
local	Wed Sep 19 2012 10:23:52 GMT-0700 (PDT)		Mismatch
system	Wed Sep 19 2012 18:24:07 GMT+0100 (GMT Daylight Time)		
Browser			

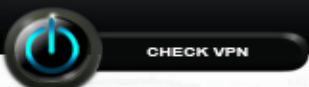
Extended

BEST DOUBLE VPN

-20% FOREVER

double vpn serice

Other services – Whoer.net



News

15.08.2012
Summer SALE 50% OFF!!!

31.07.2012
USA server in PA, Scranton has been moved to GA, Atlanta

25.02.2012
The third VPN server in the USA

23.01.2012
Any server could be used as reserved

10.01.2012
New VPN server in Egypt


24.11.2011
-20% FOREVER!


20.10.2011
Autumn SALE 50%!!!

Support

536636

vpn@vpnlab.ru
(guaranteed answer)





VPNLab is a service providing your security on the Internet by encryption of original traffic. Our service is designed for a broad spectrum of clients: webmasters, SEO-optimizers, traders, businessmen and people, who care about their personal security. We set a special encrypted channel between your computer and our foreign servers. The channel is installed based on OpenVPN technology and encrypted using 2048 bit key and thanks to sophisticated algorithms all the information is unreadable for your provider. Average users don't see the necessity of the described procedure and may even find it useless, however the latest featured legal proceedings involving people who were just expressing their opinions in their own web-diaries show the seriousness of Internet security issue.

The creation of VPNLab is based on 5 main concepts:

- **Reliability.** The reliability of encryption by open 2048 bit key algorithms is unquestionable and was repeatedly confirmed during the ten years of this technology's existence. Our servers are located in proven foreign datacenters, the DoubleVPN technology will allow you to set a chain of two servers. VPNLab's main goal is to provide anonymous and secure connection.
- **Convenience.** Our service allows to start working in five minutes after the registration. All you need to do is to register, pay and start working. You'll receive all the configuration files after the payment. Additional features:
 - monthly (clear for users) change of outgoing IP addresses
 - ports forwarding by request
 - possibility to set a dedicated IP address
 - existence of reserved servers, which can be used in case of work interruptions
 - possibility to switch to other servers in minutes
- **Independency.** Our service is fully independent from technical support. In your account you will find a user-friendly service control panel that will allow you to work with all its components, including individual pricing plans.
- **Flexibility.** Our service can be accessed from any computer with any type of

Login

Login:

Password:

[Register](#)

[Recover](#)

Accept









Other services – VpnLab.ru

Monetization

Cash flow

- Proxy reseller
 - Proxybox
 - VPNLab

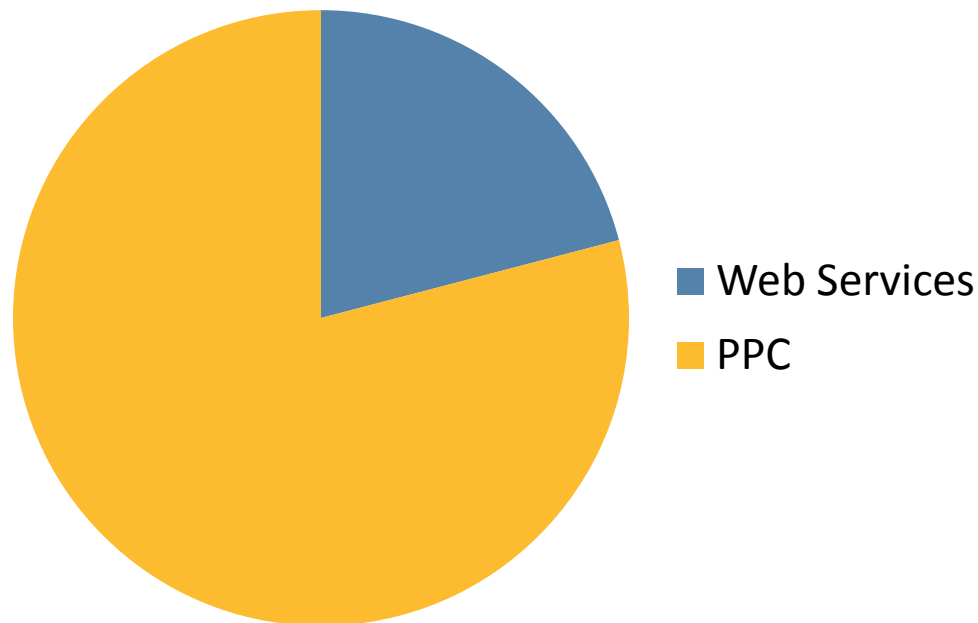
- Pay-per-click affiliate
 - 40,000 bots
 - 20 clicks per bot per day
 - \$.0005 per click
 - \$150 k per year

Average Proxy Sales

Low value click sales

Very high click volume

\$150,000 - \$170,000 annual income



Attacker Identity

Registrar and Online Payment Gateways

- VpnLab.ru
 - Private Registration
- AVCheck.ru
 - Private Registration
- www.g000gle.com.tw
 - Fake Registration Details

Attacker Identity

Registrar and Online Payment Gateways

- Proxybox.name
 - Sergej Cherchesov
 - Pyleva street, 10
 - Arkhangelsk, RU 114593
 - +1 (410) 6021343
- Whoer.net
 - Ekaterina S Timohina
 - str. Pjatnickaja 12, apt. 17
 - Moscow, RU 115998
 - +7 (963) 7902529

Attacker Identity

Registrar and Online Payment Gateways

- Liberty Reserve
 - MerchantID: U6060946 (Proxybox)
- Robokassa.ru
 - Shop name “SOCKS service”
 - Uses WebMoney Passport Account

Attacker Identity

Registrar and Online Payment Gateways

- WebMoney – Passport Account
- WMID: 428272397057 Issued to Богдан “Bogdan”
- VPNLab lists full name as “Kramarenko Bogdan Yurievich”


If you have any questions, offers or are looking for technical support, please contact us by

536636



vpn@vpnlab.ru (guaranteed answer)

Person in charge of the use of WebMoney Transfer: Kramarenko Bogdan Yurievich

WMID: 428272397057
WMZ: Z304879533221

WMID428272397057 —  [Богдан](#)





WM Passport

Verification status:	 Merchant passport issued 17 June 2008 issued by
Secondary verification:	completed
Since registration:	~ 4 years and 3 months
Special Notes:	




WMID Information

[WMID#428272397057](#)
Nickname: **Богдан**
Registration date: 13 June 2008
BL: **586**
[Complaints/Comments:](#) **0 / 0**
[View user's profile WMID#428272397057 on events.webmoney.ru](#)

Personal details

♥ Last name:	
♥ First name:	
♥ Middle name:	
Sex:	
Taxpayer Identification Number (INN):	

User location

♥ City/Country:	
Zip/Postal code:	
♥ Street address:	

Conclusion

- Russian Malware Author
 - Has infected a large number of users and manages a large botnet
 - Sophisticated understanding of windows internals
 - Many sources of income
 - Long standing persistence in the underground scene
 - Uses identities associated with several payment gateways

- Next steps
 - Monitoring botnet activity and updates
 - Command and Control Takedowns

Questions?

1

Verified Support is offline
The message will be delivered when the contact goes Available.
[Send SMS](#)

Crash Override
Hi

Verified Support
hello

Crash Override
Yes hello I have been waiting to talk to you certainly
Do you prefer Russian or English?

Verified Support
if you russian good)

Crash Override
No, only translator. Let us try English.
First, I would like to just get to know you

Verified Support
ok

Crash Override
How long has your service been available?

Crash Override 12:00 AM
It seems to be multiples of years? Available even since 2010, this is truly great.

Crash Override 12:01 AM
Allow me to "cut the cheese" so to speak, I am interested in your technical abilities. Are you the creator of the service?

Verified Support 12:02 AM
am support but you can speak with abilities ets

Crash Override 12:04 AM
Your english is perfectly clear, my good friend. I was wondering if we can be lifelong friends some day.

Now who is this "Abilities Ets" you speak of, and what are his hacker ventures I would know about. Make it snappy young man!

2

Verified Support 🤖 with me of abilities 12:05 AM

Crash Override 12:05 AM
Ahh, that is MUCH clearer. Thank you for that.

Crash Override 12:06 AM
Now, are you aware that your employer is a MALWARE DISTRIBUTOR?

Verified Support 12:07 AM
about whats service you mean?

Crash Override 12:07 AM
Do you know about Proxybox.name?

Verified Support 12:08 AM
yes
Crash Override (03:04:28 25/09/2012)
Now, are you aware that your employer is a MALWARE DISTRIBUTOR?
no i dont
what do you want?

Crash Override 12:09 AM
Well actually I am researching his ventures for a paper I plan to publish later on in the year
It would be great to talk with him!

Verified Support 12:09 AM
you can write to email

Crash Override
Ok which email do I write to
I tried Bogdan@Kramarenko.yu but didnt' get a response

Verified Support
Tell me what you want to convey to him

Crash Override
Great! What an opportunity, thank you very much for this chance!
Hmm what to ask

Crash Override
First of all, I would like to know if his mother knows what he does for a living
Is Mrs. Yurievich in on the malware?????

3

Crash Override 12:15 AM
Ok, well maybe I should come clean I work for an american Anti-Virus company

Verified Support 12:16 AM
and?

Crash Override 12:16 AM
I just want to say I love your guys work, you really are providing a great service to the world

Verified Support 12:16 AM
ok

Crash Override 12:16 AM
Especially the filesystem rootkit in the last version of the proxy malware! Oh man that was great

Crash Override 12:17 AM
Listen, do you know if Bogdan's mom helped him write the FsFilter component? Just curious...

Verified Support 12:17 AM
i dont know

Crash Override 12:18 AM
How much does Bogdan pay you?
Богдан, right?

Crash Override 12:19 AM
I feel like we got off on the wrong foot, I don't want to make an enemy you seem like a cool guy.
What's your name?

Verified Support 12:20 AM
sorry i cant help you

Crash Override 12:22 AM
Are you familiar with the underground hacker, Morpheus? He was in the matrix. He gave me you as a reference. I was expecting better treatment
Trust me, you really dont want to make Keanu angry...



Thank you!

Joseph Bingham

Joseph_Bingham@symantec.com

(424) 750 7749

from: **Crash Override** cr4sh0v3r1d3r@gmail.com

to: vpn@vpnlab.ru

date: Mon, Sep 17, 2012 at 7:38 PM

I am interested in talking with you about buying service. I have thousands of customers I need to provide proxy service. Please contact me as soon as possible

from: **VPNLab.ru administration** vpn@vpnlab.ru

to: Crash Override <cr4sh0v3r1d3r@gmail.com>

date: Tue, Sep 18, 2012 at 5:50 PM

Good day. Do you want to buy service vpnlab.ru?

Sincerely,

administration VPNLab.ru

from: **Crash Override** cr4sh0v3r1d3r@gmail.com

My associate Acid Burn and I have been studying you for a long time. We think you may be the one to break us free from the matrix. We would like to talk to you when you are available in ICQ

from: **VPNLab.ru administration** vpn@vpnlab.ru

Good day. Your suggestion is clear. You will be able to talk to the owner and creator of the 10 days, he is currently on leave. Then you can discuss all the details.

Yes, ICQ available now. You can write on e-mail.

from: **Crash Override** cr4sh0v3r1d3r@gmail.com

When you talk to "the owner", please ask him if his grandmother helped him write the code for the file system filter "FsFilter.cpp"

Я заинтересован в разговоре с вами о покупке сервиса. У меня есть тысячи клиентов мне необходимо предоставить прокси-сервис. Пожалуйста, свяжитесь со мной как можно скорее

Доброго дня. Вы хотите приобрести сервис vpnlab.ru?

С уважением,
администрация VPNLab.ru

Мой коллега Acid Burn и я изучал вас в течение долгого времени. Мы думаем, что вы можете быть тем, чтобы разорвать нас от матрицы. Мы хотели бы поговорить с вами, когда вы доступны в ICQ

Доброго дня. Ваше предложение понятно. Вы сможете переговорить с владельцем и создателем через 10 дней, он сейчас в отпуске.

Тогда вы сможете обговорить все детали.

Да, ICQ недоступно сейчас. Вы можете писать на почту.

Когда вы говорите с "владельцем", пожалуйста, спросите его, если его бабушка помогла ему написать код для фильтра файловой системы "FsFilter.cpp"

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.