

Criminal Abuse in RIPE IP space

October 18th, 2018, Amsterdam

Anti-Abuse WG

Dhia Mahjoub, PhD., Head of Security R&D, Cisco Umbrella

RIPE77
Amsterdam, Netherlands
15 - 19 Oct 2018

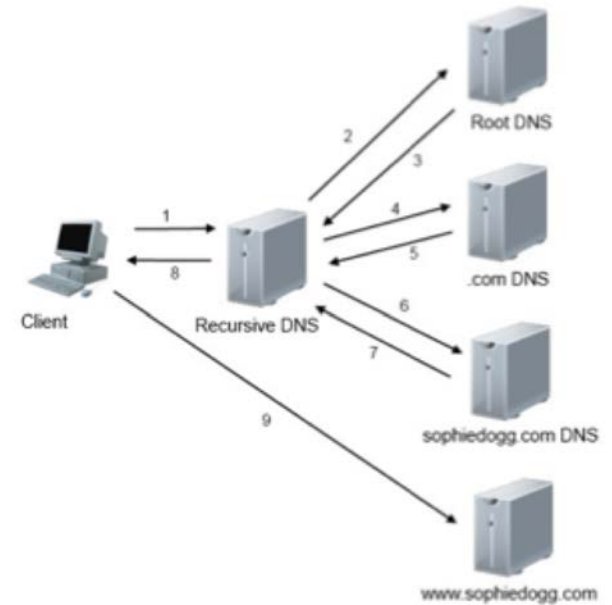
Who am I ?

- * @DhiaLite
- * Head of Security R&D at Cisco Umbrella
- * 15+ years experience in network security, network traffic analysis
- * PhD in graph algorithms applied on sensor networks problems
- * Regular speaker at Black Hat, Defcon, Flocon, Virus Bulletin, NCSC One Conference, FIRST, TF-CSIRT
- * Collaboration with LEAs



Worldwide DNS data

- 30 data centers worldwide, 11 in Europe
- ~150 billion queries a day
- Translates to around 24 TB a day
- Valuable client query information

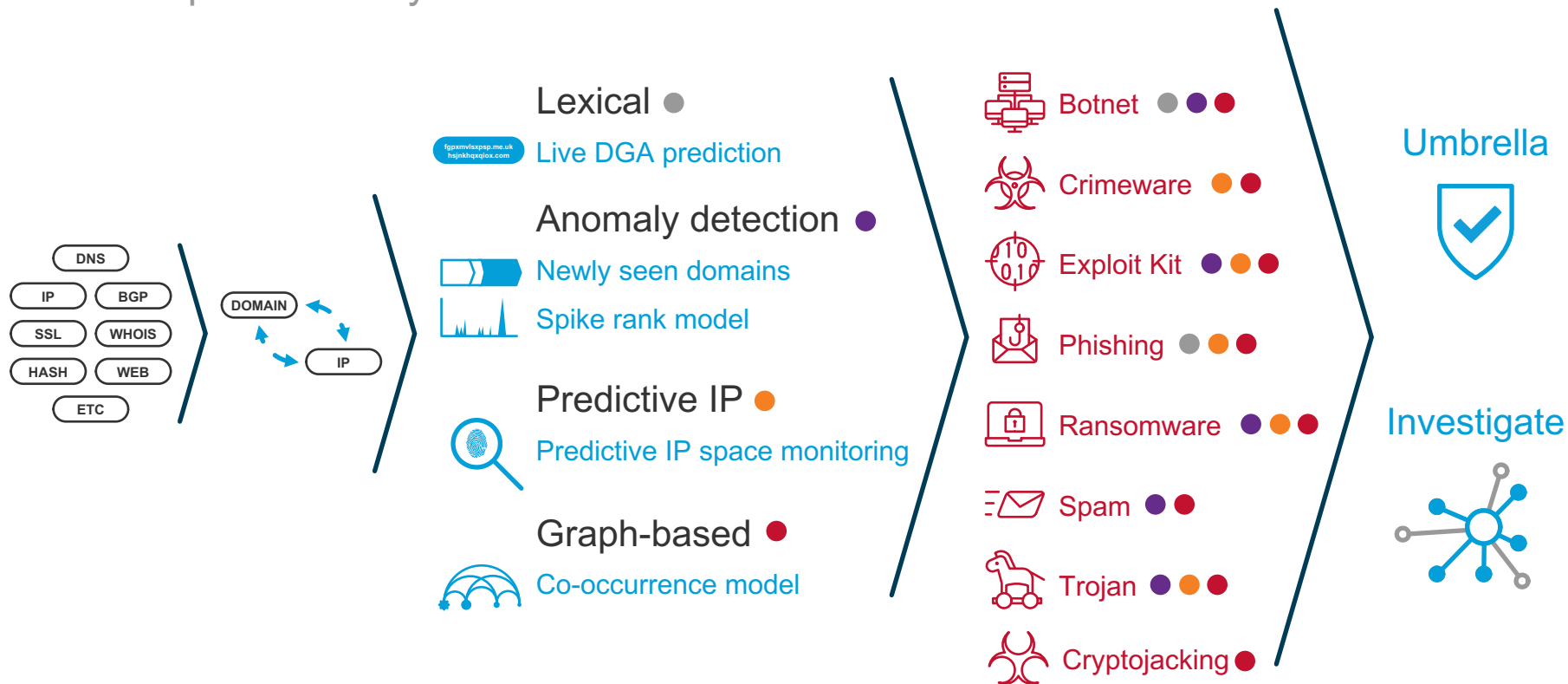


Data center locations



Threat detection at scale

Meta-data pattern analysis at scale



Cyber-crime attacks

IP space

Rogue outgoing traffic

- SSH/wordpress brute-forcing
- Mass scans
- DDoS attacks
- Spam sending

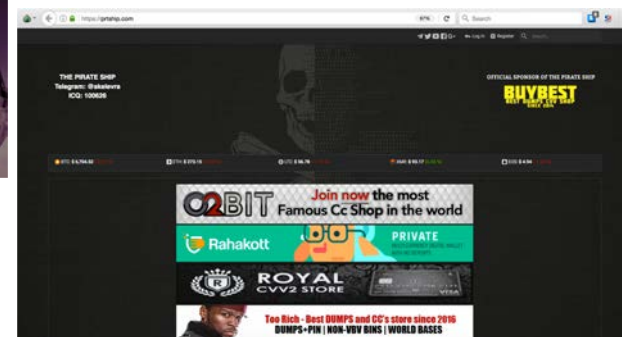
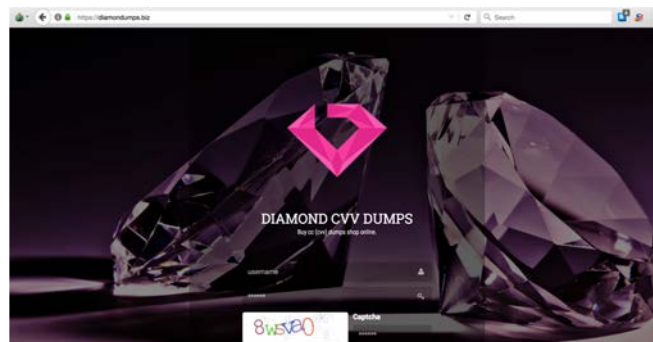
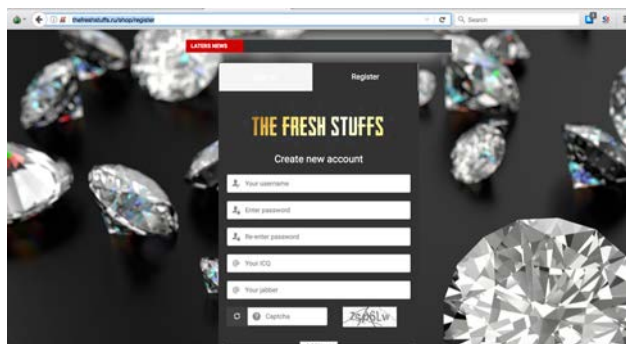


Toxic hosted content

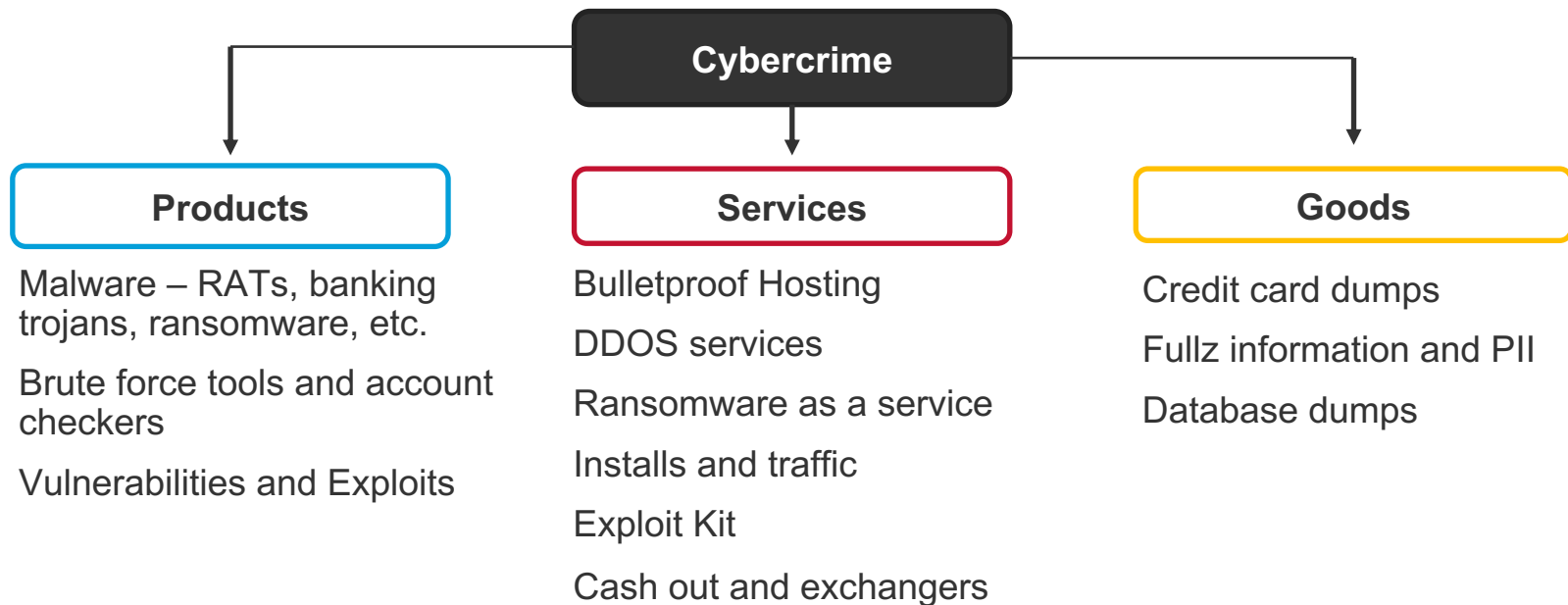


- Malware C2
- Ransomware
- Phishing
- Cybercrime forums
- Stolen credentials marketplaces
- Criminal exchange services
- Criminal jabber servers

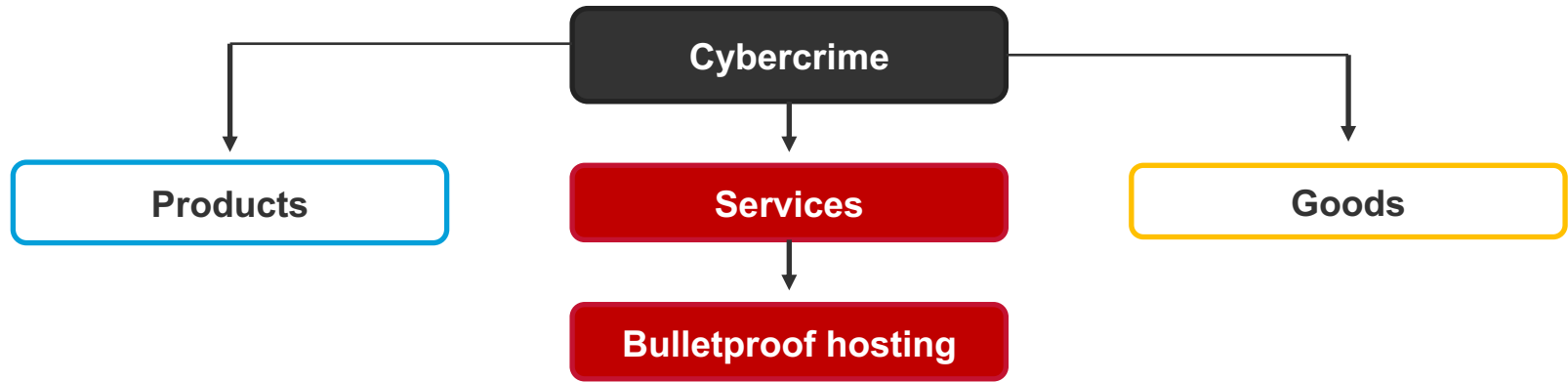




Cybercrime Ecosystem



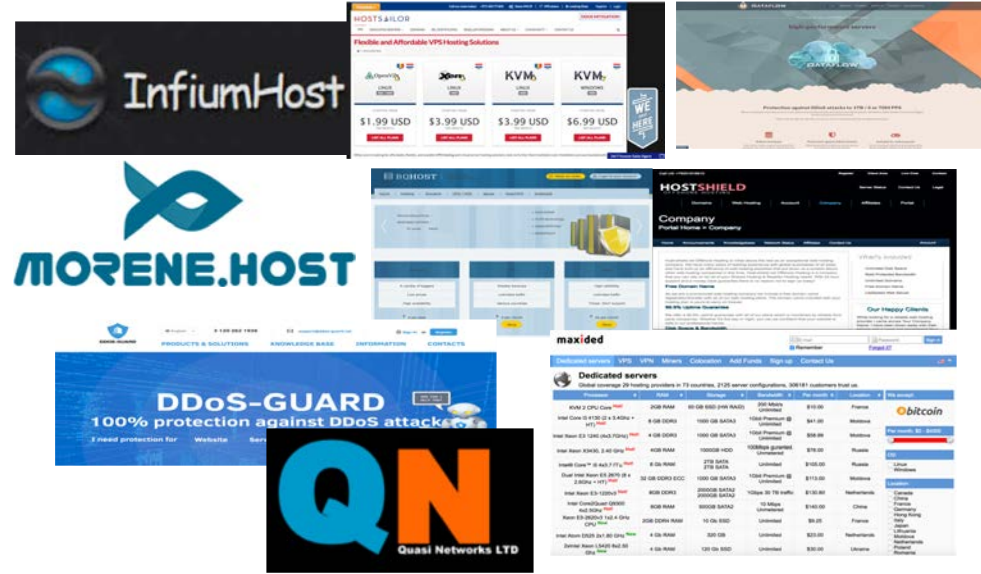
Bulletproof Hosting



Bulletproof hosting provider (BPH)

A criminal hosting provider who shields their customers from abuse complaints and take down action.

Spectrum of Hosting Providers

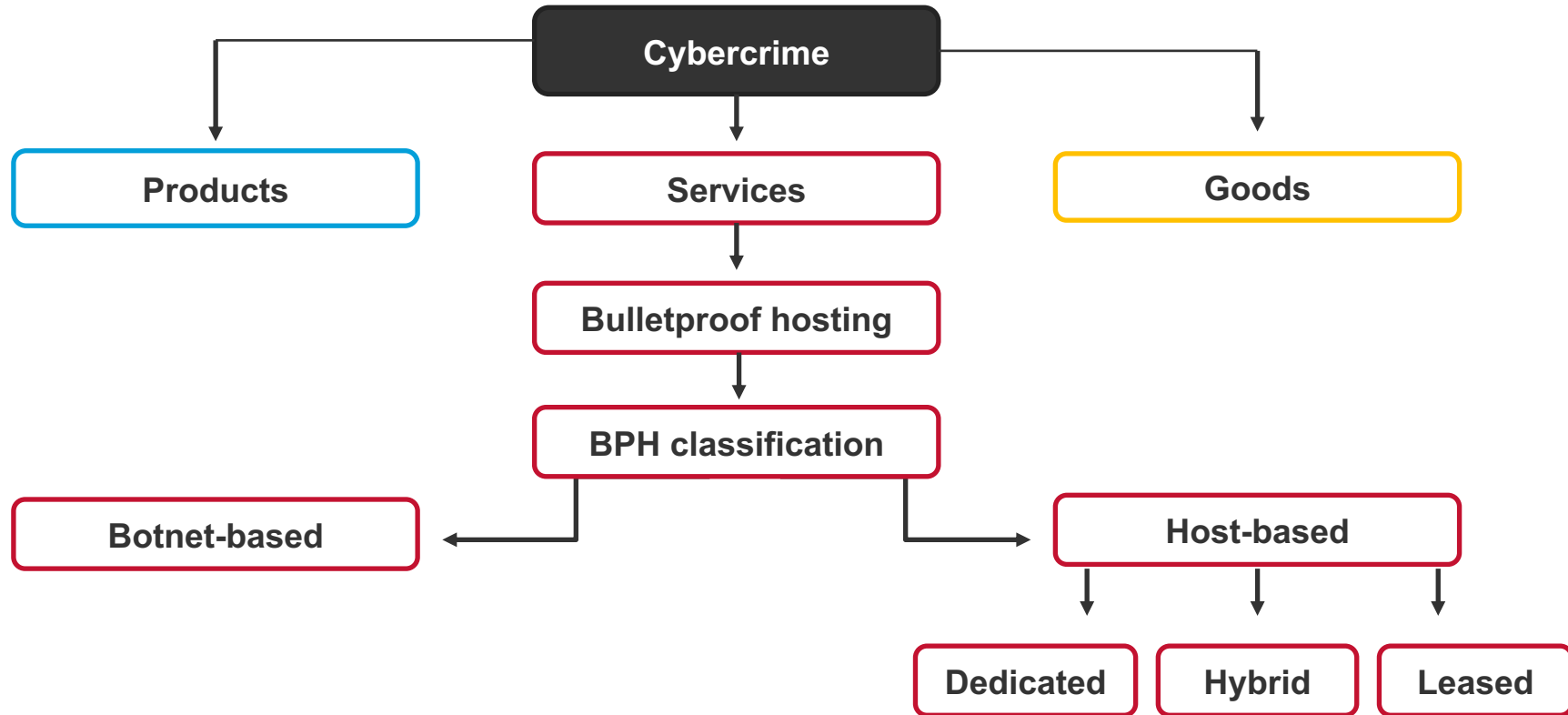


Good

Abused

Bulletproof

A Taxonomy of BulletProof Hosting



Bulletproof Hosting business model

Dedicated hoster recipe

Low barrier of entry (Approx <\$2K)

1. Register business offshore
2. Register own ASN and lease IP space
3. Setup website(s) or stay underground
4. Drive customers – forums (open, closed), social media
5. Generate revenue through hosting or sending traffic
7. Handle abuse
8. Shut down, move elsewhere, repeat

Dedicated BPH technical features

Leaf ASN

Offshore business registration

Anonymous payment methods

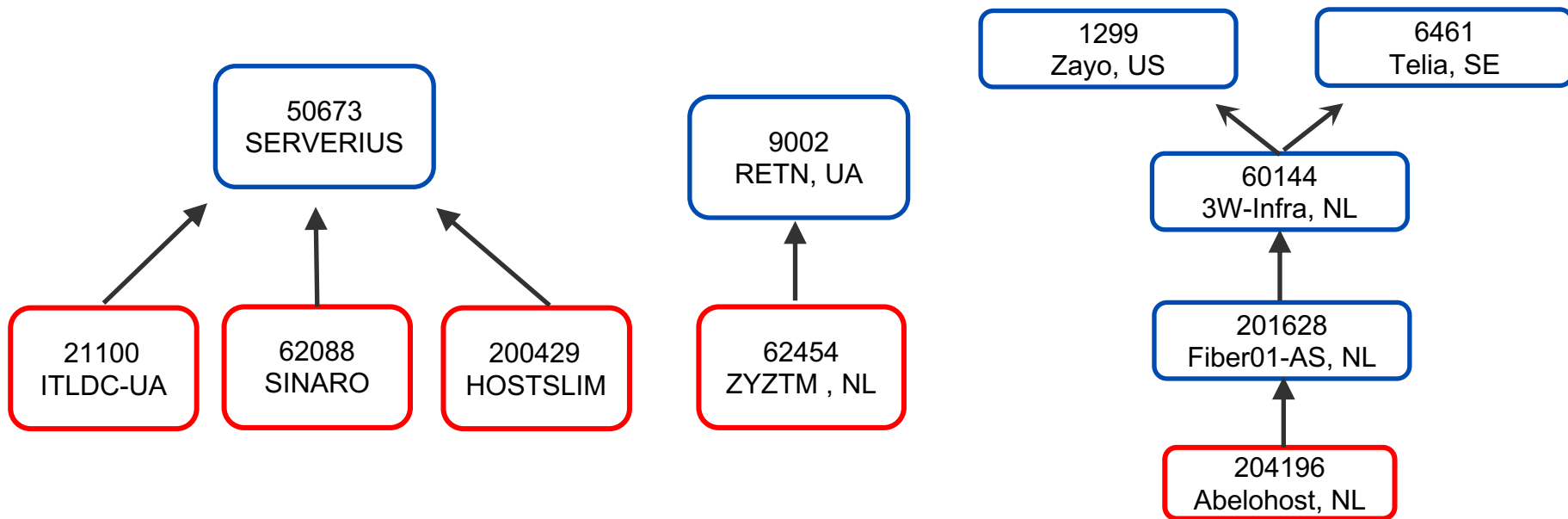


Small IP range

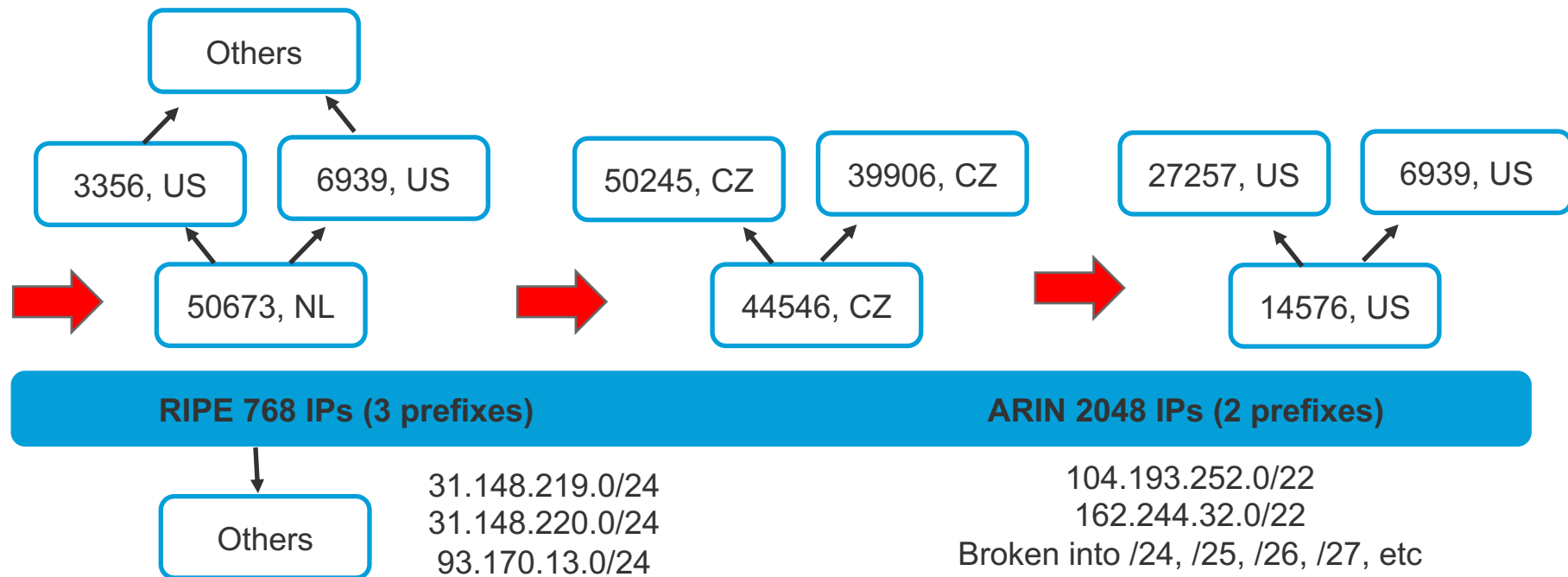
Toxic hosted content or outgoing traffic

Leaf (Stub) ASN or leaf ASNs chain

- Have only upstream peers, no downstream
- Frequent pattern for questionable/bulletproof hosters



1 hosting provider spreading footprint on multiple ASNs



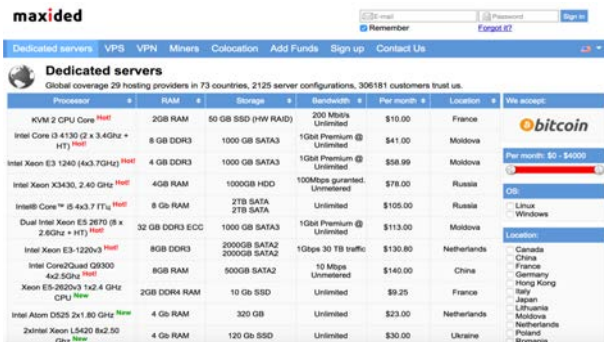
Example: **King Servers:** Serverius - Alfa Telecom - Hosting Solutions

Resellers: 1 ASN used by multiple hosting providers

Worldstream



QHoster website screenshot showing dedicated servers, cPanel hosting, and various services. The main banner advertises Intel Xeon CPUs and 16Gb RAM for \$169.95. Navigation links include CHANEL WEB HOSTING, CHANEL RETAILER HOSTING, VIRTUAL SERVERS (VPS), DEDICATED SERVERS, DOMAINS, and SSL CERTIFICATES. A 'PROMOTIONS' button is visible in the top right.



maxided website screenshot showing a table of dedicated servers. The table lists various configurations including processor, RAM, storage, bandwidth, and location. A Bitcoin logo is visible on the right side of the table.

Processor	RAM	Storage	Bandwidth	Per month	Location	Web accept
KVM 2 CPU Core	20GB RAM	50 GB SSD (H/W RAID)	200 Mbits Unlimited	\$10.00	France	bitcoin
Intel Core i3 4130 (2 x 3.40GHz + HT)	8 GB DDR3	1000 GB SATA3	100M Premium @ Unlimited	\$41.00	Moldova	
Intel Xeon E3 1240 (4x3.70GHz)	4 GB DDR3	1000 GB SATA3	100M Premium @ Unlimited	\$58.99	Moldova	
Intel Xeon X3430, 2.40 GHz	4GB RAM	1000GB HDD	100Mbps guaranteed, Unlimited	\$78.00	Russia	
Intel® Core™ i5-430 7.7Tq	8 Gb RAM	2TB SATA 2TB SATA	Unlimited	\$105.00	Russia	Linux Windows
Dual Intel Xeon E3 2670 (8 x 2.80GHz + HT)	32 GB DDR3 ECC	1000 GB SATA3	100M Premium @ Unlimited	\$113.00	Moldova	
Intel Xeon E3-1220v3	8GB DDR3	2000GB SATA2 2000GB SATA2	10Mbps 30 TB traffic	\$130.80	Netherlands	Location: Canada China France Germany Hong Kong Italy Japan Lithuania Malaysia Netherlands Poland Romania
Intel Core2Quad Q8300	8GB RAM	5000GB SATA2	10 Mbps Unlimited	\$145.00	China	
Xeon E5-2620v3 14x2.4 GHz CPU	20GB DDR4 RAM	10 Gb SSD	Unlimited	\$9.25	France	
Intel Atom D525 2x1.80 GHz	4 Gb RAM	320 GB	Unlimited	\$23.00	Netherlands	
Xeon Xeon L5420 8x2.50 GHz	4 Gb RAM	120 Gb SSD	Unlimited	\$30.00	Ukraine	



EuroHoster website screenshot showing popular tariffs. The table lists various server configurations including processor, RAM, storage, bandwidth, and location. A 'discount' banner is visible on the right side of the table.

Etpu Start-the HDD	Plus is the Green	The Xeon 2.5 of L	The Xeon 3.0 of	T130
the virtual server the private	the dedicated server	the dedicated server	the dedicated server	the dedicated server
Intel Xeon E3-1220v5	AMD Opteron™ 3200	Intel Xeon X3440	Intel Xeon E3-1270	Intel Xeon E3-1240v5
1 x 3.4 GHz	8 x 2.4 GHz	4 x 2.53 GHz	4 x 3.4 GHz	4 x 3.5 GHz
2 GB DDR4 ECC	16 GB DDR3	8 GB DDR3	8 GB DDR3	16 GB DDR4 ECC
100 GB HDD	2 x 2,000 GB HDD	2x 1 TB HDD + 60 GB SSD	2 x 1,000 GB HDD	500 GB HDD
48 Mbit / s	100 Mbit / s	100 Mbit / s	100 Mbit / s	100 Mbit / s

Dedicated BPH technical features

Leaf ASN

Offshore business registration



Anonymous payment methods



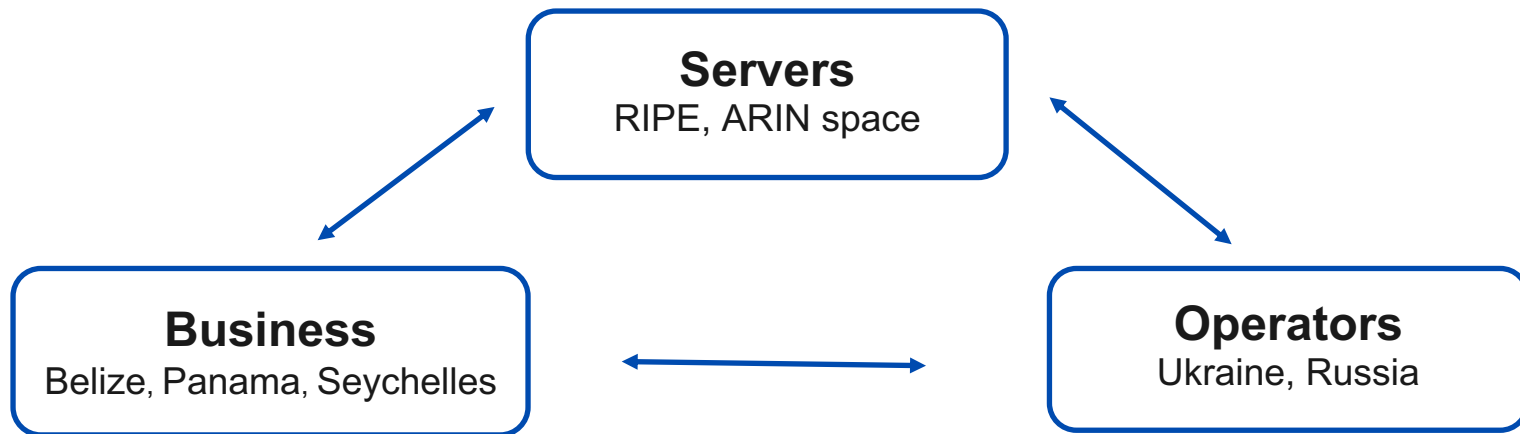
Small IP range

Toxic hosted content or outgoing traffic

Register Business in Offshore Jurisdictions

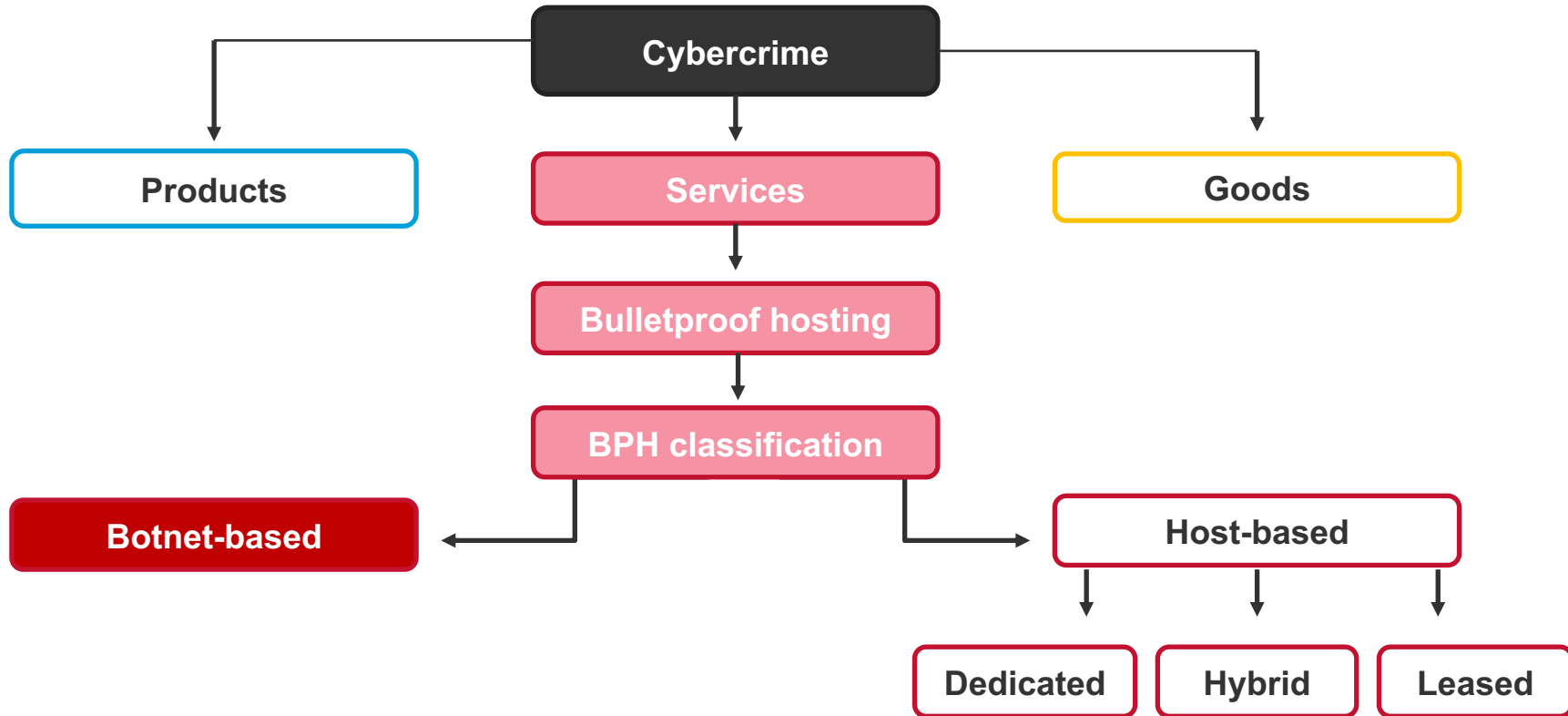


Multiple Layers of Resistance



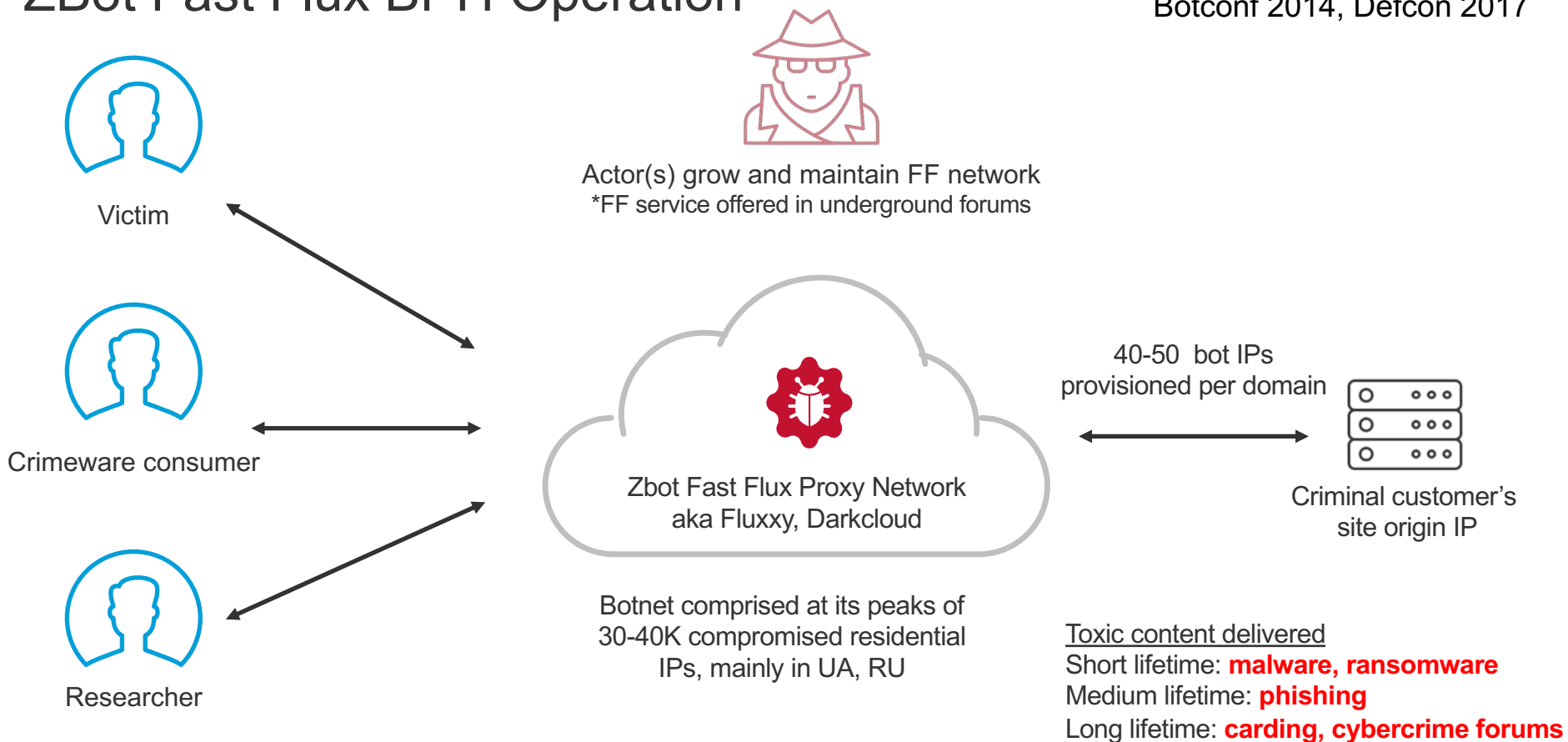
Example BPH operations

Botnet-based BPH

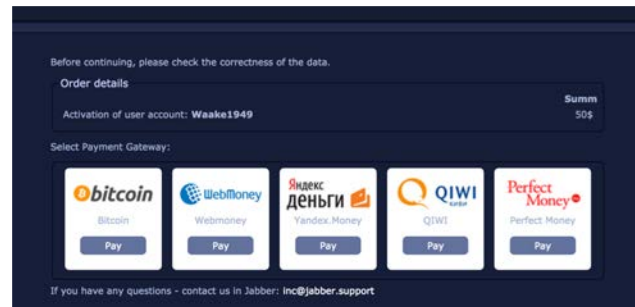
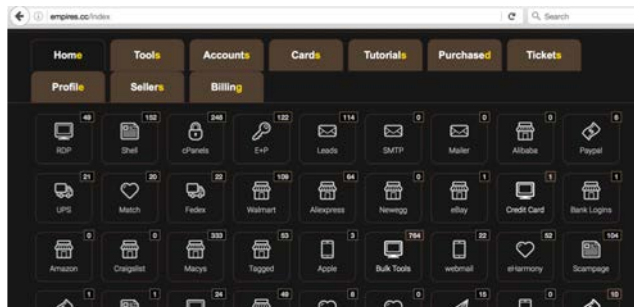
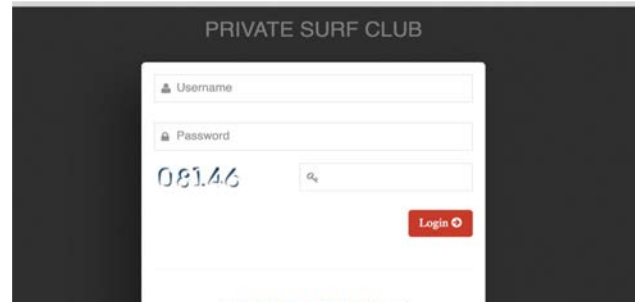
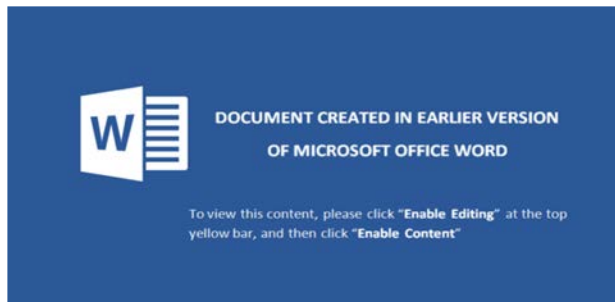


ZBot Fast Flux BPH Operation

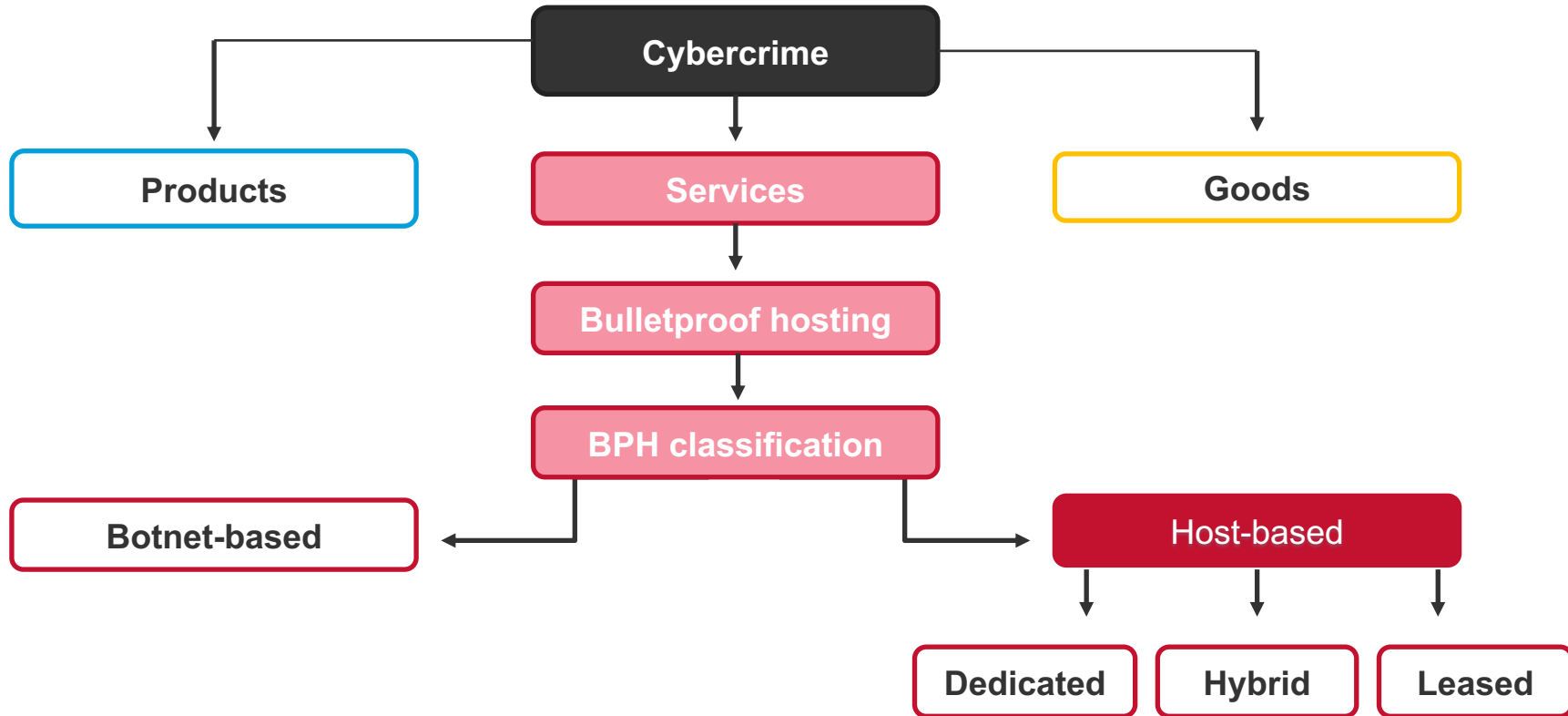
Covered at Black Hat 2014,
Botconf 2014, Defcon 2017



Threats delivered by ZBot Fast Flux proxy network



Host-based BPH



Abuse in Swiss space

HOSTED IN SWITZERLAND

OFFSHORE SERVER HOSTING

Dedicated servers from Private Layer.

OFFSHORE DEDICATED SERVERS

Key Advantages

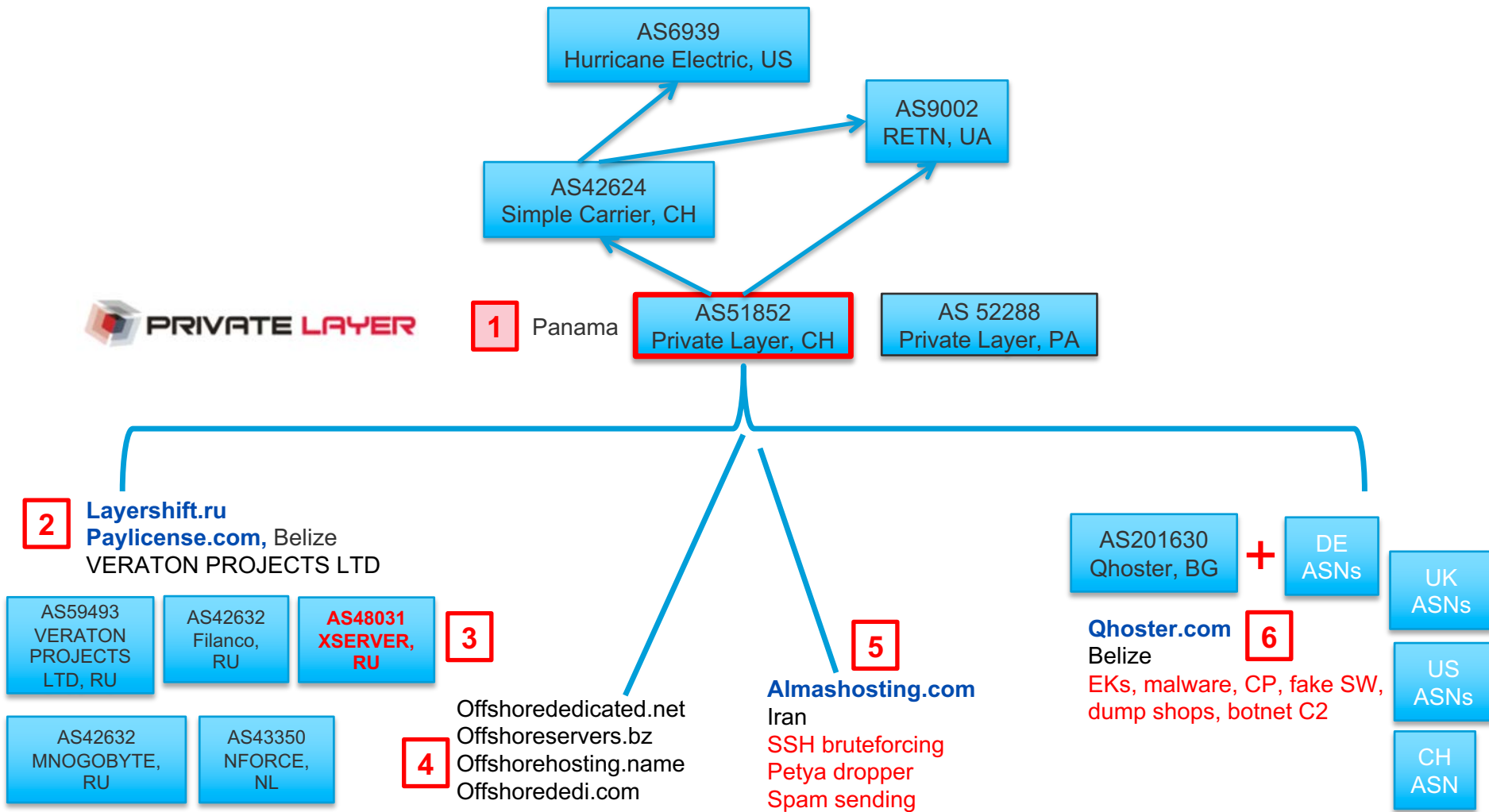


OFFSHORE HOSTING IN A NEUTRAL JURISDICTION

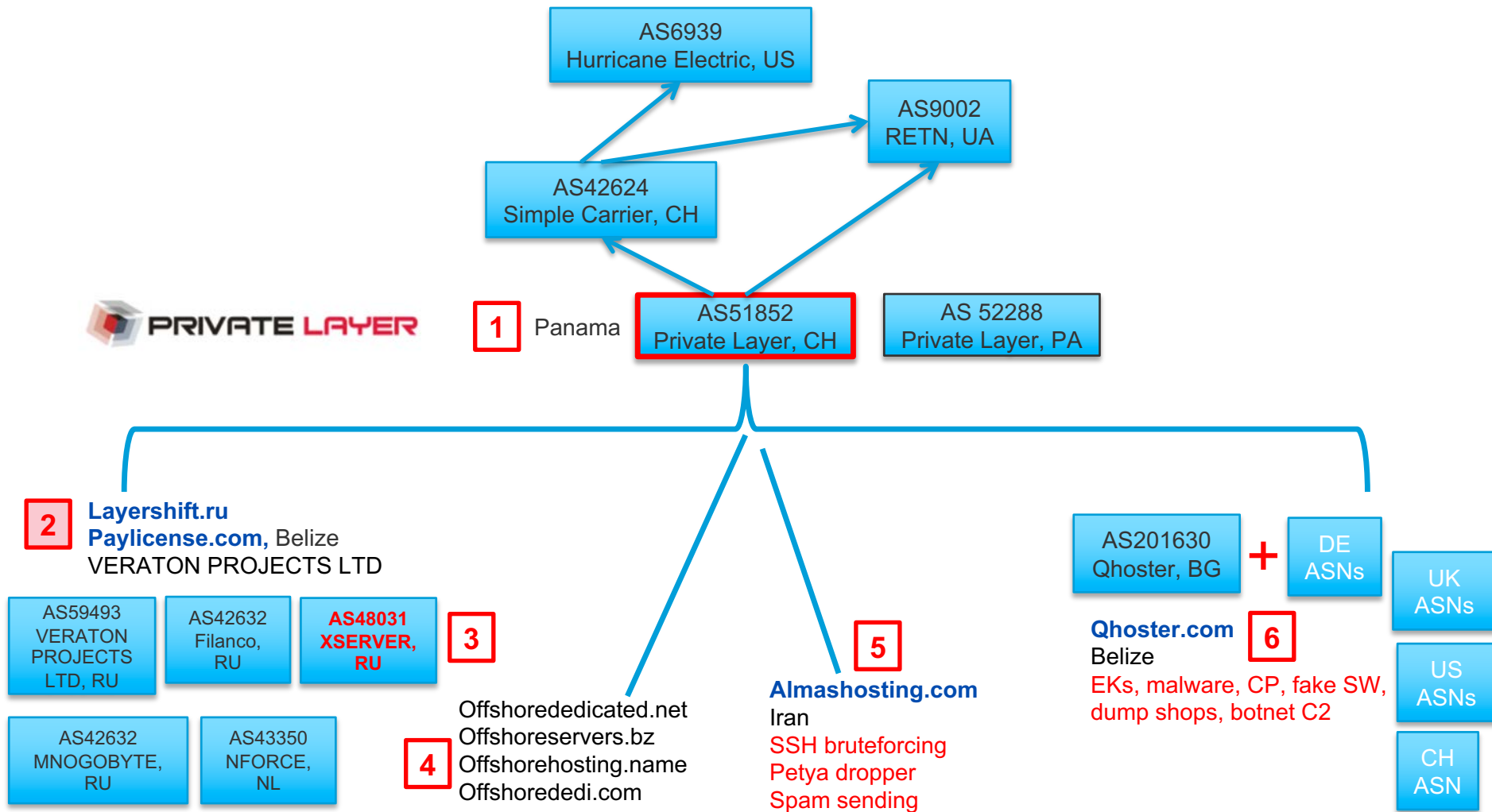
- The US NSA cannot eavesdrop within Switzerland.
- Switzerland has always been recognized as a safe haven.
- Zurich is an Internet hub, providing fast connections.
- Switzerland is protected from natural disasters.
- Private Layer was founded to provide maximum privacy.
- Hosted in the most secure facility in Zurich.
- **Enterprise Hardware - Best Prices!**

Select And Configure Your Offshore Server

Processor/s	Physical Memory	Hard Drives	Bandwidth Transfer	Price / Per Month	
Intel Xeon Westmere 5620	8 GB DDR3	1.00TB SATA	10 TB Premium Bandwidth Transfer	\$229.00	Configure



- Offers anonymous offshore hosting on shared hosting, VPS and dedicated servers
- IP space split between hosting companies operating from Panama, Switzerland, Belize, Russia, Iran





Domains
Software Licenses

Hosting
VPS OpenVZ
About us

VPS KVM

Dedicated

24/7 Tech. support Client Panel



Data center Multibyte (Russia, Moscow)

A company with 9 years of experience in the market of Internet providers and data center operators. It has its own optical network in Moscow and direct connection to all major Russian telecommunications operators.



Data Center Filanco-Datahouse (Ukraine, Kiev)

Data center launched by the group of companies "Filanco" within the framework of the DataHouse.ua project in 2012. An international traffic exchange point is deployed on the site, which ensures fast operation speed with the Russian and European segments.



Data Center ITL (Ukraine, Kharkov)

ITL Group is an international group of companies united under one brand. The main activity of the ITLDC division is the provision of colocation services, lease of dedicated servers and provision of VDS-hosting services.



Data Center Dataplace (Netherlands, Rotterdam)

The data center of Dataplace was developed in 2009. In 2010, has already accepted the first customers. It has all modern security systems, cooling and huge capacities.



The data center of Equinix (Switzerland, Zurich)

The company was founded in 1998. The data center in Zurich has a platform of more than 28 thousand square meters. The data center is certified by ISO9001: 2008 and ISO27001: 2005. Peering with more than 70 Internet providers.



Data Center Parsonline (Iran, Tehran)

The biggest data center is the center in Iran. The technical site is more than 6,5 thousand square meters. Modern equipment, air conditioning and uninterruptible power supplies.

PayLicense

The quality of services is above all. Our team has been working in the IT field for more than 12 years, until 2008 we provided hosting services exclusively for customers from the US and Latin American countries. Since the

PayLicense

Domains
Hosting
VPS OpenVZ
VPS KVM
Dedicated
Software Licenses
SSL Certificates

About us

news
About us
FAQs
Reviews
Data centers
Support
Contact Us

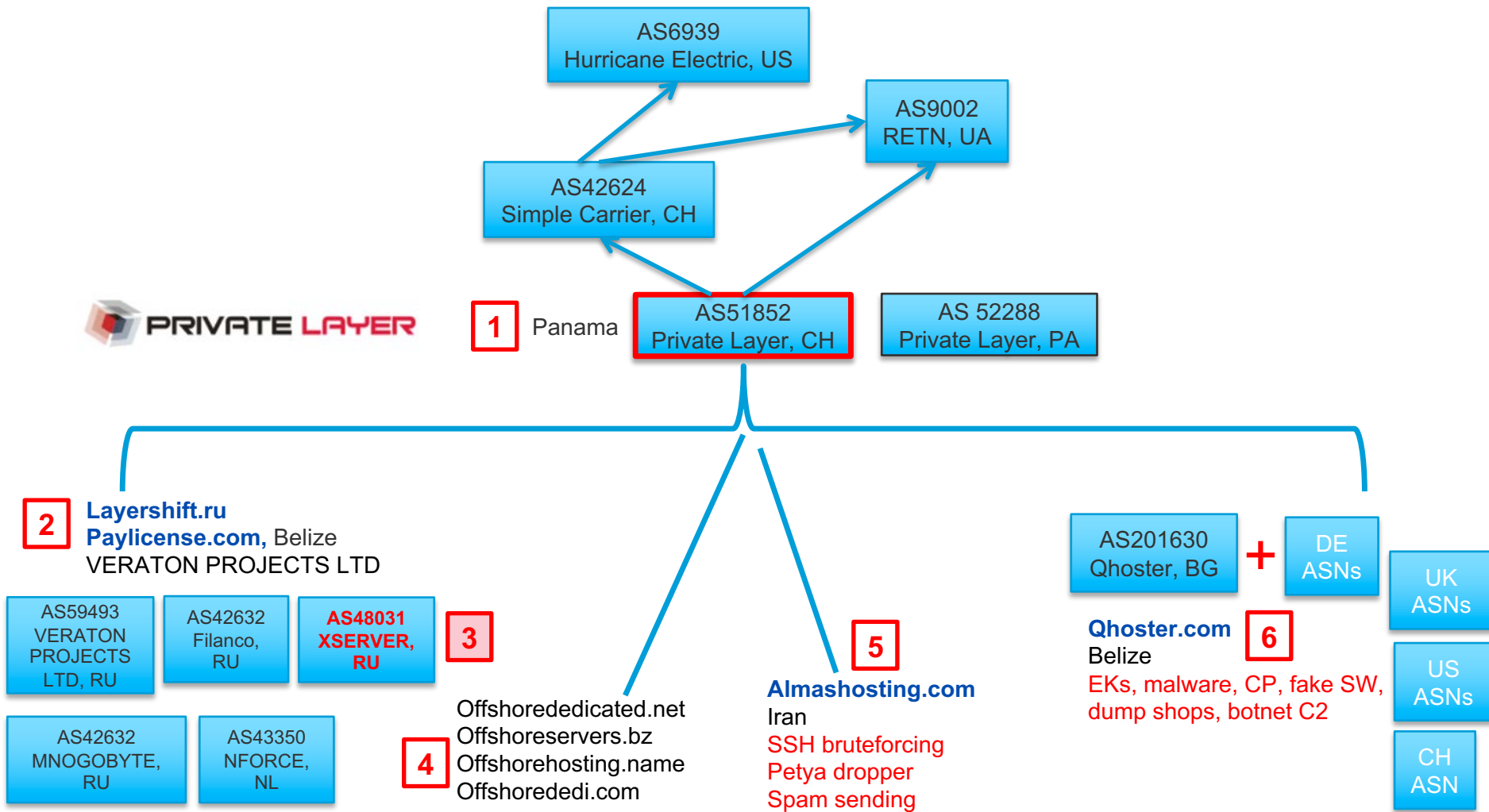
Payment Methods

We accept the following payment methods:



organisation: [ORG-VPL3-RIPE](#)
org-name: VERATON PROJECTS LTD
org-type: OTHER
address: City Belize
address: 1 mapp street
address: P.O.Box: 0000
address: Belize
address: Central America
phone: +5 078 8336509
fax-no: +5 078 8336509
abuse-c: [AR18973-RIPE](#)
admin-c: [DVVP-RIPE](#)
tech-c: [DVVP-RIPE](#)
mnt-ref: [MNT-PINSUPPORT](#)
mnt-ref: [OSC-MNT](#)
mnt-by: [OSC-MNT](#)
created: 2010-05-12T20:22:57Z
last-modified: 2017-10-30T14:53:09Z
source: RIPE# Filtered

Login to update 



[DEDICATED SERVERS](#)[VIRTUAL SERVERS](#)[SELLING SERVERS](#)[ENTRANCE](#)**CAUTION Grace dollar**

For all our customers a constant discount rate of the dollar:

\$ 1 = **20** USD.

\$ 1 = **50** rubles.



VIRTUAL SERVER



DEDICATED SERVER

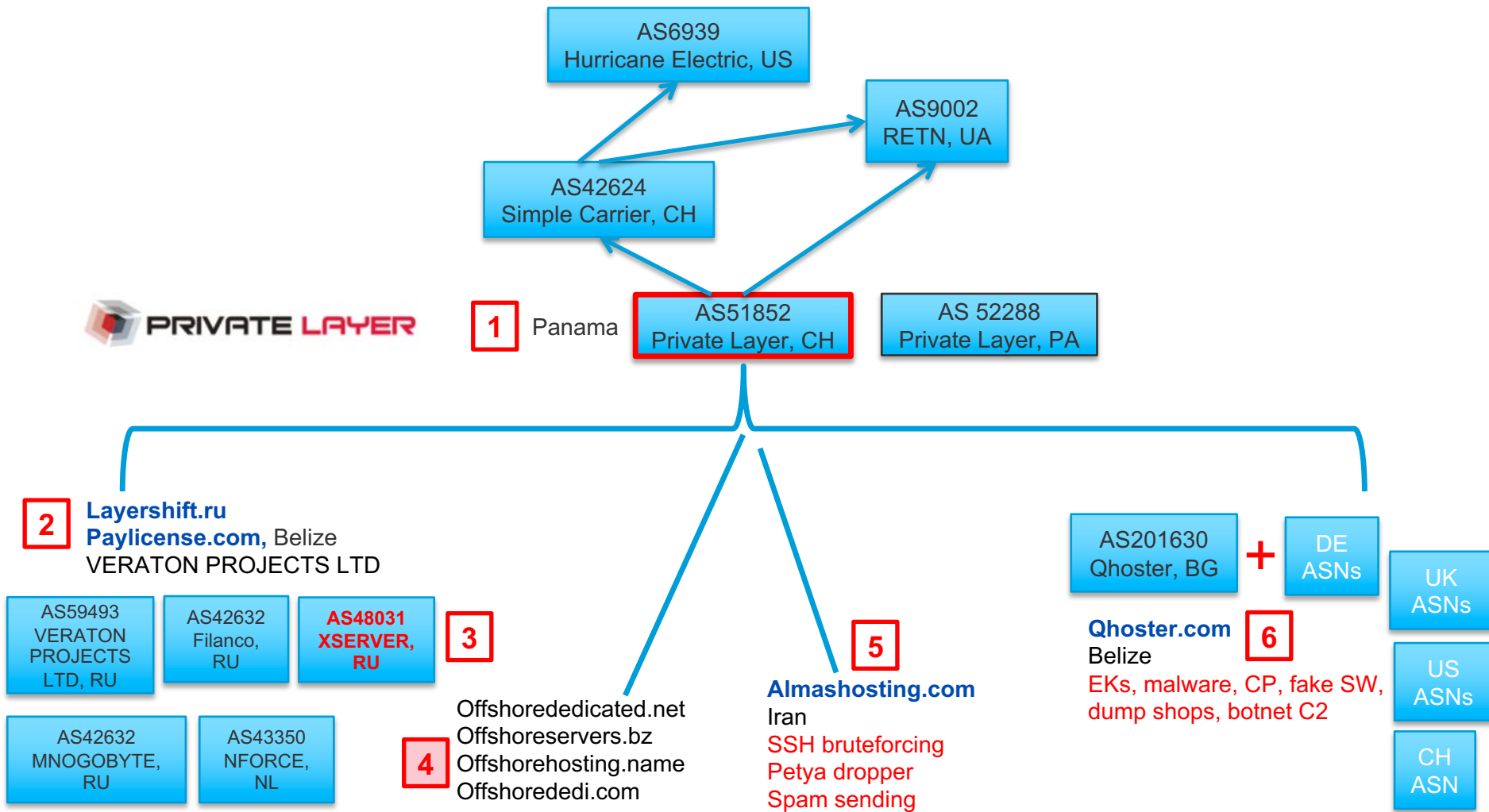
**HIGH UPTIME!**

We always strive to provide only quality services with high reliability

**WE WORK OFFICIALLY!**

We will give you all the necessary documents. If you do or do not want, we will refund you money

[Send us a message](#)[jivosite](#)



ROOT SERVER

Privacy Protected Offshore Dedicated
Servers To Satisfy Your Highest Needs.

[VIEW PLANS](#)



[SHARED HOSTING](#)

[VPS HOSTING](#)

[DEDICATED SERVER](#)

[MY ACCOUNT](#)

[OFFSHOREDEDI](#)

› Sweden Offshore VPS

› Russia Offshore VPS

› Swiss Offshore VPS

› Latvia Offshore VPS



Twitter

Tweets

[Follow](#)

OffshoreDedi @OffshoreDedi 22 Aug
Privacy is not an option, and it shouldn't be the price
we accept for just getting on the Internet.
[#OffshoreDedi](#) [#HostWithPrivacy](#)
[Expand](#)

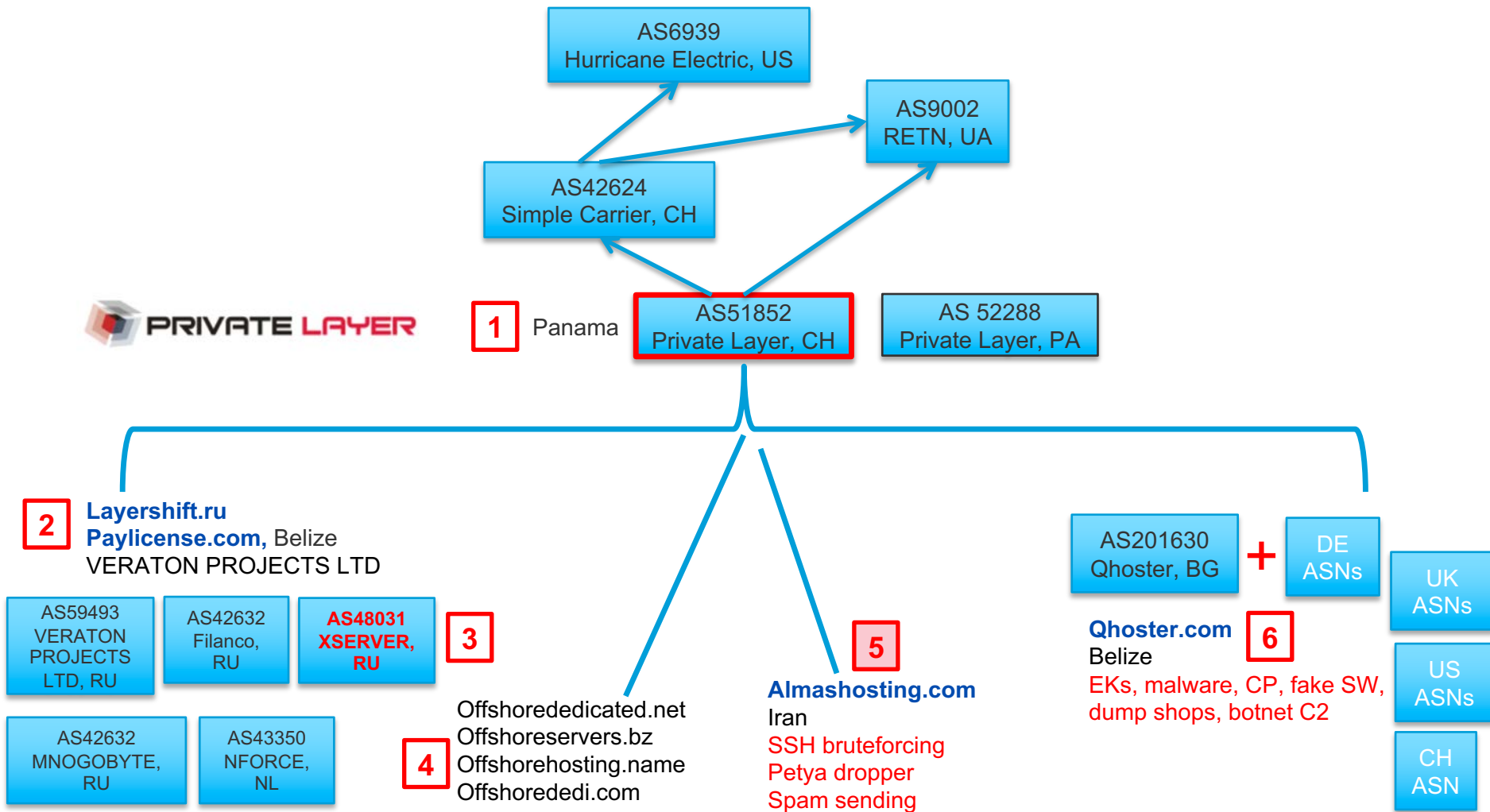
Tweet to @OffshoreDedi



Big Brother is Watching You!

We believe the internet should be free and anonymous, we respect your opinion and do not believe that current copyright laws are made for this digital age that we currently live in. We will only comply with the local laws.

info[[@](mailto:info@offshorededicated.net)]offshorededicated.net




المارس هاستينجز



ورود

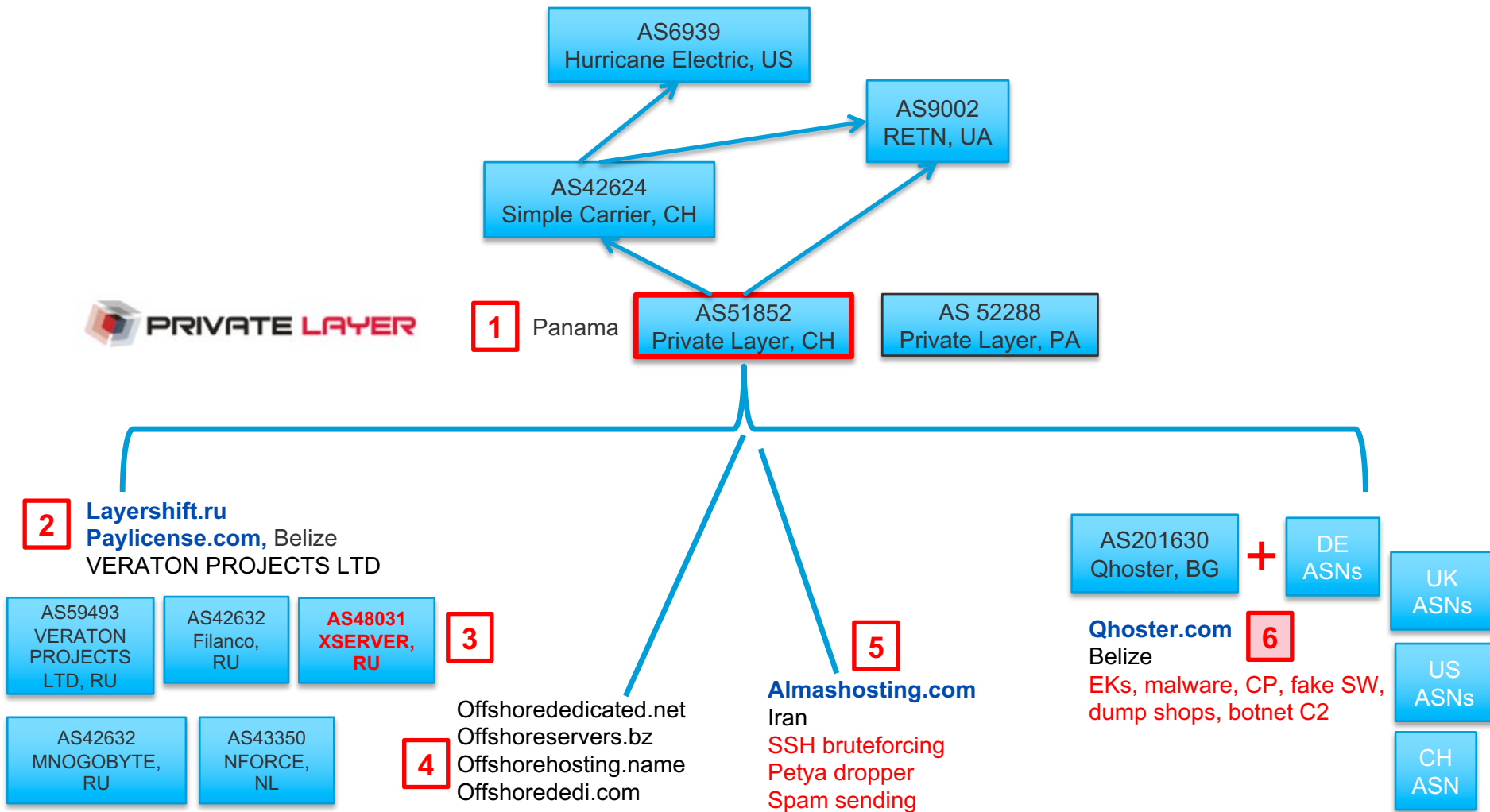


هزینه های تان را

الماس بدرخشيد

از طریق Viber و یا WhatsApp با ما ارتباط برقرار کنید

فقط کافیست پس از نصب برنامه های بالا، شما



DEDICATED SERVERS

Intel Xeon CPUs & 1Gbits Port

- Rapid Deployment - No Need to Wait!
- Reliable Hardware & Network
- CentOS, Debian, Ubuntu & Windows Server
- Location Choice - Europe & USA

save
20%

regularly \$212.44

\$169.95
/mo.

ORDER DEDICATED
SERVER



[PayPal](#) [NETELLER](#) [Skrill](#) [Payza](#) [WebMoney](#) [Perfect Money](#) [bitcoin](#) [Ukash](#) [cashU](#) [litecoin](#) [SolidTrust](#) [PAY](#) [paysafecard](#) [CHECK ALL](#)

[cPanel Web Hosting](#)

[Linux VPS](#)

[Windows RDP VPS](#)

[Dedicated Servers](#)

[Domains](#)



**CPANEL
HOSTING**

\$1.95
/mo.



- PHP, MySQL, Perl, Python, CGI, Ruby (RoR)
- SMTP, POP3/IMAP, Anti-spam/virus



**CPANEL
RESELLER**

\$24.95
/mo.



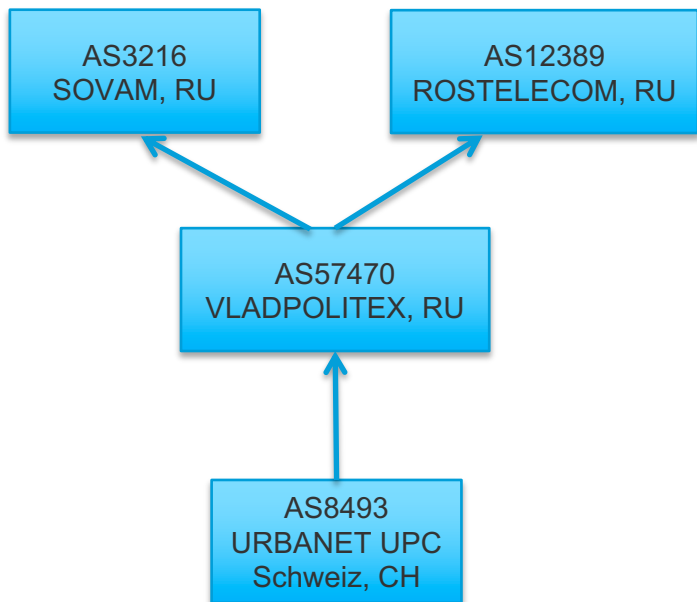
- UNLIMITED** cPannels
- FREE** Site Builder Software

Top 6 Reasons

Why to Choose QHoster?



Web Hosting Provider Since 2004



A single /23

Phishing, dump shops,
money mule recruiting,
Android trojans

un service de **cablecom**

Home News Produits Support **Contact** Services

Contact

Service après-vente (SAV)

c/o Cablecom
Rue de Galilée 2
CH-1400 Yverdon-les-bains
Hotline : 0844 844 770
Fax : 024 423 36 01
Email : info@urbanet.ch
URL : <http://www.urbanet.ch>
RDV pour mises en service, changement d'abonnement, résiliation, déménagement, dépannage modem, dérangement réseau pour notre clientèle privée.

Le SAV est ouvert du lundi au vendredi de 8h 00 à 17h 00

Helpdesk Clients réseaux SEIC & TRN

Hotline : 0900 900 770
URL : <http://www.urbanet.ch>
Communes concernées : Luins ; Vinzel ; Gland ; Prangins ; Nyon ; Crassier ; Duillier ; Coinsins ; Vich ; Begnins ; Trélex ; Genolier ; Grens ; Signy ; Chésereg ; Gingins ; Arnex ; Borex ; Commugny ; Tannay ; Coppet ; Founex ; Crans

Le helpdesk est ouvert du lundi au vendredi de 8h 30 à 19h 30 (gratuit)

Support Clients réseau TVT Services SA

Hotline : 021 631 51 20
URL : <http://www.tvtservices.ch>
Communes concernées : 1020 Renens ; 1022 Chavannes-Près-Renens ; 1023 Crissier ; 1024 Crissier.

Contact

- Administration
- Support Client

last carding service



usa dumps. local states

ICQ 2238395 - NEW ICQ

JABBER lastcarding@jabbin.cz
email lastcarding@safe-mail.net

Attention! ~~ICQ -2238456~~ was HACKED and STOLEN
Be careful and use new contacts! [Click here for info](#)

News
Main page

Rules &
Service
Policy

USA
Dumps

Tips
Tutorial
Software

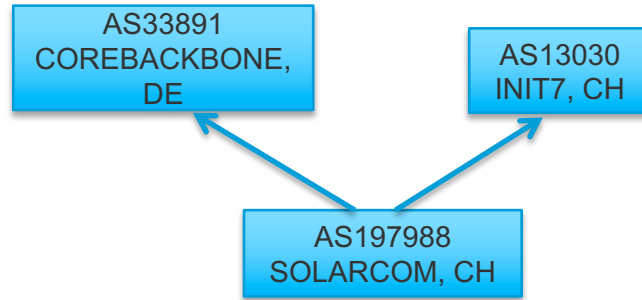
Chip EMU Software 2016 [Click here for info](#)
Write 201,221 code track2 on chip, works worldwide

Last Carding News

02 October 2017 [ultrafresh base](#) update

HUGE MEGA UPDATE: AZ,CA,CO,CT,DC,FL
GA,HI,ID,IL,IN,KY,MA,MD,MI,MS,NC
ND,NJ,NV,NY,OK,OR,SC,TX,VA,WA,WI,WY

18 September 2017 [ultrafresh base](#) update



Illegal video streaming,
pharma, fake merchandise,
exchange services (PM-bitcoin),
bitcoin mining,
bitcoin based gambling,
freedom of speech: free snowden,
justice for assange, wikileaks



Exchange service features:

- Constant monitoring of exchange market to set the most favorable rates;
- Cumulative discounts for regular customers;
- Discounts depending on the amount of exchange;
- Handy exchange calculator;
- Affiliate program with payment up to 30% of our profit;
- Exchange form can be built into your site;

Rus Eng

Login:

Pass:

Enter

[Forgot password?](#)

[Register](#)

Exchange

Exchange Rates

Partner

Discount

Agreement

About

Contacts

Reserve notification

Not enough reserve? Fill
Notification form!

Our accounts

Attention! We do not offer this service in the US (67.215.89.21) zone. We apologize for the inconvenience.

Automatic instant exchange Perfect Money, BitCoin, Payeer, AdvCash, Dash, LiteCoin, Zcash, eCoin, Exmo, Z-Payment

Spend:



Please select exchange direction. In the left column "Spend" - choose the currency you want to give, in the right column "Receive" - choose the currency you want to get. Reserves may vary depending on the exchange direction.

Receive:



Exchange History

Statistics

Banners

Forms

Export Rates

Settings

News

2017-09-18:
Exchange WEX USD and WEX EUR was added.

[More](#)

2017-09-05:
Reducing the number of confirmations for incoming Zcash payments.

Abuse in Dutch space

Hostzealot - Fortunix



CERTIFICATE OF REGISTRATION OF A LIMITED PARTNERSHIP

Partnership No. 10336

I hereby certify that the firm

FORTUNIX NETWORKS L.P.

having lodged a statement of particulars pursuant to section 8 of the Limited Partnership Act 1907, is this day registered as a limited partnership

Given at Companies House, Edinburgh, the 7th March 2012.

Bulgarian hoster with UK business registration;
address used by officers featured in the Panama
papers/offshore leaks

**Suite 1 78 Montgomery Street, Edinburgh,
Scotland, EH7 5JA**

Fortunix Networks

Customized Dedicated Server, Clustering & Co-location solutions in Europe, North America and Asia.

email: info@fortunix.net

Image phone: [1.888.9325681](tel:18889325681)

the DBA: hostzealot.com



Servers VPS hosting domains SSL



USD ▼

dedicated servers

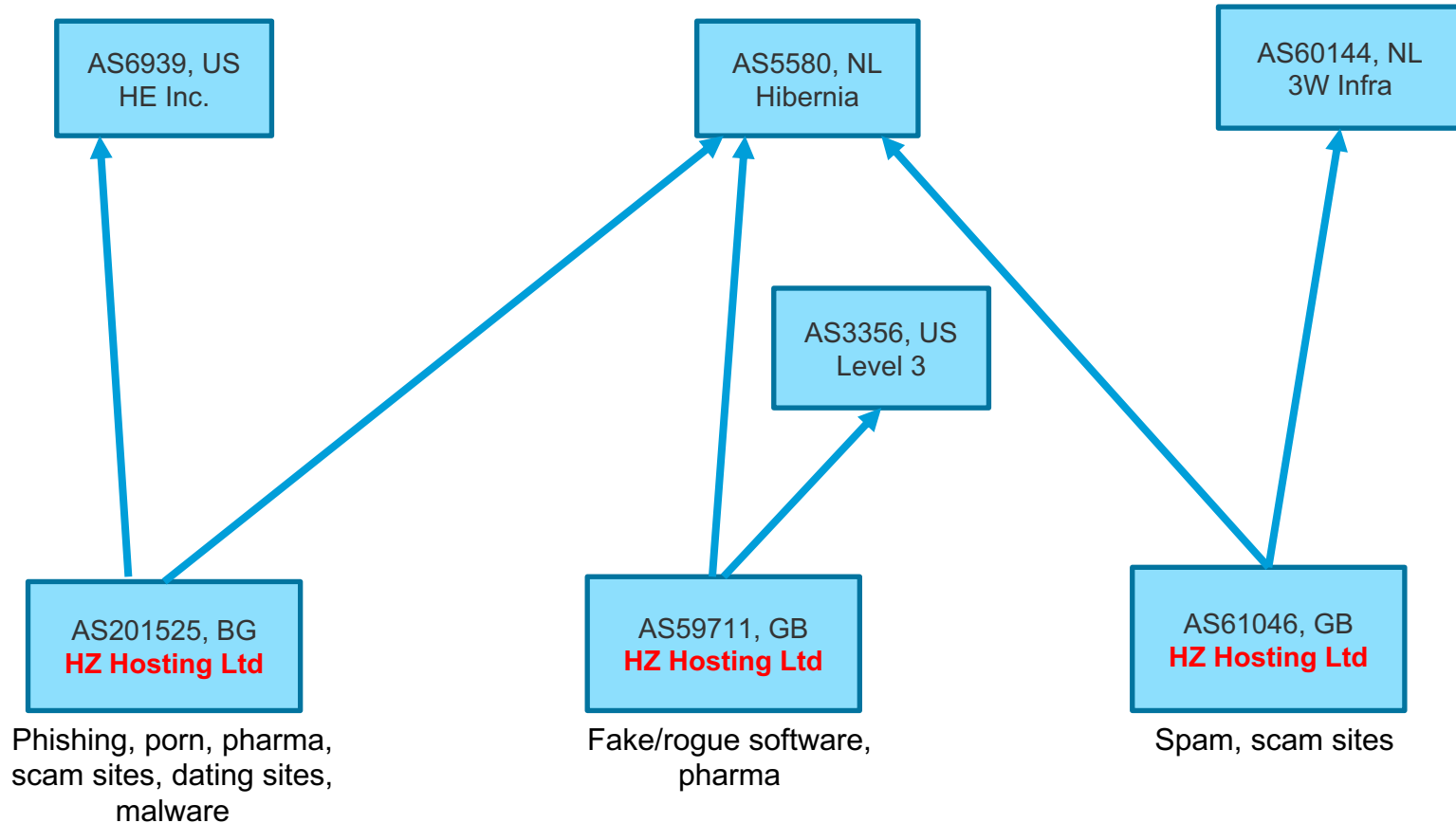


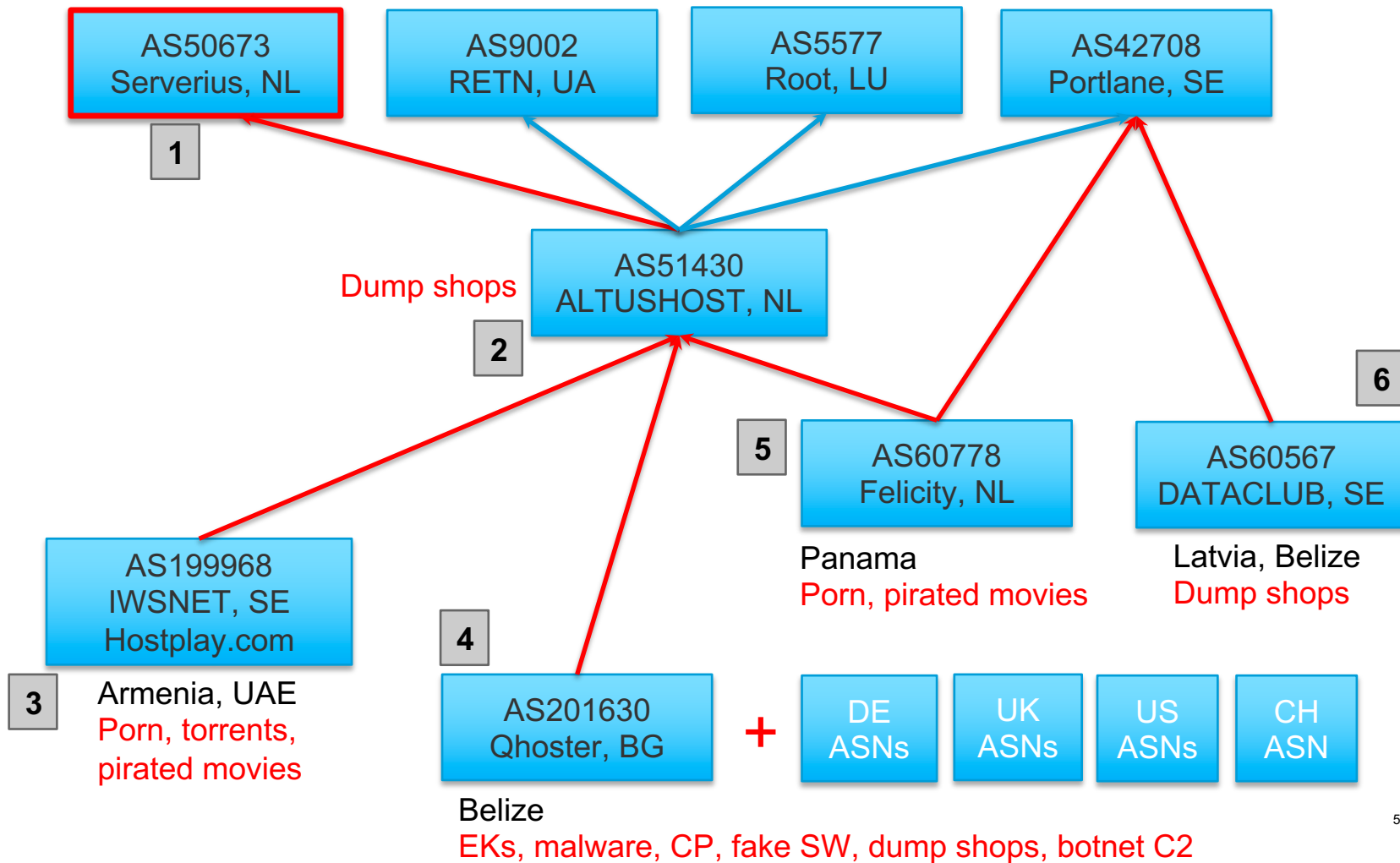
single-processor servers

CPU	Frequency	RAM	Disk	traffic	Price	
Intel Atom C2750	8x2.4 GHz	4GB	250 GB	5TB	\$ 59 / month	BUY
Intel Core i3-series	2x3.5 Ghz	8GB	500 GB	10 TB	\$ 89 / month	BUY
Intel Xeon E3-1230v2	4x3.3 GHz	8GB	500 GB	10 TB	\$ 99 / month	BUY

online

Hostzealot infrastructure





Kings-servers
Hosting-Solutions

Upstream

50673

6939

174

AS32338,
AS202951
Hostiserver

Adult and
child
porn

50673

14576

44596

EK, malware, porn,
pharma, fake sw



201; THE ROGERS OFFICE BUILDING;
EDWIN WALLACE REY DRIVE; GGEORGE
HILL; **ANGUILLA** B.W.I.

165 credit
card dump
shops

203339

202920

203557

52048

60567



99 Albert Street; Belize City;
Belize

Dataclub.biz

MPAA (movie) piracy

Ferazko
Holding.ru

197812

2

FreZZko Business Inc.

registered address

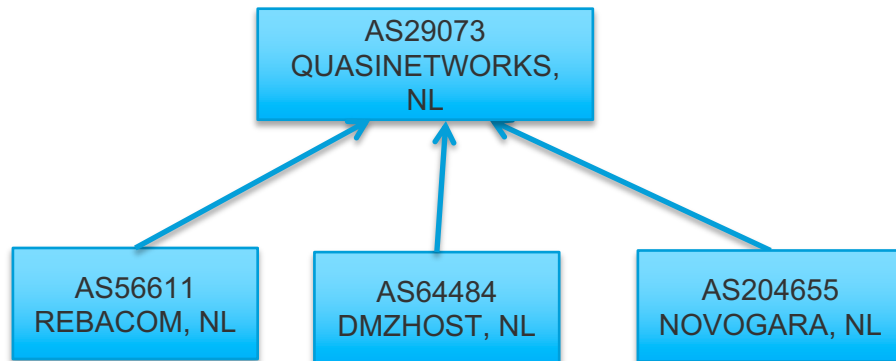
Ecatel

29073

movie piracy,
child porn, etc



Suite 1; Second Floor; Sound &
Vision House; Francis Rachel
Street; Victoria; Mahe; **Seychelles**



dmzhost.co

Brute-forcing,
phishing (Airbnb,
Amex, etc.)

JUPITER25
LIMITED

AS206703
OKSERVERS,
US

okservers.net

-Created Nov
14, 2016
-Last visible
Sep 8, 2018

Brute-forcing,
porn, pharma, fake
merchandise

-Site is down
since March
2018

DMZHOST

Terms of services Privacy Policy Contact Us Abuse Client Login

WEB HOSTING		VIRTUAL SERVERS			DEDICATED SERVERS		IPV4	
Plan	OS	RAM	CPU	Uplink	Storage	Bandwidth	Price	Order
VSW-0	Windows	768Mb	2 Cores	1Gbps	15GB SSD	1.5TB p.m	€ 5/m	Customize Now!
VSW-1	Windows	2.5Gb	2 Cores	1Gbps	25GB SSD	2.5TB p.m	€ 10/m	Customize Now!
VSW-02	Windows	4GB	2 Cores	1Gbps	50GB SSD	6TB p.m	€ 20/m	Customize Now!
VSW-03	Windows	6GB	2 Cores	1Gbps	75GB SSD	9TB p.m	€ 30/m	Customize Now!
VSW-04	Windows	12GB	4 Cores	1Gbps	100GB SSD	12TB p.m	€ 45/m	Customize Now!
VSW-05	Windows	16GB	4 Cores	1Gbps	120GB SSD	14TB p.m	€ 60/m	Customize Now!
VSL-K-00	Linux	768Mb	2 Cores	1Gbps	15GB SSD Or 30GB HDD	1.5TB p.m	€ 5/m	Customize Now!
VSL-K-01	Linux	2.5GB	2 Cores	1Gbps	30GB SSD Or 80GB HDD	2.5TB p.m	€ 10/m	Customize Now!

OkServers

About Solutions Looking Glass FAQ Dedicated Servers Contact Locations Account

OkServers LLC

High performance dedicated hosting

OkServers offers hosting solutions for clients all around the world. We maintain a central presence in both the US and EU to maintain low latency on a global scale. We cater to the needs of any client for hosting solutions large and small.

Solutions We Offer

Dedicated Servers

OkServers provides one of the highest tier hosting platforms online today. All of our dedicated servers are designed to power uptime critical services and resource demanding applications. Our brand new, latest generation hardware and highly resilient network infrastructure allow for an unbeatable hosting experience.

Managed Hosting

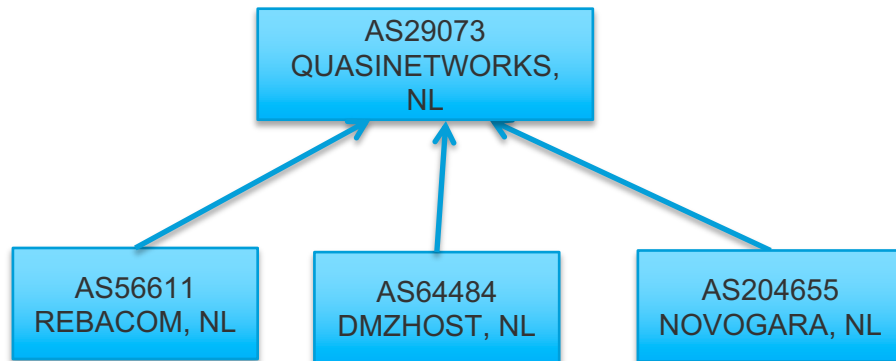
Take the technical know-how out of hosting. Allow our technical team with years of experience manage software services on your dedicated server. We can fully manage your server, from small configuration changes to fine tuning critical runtime applications for high load processing of any form, we assure no request is too big or small.

Network & Transit

OkServers provides expert level network consulting, we can help you expand your current network infrastructure or help plan for future endeavors. We can provide dedicated layer 3 network transit services for IP traffic, a perfect solution for those with large scale projects or high volume server clusters that require over 10Gbps bandwidth.

Colocation Services

Employ your own hardware? No worries, OkServers provides premium tier colocation services. We will accept shipment of your hardware, rack and stack free of charge, provide necessary PDU's, power / network cables, etc. All colocation services are credit to 30 minutes of free remote hands per month, and a 10Gbit internet uplink.



dmzhost.co

Brute-forcing,
phishing (Airbnb,
Amex, etc.)

JUPITER25
LIMITED

AS206703
OKSERVERS,
US

okservers.net

-Created Nov
14, 2016
-Last visible
Sep 8, 2018

Brute-forcing,
porn, pharma, fake
merchandise

Companies House

BETA This is a trial service — your [feedback](#) will help us to improve it.

[Sign in / Register](#)

JUPITER 25 LIMITED

Company number **10282369**

[Follow this company](#)

Overview

Filing history

People

Registered office address

60 Paul Street, London, England, EC2A 4NE

Company status

Dissolved

Company type

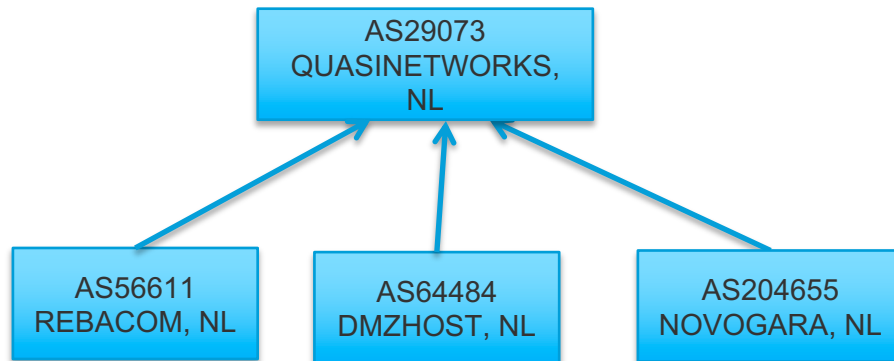
Private limited Company

Nature of business (SIC)

96090 - Other service activities not elsewhere classified

Dissolved on
27 February 2018

Incorporated on
16 July 2016



dmzhost.co

Brute-forcing,
phishing (Airbnb,
Amex, etc.)

JUPITER25
LIMITED

-Created Nov
14, 2016
-Last visible
Sep 8, 2018

AS206703
OKSERVERS,
US

okservers.net

Brute-forcing,
porn, pharma, fake
merchandise

Companies House

BETA This is a trial service — your [feedback](#) will help us to improve it.

[Sign in / Register](#)

Search for a company or officer

JUPITER 25 LIMITED

Company number 10282369

Follow this company

Overview Filing history People

Filter by category

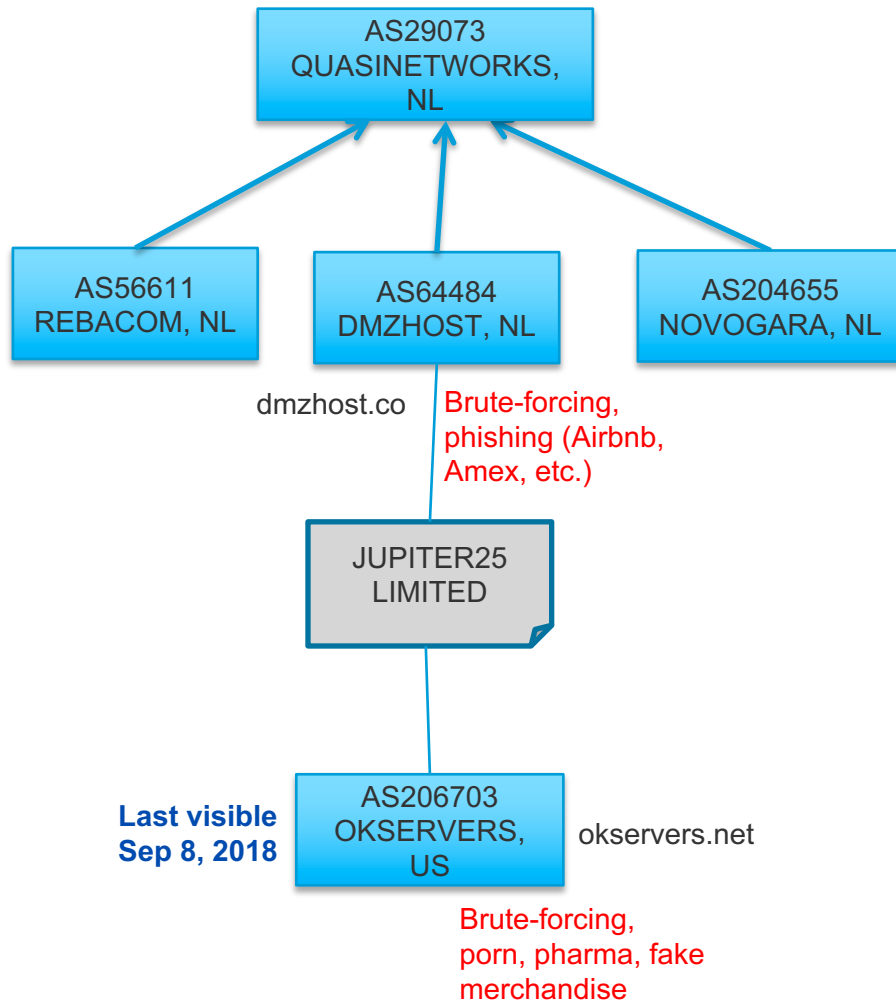
☐ Show filing type

☐ Accounts ☐ Confirmation statements / Annual returns

☐ Capital ☐ Incorporation

☐ Charges ☐ Officers

Date	Description	View / Download
27 Feb 2018	Final Gazette dissolved via compulsory strike-off	View PDF (1 page)
10 Oct 2017	Registered office address changed from 35 Firs Avenue London N11 3NE United Kingdom to 60 Paul Street London EC2A 4NE on 10 October 2017	View PDF (1 page)
10 Oct 2017	Termination of appointment of Darren Symes as a director on 16 July 2016	View PDF (1 page)
10 Oct 2017	Cessation of Darren Symes as a person with significant control on 16 July 2016	View PDF (1 page)
10 Oct 2017	First Gazette notice for compulsory strike-off	View PDF (1 page)
16 Jul 2016	Incorporation Statement of capital on 2016-07-16 GBP 1 • Model articles adopted	View PDF (10 pages)



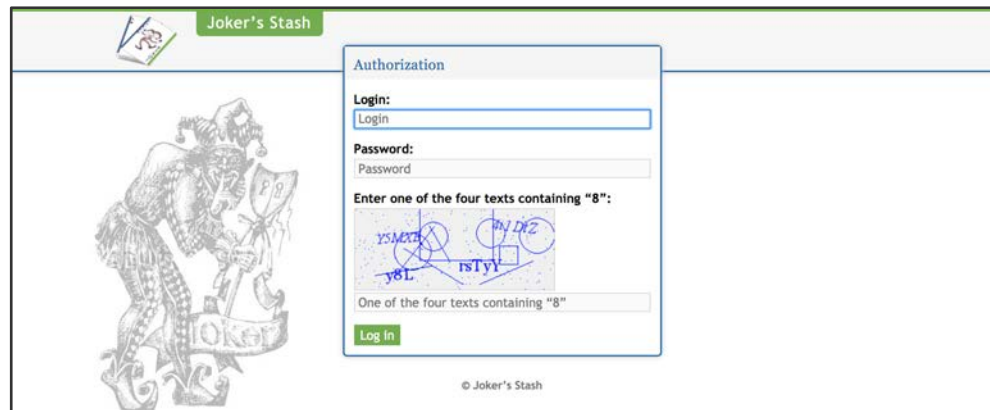
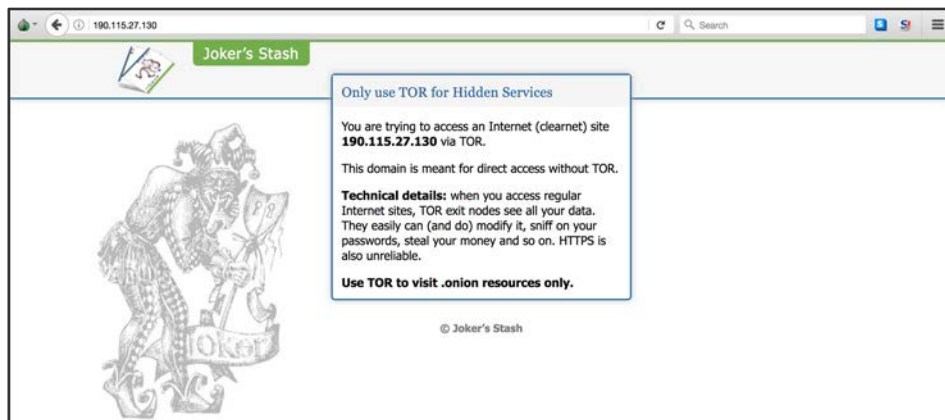
Historical Whois (AS206703) BETA

	2016-11-22 09:53:15	2018-09-04 11:54:47
aut-num	AS206703	AS206703
version:	2016-11-22 09:53:15	2018-09-04 11:54:47
status:	ASSIGNED	ASSIGNED
created:	2016-11-22 09:53:15	2016-11-22 09:53:15
validity:	From 2016-11-22 09:53:15 To 2016-11-23 07:14:24	From 2018-09-04 11:54:47 To 2018-10-17 12:38:00
aut-num:	AS206703	AS206703
as-name:	OKSERVERS	NOLONGERUSEDFROMCUSTOMER
source:	RIPE	RIPE
mnt-by:	RIPE-NCC-END-MNT [mntner], CYBR-DMZ [mntner]	RIPE-NCC-END-MNT [mntner], CYBR-DMZ [mntner]
admin-c:	ACRO1670-RIPE	ACRO1670-RIPE [role]
sponsoring-org:	ORG-DETL1-RIPE [organisation]	ORG-DETL1-RIPE [organisation]
org:	ORG-JA346-RIPE [organisation]	ORG-JA346-RIPE [organisation]
tech-c:	+ ACRO1670-RIPE	-

close compare

Top carding and cybercrime forums

Top carding site: Joker's stash



Top carding site: Joker's stash

- All Joker's stash domains have been on RIPE IP space + some Iranian hosters
- 190.115.27.130: Banner on port 443/tcp on 190.115.27.130: [ssl] cipher:0xc013 , [jstash03.link](#), [jstash-bazar.link](#), [jstash-bazar.store](#), [jstash03.link](#), [jstashbazar.link](#), [www.jstash-bazar.link](#), [www.jstash-bazar.store](#), [www.jstash03.link](#), [www.jstashbazar.link](#)
- 190.115.27.130 is on AS262254, Dancom LTD, registered in Belize, but part of the DDOS-GUARD, RU operation



Black Hat 2016



Top carding site: Joker's stash

Other hosters used by Joker's stash domains:


- INFIUM, UA (AS50297)
- DOTSI, PT (AS49349) a.k.a BlazingFast
- SINARO, NL (AS62088), a.k.a Morehost

All three have regularly been involved in hosting toxic content: abused or complicit ??



Top cybercrime forum:maza

[User CP](#) [FAQ](#) [Members List](#) [Calendar](#) [New Posts](#) [Search](#) [Quick Links](#) [Escrow](#) [Prices](#) [Log Out](#)

 MF

Welcome, [Guest](#)
You last visited: Today at
[Private Messages](#): Unread 0, Total 0.

[mazaforum > Основной раздел > Программирование в сфере кардинга](#)
Zeus.

"хороший партнер, своевременные выплаты, никакого обмана :)"
- Dee_Kline

Best курс U-kash, LR, WMZ обмен/вывод
ОБНАЛ, ВЫВОД, ВВОД WM, LR, ЯД, WIRE
ВАШ СКУП СЕРВИС

АВТОМАТИЧЕСКИЙ СЕРВИС ГАРАНТА
НЕТ ПОРУЧИТЕЛЕЙ? ВНЕСИ ДЕПОЗИТ!
BLACK HOLE EXPLOITS KIT

Answer cc tools для FF
WMZ, LR, BITCOIN, WIRE, ALFA, PRIVAT

All times are GMT -5. The time now is 10:43.


[Ответить](#)

Page 1 of 5 1 2 3 4 5 >


Thread Tools Search this Thread Rate Thread Display Modes

13th October 2010, 15:16




[harderman](#)
Member



Join Date: Jul 2010
Location:
Posts: 44

 **Zeus.** (2)

Доброго времени суток!

С сегодняшнего дня и в будущем обслуживать продукт Zeus/Зевс версий 2.0 буду я. Мне переданы исходные коды на безвозмездной основе для того, что бы клиенты купившие софт не остались без технической поддержки продукта. Славик более продукт не поддерживает, исходные коды у себя удалил, не продает и никакого отношения к нему не имеет. Так же никакого бизнеса в интернете не ведет, его контакты через несколько дней будут не действительны. Он просил меня передать, что ему было приятно со всеми работать, у кого остались какие не решенные вопросы, просьба в ближайшие дни с ним связаться. Все клиенты купившие софт у Славика, будут обслуживаться у меня на тех же условиях что и были ранее. По всем вопросам просьба обращаться непосредственно ко мне.
Всем спасибо за внимание!
Для связи со мной используйте жабер:   

Robots have seen things you people wouldn't believe. ... And they have a plan.

Top cybercrime forum:maza

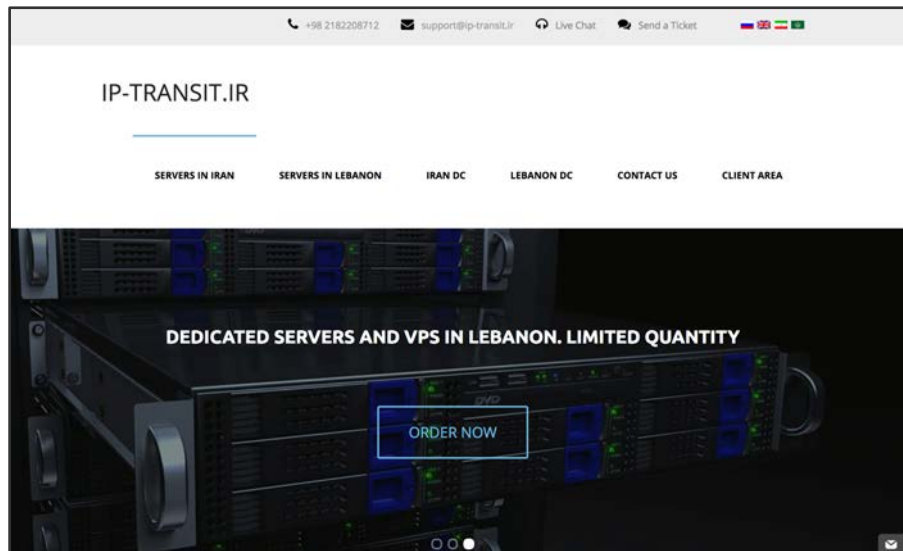
- Maza domains used RIPE IP space + currently on Iranian BPH hoster
- Current IP has also hosted Joker's stash domains and their jabber server

Known domains hosted by 193.142.30.30

maza.cc mfbook.in mfclub.ws mfshop.me xmpp.jclub.pw privetarnold.net www.jclub.pw www.privetarnold.com jclub.pw privetarnold.com pay.privetarnold.net

AS59580
BATTERFLYAIMEDIA,
IR

AbdAllah (aka Mykhailo Rytikov,
Webhost, Whost



Operational Recommendations

1. Understand and expose TTPs of rogue/gray hosting providers
2. Share intel with security community/LE, monitor and take early action
3. Ask registries to scrutinize ASN and IP space requests more closely?
4. Work on whois policies with RIPE
5. Datacenters scrutinize peering or co-location requests?

Some related Work

- Hack in the Box, Amsterdam 2018 <https://conference.hitb.org/hitbsecconf2018ams/sessions/commsec-privacy-and-protection-for-criminals-behaviors-and-patterns-of-rogue-hosting-providers/>
- SANS CTI Summit 2018 <https://www.youtube.com/watch?v=gHewB06Bnrk>
- FIRST/OASIS Borderless Cyber Conference and Technical Symposium 2017 [https://www.oasis-open.org/events/sites/oasis-open.org.events/files/Borderless Cyber 2017%20final Dec7 2017.pdf](https://www.oasis-open.org/events/sites/oasis-open.org.events/files/Borderless%20Cyber%202017%20final%20Dec7%202017.pdf)
- Virus Bulletin 2017 <https://www.virusbulletin.com/blog/2017/11/vb2017-paper-beyond-lexical-and-pdns-using-signals-graphs-uncover-online-threats-scale/>
- Defcon 2017 <https://www.youtube.com/watch?v=AbJCOVLQbjs>
- Black Hat 2017 <https://www.youtube.com/watch?v=PGTTRN6Vs-Y&feature=youtu.be>
- NCSC One Conference 2017
- Black Hat 2016 <https://www.youtube.com/watch?v=m9yqnwuqdSk>
- RSA 2016 <https://www.rsaconference.com/events/us16/agenda/sessions/2336/using-large-scale-data-to-provide-attacker>
- BruCon 2015 <https://www.youtube.com/watch?v=8edBgoHXnwg>
- Virus Bulletin 2014 <https://www.virusbtn.com/conference/vb2014/abstracts/Mahjoub.xml>
- Black Hat 2014 <https://www.youtube.com/watch?v=UG4ZUaWDXS>

Thank you

Dhia Mahjoub, dmahjoub@cisco.com, @DhiaLite

Thanks

Atheana Altayyar
Intel471
Sarah Brown