Becoming the 6-million-dollar Man

Gunter Ollmann, VP Research
gollmann@damballa.com
• 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/
ALL CHARACTERS AND EVENTS IN THIS SHOW--
EVEN THOSE BASED ON REAL PEOPLE--ARE ENTIRELY FICTIONAL.
ALL CELEBRITY VOICES ARE IMPERSONATED.....POORLY. THE FOLLOWING PROGRAM CONTAINS
COARSE LANGUAGE AND DUE TO ITS CONTENT IT SHOULD NOT BE VIEWED BY ANYONE
• What this talk is...
  – Understanding the profession
  – Demystifying a sophisticated threat
  – Examining monetization models

• What this talk isn’t...
  – A “how to” guide on building a better botnet
  – Being a better criminal
BOTNETS – are not as scary as you may think...
A collection of “bits and pieces”

A piece of “art”
Key stages to becoming a millionaire

• Build a business plan,
• Execute the business plan,
• Avoid attention,
• Retire early.
• Different countries, different laws...
  – Botnets may not be illegal
  – Building/distributing malware may not be illegal

• Building botnets for fun & profit
  – Don’t need to be hard-core criminal
  – Tools, guides, how-to’s, vendors, sponsors, etc.
  – It’s a “business like any other”
A Newbie Botmasters code

• Don't get caught
  – Take extreme care when setting things up
  – Don't start any bad habits from the beginning
  – Mistakes & leaks at the beginning are fatal

• Don't to criminal harm
  – Don't want to start a war nor be involved in deeply political events
  – Don't want to case any deaths
  – Don't want to get in bed with organized crime (as customers = ok)
Key things to remember

• Resilience is damned important
  – Triple modular redundancy (TMR)

• Botnets are the tool
  – Don't blame the tool!

• Show me the money!
  – Cashless ecosystems are ok...
  – ...but you can’t retire with them

• Want to be rich!
  – But want to retire rich; not in jail!
Connecting to the CnC (1)

• Separate work from pleasure
  – Dedicated laptop(s) for building and running the botnet business

• (Un)traceability
  – Change MAC addresses regularly
  – Different Web browsers and turned off cookie caching.
  – Use a (patched) base install machine

• Encrypt all CnC traffic
  – Asymmetric keys = much preferred.
• Deniability is important -
  – Open WiFi is your friend
  – Locations that don't have CCTV
• Don't connect directly - Ever!
  – Anonymous proxy and TOR networks are preferred
• Hiding in the masses
  – Academic networks + libraries
• Free WiFi access points
  – Physical location changes
• Change the MAC address
• Don’t want initial “seed money” traced
  – Rebate cards and systems
    • Deniability and no trace back
  – Visa rebate cards vs gift cards
    • Theft not necessary initially
• Payment for initial services
  – Domain, NS, hosting, proxy, etc.
  – Toolkits, plug-ins, exploit packs, contractors
Foreign Bank Accounts

• Create foreign banking accounts
  – "In person" account creation = less evidence
  – May need a physical address

• In threes...
  – Swiss numbered account
    • Minimum balance to open the account (plus fees)
  – Cayman Island Account
  – Panama Bearer Share Corporation account

• Bilateral agreements covering fraud
  – Disclosure of owner details
  – want to stay away from the fraud aspect

• Most accounts include
  – Credit cards
  – online banking
Retirement Planning?

- Afghanistan
- Algeria
- Andorra
- Angola
- Armenia
- Bahrain
- Bangladesh
- Bosnia and Herzegovina
- Bhutan
- Botswana
- Brunei
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Cape Verde
- Central African Republic
- Chad
- China
- Comoros
- Cote d' Ivoire
- Congo
- Djibouti
- Equatorial Guinea
- Ethiopia
- Gabon
- Guinea
- Guinea Bissau
- Indonesia
- Iran
- Ivory Coast
- Jordan
- Kuwait
- Laos
- Lebanon
- Libya
- Madagascar
- Marshall Islands
- Mali
- Maldives
- Mauritania
- Mongolia
- Morocco
- Mozambique
- Nepal
- Niger
- Oman
- Philippines
- Qatar
- Russian Federation
- Rwanda
- Samoa
- Sao Tome e Principe
- Saudi Arabia
- Senegal
- Somalia
- Sudan
- Syria
- Togo
- Tunisia
- Uganda
- United Arab Emirates
- Vanuatu
- Vietnam
- Yemen
- Zaire
- Zaire
- (Plus some more...)

aka. non-extradition countries (with the USA)
A Business Plan

• 12 month plan
  – loaded to the back end - increase profit percentage

• **Goal of earning $6million within a year**
  – Must be profitable
  – Don't want to be in Jail
  – Would prefer to have a robust business
    • have higher revenue (and profits) in Year 2.

• **12 month plan/target**
  – Q1 - $400k - 10% ($40k - $13.3kpm)
  – Q2 - $800k - 15% ($120k - $40kpm)
  – Q3 - $1.6m -20% ($320k - $106kpm)
  – Q4 - $3m - 25% ($750 - $250kpm)
  – $1.23m profit "tax free"
• Getting started in the criminal botnet business isn’t for the feint-hearted.
The First Botnet

• “Off the shelf” DIY botnet construction kit
  – Zeus, SpyEye, Butterfly, etc.

• Seeding torrents & newsgroups
  – Anonymous submission
  – Very difficult to trackback
  – Doesn't rely upon
  – Natural propagation & infection

• Dynamic DNS for CnC
  – Free and anonymous
Simple Hierarchical CnC Structure

- **Multiple CnC servers**
  - Bot agent communications over HTTP
  - Service paid via reward/rebate cards
- **First botnet(s) = PoC**
  - Validating principles
  - Default agent functions – password/identity theft
Underground Newbie Reputation

• Need to build a reputation...
  – Peer recognition and "trust" is key
    • Initially rely upon other people vouching
  – Activity on various hacker/botnet forums
    • Could use translators to hide identity origins
      ...but probably too much effort
  – Offer a lot of data/tools for free
    • Work to establish professional reputation
    • Value often based upon "freshness" of data

• How to pay
  – Non-revocable money transfers
  – Volumes of stolen credentials
  – Segments of a botnet
<table>
<thead>
<tr>
<th>Thread / Author</th>
<th>Replies</th>
<th>Views</th>
<th>Rating</th>
<th>Last Post</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Release] 666 Auto-Whaler v2.0</td>
<td>202</td>
<td>6,332</td>
<td>4</td>
<td>Today 01:17 PM, Last Post: sean013</td>
</tr>
<tr>
<td>NEW FACEBOOK HACK HURRY WILL NOT WORK SOON..</td>
<td>25</td>
<td>199</td>
<td>4</td>
<td>Today 01:17 PM, Last Post: VirtualDUDE</td>
</tr>
<tr>
<td>[DEV] xDos v1 Revision1 [DEV] ePixel</td>
<td>2</td>
<td>42</td>
<td>4</td>
<td>Today 01:13 PM, Last Post: LEGIT</td>
</tr>
<tr>
<td>Poll: [ YouTube ] Comment 4 Comment - More Views</td>
<td>4</td>
<td>30</td>
<td>4</td>
<td>Today 01:10 PM, Last Post: carl08s</td>
</tr>
</tbody>
</table>

VipVince
I am Ownage.

Posts: 1,552
Joined: Apr 2008
Reputation: 46
h4x$: 2,217.00

MortalKombat
Administrator

Internet Explorer (6/7) Remote Code Execution - Remote User Add Exploit

Code:
Content visible to Active users only. For Active Your User Read This :
Read This First - Before You Register - Or - Post Your Introduction.
Evolution of the “standard” bot agent

• As the botnet grows, new demands...
  – More bots, more spreading – more detection

• Malware doing slightly more
  – Pull back stored personal data
  – Keylogging etc.
  – Harvesting more data that may be saleable - email addresses etc.

• Malware components become more important
  – Spend some money on additional functionality
  – Add a few more malware components that will be installed with the standard deployment
  – Do some serial variants - with quality control
  – Release a new variant every day
Build to Sell

ITAL FLORIDA TRIESTE

22.06.2007
• Important factors in “build to sell” models
  – Structure of the botnet
  – Past use/abuse of the botnet
  – Location of the botnet victims
  – Robustness of malware agent
  – Reputation in seller forums

• Pre-processing of botnets
  – Splitting and clustering of related victims
  – Harvesting of system and user information
  – Synchronizing malware and CnC channel
• Everyday access to 100k-2M bots
  – Price range from $200 (24hr use) to $50k (to own)
• Self-build botnet provisioning
  – Off-the-shelf tools
  – Avg. 20k bots within a week (500k if optimized)
• Commissioned building of botnet
  – Target centric pricing
Buying Botnets

<table>
<thead>
<tr>
<th>Country</th>
<th>Price for 1k</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU</td>
<td>300$</td>
</tr>
<tr>
<td>DE</td>
<td>220$</td>
</tr>
<tr>
<td>GB</td>
<td>210$</td>
</tr>
<tr>
<td>IT</td>
<td>200$</td>
</tr>
<tr>
<td>NZ</td>
<td>200$</td>
</tr>
<tr>
<td>ES</td>
<td>200$</td>
</tr>
<tr>
<td>US</td>
<td>110$</td>
</tr>
<tr>
<td>BG</td>
<td>100$</td>
</tr>
<tr>
<td>DK</td>
<td>100$</td>
</tr>
<tr>
<td>FR</td>
<td>100$</td>
</tr>
<tr>
<td>PT</td>
<td>100$</td>
</tr>
<tr>
<td>NL</td>
<td>100$</td>
</tr>
<tr>
<td>CA</td>
<td>80$</td>
</tr>
<tr>
<td>JP</td>
<td>80$</td>
</tr>
<tr>
<td>SE</td>
<td>70$</td>
</tr>
<tr>
<td>BE</td>
<td>60$</td>
</tr>
<tr>
<td>TR</td>
<td>60$</td>
</tr>
<tr>
<td>NO</td>
<td>50$</td>
</tr>
</tbody>
</table>

Order now
Lease (part of) an existing botnet

Web-based portal bot-management
For a small fee, attackers can rent/purchase members of a larger botnet. Online tools enable remote management and configuration of the botnet agents. Portals include performance monitoring tools – how fast is the spam being sent, DDoS throughput, etc.
• "Unique" malware updates – daily updates of the binary
  – QA assured malware
  – Better able to disable host defenses
  – Ability to host other malware - from third-parties

• Network propagation and reconnaissance
  – higher probability of detection
  – consider sniffing and capturing local corporate data (e.g. internal mail addresses etc.)
Malware Construction

• Serial variant production systems
  – New and unique piece of malware
  – “on the fly” creation by exploit systems

• New bot agent for every victim
  – Frequent updates of malware agents (every 24hrs)
  – Designed to avoid detection
  – “ Locked” to a victims machine & strong crypto
It’s Done for a Reason…

Infector Sites

Dropper Site

Internet

Update Site

CnC Site(s)

Dropper

Connection & Time

Identity Cache

Bot Agent

Commands & Data

Victim

Update
Using the stolen data directly

• **Payment and growth**
  – Payment for disposable services
    • Start investing in systems that will take live payment data (paypal accounts etc.) and auto procure hosting, domain names, etc.
  – Systems that allow botnets to scale
    • New domain name registrations
    • New NS provisioning

• **Begin to use them for personalizing infections**
  – Social engineering email recipients Re:

• **Social Network integration**
  – sending messages etc.
Spear Phishing Services
Lists of Executive Targets

- Access to executive target lists
  - Easy, plenty of sellers.
  - Much of the information is publicly available
Corporate Address Book Scraping

- Target corporate address books
  - Names, positions, email, phone, mobile,...
Lists of Leads – i.e. “Targets”

• Lists available through black, gray and white markets
  – Black = Acquired in underground forums & sellers
  – Gray = Sellers with clear or probable blackhat ties
  – White = Commercial leads vendors and public lists

• Conveniently formatted for automated processing
  – CVS and “standardized” file formats
  – Direct feed in to spam email tools
  – Ready for phishing template integration
Targeted Delivery

• Email and/or malware delivery services
  – Targeted at organizations, professions or whales

• Botnet rendered services
  – Targeted messaging (maybe broader than email)
  – Hosting of malware & infector components
  – Enumeration of target organization
  – Selling of existing botnet/agent access
Whaling = Targeting the biggest & most visible executives

- C-level Executives & Board
- Senior Management
- Managers
- All other employees

High cost targets
May be easy to identify and infiltrate
Company value dictates infection value
$500-$100k per instance
• **Horizontal Spear** = Targeting a specific role across similar industries using field-specific terminology.

_Multiple Organization Targets_

Tuning of message and campaign
Cost of service based upon volume
$20-$200 per head (in bulk)
**Vertical Spear Phishing**

• **Vertical Spear** = Exploiting relationships and hierarchy within the targeted organization

• Messages reference people within the organization

• Each victim helps illuminate more of the hierarchy

• Exploitation of trust relationships

• Copy/Paste of real internal email content for authenticity

---

**Single Organization Target**

Costly to perform – manual work
Cost of service based upon time
$ unknown
Multiple Botnets & Campaigns

• Common myth of one botnet per botmaster
  – Don’t want to lose everything in one go
  – Distinct botnets for specialized services
  – Easier to manage, scale and sell
• Botnet building via Campaigns
  – Multiple waves of attack
  – Multiple vectors
  – Multiple themes
  – Different payloads
• May or may not use all/some/none of existing CnC infrastructure
• OK to infect systems multiple times
Multiple Botnets & Campaigns

- **Extraction of personal/business data**
  - Different delivery vehicles = different results/yield

- **Pick different themes**
  - Adobe updates, MS updates, Fake AV etc.
  - Redirection to infection sites - use exploit kits (off the shelf) - but will swap botnets for access to 0-day

- **Selling systems to other operators**
  - Undertake custom campaigns
  - Deliver someone else's malware to a particular target
• Costs/earnings from campaign delivery
Affiliate Web Marketing/Spam
• Spam is easy...
  – Default in malware agents
  – Botnet of 10,000
    • 100+M standard emails p/day
    • 5+M malware email p/day

• Spam is hard...
  – 80% of US/EU spam generated by ~100 hard-core spam gangs
  – Not a lot of money to be made
  – EOL to most botnets
Pharmacy Affiliates

WELCOME TO GLAVMED

GlavMed is the BEST way to convert your pharmacy traffic into real money. Forget miserable sums you get, when you send your visitors to PPC pharmacy. Converting traffic this way, you're losing at least half of YOUR money.

GlavMed gives you an opportunity to eliminate any agents and sell the most popular pharmacy products directly to your customers. This way you get 30-40% revenue share.

FEATURES & BENEFITS

- Highest Industry Commissions
- Most Popular Pharmacy Products
- Biweekly Payments and Payout-on-Demand
- Co-Branding Program Open Your Own Shop
- Easy Account Setup and Friendly Support
- Advanced Realtime Statistics and Reports

Commission Based Sales (30-40%)
Revenue Aspects

- **Pharmaceutical Support**
- **Rates vary wildly**
  - Message delivery
    - 1,000 to 25,000 per $1
  - Ad injection
    - $0.01 to $0.12 per click
  - DNS/Fluxing
    - $0.5 to $20 per day/domain
  - Affiliate site hosting
    - $1 to $8 per day/domain
  - Blackhat SEO
    - $1 to $500 per day/domain
iFrame Traffic

Increase revenue from your website in 5 minutes

- All sites accepted
- Starting from 25 cents per 1000 users daily
- Absolutely clear for you visitors!
- No Illegal activities.
- No exploits, No Trojans, No Pop-ups.
- Human verified sites only.
- Simple and Fast installation. Hidden iframe 1x1 pix.

Increase your Rating popularity (Top-sites, Feeds, Banner eXchange, etc...)

- iFrame traffic ONLY for Clean Resources
- GEO Targeting
- Speed settings. (Amount of users per hour)
- Time Targeting (receive traffic only in preferred hours)
- Only real users. Without proxy and with referers.
- Only Real IP users. No fakes and cookies.
- Discounts for permanent clients.
- We accept: Webmoney, FET,
URL Management

Blackhat USA 2010 – Becoming the 6-million-dollar Man – Gunter Ollmann
Identity laundering and the grey-market

• Markets for all kinds of residential and corporate PII
• Black-market routes
  – Selling of authentication credentials
  – Fraud, theft and targeted attacks
• Grey-market routes
  – Family/Corporate “units” sold together
  – Laundering of identities
• Scamming legitimate PII outlets
  – Monetizing lists en mass
“Send your emails to more than 2,600,000+ TARGETED potential customers EVERY DAY! That means over 78,000,000+ prospects each month (and growing!). All our Email Lists are 100% Opt-in and completely legal to be used. Your ad will reach only those prospects who have asked to be included in Opt-in Email Lists for people interested in new business opportunities, products and services.”

Payment options: Paypal Western Union, Liberty Reserve…
Timeliness Matters
Fresh and (daily) validated accounts sold in batches. CSV-formatted for easy tool integration.
Raising the Stakes

• Moving beyond bulk sales of stolen data

• Gray market validation of data
  – Email addresses,
  – Personal identities,
  – Corporate mailing lists and hierarchy

• Transition from a few cents per record to a few dollars...

• Hosting of web sites that take financial application submissions
  – have to be careful not to be too obvious...
Obscuring the Source

Direct
- Hacker Forums
- Carder Forums

Reseller
- Buy/Sell in bulk
- Telemarketing lists

Proxy
- Affiliate schemes
- Vetting of lists
- Web forms

1¢
10¢
$5

7/18/2010
Blackhat USA 2010 – Becoming the 6-million-dollar Man – Gunter Ollmann
Lead Exchanges & Portals

Lead Exchanges
Matching buyers with sellers. Mixes with “work from home” Specialist and vetted exchanges
Grey-market Info Laundering

Sell Identity Profiles
Grey-market for stolen and pilfered PII.
Purchase “leads” for other scams and activities
Affiliate Programs
Sell the previously acquired leads.
Automate submission of “vetted” leads.
Pricing

**Pricing Schemes**
Quality, timeliness, details, clustering and volume all affect the value

---

**New Homeowner**
Consumers who have recently bought a home, are new to a neighborhood and have specific purchasing needs

<table>
<thead>
<tr>
<th>Qty</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>250</td>
<td>$21.25</td>
</tr>
<tr>
<td>1000</td>
<td>$82.90</td>
</tr>
<tr>
<td>5000</td>
<td>$404.00</td>
</tr>
<tr>
<td>10000</td>
<td>$788.00</td>
</tr>
<tr>
<td>25000</td>
<td>$1,920.00</td>
</tr>
<tr>
<td>50000</td>
<td>$3,745.00</td>
</tr>
</tbody>
</table>

Minimum Order: $60.00

**New Mover**
Consumers who have recently moved and are looking to establish relationships with a wide range of businesses

<table>
<thead>
<tr>
<th>Qty</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>250</td>
<td>$21.25</td>
</tr>
<tr>
<td>1000</td>
<td>$82.90</td>
</tr>
<tr>
<td>5000</td>
<td>$404.00</td>
</tr>
<tr>
<td>10000</td>
<td>$788.00</td>
</tr>
<tr>
<td>25000</td>
<td>$1,920.00</td>
</tr>
<tr>
<td>50000</td>
<td>$3,745.00</td>
</tr>
</tbody>
</table>

Minimum Order: $50.00

---

**Business**
National Business database includes demographic and credit information, all industries and geographic regions

<table>
<thead>
<tr>
<th>Qty</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>$50.00</td>
</tr>
<tr>
<td>1000</td>
<td>$97.50</td>
</tr>
<tr>
<td>2500</td>
<td>$184.50</td>
</tr>
<tr>
<td>5000</td>
<td>$250.00</td>
</tr>
<tr>
<td>10000</td>
<td>$350.00</td>
</tr>
<tr>
<td>25000</td>
<td>$750.00</td>
</tr>
<tr>
<td>50000</td>
<td>$1,475.00</td>
</tr>
</tbody>
</table>

Minimum Order: $50.00

---

**OK, count me in.** I want to try your **100% guaranteed** direct-mail mailing list of fresh, hot, responsive Opportunity Seekers names. I understand you will **refund 50¢ for each undeliverable** returned to you within 60 days from the date I place my order. On this basis please fill my order as follows:

**Please select a quantity:**
- 200 names and addresses — $25  **Sale $20**
- 500 names and addresses — $40  **Sale $32**
- 1,000 names and addresses — $70  **Sale $56**
- 2,000 names and addresses — $110  **Sale $88**
- 5,000 names and addresses — $250  **Sale $200**
- 10,000 names and addresses — $400  **Sale $320**
- 20,000 names and addresses — $680  **Sale $544**
- 30,000 names and addresses — $900  **Sale $720**

**Please select a format:**
- Pressure sensitive (peel-n-stick) labels
- On CD (standard comma-separated text file)
- 3.5" computer disk (standard text file)
- Via email (standard text file)

**Please select a zip-sorting method:**
- Random nationwide (unsorted) zip codes
- Zip-code sorted — ascending zip codes (1,000 name minimum)
The Aging Process
Identity information aging

- Stolen identity info ages rapidly
  - Abuse frequency drives down value
  - Type of abuse has most affect on value

- Sell aged leads
  - Normal cost per lead = $20
  - Price reduces by $5 every 7 days
  - Price reduces by 20% each time it is sold
  - Price for a specific state (increases by) 50%
An Aging Bot Victim

- Noisiness decreases value
  - Noticed by victim/ISP/target
- Botnet can be sold to others
  - Specialist operators

Value

Age & Noisiness

- Identity Theft
- Info Stealing
- Reputation Theft
- Botnet hosting services
- Pay-per-install
- Click Fraud
- Spam
- DDoS
Aging the Systems

- How long do I retain access and extract info from the victim systems?
- Methods of classifying the value of the host
  - IP address - certain countries are more interesting than others - trade systems with other operators
  - Corporate, hosting or residential - sale value in boutique markets
  - Has data already been extracted?
  Rate of new data is limited etc.
**Updates**

- New (signed) config.
- New “locked” agent

**Bot Agent**

- Public-key Crypto
- CnC config. signed
- Multiple CnC listed
- Unique victim ID

**CnC Servers & Drop Sites**

- Multiple CnC servers in multiple locations
- Unique victim ID verification
- Symmetric key data/channel encryption

**DNS Services**

- Multiple authoritative DNS servers
- CnC server A record fluxing (fast-flux)
- Domain Registrar NS updates (double-flux)

**Increased Agent Robustness**

7/18/2010

Blackhat USA 2010 – Becoming the 6-million-dollar Man – Gunter Ollmann
Virtual Identity

- **Botnet(s) already copied/duplicated identities**
  - Social networks, email relationships, family units
  - 2½ multiplier – “identities” versus bot installs

- **Creation of new & virtual-only identities**
  - Manage between 20 to 100 identities per bot

- **Inherited reputation**
  - Known good identity vouching for a newbie
  - Duplication of live actions to virtual identities
    - Copy comments/posts to other sites/boards
    - Replay browsing actions
Virtual Virtual Identities

• Abusing stolen identities
  – Insert messages to drive spam, infections, actions
  – Quick to get noticed & not overly scalable

• The virtual virtual identity
  – Bot-only derived/driven identities and groups
  – Recursive feedback loop of vouching & reputation
  – Email addresses, postal addresses, phone numbers, etc.
Reputation Scams

• Plenty of past abuse
  – Stock trading – inflating/deflating prices
  – “Free stuff” accounts – selling & trading objects
  – Sales rank – selective purchasing (e.g. iTunes)
  – Building groups – herd mentality

• Online reputation & voting systems key
  – Virtual votes are increasingly important
  – Can greatly influence trends and drive decisions
  – Raise or sink a business
Long-term Investment

• Sizable effort in managing/refreshing identities
  – Value increases over time (reputation aging)

• Different levels of identity
  – Non-newbie member through to full family unit w/history

• Can often use a real identity
  – If the application doesn't make it clear that they've just done something
“An Army of One”

• Reputation scams
  – Craigslist (etc.) sellers – comments on past service
  – Betting agencies – voting in “dancing with the stars”
  – Placement guarantee – “car of the year” awards
  – Influencing the news – million members for piracy
  – Lobbying – state and local “citizen” feedback

• Making money
  – Racketeering
    • Small vendors = $20 to $100 per month
  – Buying votes
    • Common social platform identities = $100 per 1,000
Conclusions

• Business models are varied
  – Botnet building is easy to grasp
  – Revenue models for botnet monetization = broad
  – Move away from short-lived/noisy to continuous p0wn

• Biggest earners on cash/reward
  – Short-term = Campaign building of botnets
  – Medium-term = Identity laundering
  – Long-term = Virtual reputation abuse
Locating Botnets

• Identification using attack output
  – Spam, DoS, Brute-force, etc.

• Based upon CnC infrastructure
  – Hosting facilities, domain names, DNS, IP, etc.

• Enumeration of victim groups
  – IRC and P2P infiltration, server hijacking, etc.

• Communications with CnC
  – Instructions being sent/received between bot master and victim
• Lets be clear though...
• The probability that “your” botnet is illegal is high...
• If you’re doing criminal things, you will be identified...
  ...and there’s a high probability you will be caught...
  ...but not guaranteed
Thank You

Gunter Ollmann

email: gollmann@damballa.com