Underground Market 101

Maxim Goncharov

TREND MICRO

POC2013
http://www.powerofcommunity.net

Who am I ?

Max Goncharov

12 years TREND MICRO

Research and Development

I live in Munich Germany

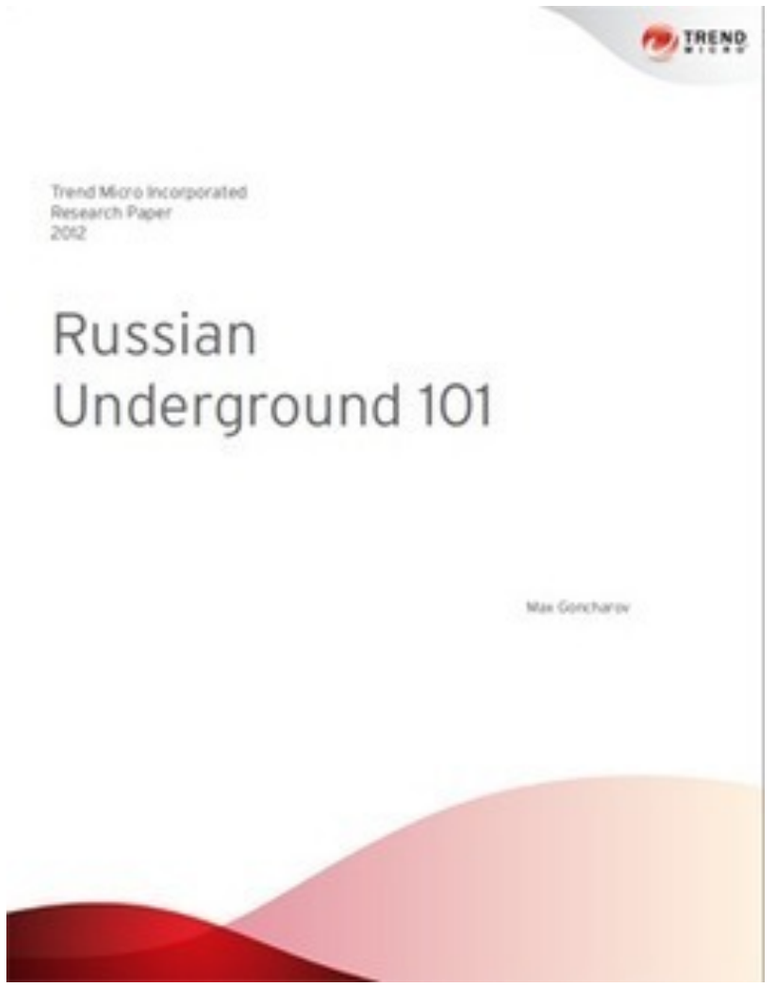
Network Analysis

Big Data Processing

Data Streaming

Underground Research

Underground Research



gmax.at/101

TREND MICRO

POC2013
http://www.powerofcommunity.net

Underground Research

Manual Information

Automated

Data Aggregation and Storage

TREND MICRO

POC2013
http://www.powerofcommunity.net

Hide

VPN bulletproof service

encrypt communication to C&C and other services

hide personal IP

hide identity

CryptoVPN
when privacy matters...

VPN-Office

WEB
BulletProof

NODMCA

STRONG
VPN PROVIDING INTERNET SERVICES SINCE 1995

Bulletproof
networks

HIDE.IO

SECRETSLINE

TREND
MICRO

POC2013
http://www.powerofcommunity.net

DoubleVPN.com

Без компромиссов...

NiGel BlackW Murai

Filter | All Records | List View

Current Filter: dICQ Include '36117973'

IDICQ [28]

dICQ* [36117973]

dDate* [2010-05-11 11:24:26]

Summary

Select a record to enter in form view, click on field name to order

#	Case ID	Date|Time	Comments
1	7564	2013-09-03 08:58:54	Dear forum members . We want to introduce you t
2	3924	2011-01-27 13:58:58	http://www.doublevpn.com -VPN service; prices: -
3	2665	2010-09-27 13:53:23	VPN service; prices: Simple VPN from 3 $, Doubl
4	1407	2010-06-29 14:19:58	VPN service http://www.doublevpn.com - All data
5	1254	2010-06-17 20:21:15	VPN service; - Simple VPN from 3 $, - Double VPN
6	1196	2010-06-15 18:45:27	vpn service; - Simple VPN from 3 $ - Double VPN
7	876	2010-06-05 21:09:20	VPN - Payment types: WebMoney , Liberty Reserve,
8	875	2010-06-05 21:08:03	VPN - Payment types: WebMoney , Liberty Reserve,
9	749	2010-06-02 11:22:57	VPN service; web:http://www.doublevpn.com - Simp

UNDERGROUND ECONOMY
ANY STREET 1234
ALMOST ANY COUNTRY

VPN $25

TOTAL: $25.00

Select kind of Botnet framework

banks

cc

Zeus Botnet

Microsoft takes dow … egister
www.theregister.co.uk/2(… wn/
Mar 26, 2012 – A Micros … takedown of key servers
associated with the infan … Trojan **botnets** on ...

Zeus Botnet Eurograbber Steals $47 Million - Security -
www.informationweek.com/.../**zeus-botnet**...steals.../24014383...
News. **Zeus Botnet** Eurograbber Steals $47 Million. Mathew J. Schwartz ... Mathew J. Schwartz | December 05, **2012** 10:13 AM. Who Is Hacking U.S. Banks?
Jóseph Mlódzíanowskì shared this on Google+

Microsoft shuts down 2 **Zeus botnet** servers – US
www.usatoday.com/tech/news/story/**2012**-03-26/...**botnet**/.../1
Mar 26, 2012 – The software giant on Friday orchestrated a su… hosting companies.

TREND MICRO

POC2013 http://www.powerofcommunity.net

blade2008

Плохой

Регистрация: 26.05.2008
Адрес: Drezden
Сообщений: 335
Репутация: **0**

Filter | All Records | List View

Current Filter: dICQ Equal to '573754454'

IDICQ [**96**]
dICQ* [**573754454**]
dDate* [**2010-05-13 21:59:17**]

Summary

Select a record to enter in form view, click on field name to order

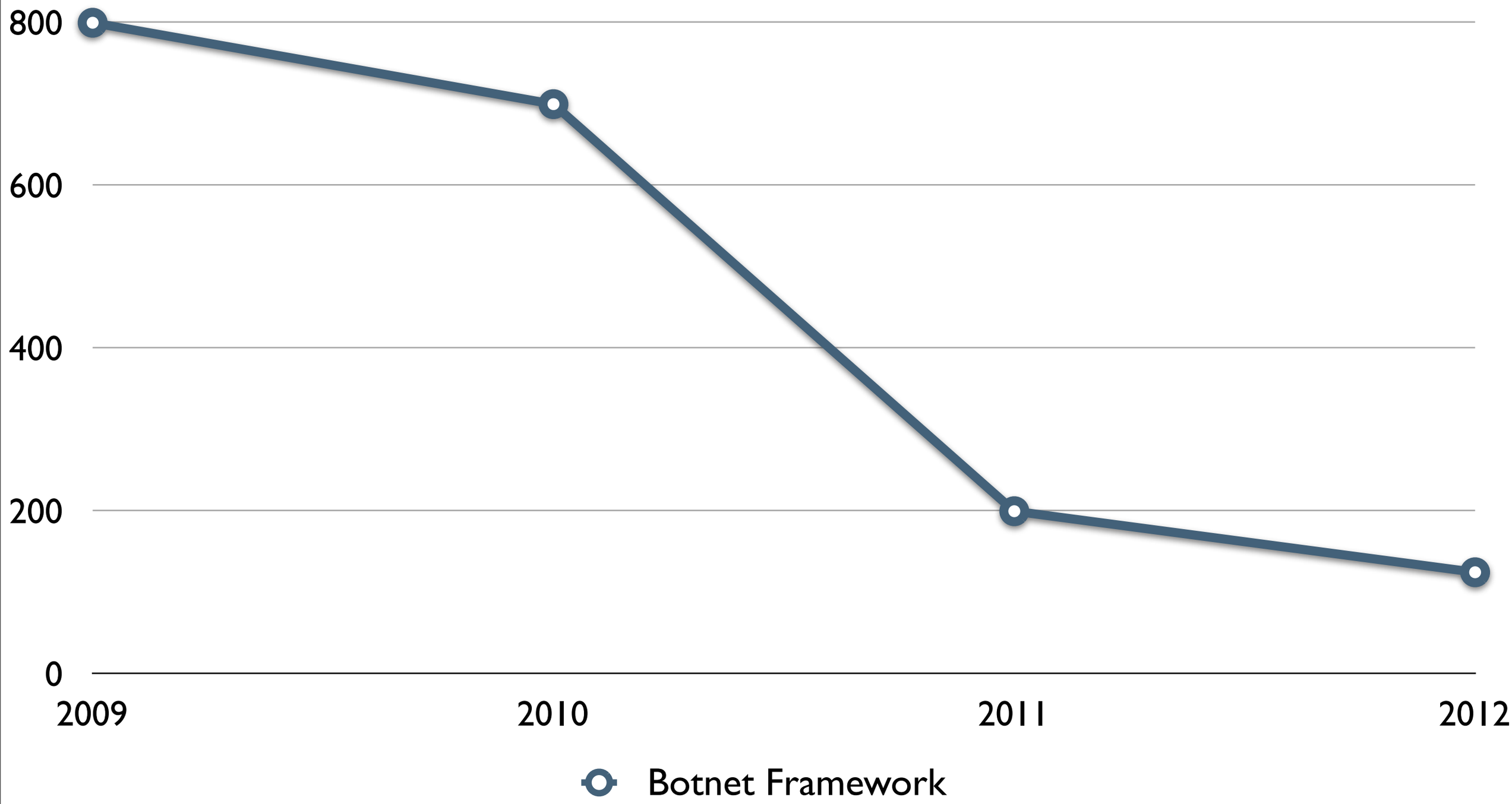
#	Case ID	Date|Time	Comments
1	4496	2011-03-30 12:47:20	ru ppi Price - 60wmz/1k
2	4425	2011-03-24 14:23:48	Zeus and Pinch installation; Exploits and loaders
3	905	2010-06-05 22:15:41	help with installing and configuring - Zeus 1.2.
4	115	2010-05-13 21:59:17	!!!UUUUUUPPPPP!!! helps with install zeus 1.2.10.

UNDERGROUND ECONOMY
ANY STREET 1234
ALMOST ANY COUNTRY

ZEUS CORE	$125
MONTHLY UPDATES	$15
24/7 SUPPORT	$25

TOTAL: $165.00

Botnet price



Bulletproof hosting

Your servers or/and servers are bulletproof

Hosting provider makes no reaction on abuse requests

It does not really matter if you host porno or C&C

TREND MICRO

POC2013
http://www.powerofcommunity.net

HostimVse!
разместим любые проекты

ABUZAM.NET

Russian Business Network RBN

James McQuaid's IP list

```
welaps.com
wmdiler.com.ua
wmdohod.com
woodiet.com
wp-host.net
www.allfan.info
www.art-parking.info
www.avtomaslo.info
www.delavgo.ru
www.fiat-punto.info
www.fifafans.ru
www.football-planet.org
www.herbalpharmshop.net
www.jphentai.com
www.keeplinkslife.com
www.kprazdniku.info
www.medhey.com
www.minika.net
www.my-rover.com
www.naykris.com
www.panaris.ru
www.pantoff.net
www.porno-magnet.com
www.real-host.ru
www.setyet.com
www.skynet73.ru
www.spontan.ru
www.terpsihora.org
www.tinysoft.info
www.toxoid.ru
www.websovet.com
www.webwm.net
www.welaps.com
www.wingift.net
www.xiromantiya.ru
www.zapzhasti.ru
wwwintimcity.ru
wwwmaw.ru
```

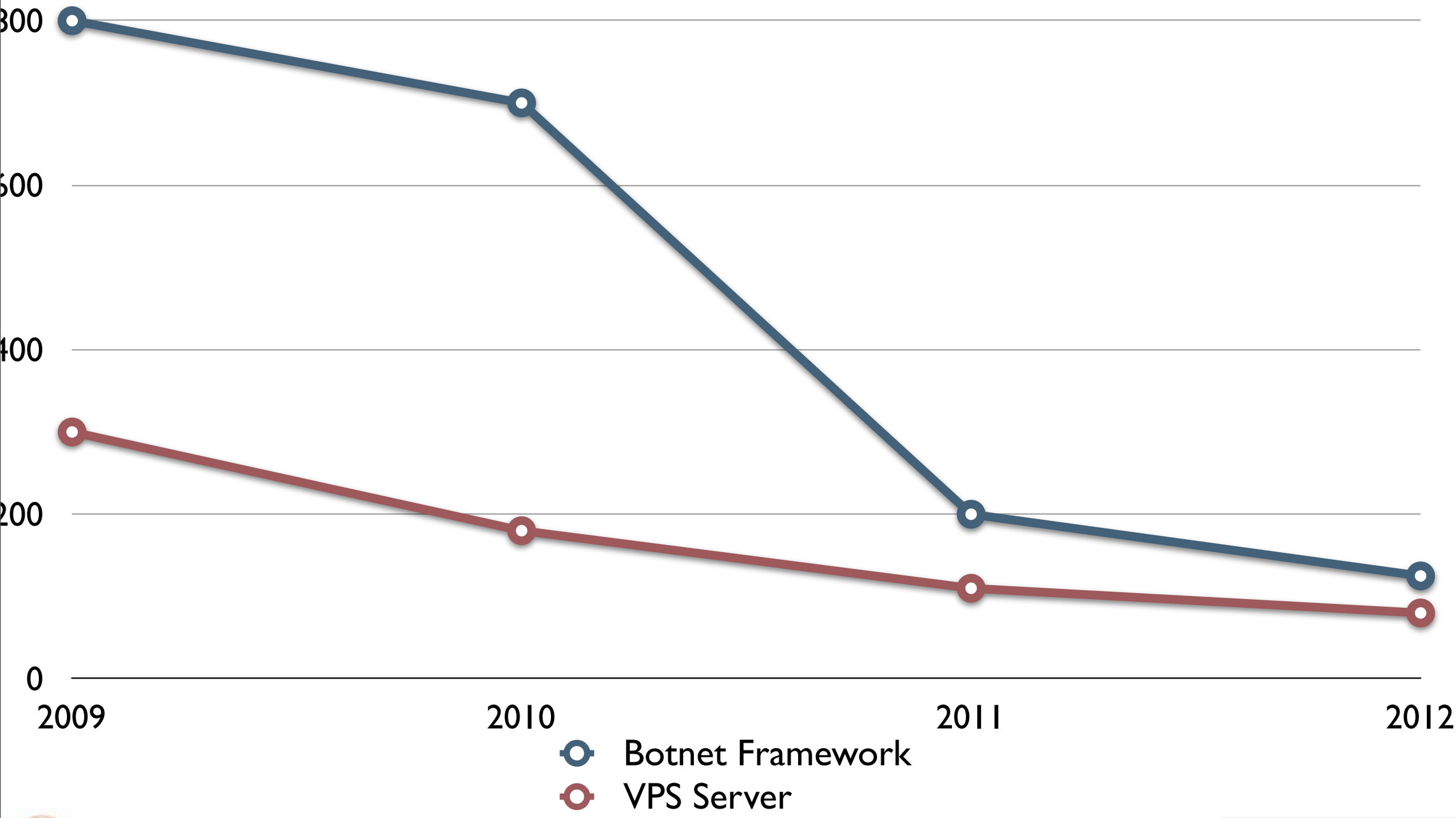
TREND MICRO

UNDERGROUND ECONOMY
ANY STREET 1234
ALMOST ANY COUNTRY

2CORE 4GB DEDIC HKG	$39
24/7 SUPPORT	$4
BULLETPROOF CHECK	$9

TOTAL: $52.00

Dedicated Server



Exploit kit

Black Hole

Phoenix

Yang Pack

Sweet Orange

Nuclear Pack

Andromeda

Update

Check and update to save

Types: Exploit
Nick Name: alexudakov
ICQ: 449832628
Email: none
Web: hack-info.ru
IRC: none
Link: https://xakepy.cc/showthread.php?t=64321'

Comment:
!!!UP!!! Phoenix Exploits Kit v2.3 - set of exploits for sale; 12 exploits in set: 1)IE6 MDAC
6)FLASH 10, 7)IEPEERS, 8)JAVA SMB, 9)HCP, 10)PDFSWF, 11)PDFOPEN, 12)PDF LIBTIFF;

Message Body:
Phoenix Exploits Kit - современная связка эксплойтов Phoenix Exploits Kit v2.3 - проду
связки (v2.2) входит 12 эксплойтов и данный набор будет постоянно обновляться: 1)

Phoenix

CVE	*Description*
CVE-2011-3544	Oracle Java Applet Rhino Script Engine Remote Code Execution
CVE-2011-0611	Adobe Flash Player Remote Code Execution Vulnerability (NPSWF32.dll plugin)
CVE-2010-0806	IE iepeers Vulnerability
CVE-2010-0188	Adobe Reader LibTiff Vulnerability
CVE-2009-4324	Adobe Reader newPlayer Vulnerability
CVE-2009-3867	Java HsbParser.getSoundBank (GSB)
CVE-2009-1869	Adobe Flash Integer Over□ow in AVM2
CVE-2009-0927	Adobe Acrobat and Reader Collab 'getIcon()' JavaScript Method RCE Vulnerability
CVE-2008-5353	Java Runtime Environment (JRE)
CVE-2008-2992	Adobe Acrobat and Reader 'util.printf()' Remote Buffer Over□ow Vulnerability
CVE-2008-2463	IE SnapShot Viewer ActiveX Vulnerability
CVE-2007-5659	Adobe Reader and Acrobat Multiple Stack-based Buffer Over□ow Vulnerabilities
CVE-2006-0003	IE MDAC

Phoenix

Phoenix Exploit's Kit 3.0 full

△CONCORDIA, INTEGRITAS, INDUSTRIA...

Simple browser statistics

Browser	Visits	Exploited	Percent
MSIE	28866	13220	45.8%
Firefox	5536	1260	22.76%
Other	2020	158	7.82%
Opera	178	15	8.43%

Main Statistics

Unique Visits	Exploited	Percent
36600	14653	40.04%

Exploit statistics

Exploit	Exploited	Percent
JAVA TC	1785	4.88%
JAVA SMB	5195	14.19%
JAVA RHINO	4120	11.26%
PDF COLLAB	596	1.63%
PDF PRINTF	32	0.09%
JAVA RMI	251	0.69%
PDF LIBTIFF	304	0.83%
IE CSS	10	0.03%
IEPEERS	125	0.34%
JAVA TRUST	1196	3.27%
HACKING ATTEMPT	51	0.14%
MDAC	913	2.49%
HACKING ATTEMPT	46	0.13%
FLASH 10	29	0.08%

Menu

Simple statistics
Advanced statistics
Countries statistics
Referers statistics
Sources statistics
Clear statistics
Upload .exe
Exit

UNDERGROUND ECONOMY
ANY STREET 1234
ALMOST ANY COUNTRY

PHOENIX EXPLOIT KIT	120$
24/7 SUPPORT	38$

TOTAL: $158.00

Andromeda

Base Version $300
Advance Version with firewall bypass $500
Source code $7000
ICQ 5777677
jabber ar3s@dlab.org.in

Filter | All Records | List View

Current Filter: sNick Include 'waahoo'

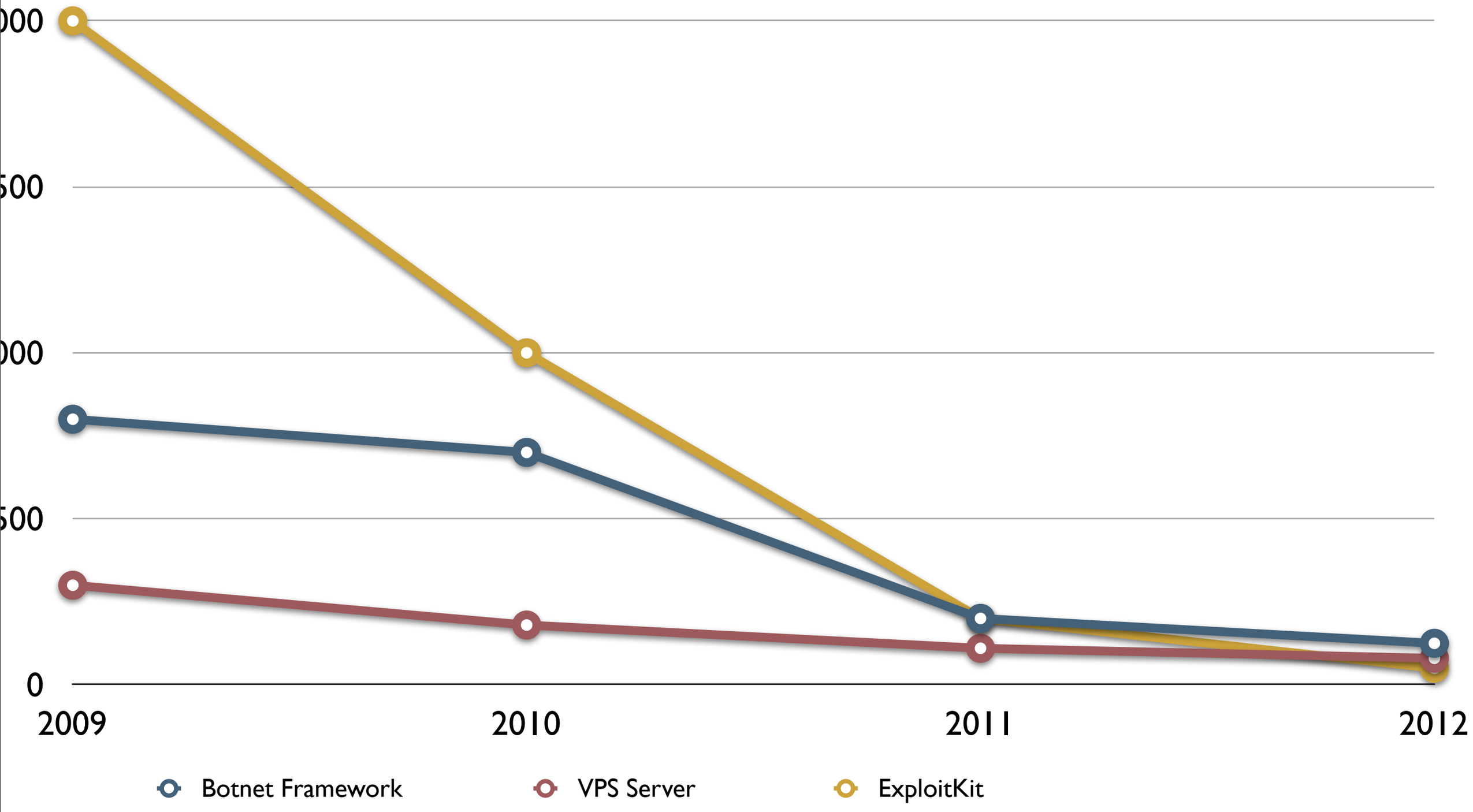
IDNick [1192]
sNick* [waahoo]
dDate* [2010-08-10 11:14:50]

Summary

Select a record to enter in form view, click on field name to order

#	Case ID	Date|Time	Comments
1	5403	2011-08-21 20:29:39	andromeda bot(software for using in botnet); pric
2	3812	2011-01-21 13:33:03	Jabber backdoor (asm) size - 8,5kb Clean 0/33 ht
3	3284	2010-11-22 11:42:00	!!!UP!!! jabber backdoor + shell backdoor - size
4	3279	2010-11-22 11:31:15	TeamViewerQS - local keylogger Price - 30wmz
5	1906	2010-08-10 11:14:50	Crypt(gluing) Price - 30wmz

Exploit Kit



Domain names for C&C

Your domain names (FQDN) are bulletproof

Almost nobody can bring your domain down

You can keep you privacy hidden

Good for fast-flux domain technics

Directnic.com

Internet.bs DomainContext

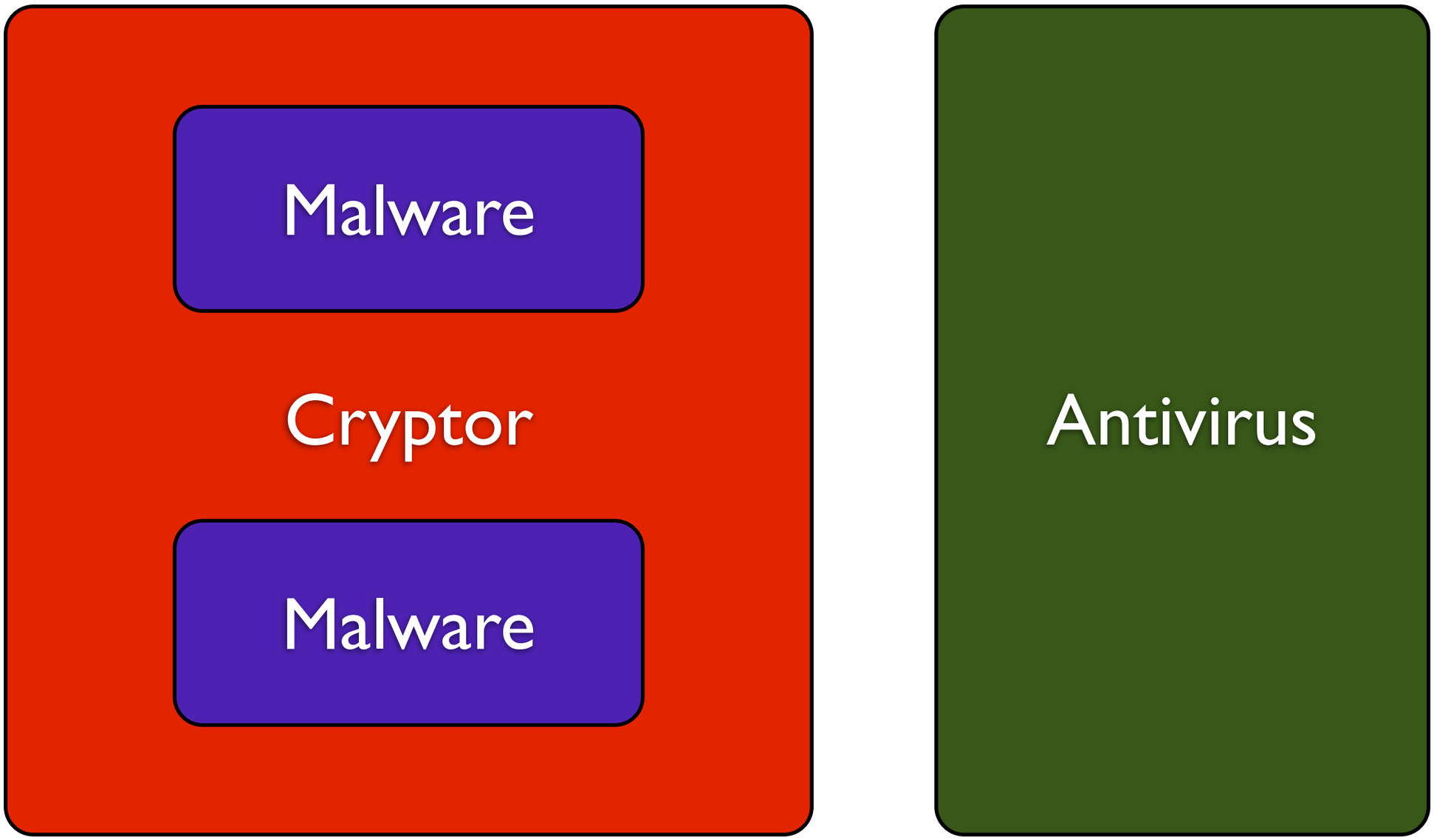
NetChinese
www.net-chinese.com
Global Domain Name Registration Center
繁體中文

UNDERGROUND ECONOMY
ANY STREET 1234
ALMOST ANY COUNTRY

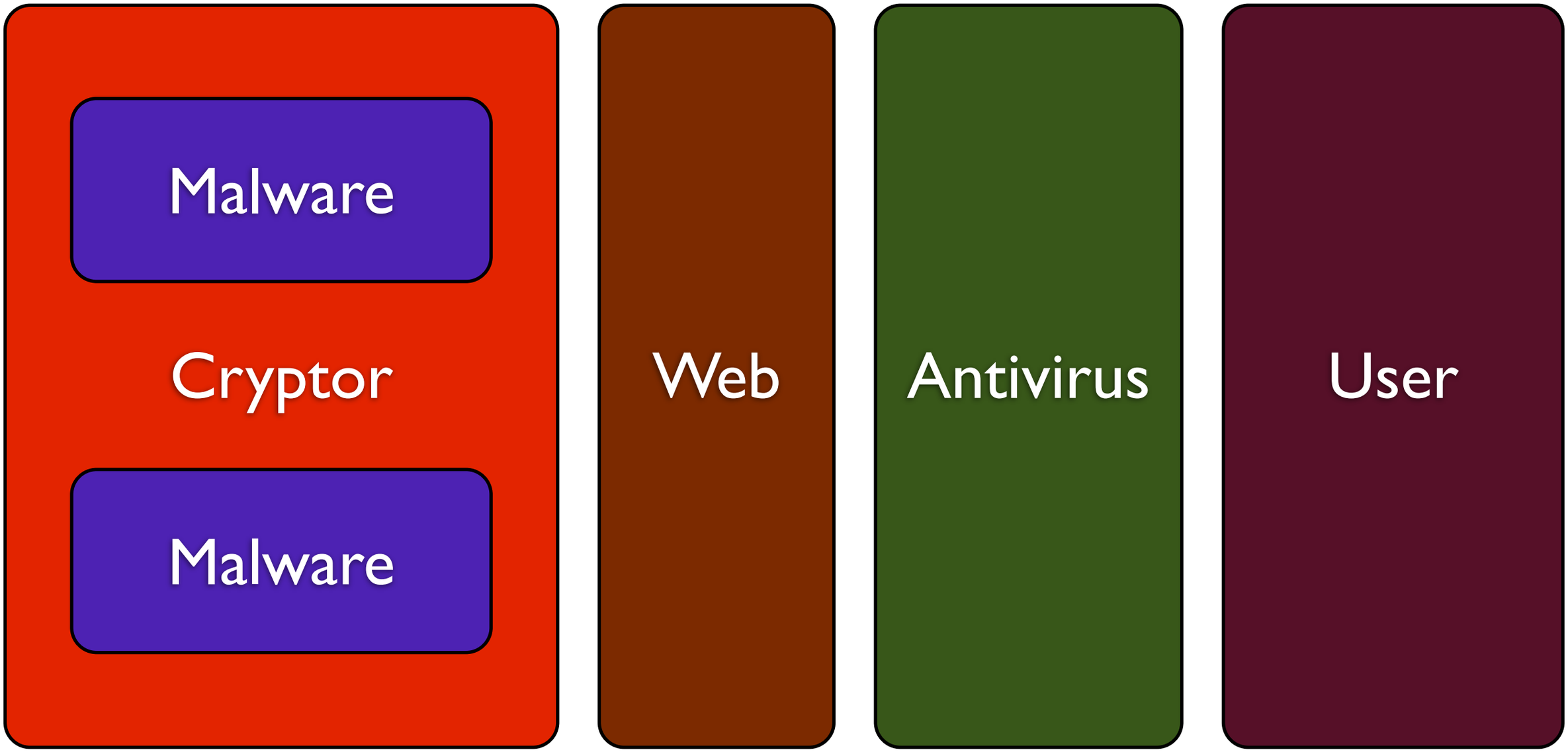
DOMAIN REG X10 $20

TOTAL: $20.00

Dropper file and crypt



Dropper file and crypt



Dropper file and crypt

Crypt files to make invisible for AV industry

Use self written crypt and stub files

Daily checks on cyber 'VirusTotal' like services

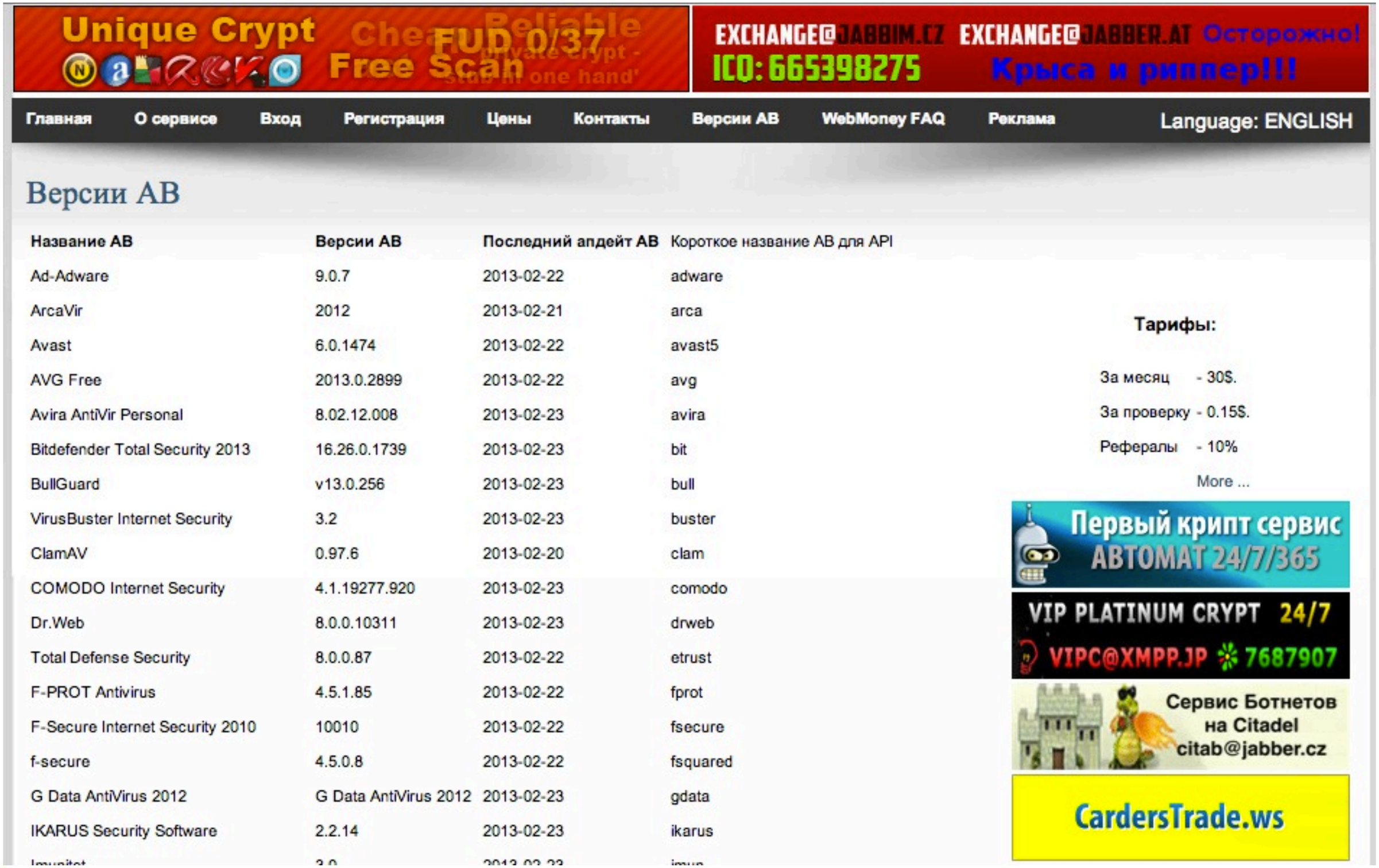
Updates if some of AV vendors detect dropper

Контакты:
http://www.darksapphire.ru/
ICQ = 616461816
Jabber = MrBlackGeneral@dlab.org.in
Skype = MrBlackGeneral

DLab
security laboratory

Sapphire Technology

Dropper file and crypt

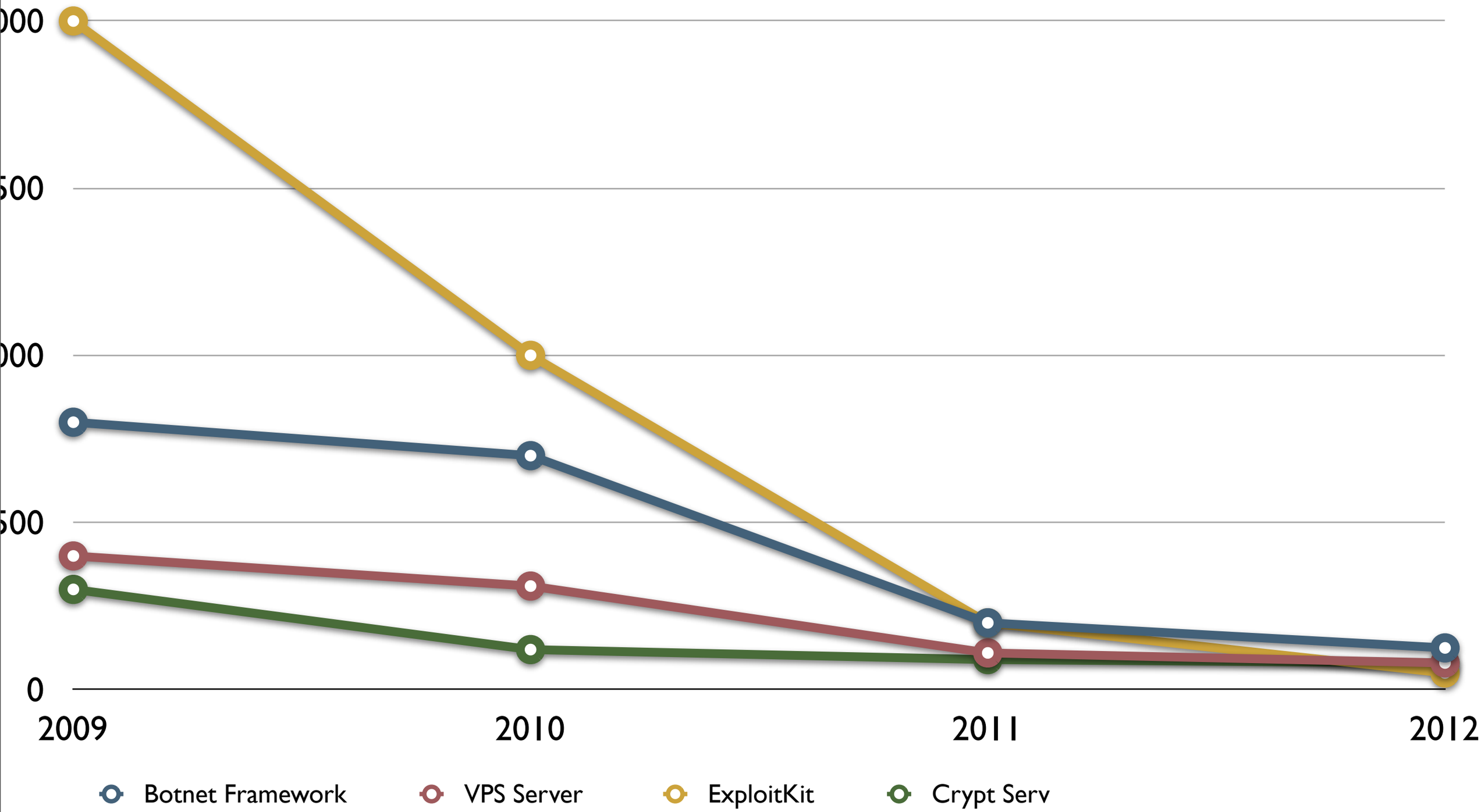


UNDERGROUND ECONOMY
ANY STREET 1234
ALMOST ANY COUNTRY

CRYPTOR	$14
AUTORUN INJECTOR	$8
ANTISANDBOX	$3
DAILY AV CHECK	$70

TOTAL: $95.00

Crypt Services



Injectors and other modules

Pin/Tan grabbers

Injectors for most bank accounts US/DE/UK/FR/ES

Setup maximum of withdrawals limit

Fake the balance amount after grabbin'

US:

##

BOFA - cc\cvv\exp\ssn\dob\adress\fullname\questions\answe rs\Balnce grabber.

CHASE - cc\cvv\pin\exp\mmn\dob\ssn\Balance grabber.

citizensbankonline.com - cc\cvv\exp\ssn\dob\adress\fullname\questions\answe rs\mail_adress.

firstcitizens.com - cc\cvv\exp\ssn\dob\adress\fullname\questions\answe rs.

pnc.com - cc\cvv\exp\ssn\dob\adress\fullname\questions\answe rs.

citybank.com - cc\pin\exp\ssn\dob\adress\fullname

wellsfargo- cc\cvv\pin\exp\mmn\dob\ssn\Balance grabber.

UNDERGROUND ECONOMY
ANY STREET 1234
ALMOST ANY COUNTRY

STANDART INJ. PACK	$80
SUPPORT 24/7	$8

TOTAL: $88.00

Total

	monthly	onetime
VPN Service	$25	$0
Botnet Framework	$40	$125
Bulletproof hosting	$52	$0
Exploit Kit	$38	$120
Domain names	$0	$20
Dropper file and crypt	$70	$25
Modules	$8	$80

Total: $225 $370

$595

Questions?

Thanks!