Introduction to Botnets
Who Uses Them & How

Jeff Bardin
www.treadstone71.com
207.415.4021
Intro to Botnets
What are they?
Botnets are the primary means for cyber-criminals to carry out their malicious tasks:

- sending spam mails
- launching denial-of-service attacks
- stealing personal data such as mail accounts, intellectual property, military secrets, embarrassing information or bank credentials
Bots: Putting the ‘(D)’ in (D)DoS

- A *bot* is a servant process on a compromised system (unbeknownst to the owner) usually installed by a Trojan or Worm.

- Communicates with a *handler* or *controller* via public servers or other compromised systems.

- A *botmaster* or *botherder* commands bots to perform any of a number of different functions.

- System of bots and controller(s) is referred to as a *botnet* or *zombie network*.

**Diagram:**

- **Attacker** (Botmaster)
- **Zombies**
Bot - a small program to remotely control a computer

Characterized by

- Remote control & communication (C&C) channels to command a victim
  - For ex., perform denial-of service attack, send spam
- The implemented remote commands
  - For ex., update bot binary to a new version, turn on your audio, video, keystroke log
- The spreading mechanisms to propagate it further
  - For ex., port scanning, email, privilege escalation
Botnets
DDoS
Anatomy of a DDoS Attack

Systems Become Infected

UK Broadband

Bots connect to a C&C to create an overlay network (botnet)

Provider

Internet Backbone

Bots attack

US Corp

Bye Bye!

US Broadband

BM

Botnet master issues attack command

Controller

Connects Botnet master

Issues attack

Command

Bots

Anatomy of a DDoS Attack
C&C channel

- Means of receiving and sending commands and information between the botmaster and the zombies.

- Typical protocols
  - IRC
  - HTTP – HTTPS

- Protocols imply (to an extent) a botnet’s communication topology.
  - The topology provides trades-off in terms of bandwidth, affectivity, stealth, and so forth.
How is a botnet organized?
Based on C&C channels, there are two typical botnet topologies:

- **Centralized**
- **Decentralized (P2P)**

**Traditional botnet metrics:**

- **Resiliency**
  - A botnet ability to cope with a loss of members (zombies) or servers
- **Latency**
  - Reliability in message transmission
- **Enumeration**
  - An ability to accurately estimate a botnet size
  - Difficulty for security analysis
- **Re-sale**
  - A possibility to carve off sections of the botnet for lease or resale to other operators.
Centralized botnet

- Classical communication method IRC (Internet Relay Chat)

Communication between attacker and zombies goes via centralized server
Centralized botnet topologies

- Centralized topology can be represented in different shapes.
- The exact organization of botnet depends on the bot operator.
  - nothing prevents a bot operator to come up with a new topology.
- Often seen topologies:
  - Star
  - Multi-Server
  - Hierarchical
  - Random

<table>
<thead>
<tr>
<th>Pros</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet awareness</td>
<td>Highly resilient</td>
<td>Command latency</td>
</tr>
<tr>
<td>Interception or hijacking of bot agents will not enumerate all members of the botnet and is unlikely to reveal the C&amp;C server.</td>
<td>Lack of a centralized C&amp;C infrastructure and the many-to-many communication links between bot agents make it very resilient to shutdown.</td>
<td>The ad hoc nature of links between bot agents make C&amp;C communication unpredictable, which can result in high levels of latency for some clusters of bot agents.</td>
</tr>
<tr>
<td>Ease of re-sale</td>
<td></td>
<td>Botnet enumeration</td>
</tr>
<tr>
<td>A botnet operator can easily carve off sections of their botnet for lease or resale to other operators.</td>
<td></td>
<td>Passive monitoring of communications from a single bot-compromised host can enumerate other members of the botnet.</td>
</tr>
</tbody>
</table>
How do they hide?
Outline

Encryption

Public Key

Private Key

Make sure you keep this to yourself, but we just found out...

7e6156506e... 2e7b27b1b16e 3255aeb7e916d 178884e518c1e84d2...

Fast Flux

IP1

IP2

IP3

IP4

IP5

IP6

IP7

IP8

Rootkit

Make sure you keep this to yourself, but we just found out...
Botnet malware use encryption techniques to avoid being detected by
**signature-based** Intrusion detection system.

<table>
<thead>
<tr>
<th>Rule (Signature)</th>
<th>Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet content includes:</td>
<td>07/23-09:46:41.866911 192.168.1.10 -&gt; 192.168.1.1 ICMP TTL:50 TOS:0x0 ID:2403</td>
</tr>
<tr>
<td>“08 09 0a 0b 0c 0d 0e 0f”</td>
<td>ID:8474  Seq:256 ECHO</td>
</tr>
<tr>
<td></td>
<td>36 12 7B 39 1B C6 0B 00</td>
</tr>
<tr>
<td></td>
<td>08 09 0A 0B 0C 0D 0E 0F</td>
</tr>
<tr>
<td></td>
<td>01 11 12 13 14 15 16 17</td>
</tr>
<tr>
<td></td>
<td>18 19 1A 1B 1C 1D 1E 1F</td>
</tr>
<tr>
<td></td>
<td>20 21 22 23 24 25 26 27</td>
</tr>
<tr>
<td></td>
<td>28 29 2A 2B 2C 2D 2E 2F</td>
</tr>
<tr>
<td></td>
<td>!&quot;#$%&amp;'()+,-./</td>
</tr>
<tr>
<td></td>
<td>30 31 32 33 34 35 36 37</td>
</tr>
<tr>
<td></td>
<td>01 23 45 67</td>
</tr>
</tbody>
</table>

**Matched**

**ALERT**
Fast Flux

IP addresses that are rotated in seconds against the same domain.

For example:

[QUESTION] Website name: www.lijg.ru

[ANSWER] IP Addresses:

- [www.lijg.ru](http://www.lijg.ru) → 68.124.161.76
- [www.lijg.ru](http://www.lijg.ru) → 69.14.27.151
- [www.lijg.ru](http://www.lijg.ru) → 70.251.45.186
- [www.lijg.ru](http://www.lijg.ru) → 71.12.89.105
- [www.lijg.ru](http://www.lijg.ru) → 71.235.251.99
- [www.lijg.ru](http://www.lijg.ru) → 75.11.10.101
- [www.lijg.ru](http://www.lijg.ru) → 75.75.104.133
- [www.lijg.ru](http://www.lijg.ru) → 97.104.40.246
- [www.lijg.ru](http://www.lijg.ru) → 173.16.99.131

.................
An Example of Fast Flux

2007-02-03 11:10:10 UTC Saturday

24 Hours of Fast-Flux

"Mothership"

Mom or Pops

Geo-location of IPs in flux for 1 domain (Web and DNS) - SANSFIRE 2007

A **rootkit** is a tool that is designed to hide itself and other processes, data, and/or activity on a system.

To hide what is taking place an attacker wants to:
- Survive system restart
- Hide processes
- Hide services
- Hide listening TCP/UDP ports
- Hide kernel modules
- Hide drivers
What do botnets do?
Botnet Activities

The least damage caused by Botnets:

Bandwidth Consumption

Other things:

- DDoS attacks
- Spam
- Click Fraud
- Data Theft
- Phishing
- Mistrustful services
DDoS

Bots connect to a C&C to create an overlay network (botnet)

Bye Bye!

Bots attack

Botnet master issues attack command

US Corp

US Broadband

Provider

Systems become infected

Internet Backbone
Click Fraud

- **Pay per Click (PPC)** is an Internet advertising model used on websites in which advertisers pay their host only when an ad is clicked.
- **Famous Bots:** ClickBot (100k), Bahama Botnet (200k)

### Overall Click Fraud Rate by Quarter

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Click Fraud Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q3-2008</td>
<td>16.0%</td>
</tr>
<tr>
<td>Q4-2008</td>
<td>17.1%</td>
</tr>
<tr>
<td>Q1-2009</td>
<td>13.8%</td>
</tr>
<tr>
<td>Q2-2009</td>
<td>12.7%</td>
</tr>
<tr>
<td>Q3-2009</td>
<td>14.1%</td>
</tr>
</tbody>
</table>
Click Fraud - FFSearcher

Trojan downloads file from a remote site/
Other malware drops file/
User unknowingly downloads file while visiting malicious websites

Trojan attaches an ADS to the legitimate system file,
netcfgx.dll:Zone.Identifier

Trojan connects to http://(BLOCKED).2.com/(Random characters)?version= to download its configuration file

Trojan saves the downloaded file as
%Documents and Settings%\All Users\Documents\gifnoc.xtx

Trojan monitors the user’s Web-browsing activities/
Trojan redirects Google searches to the website found in the configuration file

1. User’s system gets infected
2. User of an affected system searches on Google.com
3. Malware rewrites search results’ URLs
4. Google, thinking the user was referred by an "affiliate," pays the cybercriminals
5. Cybercriminals who rewrote the URLs earn money from Google each time a user clicks these
6. The more clicks on a rewritten URL, the more money cybercriminals earn

Data Theft

❖ Accounts for a great deal of botnet activity.
❖ Purpose: Harvesting user data
  ○ Screen captures
  ○ Typed data
  ○ UserIDs / Passwords
  ○ Audio/video
  ○ Files
❖ Anti-Malware
  ○ Bogus anti-virus software

Phishing

- A deceptive email/website/etc. to harvest confidential information.

![Phishing Example Image]
Botnets – The Cybercrime/Cyber Espionage Underground
How Cybercrime against Banks Works

1. Malware coder writes malicious software to exploit a computer vulnerability and installs a trojan.
2. Victim infected with credential-stealing malware.
4. Hacker retrieves banking credentials.
5. Remote access to compromised computer.
6. Hacker logs into victim’s online bank account.
7. Money transferred to mule.
8. Money transferred from mule to organizers.

Victims are both financial institutions and owners of infected machines.

Money mules transfer stolen money for criminals, shaving a small percentage for themselves.

Criminals come in many forms:
- Malware coder
- Malware exploiters
- Mule organization
Limit: 119 check(s) for next 2999 second(s).

// We set limit for this gate in security reasons. All u have 150 checks per each hour.

Amount: $ 0.10 - 9.95  Cost: 1 check.

Check track2
Format: NUMBER=YYMM, for example 4610460580687572=0506
Accept VISA, MASTERCARD, AMEX.

<table>
<thead>
<tr>
<th>CC_number</th>
<th>Auth_code</th>
<th>Auth_result</th>
<th>Amount</th>
<th>Type 1</th>
<th>Type 2/Region</th>
<th>Bank</th>
<th>Country</th>
<th>State</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>37127386192008</td>
<td>00</td>
<td>APPROVAL</td>
<td>4.43</td>
<td>Debit</td>
<td>PLATINUM</td>
<td>Sovereign Bank</td>
<td>United States</td>
<td>Pennsylvania</td>
<td>Wyoming</td>
</tr>
<tr>
<td>4036027070042487</td>
<td>00</td>
<td>APPROVAL</td>
<td>7.78</td>
<td>Debit</td>
<td>PLATINUM</td>
<td>Bankers Bank, The</td>
<td>Georgia</td>
<td>Atlanta</td>
<td></td>
</tr>
<tr>
<td>5516720000423419</td>
<td>00</td>
<td>APPROVAL</td>
<td>1.81</td>
<td>Debit</td>
<td>USA</td>
<td>Bankers Bank, The</td>
<td>New York</td>
<td>New York</td>
<td></td>
</tr>
<tr>
<td>5468110009832430</td>
<td>00</td>
<td>APPROVAL</td>
<td>3.93</td>
<td>Debit</td>
<td>USA</td>
<td>Citibank South Dakota, N.A.</td>
<td>New York</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4024115170688163</td>
<td>00</td>
<td>APPROVAL</td>
<td>4.18</td>
<td>Credit</td>
<td>GOLD/FREM</td>
<td>Visa Card Services, National Assoc</td>
<td>Delaware</td>
<td>Wilmington</td>
<td></td>
</tr>
<tr>
<td>4081010509816498</td>
<td>00</td>
<td>APPROVAL</td>
<td>0.91</td>
<td>Credit</td>
<td>SIGNATURE</td>
<td>Chase Bank USA, National Assoc</td>
<td>Delaware</td>
<td>Newark</td>
<td></td>
</tr>
<tr>
<td>4071141004744429</td>
<td>00</td>
<td>APPROVAL</td>
<td>1.88</td>
<td>Debit</td>
<td>PLATINUM</td>
<td>Bank of America, National Assoc</td>
<td>United States</td>
<td>North Carolina</td>
<td>Charlotte</td>
</tr>
<tr>
<td>403533000150674</td>
<td>00</td>
<td>APPROVAL</td>
<td>0.15</td>
<td>Debit</td>
<td>CLASSIC</td>
<td>New Bedford Credit Union</td>
<td>United States</td>
<td>Massachusetts</td>
<td>New Bedford</td>
</tr>
<tr>
<td>4045940089488312</td>
<td>00</td>
<td>APPROVAL</td>
<td>2.91</td>
<td>Debit</td>
<td>CLASSIC</td>
<td>Metro Credit Union</td>
<td>Massachusetts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40602043930068</td>
<td>00</td>
<td>APPROVAL</td>
<td>7.89</td>
<td>Debit</td>
<td>CLASSIC</td>
<td>Northern Bank &amp; Trust Company</td>
<td>Massachusetts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>406317000275617</td>
<td>51</td>
<td>DECLINE</td>
<td>6.27</td>
<td>Debit</td>
<td>CLASSIC</td>
<td>Merrimack Valley Federal Credit Un</td>
<td>United States</td>
<td>Rhode Island</td>
<td>North Andover</td>
</tr>
</tbody>
</table>

Checked: 19 pcs
Good day to all.

In stock for sell this countrys:

United States $2
United Kingdom $4
Europe - (it/fr/no/dk/es) $4 - $8
Germany $6

+ All time Online . Instant replace for bad ccs.
+ Good Discount for big amount orders.
+ Could check ccs before sell . if u want it .
+ MoneyBack - only if ccs were decline.

Replace
- I will change ccs withing 72h if urs checker result will be Decline or Hold-on by ccnum+exp
- I willnot guaranty good balance and any VBV/3D.
- If i find some Approved ccs from urs bad cc that u would replace - i willnot replace any ccs.
Contact ICQ : 676-003
I accept : Webmoney (WM) - Western Union (WU)
Dumps from FIRST HANDS (USA, EU)

I provide service, dumps from first hands.
Bin list ON REQUEST.
All dumps track2 only, sometimes both tracks!
In stock real great EU database. And US. AND ASIA
Dumps can be checked if u wish. or replace withing 48 hours unchecked
Minimum for order - 1 dump for webmoney payment
For WU, MG - 1500$

US, CANADA
VISA, MC CLASSIC - 20$
GOLD, PLATINUM/BUSINESS/CORP/SIGNATURE - 30$
AMEX - 15$ (ALL)
DISCOVER - 20-30$

EUROPE, ASIA, OTHER:
CLASSIC Swiss France Italy Turkey Germany Spain Australia - 100$(exclude known bins)
GOLD, PLATINUM/BUSINESS/CORP/SIGNATURE - 130$(exclude known bins)

Other countries - (201 code, etc)
CLASSIC - 60$
GOLD, PLATINUM/BUSINESS/CORP/SIGNATURE - 80$

Special price:
For Amex (us, eu)
For expired in this month price cost 1/2 of dump price.

We dont sell dumps with PIN, CVV2

ICQ - 164419326

Last edited by nCuX; 09-07-2007 at 12:21 AM.
Cyber Espionage Example

Finance person receives a junk email

Opens to see 2012 Recruitment plan with .xls file

RAT program installed utilizing Adobe Flash vulnerability

Pulls email out of junk email

Opens attachment from unknown sender

User has full desktop admin rights
System unpatched

Flat network allows full network scan

NMAP scan of network to collect sensitive information

Poison Ivy malware is initiated

FTP ports open
Server access allows elevation of privileges
Spread to other locations

FTP looks like all others
1000s of FTP servers already running

Sensitive information not encrypted

Collect data over a period of time

Split file, encrypt, ftp to good.mincesur.com (collection server)

Company is in the headlines
The Underground IT Organization

- **Botnet Owners**
  - Botnet Services
    - Malware Distribution Service
    - Data Acquisition Service
  - Intellectual Property Sensitive Info
    - Malware Writers
- **Validation Service**
  - Payment Gateways Intel Services
  - eCommerce Site
  - ICQ
  - Card Forums
- **Data Mining & Enrichment**
  - Information Collectors Intelligence
  - Trade Secrets – Military Data
- **Data Sales**
  - Credit Card Users
  - Master Criminals
- **Cashing**
- **Gambling**
  - eCurrency
  - Wire Transfer
  - Drop Service

**Nation-States – Foreign Intelligence Services - Cybercriminals – Cyber Terrorists – Industrial Espionage – Cyber Proxies**
Admin
Admin
Admin
Admin

Global Moderator
Supervises Content
Arbitrates Disputes

Moderator
Moderator
Moderator

Site Management (1st Level)
Reviewer
Reviewer
Reviewer
Reviewer

Monitor Individual
Topic Areas

Reviewer
Reviewer
Reviewer
Reviewer

Assess Quality of
Vendor Products

Reviewed Vendor
Reviewed Vendor
Reviewed Vendor
Reviewed Vendor

Hackers/Coders/Data Thieves
Reviewed Vendor
Reviewed Vendor
Reviewed Vendor
Reviewed Vendor

Have Permission
to Sell Goods/Services
To Forum Members

cybercriminals

Member
Member
Member
Member

Member
Member
Member
Member

Member
Member
Member
Member

Member
Member
Member
Member

Member
Member
Member
Member

Member
Member
Member
Member

Member
Member
Member
Member

Member
Member
Member
Member

Member
Member
Member
Member
Botnet Spread
Power Grid for North and South America?
Passive data collection by infiltrating the botnets directly with sophisticated risk analysis – compromised public IPs

Trojan-Downloader:W32/Hiloti identifies a family of programs that download and execute malicious files onto the affected system. When executed, the malware connects to a remote host to download configuration data, which may contain instructions to perform any of the following actions:

- Download and execute arbitrary files
- Display pop-ups
- Modify the content of HTML pages viewed by the user
- Insert scripts into HTML pages viewed by the user
Palevo is a so called bot kit that is being sold in underground forums (like ZeuS) using the name BUTterFly BOT. Therefore there are dozens of different botnets out there run by different criminal groups.

P2P filesharing programs (bearshare, imesh, emule, limewire etc.)
Instant messaging (MSN- / Windows Live Messenger)
Removable drives (like USB-Sticks)
In addition, criminals have been observed linking other spreading mechanisms such as windows filesharing spread with palevo to achieve maximum impact.
Geospatial view – Undetected by AV, Firewalls, IDS, etc
Coreflood Takedown
Operation Adeona
Coreflood

- Visit an infected website
  - Redirect to another site
  - Browser downloads malicious code
    - Executed

- Searches for data
  - Sensitive data
  - Aggregates data
  - Harvests userIDs / passwords in real time

- 8,485 bank accounts
- 3,233 credit card accounts
- 151,000 e-mail accounts
- 4,237 online retailer accounts
- 416 stock trading accounts
- 869 payment processor accounts
- 413 mortgage accounts and
- 422 finance company accounts
Coreflood Evolving

- One of the oldest botnets in continuous operation (+10 years)
- Motive turned from DDoS to selling anonymity services to full-fledged bank fraud
- Entire Windows domains infected at once (thousands of computers at some organizations)
- Over 378,000 computers infected during 16-month time frame
- Infected businesses, hospitals, government organizations, and even a state police agency

- FBI had to act
  - New variant about to be released
Defendants from running Coreflood on any computers not owned by the

Defendants, among other relief;

NOW, THEREFORE, IT IS HEREBY ORDERED AND DECREED

as follows:

1. The Defendants shall appear before this Court and

show cause, if any, why the Court should not enter a preliminary

injunction against them, providing the relief set forth in the Temporary

Restraining Order until final determination of this action, on the 25th
day of April 2011, at 10:00 a.m./p.m.

Dated: April 12, 2011

Hartford, Connecticut

IT IS SO ORDERED.

HON. VANESSA L. BRYANT
UNITED STATES DISTRICT JUDGE
SUPPLEMENTAL TEMPORARY RESTRAINING ORDER

WHEREAS the Court previously issued a Temporary
Restraining Order which, inter alia, authorized the Government to
operate a substitute server for the purpose of responding to command
and control requests from infected computers with instructions for the
Coreflood software to stop running; and

WHEREAS the Government has shown good cause to
operate a second such server for a period of approximately one week
for the same purpose;

NOW, THEREFORE, IT IS HEREBY ORDERED AND

this ___ day of April 2011, at _____ a.m./p.m.:

2. Pursuant to the authority granted by 28 U.S.C. § 566,
the United States Marshal for the District of Connecticut ("USMS")
shall execute and enforce the Temporary Restraining Order, with the
assistance of the Federal Bureau of Investigation ("FBI") if needed, by
establishing a second substitute server that will respond to requests
addressed to the Coreflood Domains by issuing instructions that will
cause the Coreflood software on infected computers to stop running,

4. Nothing in this Order shall permit the USMS or FBI to
store, review, or otherwise use any data that may be transmitted to
the second substitute server from an infected computer, other than
the originating IP address, network port, and the date and time of
transmission.

5. A copy of the Order shall be served on the Defendants
in accordance with the Order Authorizing Service.

The COREFLOOD DOMAINS

(1) adv-webhost.com
  Tertiary domain names:
    node1.adv-webhost.com
    alex.adv-webhost.com
  Registrant: Unknown
  Registry: Verisign, Inc.
  21355 Ridgetop Circle
  Dulles, Virginia
  DNS provider: Above.com Pty Ltd
  8 East Concourse,
  Beaumaris, VIC 3193, Australia

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia
Registrar: Above.com Pty Ltd
8 East Concourse,
Beaumaris, VIC 3193, Australia
To maximize the difficulty of taking down this bot, the criminal spread his domain registrations all over the world. He used Wild West Domains (US-AZ), Above.com (of Australia), Big Rock Solutions (of Mumbai), LiquidNet (UK), Network Solutions (US-Virginia), Active Registrar (Singapore), 1&1 Internet (Germany), TuCows (Toronto), Dotster (US-Washington), MyDomain, Inc (US-Washington), DomainRegistry.com (US-New Jersey), and Melbourne IT (which is Yahoo!’s registrar of choice), Mesh Digital (UK), Misk.com (US-NY), Moniker (US-Florida), and Directi (India), respectively. The Internet domain names used to identify the C&C servers for the Coreflood Botnet are changed and updated regularly.

A mutual legal assistance treaty is an agreement between two countries for the purpose of gathering and exchanging information in an effort to enforce public laws or criminal laws. Assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries. Some treaties may encourage assistance with legal aid for nationals in other countries.
a. Each registry or registrar of one of the Coreflood Domains receiving notice of this Order shall set the authoritative DNS name servers for that Internet domain name as follows, and shall impose a registry lock on the Internet domain name and shall lock any account associated with the registrant of the Internet domain name to prevent any change, transfer, or deletion of such Internet domain name or account:

   SINKHOLE-00.SHADOWSERVER.ORG
   IP address: 87.106.24.200

   SINKHOLE-01.SHADOWSERVER.ORG
   IP address: 87.106.26.9

b. Each DNS provider for one of the Coreflood Domains receiving notice of this Order shall respond to DNS resolution requests for that Internet domain name by returning the IP address 127.0.0.1, and shall lock any account associated with the Internet domain name to prevent any change, transfer, or deletion of such account.
Shadowserver Sinkholes

C&C – Command and Control Servers
Bot – infected PCs
Shadowserver.org
After the Takedown

Operation ADEONA: Daily Coreflood beacons
Thousands of beacons

<table>
<thead>
<tr>
<th>Date</th>
<th>Beacons</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/13</td>
<td>800</td>
</tr>
<tr>
<td>4/14</td>
<td>700</td>
</tr>
<tr>
<td>4/15</td>
<td>600</td>
</tr>
<tr>
<td>4/16</td>
<td>500</td>
</tr>
<tr>
<td>4/17</td>
<td>400</td>
</tr>
<tr>
<td>4/18</td>
<td>300</td>
</tr>
<tr>
<td>4/19</td>
<td>200</td>
</tr>
<tr>
<td>4/20</td>
<td>100</td>
</tr>
<tr>
<td>4/21</td>
<td>100</td>
</tr>
<tr>
<td>4/22</td>
<td>0</td>
</tr>
</tbody>
</table>
Introduction to Botnets

- Introduction to Botnets
- Organization
- How they hide
- What do they do
- Cybercrime – Cyber Espionage
- Coreflood takedown
jbardin@treadstone71.com
www.treadstone71.com
207.415.4021 – Cell/SMS