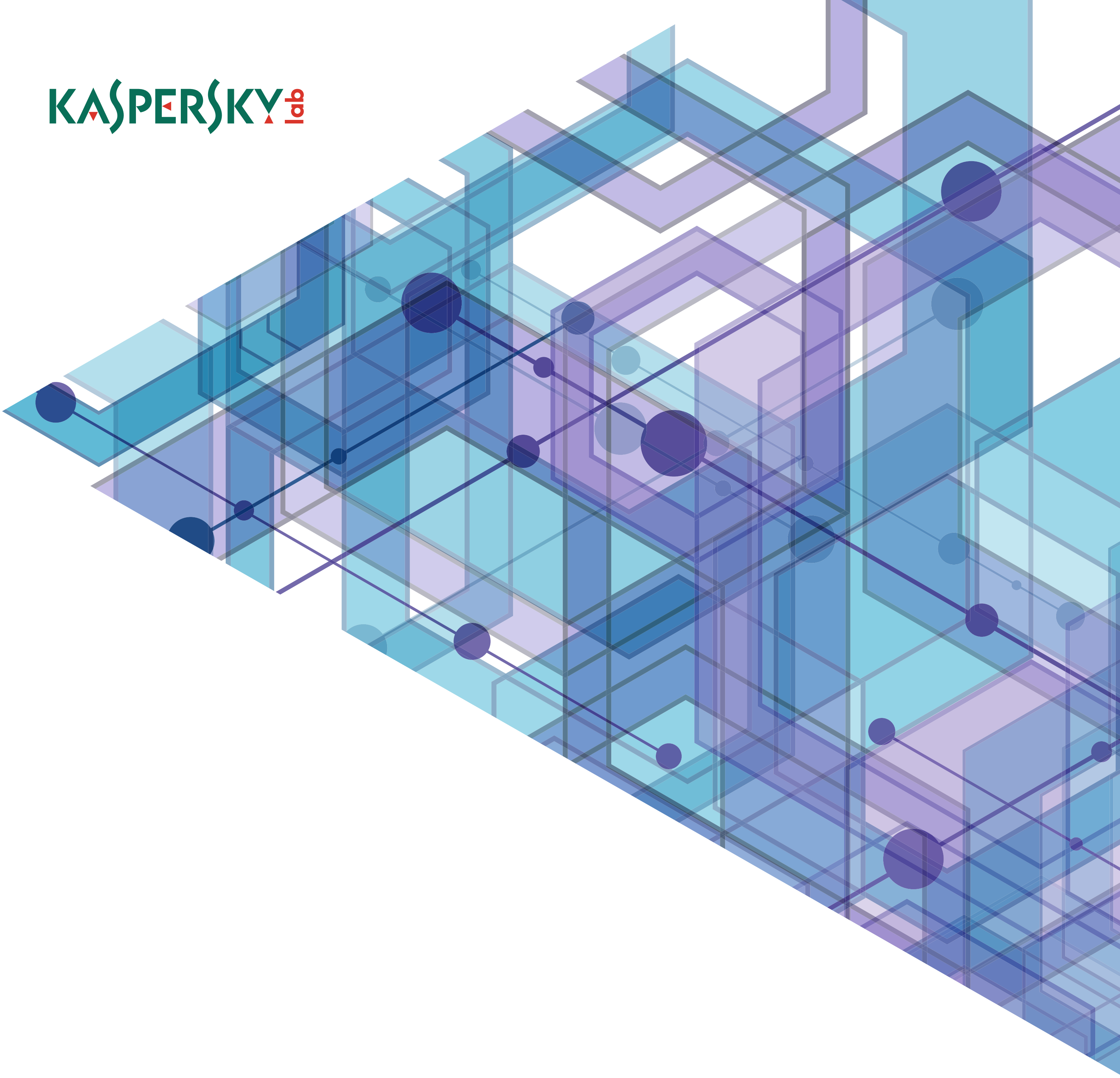


THE XDEDIC MARKETPLACE

Version: 1.0 (15 June 2016)

*Distribution: this document is **WHITE.** For more information on TLP, please see https://www.us-cert.gov/tlp*

Executive summary

Over last two years a new kind of underground market has flourished, and xDedic is a perfect example.

“xDedic” is a trading platform where cybercriminals can purchase any of over 70,000 hacked servers from all around the internet. It appears to be run by a Russian-speaking group of hackers.

The forum provides members with tools to patch RDP (Remote Desktop Protocol) servers to support multiple user logins, as well as other hacking tools, such as proxy installers and sysinfo collectors. The main goal of the xDedic forum is to facilitate the buying and selling of credentials for hacked servers which are available through RDP.

From governmental networks to corporations, it is possible to find almost anything on xDedic for as little as 6 USD per server. This one-time cost provides a malicious "customer" with access to all the data on the server and endless other possibilities, such as using the access to launch further attacks.

To investigate xDedic, Kaspersky Lab teamed up with a European ISP. This research allowed us to collect data about the victims and the way the marketplace operates.

This report in a nutshell:

- Description of the xDedic marketplace and its offering.
- Statistics about servers for sale and their profile.
- How the attackers get access to the servers.
- What tools and Trojans they install in the hacked servers.
- High profile victims with hacked servers on the market.
- Attribution of the administrators of the forum.

For more information contact: intelreports@kaspersky.com

The Marketplace

The marketplace is located at the domain xdedic[.]biz and anyone can register to use it. New members need to use their account within 72 hours of registration, otherwise the account is automatically removed unless they pay a fee of 10 USD.

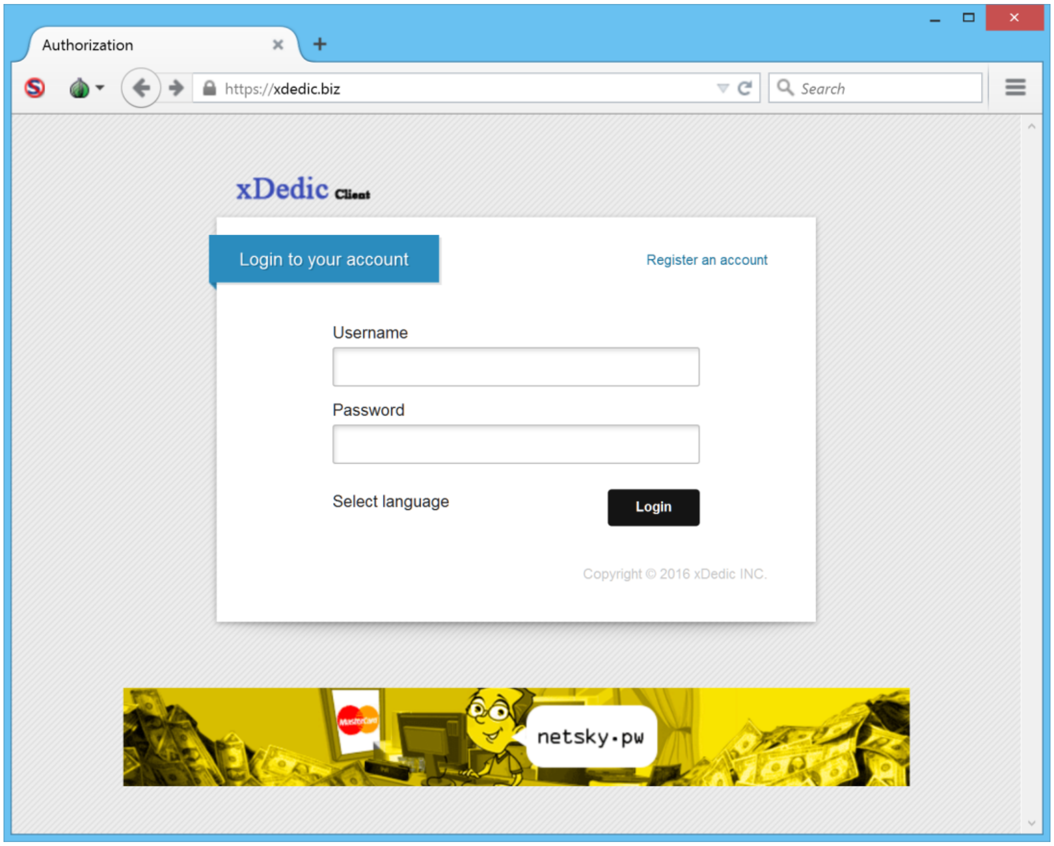


Figure 1. xDedic main login

During registration, the user is asked to provide either an e-mail address or a Jabber account. In the case of Jabber-account based registration, a confirmation code is sent in order to validate the account.

We strongly advice not to register to the xDedic marketplace, as any activity in the marketplace might be in dangerous or even illegal.

According to an analysis of the information available in the marketplace, the service was started some time in 2014 and gained major popularity in the middle of 2015 when over 3,000 servers were added to the marketplace. Since then many new offerings have been posted and re-posted on the forum.

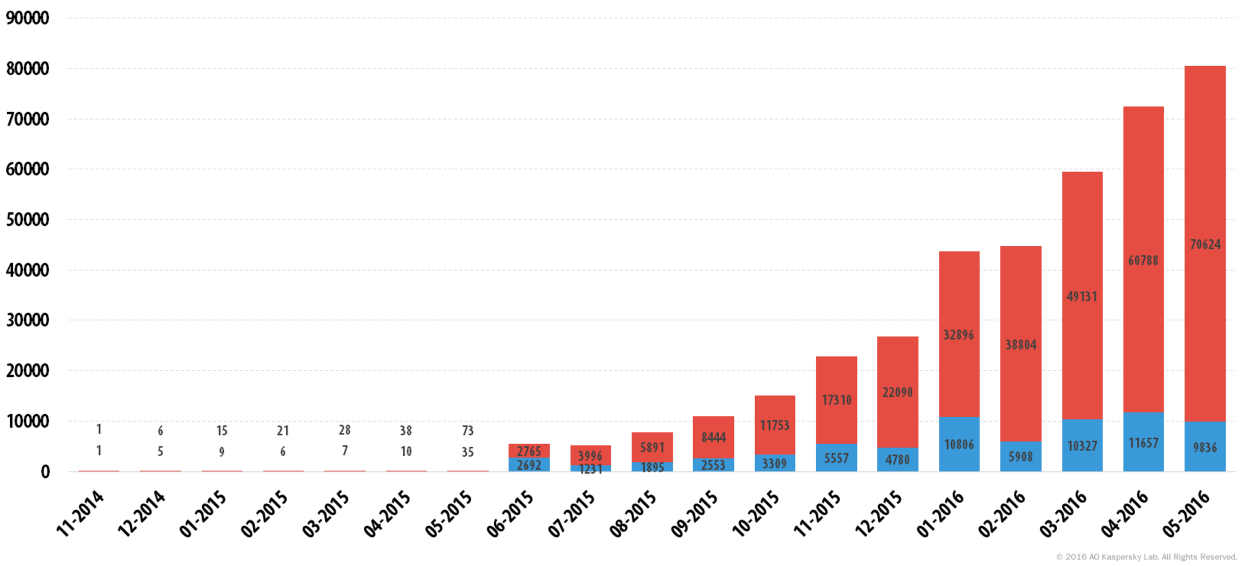
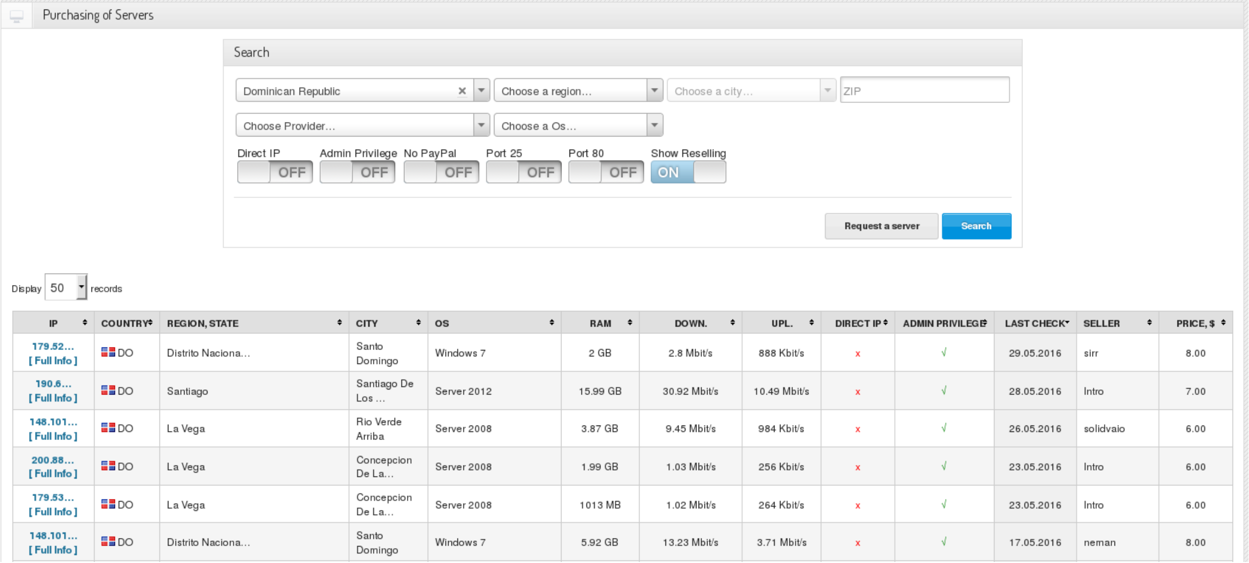


Figure 2. Marketplace activity in number of new server offerings

Once logged into the forum, the user can access a Dashboard with general news as well as a page with a list of servers available for purchase.



Purchasing of Servers

Search

Dominican Republic ×
Choose a region...
Choose a city...
ZIP
Choose Provider...
Choose a Os...

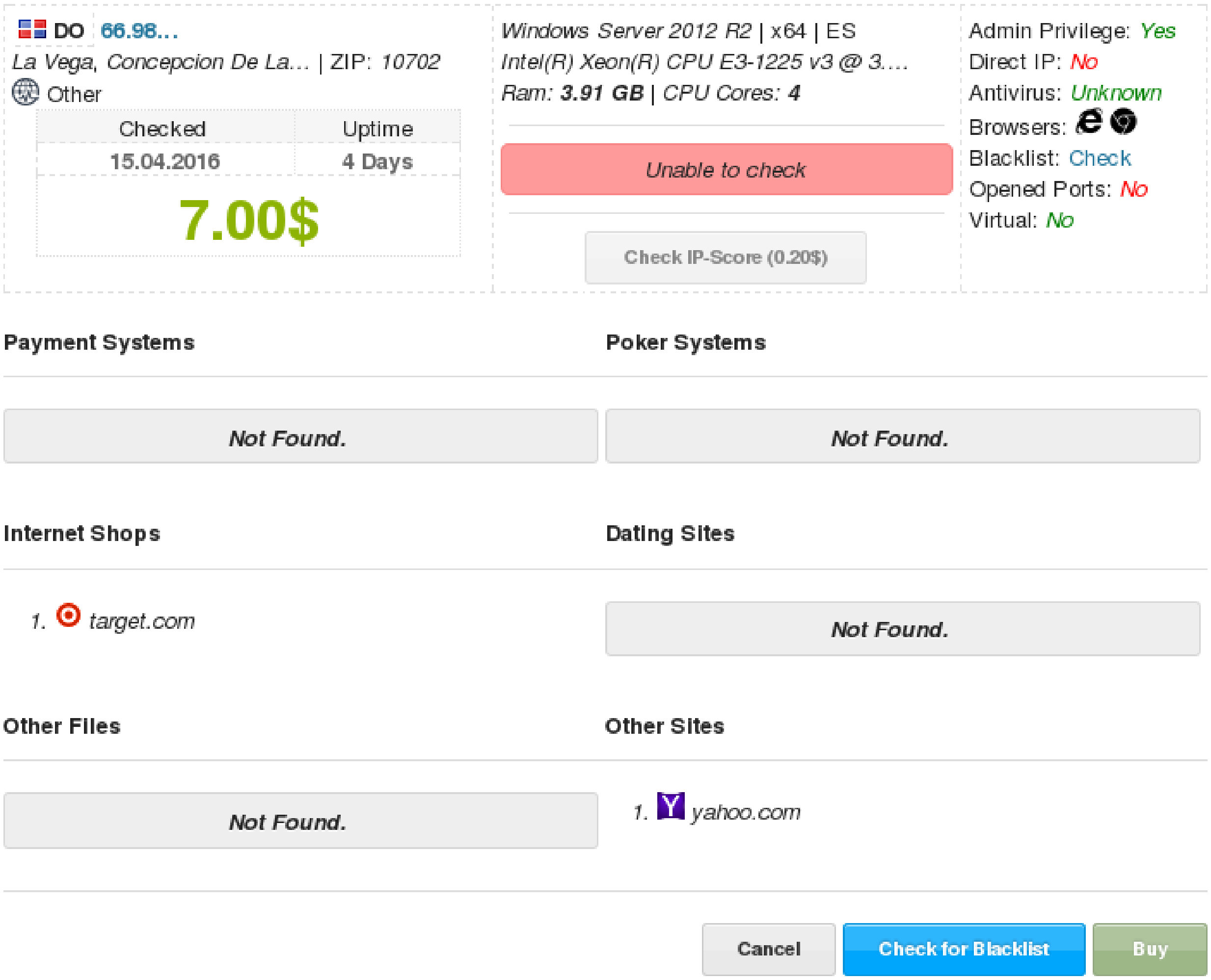
Direct IP OFF
Admin Privilege OFF
No PayPal OFF
Port 25 OFF
Port 80 OFF
Show Reselling ON

Display 50 records

IP	COUNTRY	REGION, STATE	CITY	OS	RAM	DOWN.	UPL.	DIRECT IP	ADMIN PRIVILEGE	LAST CHECK	SELLER	PRICE, $
179.52... [Full Info]	DO	Distrito Naciona...	Santo Domingo	Windows 7	2 GB	2.8 Mbit/s	888 Kbit/s	x	√	29.05.2016	sirr	8.00
190.6... [Full Info]	DO	Santiago	Santiago De Los ...	Server 2012	15.99 GB	30.92 Mbit/s	10.49 Mbit/s	x	√	28.05.2016	Intro	7.00
148.101... [Full Info]	DO	La Vega	Rio Verde Arriba	Server 2008	3.87 GB	9.45 Mbit/s	984 Kbit/s	x	√	26.05.2016	solidvaio	6.00
200.88... [Full Info]	DO	La Vega	Concepcion De La...	Server 2008	1.99 GB	1.03 Mbit/s	256 Kbit/s	x	√	23.05.2016	Intro	6.00
179.53... [Full Info]	DO	La Vega	Concepcion De La...	Server 2008	1013 MB	1.02 Mbit/s	264 Kbit/s	x	√	23.05.2016	Intro	6.00
148.101... [Full Info]	DO	Distrito Naciona...	Santo Domingo	Windows 7	5.92 GB	13.23 Mbit/s	3.71 Mbit/s	x	√	17.05.2016	neman	8.00

Figure 3. Servers purchase form

For each server, detailed information such as price, location, speed, anti-virus installed, etc. is provided.



DO 66.98…
La Vega, Concepcion De La… | ZIP: 10702
Other

Checked	Uptime
15.04.2016	4 Days

7.00$

Windows Server 2012 R2 | x64 | ES
Intel(R) Xeon(R) CPU E3-1225 v3 @ 3.…
Ram: **3.91 GB** | CPU Cores: **4**

Unable to check

Check IP-Score (0.20$)

Admin Privilege: Yes
Direct IP: No
Antivirus: Unknown
Browsers:
Blacklist: Check
Opened Ports: No
Virtual: No

Payment Systems

Not Found.

Poker Systems

Not Found.

Internet Shops

1. target.com

Dating Sites

Not Found.

Other Files

Not Found.

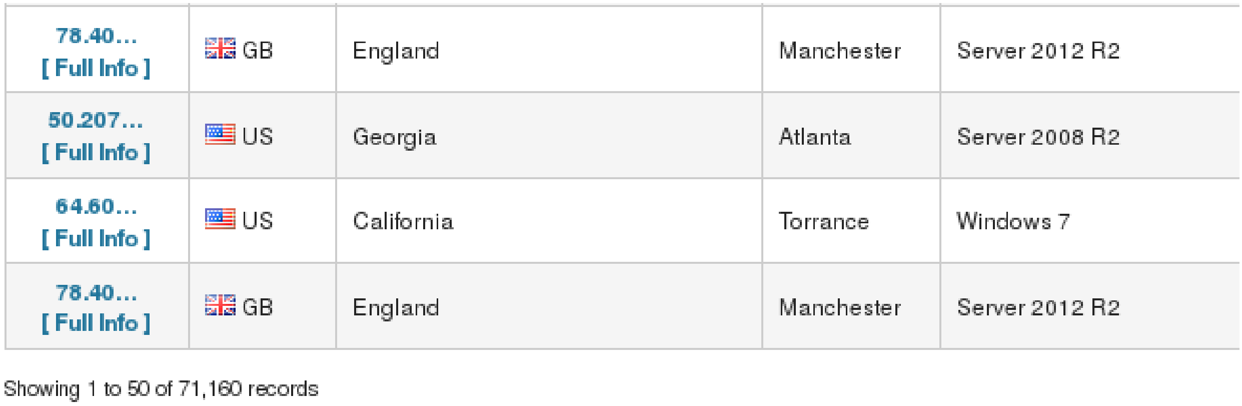
Other Sites

1. yahoo.com

Figure 4. Additional server details

The owners of xdedic[.]biz claim not to be related to the sellers of hacked server access, but only to provide a secure trading platform for others. It is possible to see the seller´s nickname in the list of available servers (see Figure 2).

As of May 2016, access to 70,624 dedicated servers worldwide was offered for sale.



78.40... [Full Info]	GB	England	Manchester	Server 2012 R2
50.207... [Full Info]	US	Georgia	Atlanta	Server 2008 R2
64.60... [Full Info]	US	California	Torrance	Windows 7
78.40... [Full Info]	GB	England	Manchester	Server 2012 R2

Showing 1 to 50 of 71,160 records

Figure 5. Number of servers available

Detailed statistics of available servers

In March 2016, the sales inventory included access to **51,752 servers** from **183 countries**, located in **11,050** different **subnets**. There were **425 unique sellers** on the marketplace.

In May 2016, we counted **70,624 servers** from **416 unique sellers** in **173 affected countries**. This shows that the database of users and servers is carefully maintained.

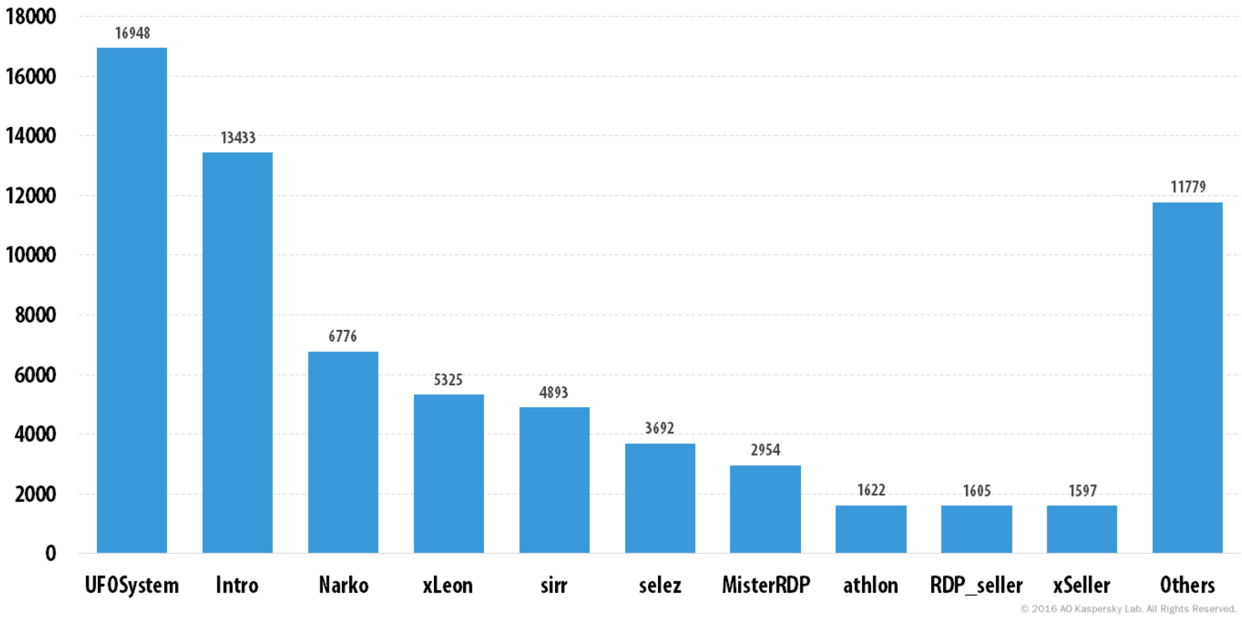


Figure 6. Top 10 sellers - May 2016

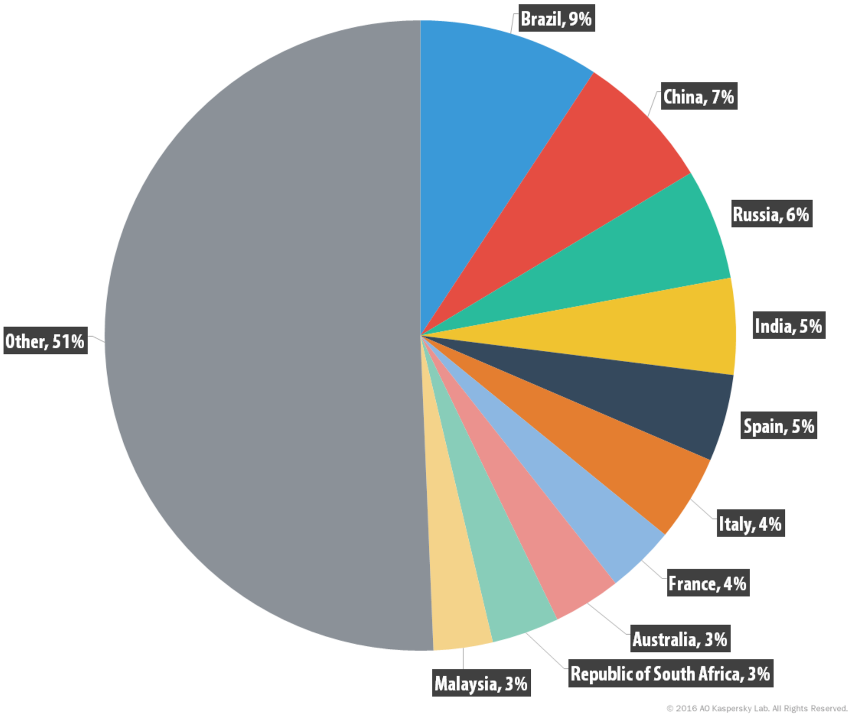


Figure 7. Top 10 countries with servers on sale - May 2016

Detailed information on the TOP 20 affected countries (as of May 2016) is provided below:

Num of offerings	Country Code
6540	BR
5023	CN
4020	RU
3488	IN
3155	ES
3119	IT
2474	FR
2448	AU
2438	ZA
2140	MY
1767	GB
1460	MX
1413	CO
1395	US
1296	DE
1292	PL
1236	TW
1224	UA
1217	AR
1204	TR
22275	Other

The RDP servers can be used by cybercriminals in many different ways. That´s why the marketplace tags the RDP servers that have been proven, through specific testing, not to have been blacklisted by certain online resources. The owners of xDedic owners have developed a tool that can automatically collect information about the system, including websites that are available from it, any software installed and so on.

Figure 8. RDP server tags

The tags provide a broad overview of the cybercriminals' focus in 2016.

Online Gambling and Betting	Online Shops and Trading	Banks and Payment Systems
188bet.com	airbnb.com	aib.ie
21novacasino.com	amazon.com	barclaycardus.com
32redpoker.com	bestbuy.com	capitalone.com
770.com	bhphotovideo.com	chase.com
888poker.com	craiglist.org	chaseonline.chase.com
Amateurmatch.com	ebay.com	coinbase.com
bet365.com	farfetch.com	entropay.com
betfair.com	lowes.com	liqpay.com
boylepoker.com	newegg.com	moneybookers.com
bwin.com	officedepot.com	money.yandex.ru
es.towertorneos.com	qvc.com	open24.ie
fulltiltpoker.com	sears.com	payeer.com
ipoker.com	steampowered.com	paypal.com
keller.sports.de	store.apple.com	paysurfer.com
leonbets.net	target.com	perfectmoney.com
luckyacepoker.com	walmart.com	qiwi.com
mansion.com		suntrust.com

match.com		skrill.com
partypoker.com		webmoney.ru
poker.paddypower.com		wellsfargo.com
pokerstars.eu		westernunion.com
redstarpoker.eu		
sportingbet.com		
sportingbet.ru		
titanpoker.com		
unibet.com		
williamhill.com		

Dating Websites	Ad Networks	ISP/Cell phone operators
amateurmatch.com	adwords.google.com	att.com
cupid.com	exoclick.com	business.att.com
date.com	juicyads.com	sprint.com
datehookup.com	plugrush.com	verizonwireless.com
meetic.com	popads.net	vzw.com
meetme.com	zeropark.com	verizon.com
zoosk.com		

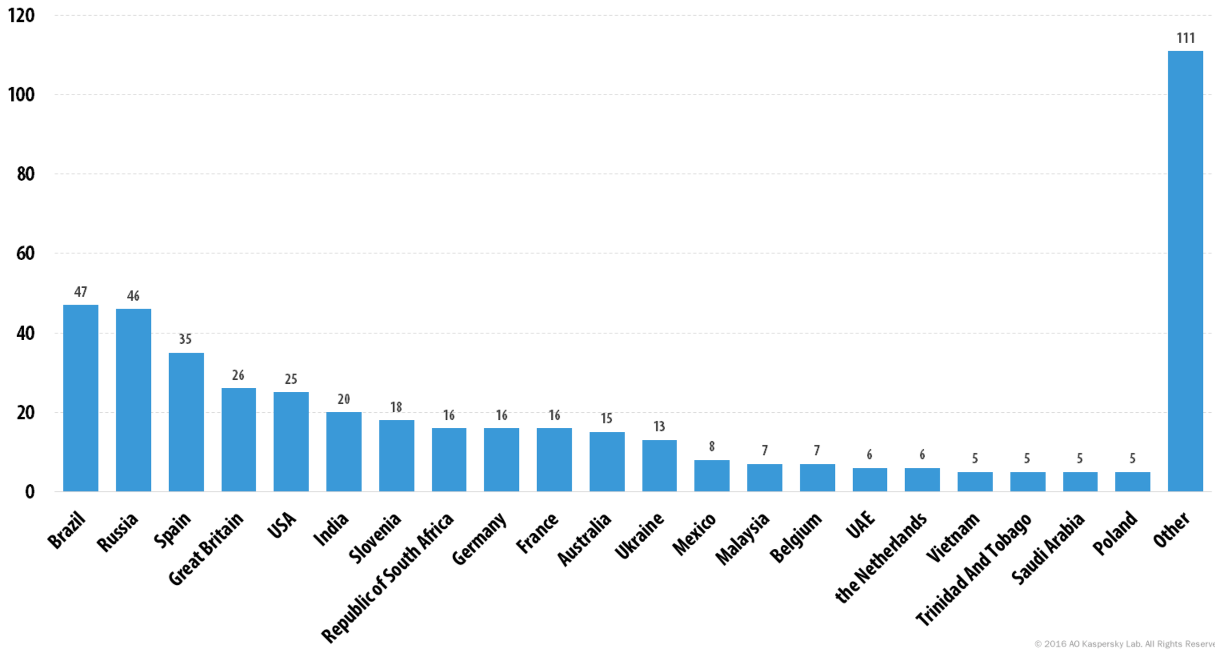
E-Mail providers	Browsers and IM	Other
gmail.com	Chrome	indeed.com
hotmail.com	Firefox	sendspace.com
yahoo.com	Internet Explorer	skype.com
	Opera	starbucks.de
	Skype	swiftunlocks.com
	Steam	ups.com
		whoer.net

In addition to the lists of public websites and common software, there is specific link to software that could be used as a source of fraudulent money. While the criminals sometimes install additional software in the controlled system (for newly created users only) the list of software below was pre-installed by the legitimate owner of the system. In the case of some proxifiers or mass-email sending software, these pre-installed features can be leveraged by the criminals to send out spam or use proxy software without arousing suspicion.

There is a strong interest in accounting, tax reporting and point-of -sale (PoS) software which apparently opens up many opportunities for fraudsters.

Spam and Attacking Tools	Gambling and Financial Software	POS Software
Advanced Mass Sender	Full Tilt Poker	PosWindows
Bitvise Tunnelier	iPoker Network	BrasilPOS
DU Brute	UltraTax 2010 (2011,..,2015)	POS AccuPOS
LexisNexis Spam Soft	Abacus Tax Software	POS Active-Charge
LexisNexis Proxifier	CCH tax14 (tax15)	POS Amigo
Proxifier	CCH Small Firm Services	POS Catapult
Spam Soft	ChoicePoint	POS Firefly
	ProSeries TAX (2014,2015)	POS ePOS
	ProSystem fx Tax	POS EasiPos
	TAX Software	POS Revel
	2015 Tax Praparation	POS Software (Generic)
	Tax Management Inc.	POS Toast
	Lacerte Tax	POS QBPOS
		PosTerminal
		POS kiosk.exe
		POS roi.exe
		POS PTService.exe
		POS pxpp.exe
		POS w3wp.exe
		POS DpsEftX.ocx
		POS AxUpdatePortal.exe
		POS callerIdserver.exe
		POS PURCHASE.exe
		POS XPS.exe
		POS XChgrSrv.exe

We counted **453 servers** from **67 countries** with PoS software installed:

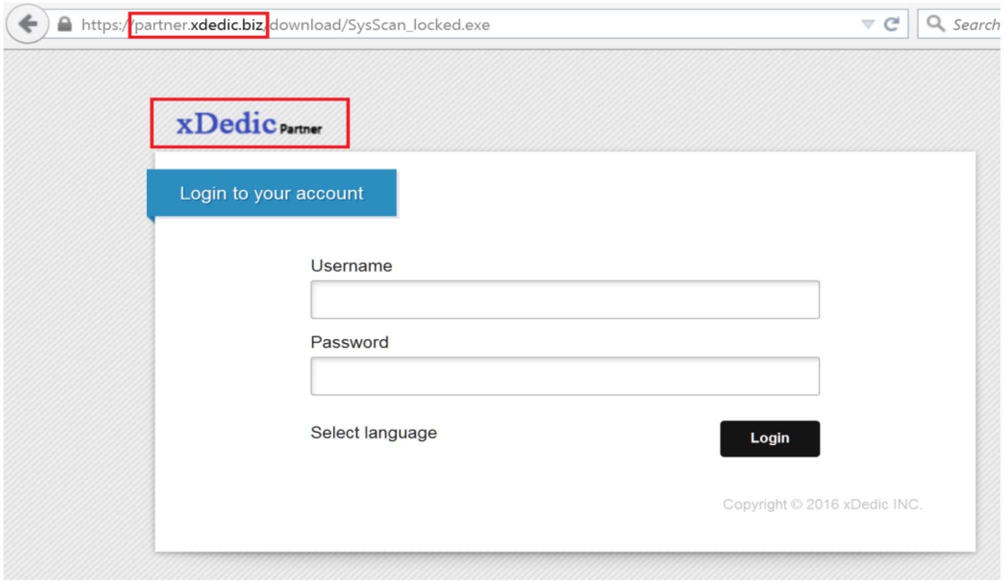


© 2016 AO Kaspersky Lab. All Rights Reserved.

Figure 9. Servers for sale with Point-of-Sale software - May 2016

The xDedic validator tool

There is a separate portal for the so-called “partners” of the xDedic forum. These are essentially the sellers who are offering the hacked servers on the market. The partners’ portal is password-protected and can be found at “partner.xdedic[.]biz”:



https://partner.xdedic.biz/download/SysScan_locked.exe

Figure 10. xDedic partners portal

The partner’s portal has a different set of tools available for download. From these, the most interesting is “SysScan”. “SysScan” is a validator tool used by xDedic partners to profile servers which are to be made available for sale on the main forum.

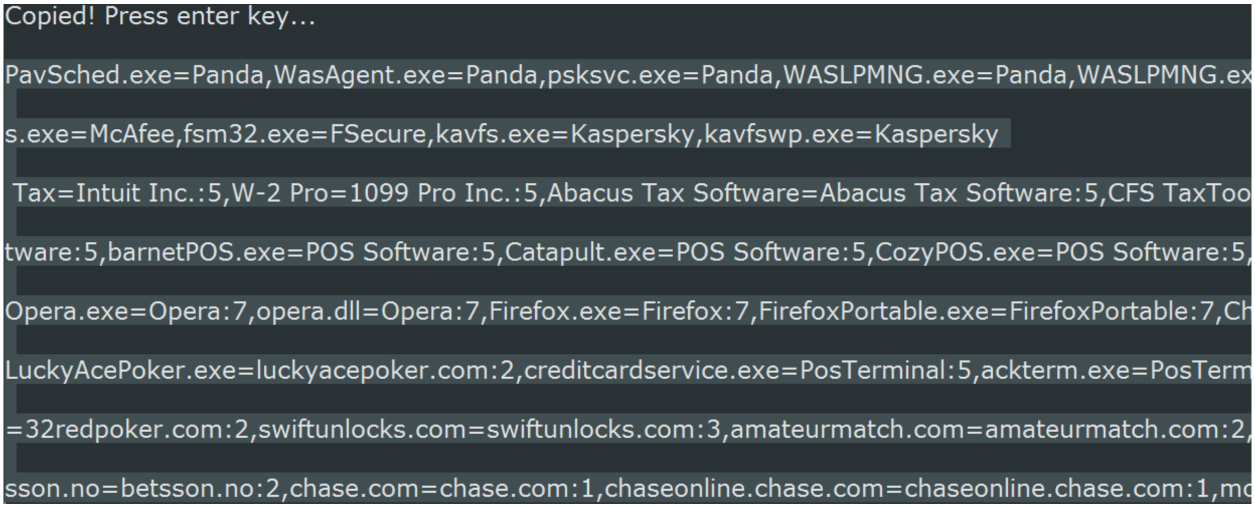
We were able to find several versions of “SysScan”, listed below by their MD5s:

- `fac495be1c71012682ebb27092060b43`
- `e8cc69231e209db7968397e8a244d104`
- `a53847a51561a7e76fd034043b9aa36d`
- `e8691fa5872c528cd8e72b82e7880e98`
- `F661b50d45400e7052a2427919e2f777`

The “SysScan” tool connects to a C&C server in order to report information about the system once it is executed. The information reported includes:

- Server_ID, Username
- Windows version
- System Language
- if system is 64 bits or not
- size of installed memory
- CPU type
- if ports 25 and 80 are open
- if the system is virtual or physical
- what type of VM software is used
- Antivirus software, if any

Then it checks the server´s upload and download speeds using a set of speed-check scripts.
Finally, it checks what kind of software is installed in the system (see the list of available software above).



```
Copied! Press enter key...

PavSched.exe=Panda,WasAgent.exe=Panda,psksvc.exe=Panda,WASLPMNG.exe=Panda,WASLPMNG.ex

s.exe=McAfee,fsm32.exe=FSecure,kavfs.exe=Kaspersky,kavfswp.exe=Kaspersky

 Tax=Intuit Inc.:5,W-2 Pro=1099 Pro Inc.:5,Abacus Tax Software=Abacus Tax Software:5,CFS TaxToo

tware:5,barnetPOS.exe=POS Software:5,Catapult.exe=POS Software:5,CozyPOS.exe=POS Software:5,

Opera.exe=Opera:7,opera.dll=Opera:7,Firefox.exe=Firefox:7,FirefoxPortable.exe=FirefoxPortable:7,Ch

LuckyAcePoker.exe=luckyacepoker.com:2,creditcardservice.exe=PosTerminal:5,ackterm.exe=PosTerm

=32redpoker.com:2,swiftunlocks.com=swiftunlocks.com:3,amateurmatch.com=amateurmatch.com:2,

sson.no=betsson.no:2,chase.com=chase.com:1,chaseonline.chase.com=chaseonline.chase.com:1,mc
```

Figure 11. Example of software information gathered

After gathering all this information, the SysScan tool encrypts it with AES using a hardcoded derived password (- k8iJGx3oGo) and posts the data to the C&C in the /manual_result path.

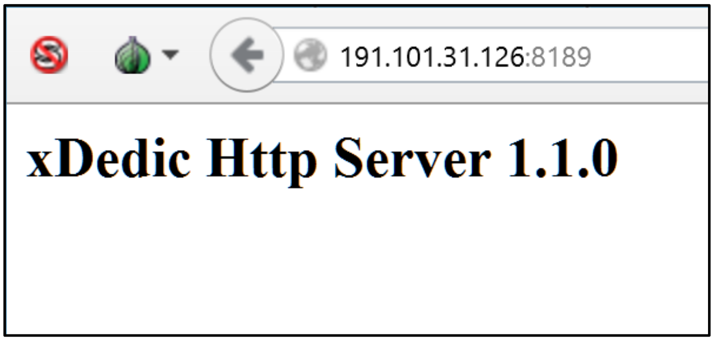
This tool also checks if the RDP service is available and patches it if needed. It also adds the following modifications to the Windows registry:

```
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v
UserAuthentication /t REG_DWORD /d

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-
Tcp" /v UserAuhentication /t REG_DWORD /d 1 /f& reg delete

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
legalnoticecaption /f& reg delete

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
legalnoticetext /f
```

The following is a list of all the known C&Cs that Syscan uses to send its results:

- http://37.49.224[.]144:8189/manual_result
- http://37.49.224[.]144/ptest.php
- http://37.49.224[.]144/sp.php
- http://37.49.224[.]144/test_servers.xml
- http://37.49.224[.]144/gfileset.php
- hxxp://5.56.133[.]145
- http://191.101.31[.]126/ptest.php
- http://191.101.31[.]126/sp.php
- http://191.101.31[.]126/test_servers.xml
- http://191.101.31[.]126/gfileset.php
- http://191.101.31[.]126:8189/manual_result

Interestingly, the C&C server at 191.101.31[.]126 has a very specific banner on port 8189:



191.101.31.126:8189

xDedic Http Server 1.1.0

Figure 12. xDedic C&C banner

Hacking the servers

When we started our investigation, the assumption was that xDedic partners use brute-forcing attacks in order to get access to the servers they control. On a machine where the xDedic validator tool (sysscan.exe) was detected, we also found tools that specialized in performing brute-force attacks against RDP servers, such as DUBrute and XPC (detected as Hacktool.Win32.Bruteforce). Later, we were able to confirm this hypothesis with one of the victims.

The SCCLIENT Trojan

Thanks to a partner in our investigation, we were able to analyse a server that had been hacked and put up for sale on the xDedic market. This section provides some information about the very interesting malware found on it.

Once the server was compromised by the attackers through RDP password brute-forcing, they installed a custom piece of malware in the path "/Windows/System32/scclient.exe" and registered it as a service that would start automatically upon system boot. Interestingly, the attackers also installed bitcoin-mining software, to use the idle time while they waited for a buyer for the server.

This SCClient Trojan connects to one of eight C&C servers:

- q968787.ignorelist[.]com:32973
- q968787.mooo[.]com:32973
- q968787.homenet[.]org:32973
- q968787.strangled[.]net:32973 - SINKHOLED by Kaspersky Lab
- q96b7b7.ignorelist[.]com:32973 - SINKHOLED by Kaspersky Lab
- q96b7b7.mooo[.]com:32973 - SINKHOLED by Kaspersky Lab
- q96b7b7.homenet[.]org:32973 - SINKHOLED by Kaspersky Lab
- q96b7b7.strangled[.]net:32973 - SINKHOLED by Kaspersky Lab

We were able to sinkhole five of them, which allowed us to collect information about other hacked servers running the same malware. During the first 12 hours, we received connections from over 3600 unique IPs.

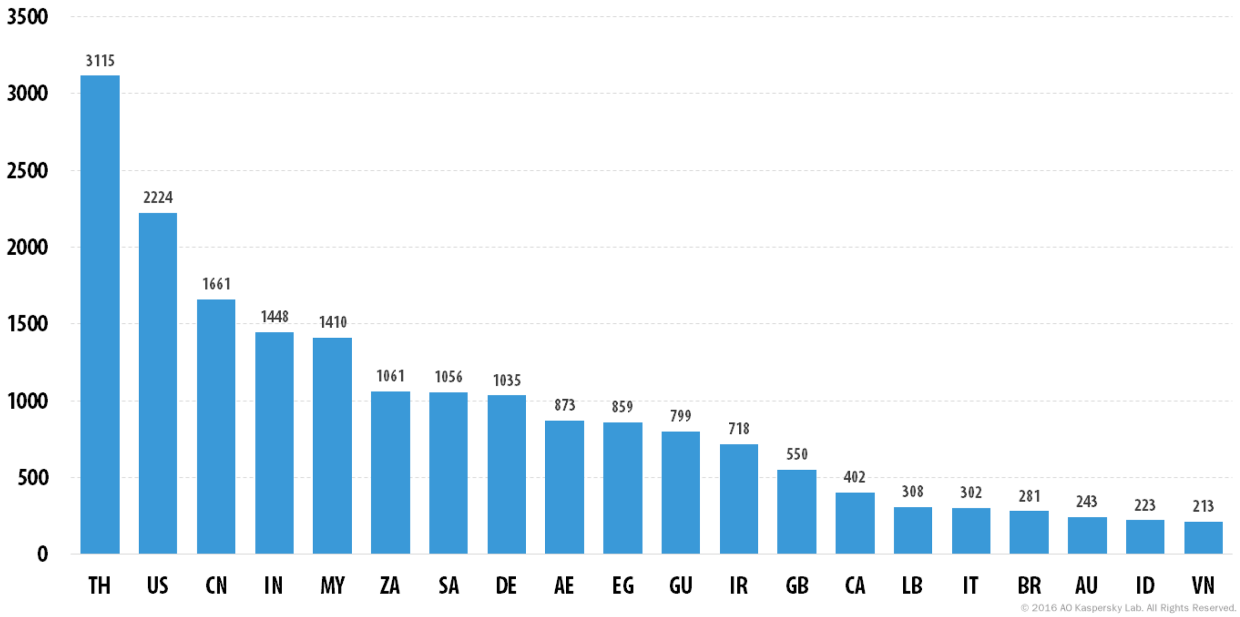
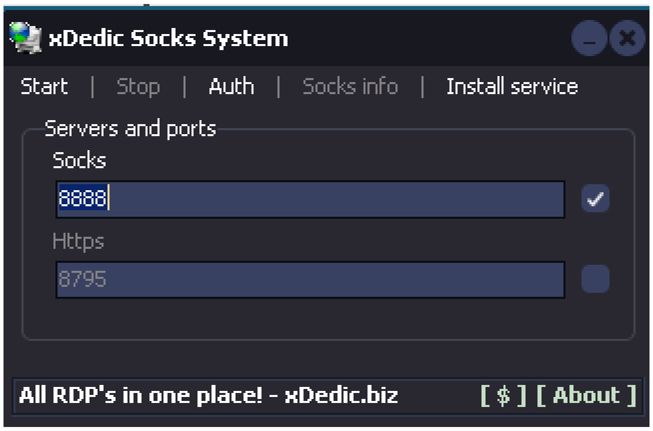


Figure 13. Victim servers hitting our sinkhole during the first 12 hours

We were able to identify some high profile victims such as Governmental entities and universities. During the investigation, we worked with several partners which allowed us to notify some of the victims about the infections in their networks.

xDedic Socks System tool

In one of the topics opened by the xDedic team in the forum vor[.]ac, another piece of software was introduced. They call it the **xDedic Socks System**:


xDedic Socks System
Start | Stop | Auth | Socks info | Install service
All RDP's in one place! - xDedic.biz [$] [About]

Servers and ports
Socks
8888 ☑
Https
8795 □

Figure 14. xDedic Socks System tool

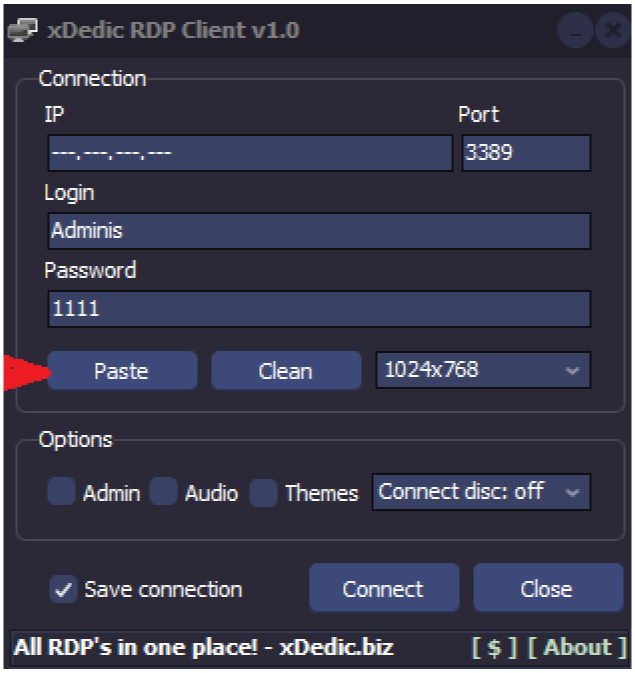
This is actually a wrapper for a popular proxy tool known as “3proxy tiny proxy”. The xDedic Socks System can install the 3proxy tool in the system with the click of a button.

The tool basically opens the chosen ports (by default 8975 for SOCKS and 8795 for HTTPS) on the infected server, turning it into a SOCKS or HTTPS proxy, with or without password-protection.

The tool could be run as a service. In order to do that, it simply drops an instance of 3proxy as \AppData\Local\Temp\pxsrvc\pxsrvc.exe and runs it with “shell execute” as a process or service, with portnames set by the user via GUI.

xDedic RDP Client

The xDedic team also developed their own RDP Client for Windows:



xDedic RDP Client v1.0

Connection

IP: ---.---.---.---

Port: 3389

Login: Adminis

Password: 1111

Resolution: 1024x768

Options

□ Admin □ Audio □ Themes

Connect disc: off

☑ Save connection

All RDP's in one place! - xDedic.biz

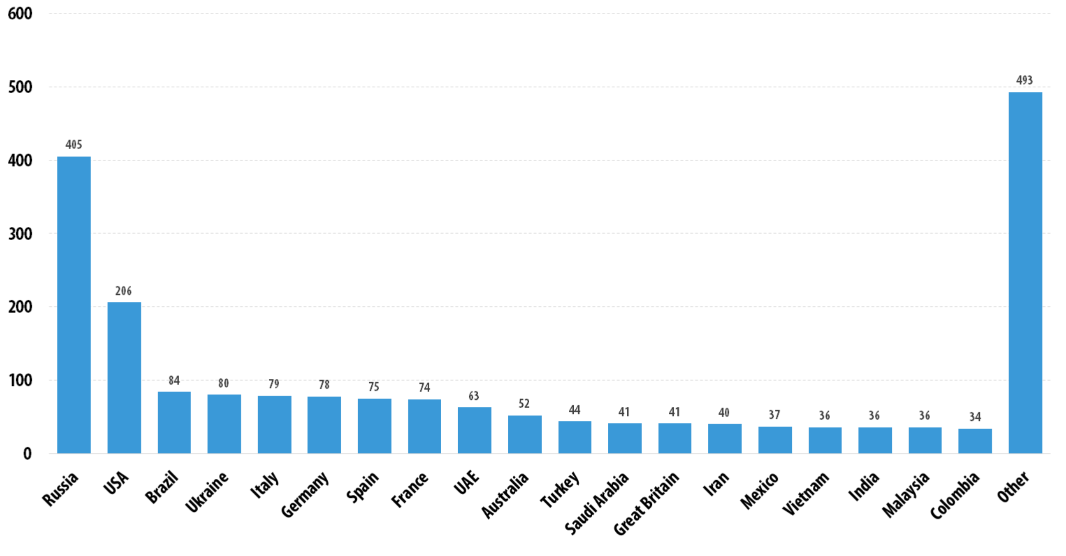
Figure 15. xDedic RDP client

According to them:
“xDedic RDP Client is primarily designed to make life easier for our customers. Copying ip, login, password into a rdp conection window takes long time. Now just go to your purchase history, and click "Copy" on the contrary the server to which you want to log in. Then switch to program, press the button "Paste", information about RDP will be inserted into the fields, then simply press a Connect button.”

xDedic tools: KSN statistics

We were able to get statistical information about the geographical distribution of all the xDedic tools described above from Kaspersky Security Network.

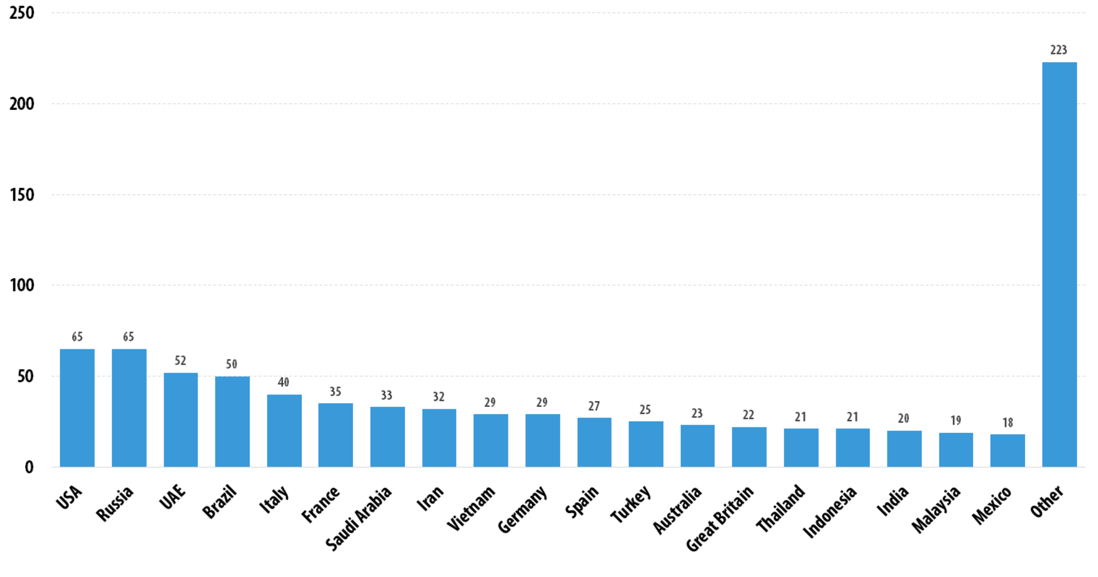
The first chart provides the geographical distribution based on all detections:



© 2016 AO Kaspersky Lab. All Rights Reserved.

Figure 16. xDedic detections, geographical distribution

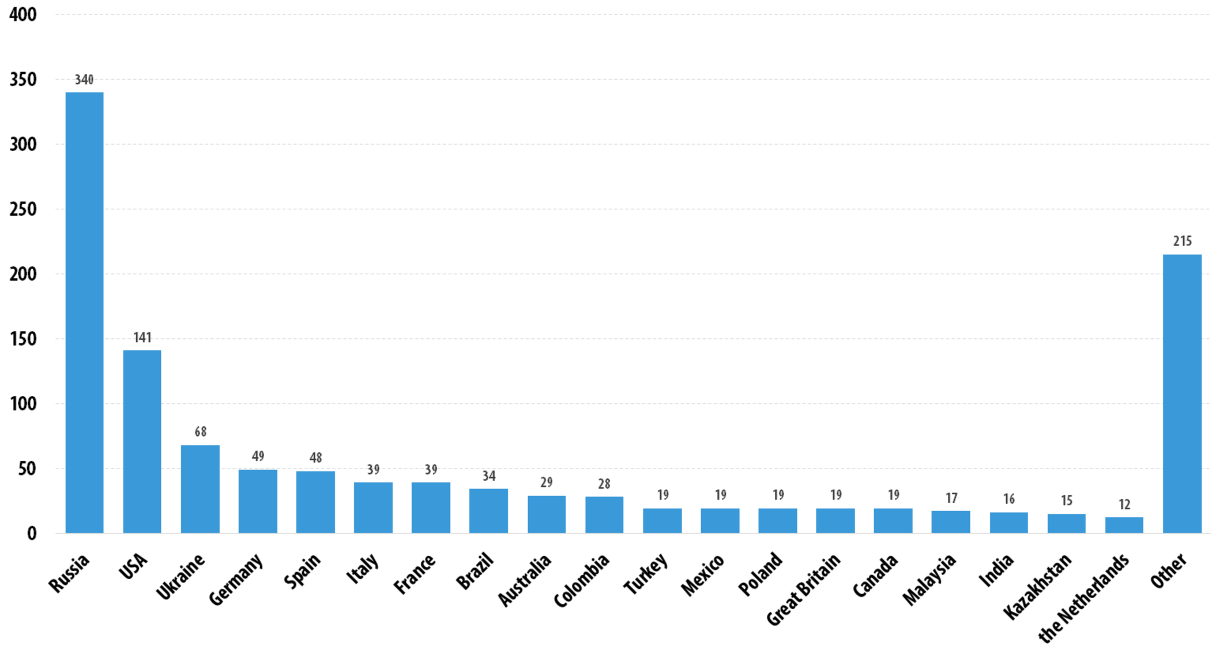
The second chart provides geographical detection for servers:



© 2016 AO Kaspersky Lab. All Rights Reserved.

Figure 17. xDedic server detections, geographical distribution

The final chart provides geographical detection based on desktop detections:



© 2016 AO Kaspersky Lab. All Rights Reserved.

Figure 18. xDedic desktop detections, geographical distribution

As can be seen above, there are more detections on desktop users than on servers, as antivirus is much more popular on desktops.

Detections of xDedic tools on servers prevail in three regions: Europe, US and Middle East. In total we found these tools on servers from more than 50 different countries.

Desktop detection statistics are very interesting in two countries: Russia and Ukraine. This supports the theory that this service was initially founded by Russian-speaking people.

Kaspersky Labs products detect this set of tools as Hacktool.Win32.Rpdpatch.gen

Attribution

The Whois for the xdedic[.]biz (хдедик) domain is registered to:

```
Registrant Name:           Mikhail Mikhail
Registrant Organization:   Mikhail
Registrant Address1:       str.Molova 21
Registrant City:           Moscow
Registrant State/Province: Moscow
Registrant Postal Code:    193350
Registrant Country:         Russian Federation
Registrant Country Code:    RU
Telephone:                  78122842923
Fax:                        78122842923
Created:                    09/11/2014
Expired:                    09/10/2016
Email:                      support@e-investhost.com
```

and currently resolves to:

- 104.28.18.107 (CloudFlare)
- 104.28.19.107 (CloudFlare)

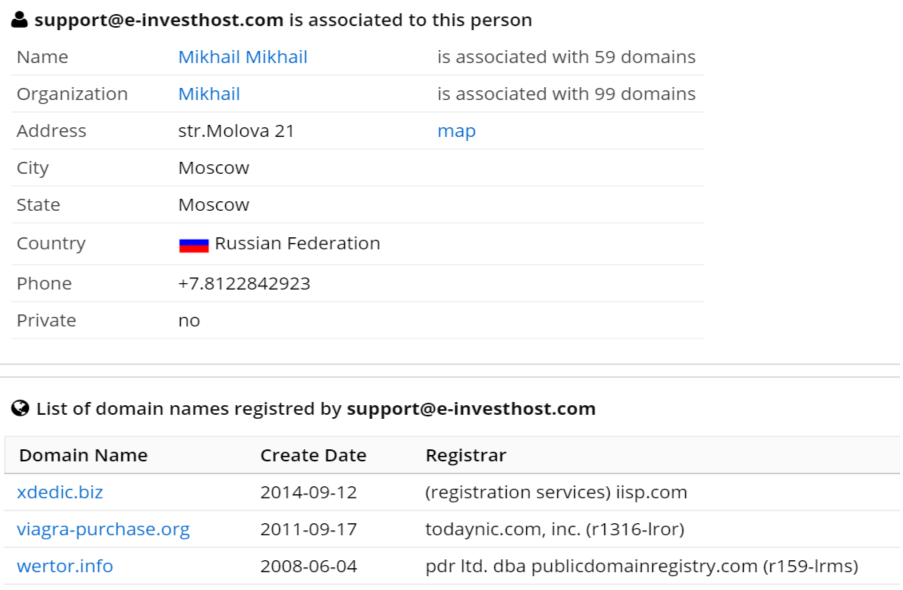
Last year the forum was hosted on a different IP which was found via Passive DNS. The following IPs appear to point to the forum backends behind CloudFlare:

- 144.76.82.238 (Apache web server, shared hosting, old), Hetzner AG, Germany
- 136.243.130.185 (nginx), Hetzner AG, Germany.
  - Content from latest xdedic[.]biz confirmed from the server certificate.

```
Server certificate:
subject: C=AU; ST=Some-State; O=Internet Widgits Pty Ltd; CN=xdedic.biz;
emailAddress=qwe@xdedic.biz <mailto:emailAddress=qwe@xdedic.biz>
start date: 2015-12-08 14:26:01 GMT
expire date: 2016-12-07 14:26:01 GMT
issuer: C=AU; ST=Some-State; O=Internet Widgits Pty Ltd; CN=xdedic.biz;
emailAddress=qwe@xdedic.biz <mailto:emailAddress=qwe@xdedic.biz>
SSL certificate verify result: self signed certificate (18), continuing anyway.
```

The service also provides a Jabber server for support, running on xdedic[.]tk (87.236.215[.]18).
This server (87.236.215[.]18) is known for spreading malware in the past.

The previous email at e-investhost[.]com was also used to register other domains, such as Xdedic[.]biz, viagra-purchase[.]org, wertor[.]info, omerta[.]cc, pharmaplus[.]biz, qualitypillsnorx[.]com. The person behind them uses different Russian addresses and telephone numbers.



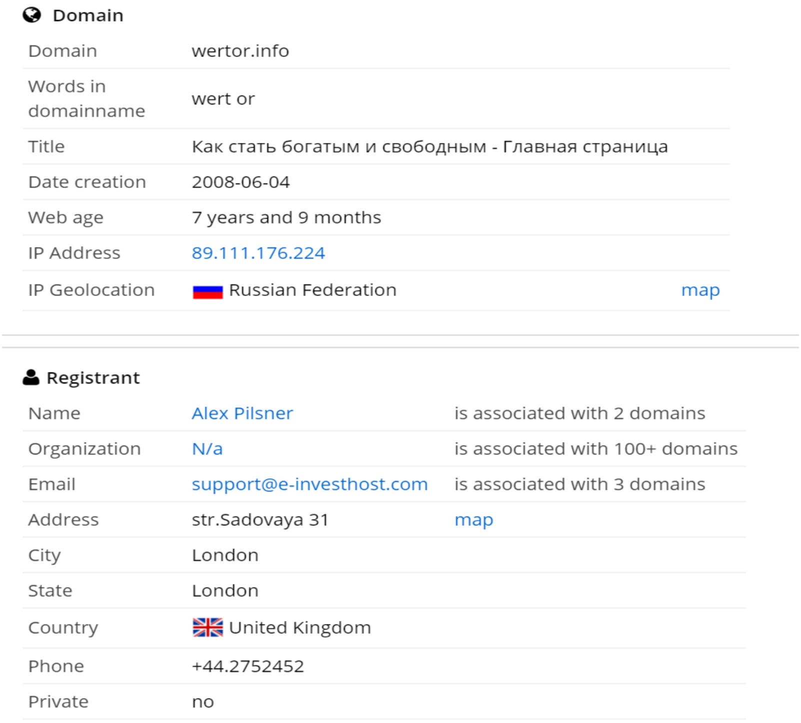
support@e-investhost.com is associated to this person

Name	Mikhail Mikhail	is associated with 59 domains
Organization	Mikhail	is associated with 99 domains
Address	str.Molova 21	map
City	Moscow	
State	Moscow	
Country	Russian Federation	
Phone	+7.8122842923	
Private	no	

List of domain names registred by **support@e-investhost.com**

Domain Name	Create Date	Registrar
xdedic.biz	2014-09-12	(registration services) iisp.com
viagra-purchase.org	2011-09-17	todaynic.com, inc. (r1316-lror)
wertor.info	2008-06-04	pdr ltd. dba publicdomainregistry.com (r159-lrms)

Wertor[.]info (scam website) and viagra-purchase[.]org domain information provide a different name: Alex Pilsner.



Domain

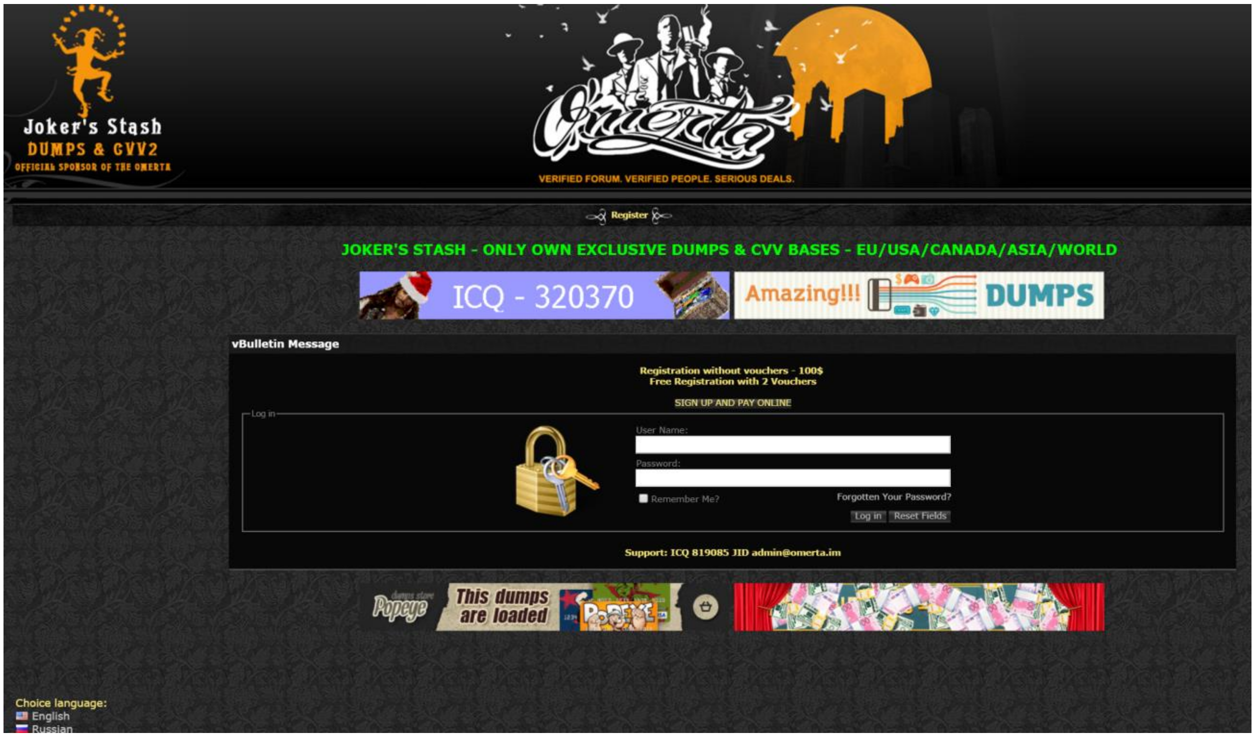
Domain	wertor.info	
Words in domainname	wert or	
Title	Как стать богатым и свободным - Главная страница	
Date creation	2008-06-04	
Web age	7 years and 9 months	
IP Address	89.111.176.224	
IP Geolocation	Russian Federation	map

Registrant

Name	Alex Pilsner	is associated with 2 domains
Organization	N/a	is associated with 100+ domains
Email	support@e-investhost.com	is associated with 3 domains
Address	str.Sadovaya 31	map
City	London	
State	London	
Country	United Kingdom	
Phone	+44.2752452	
Private	no	

Pivoting on this new name, we find a new interesting domain:

```
Domain Name: OMERTA.CC
Registry Domain ID: 96489781_DOMAIN_CC-VRSN
Registrar WHOIS Server: whois.1api.net
Registrar URL: http://www.1api.net
Updated Date: 2016-02-19T07:48:20Z
Creation Date: 2011-03-29T10:46:04Z
Registrar Registration Expiration Date: 2018-03-29T10:46:04Z
Registrar: 1API GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@1api.net
Registrar Abuse Contact Phone: +49.68416984x200
Reseller: IISP.com, Inc. iisp.com
Domain Status: ok - http://www.icann.org/epp#OK
Registry Registrant ID:
Registrant Name: Alex Pilsner
Registrant Organization: Private Person
Registrant Street: Sadovaya 27
Registrant City: SPB
Registrant State/Province:
Registrant Postal Code: 193059
Registrant Country: RU
Registrant Phone: +7.81228492929
Registrant Phone Ext:
Registrant Fax: +7.81228492929
Registrant Fax Ext:
Registrant Email: omerta.sup@gmail.com
```



Joker's Stash
DUMPS & CVV2
OFFICIAL SPONSOR OF THE OMERTA
Omerta
VERIFIED FORUM. VERIFIED PEOPLE. SERIOUS DEALS.
Register
JOKER'S STASH - ONLY OWN EXCLUSIVE DUMPS & CVV BASES - EU/USA/CANADA/ASIA/WORLD
ICQ - 320370
Amazing!!! DUMPS
dumps store Popeye
This dumps are loaded
Choice language:
English
Russian

vBulletin Message

Registration without vouchers - 100$
Free Registration with 2 Vouchers

SIGN UP AND PAY ONLINE

Log in

User Name:

Password:

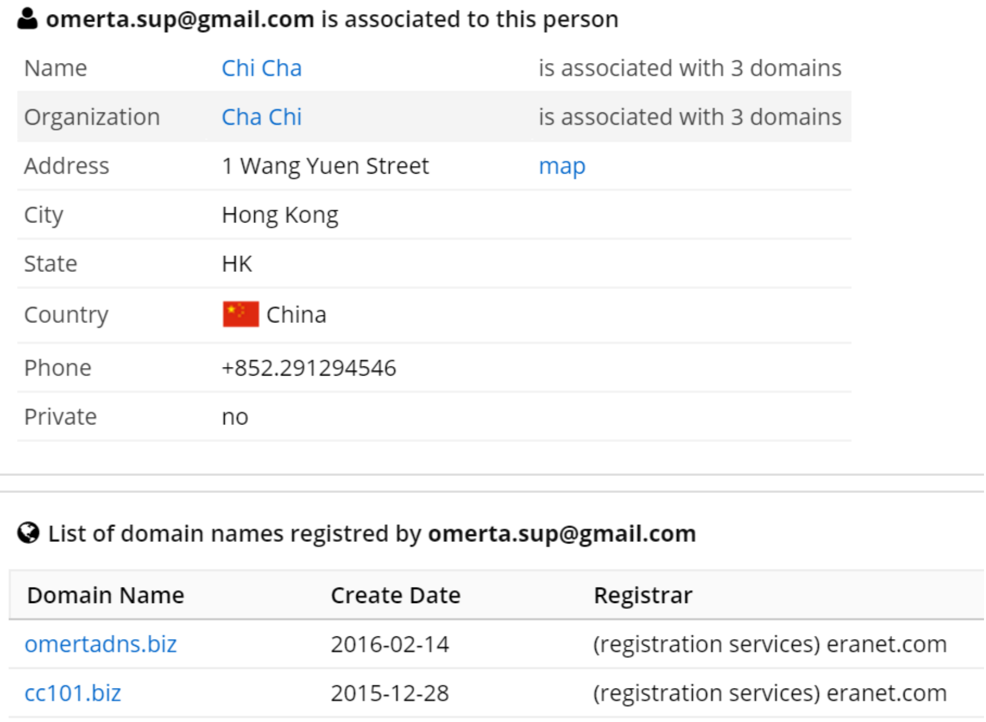
□ Remember Me? Forgotten Your Password?

Log in Reset Fields

Support: ICQ 819085 JID admin@omerta.im

Figure 19. Omerta[.]cc – A carders forum

With the new Omerta email address we find yet more new domains and a new alias (Chi Cha):



omerta.sup@gmail.com is associated to this person

Name	Chi Cha	is associated with 3 domains
Organization	Cha Chi	is associated with 3 domains
Address	1 Wang Yuen Street	map
City	Hong Kong	
State	HK	
Country	China	
Phone	+852.291294546	
Private	no	

List of domain names registred by **omerta.sup@gmail.com**

Domain Name	Create Date	Registrar
omertadns.biz	2016-02-14	(registration services) eranet.com
cc101.biz	2015-12-28	(registration services) eranet.com

Regarding the domain used in the original registration email, the website “E-Investhost[.]com” is a well-known bullet-proof hosting site for Russian cybercriminals. An excerpt from the website description (translated from Russian):

“BulletProof Hosting - for hyip, surf, warez, adult websites DDOS Protection (DDOS protection). Protect your site, coordinate already under DDOS attack! We register Abuse-resistant domains (blocking probability is minimal)”.

Conclusion

The existence of shady forums dedicated to cybercrime is old news. However, it is interesting to see how the main focus of cybercriminals has changed over the last few years, the high degree of specialization achieved by the administrators of the forums and what the relevance of such services might be in the era of APTs.

We will start with the last point. The vast amount of servers for sale on the xDedic marketplace offers a very likely alternative for APT actors with low resources, willing to fly under the radar or having difficulties in getting a foothold in any of its victims. 8 USD is a very cheap price to pay for full access to potential high profile targets. Usually overlooked, servers that have been hacked using brute-force methods might present an opportunity for APT actors that doesn’t arouse suspicion.

Other than the implications for APTs, the marketplace´s statistics show a consistent number of servers available for sale in very different locations. The tagging system makes it easy for opportunistic attackers to find new targets according to their needs, and the bitcoin mining might be a nice side-line for the criminals.

All in all, not only can this successful model be easily replicated, but we expect to see even more specialized marketplaces appear where APT-as-a-service becomes a reality.

Appendix I – Indicators of Compromise

Hashes

SysScan

```
fac495be1c71012682ebb27092060b43
e8cc69231e209db7968397e8a244d104
a53847a51561a7e76fd034043b9aa36d
e8691fa5872c528cd8e72b82e7880e98
F661b50d45400e7052a2427919e2f777
```

Registry entries

```
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v
UserAuthentication /t REG_DWORD /d

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-
Tcp" /v UserAuhentication /t REG_DWORD /d 1 /f& reg delete

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
legalnoticecaption /f& reg delete

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
legalnoticetext /f
```

C&Cs

```
http://37.49.224[.]144:8189/manual_result
http://37.49.224[.]144/ptest.php
http://37.49.224[.]144/sp.php
http://37.49.224[.]144/test_servers.xml
http://37.49.224[.]144/gfileset.php
hxxp://5.56.133[.]145
http://191.101.31[.]126/ptest.php
http://191.101.31[.]126/sp.php
http://191.101.31[.]126/test_servers.xml
http://191.101.31[.]126/gfileset.php
http://191.101.31[.]126:8189/manual_result
q968787.ignorelist[.]com:32973
q968787.mooo[.]com:32973
q968787.homenet[.]org:32973
q968787.strangled[.]net:32973    - SINKHOLED by Kaspersky Lab
q96b7b7.ignorelist[.]com:32973   - SINKHOLED by Kaspersky Lab
q96b7b7.mooo[.]com:32973         - SINKHOLED by Kaspersky Lab
q96b7b7.homenet[.]org:32973            - SINKHOLED by Kaspersky Lab
q96b7b7.strangled[.]net:32973    - SINKHOLED by Kaspersky Lab
```

SCCLIENT installation file path

```
%SystemRoot%\System32\scclient.exe
```

Yara rules

```
rule xDedic_SysScan_unpacked {

meta:

        author = " Kaspersky Lab"
        maltype = "crimeware"
        type ="crimeware"
        filetype = "Win32 EXE"
        date = "2016-03-14"
        version = "1.0"
        hash = "fac495be1c71012682ebb27092060b43"
        hash = "e8cc69231e209db7968397e8a244d104"
        hash = "a53847a51561a7e76fd034043b9aa36d"
        hash = "e8691fa5872c528cd8e72b82e7880e98"
        hash = "F661b50d45400e7052a2427919e2f777"

strings:

        $a1="/c ping -n 2 127.0.0.1 & del \"SysScan.exe\"" ascii wide
        $a2="SysScan DEBUG Mode!!!" ascii wide
        $a3="This rechecking? (set 0/1 or press enter key)" ascii wide
        $a4="http://37.49.224.144:8189/manual_result" ascii wide

        $b1="Checker end work!" ascii wide
        $b2="Trying send result..." ascii wide

condition:

        ((uint16(0) == 0x5A4D)) and (filesize < 5000000) and
        ((any of ($a*)) or (all of ($b*)))
}


import "pe"

rule xdedic_packed_syscan {
        meta:
                author = "Kaspersky Lab"
                company = "Kaspersky Lab"
        strings:
                $a1 = "SysScan.exe" nocase ascii wide
        condition:
                uint16(0) == 0x5A4D
                and any of ($a*) and filesize > 1000000 and filesize <1200000 and
pe.number_of_sections == 13 and pe.version_info["FileVersion"] contains "1.3.4."
}
```