



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.**



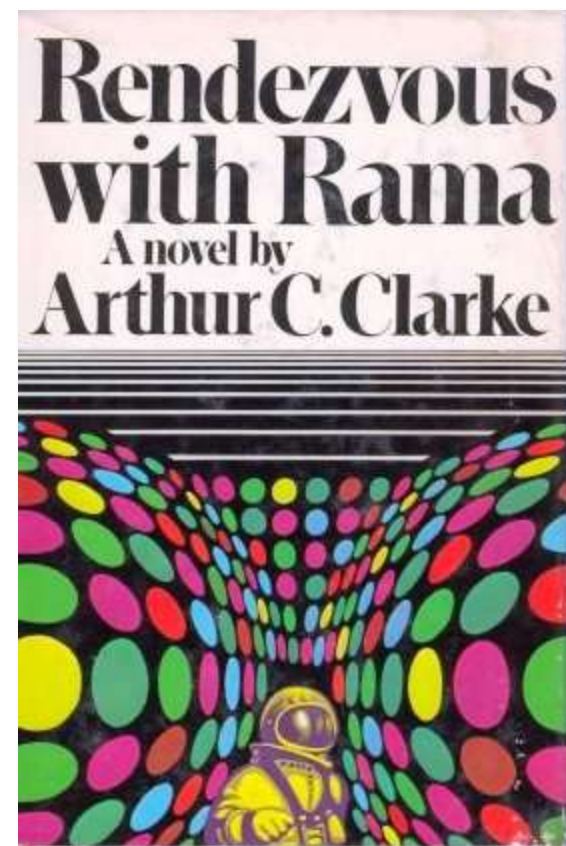
- **Different countries, different laws...**
 - Botnets may not be illegal
 - Building/distributing malware may not be illegal
- **Building botnets for fun & profit**
 - Don't need to be hard-core criminal
 - Tools, guides, how-to's, vendors, sponsors, etc.
 - It's a "business like any other"



- **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)



- **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!



- **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.



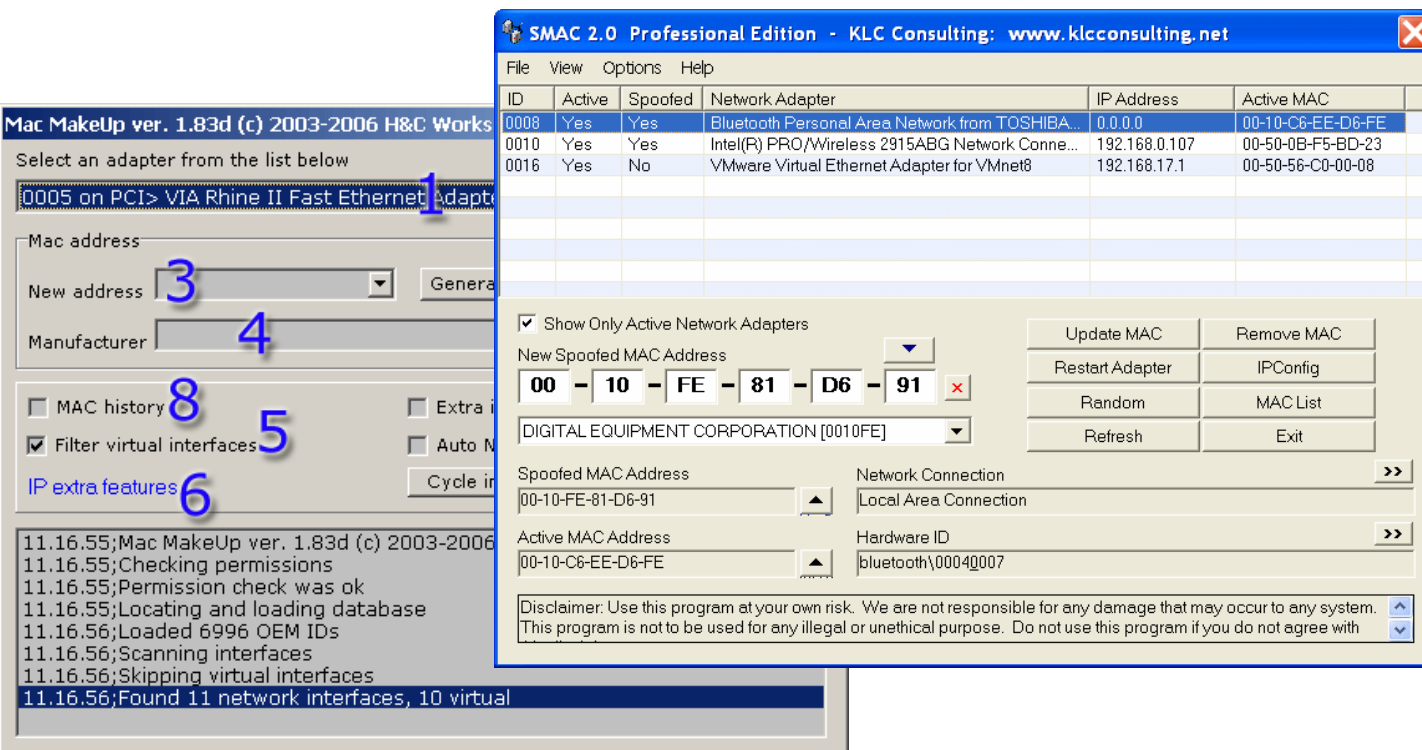
- **Deniability is important -**
 - Open WiFi is your friend
 - Locations that don't have CCTV
- **Don't connect directly - Ever!**
 - Anonymous proxy and TOR networks are preferred
- **Hiding in the masses**
 - Academic networks + libraries



- **Free WiFi access points**
 - Physical location changes
- **Change the MAC address**



Apple Stores
Atlanta Bread Company
Barnes & Noble
Border Books
Caribou Coffee
Hooters
Krystal Restaurants
McDonalds
Office Depot
Panera Bread Company
Staples
Starbucks
Etc.



SMAC 2.0 Professional Edition - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofer	Network Adapter	IP Address	Active MAC
0008	Yes	Yes	Bluetooth Personal Area Network from TOSHIBA...	0.0.0.0	00-10-C6-EE-D6-FE
0010	Yes	Yes	Intel(R) PRO/Wireless 2915ABG Network Conne...	192.168.0.107	00-50-0B-F5-BD-23
0016	Yes	No	VMware Virtual Ethernet Adapter for VMnet8	192.168.17.1	00-50-56-C0-00-08

Mac MakeUp ver. 1.83d (c) 2003-2006 H&C Works

Select an adapter from the list below

0005 on PCI> VIA Rhine II Fast Ethernet Adapter

Mac address

New address: 3

Manufacturer: 4

MAC history: 8

Filter virtual interfaces: 5

IP extra features: 6

11.16.55;Mac MakeUp ver. 1.83d (c) 2003-2006
11.16.55;Checking permissions
11.16.55;Permission check was ok
11.16.55;Locating and loading database
11.16.56;Loaded 6996 OEM IDs
11.16.56;Scanning interfaces
11.16.56;Skipping virtual interfaces
11.16.56;Found 11 network interfaces, 10 virtual

SMAC 2.0 Professional Edition - KLC Consulting: www.klcconsulting.net

File View Options Help

Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 10 - FE - 81 - D6 - 91

DIGITAL EQUIPMENT CORPORATION [0010FE]

Spoofed MAC Address: 00-10-FE-81-D6-91

Network Connection: Local Area Connection

Active MAC Address: 00-10-C6-EE-D6-FE

Hardware ID: bluetooth\00040007

Update MAC Remove MAC
Restart Adapter IPConfig
Random MAC List
Refresh Exit

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

- **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



Visa Gift Card - pick one up in person or online

In Person >

Online >



Thoughtful
Give the gift of freedom

Convenient
Just like your debit card

Secure
Safer than giving cash

Give people the freedom to buy what they want: online, in person, or by phone

GET A GIFT CARD

Gift Card Benefits Buying a Gift Card Use Your Gift Card



Visa Gift Card

Visa Gift cards are perfect for any occasion - smart, thoughtful, and always well received.

Give one today>

Quick Links

- [Get a Gift Card](#)
- [Use Your Gift Card](#)
- [Know Your Balance](#)
- [FAQ](#)

- **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



- 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
- Zimbabwe
- (Plus some more...)

aka. non-extradition countries (with the USA)

- **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.**

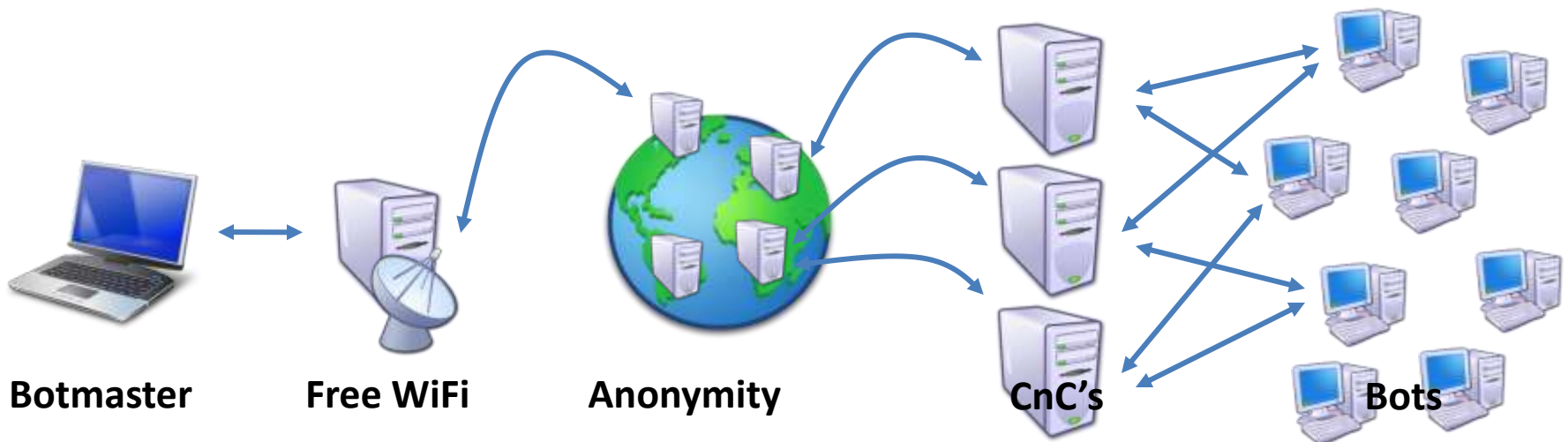


- **“Off the shelf” DIY botnet construction kit**
 - Zeus, SpyEye, Butterfly, etc.
- **Seeding torrents & newsgroups**
 - Anonymous submission
 - Very difficult to trackback
 - Doesn't rely upon
 - Natural propagation & infection
- **Dynamic DNS for CnC**
 - Free and anonymous



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





- **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




Hacking Tools and Programs Mark this forum read

Thread / Author	Replies	Views	Rating	Last Post [asc]
  [Release] 666 Auto-Whaler v2.0 Get loads of accounts! (Pages: 1 2 3 4 ... last) sean013	202	6,332	★★★★★	Today 01:17 PM Last Post: sean013
 NEW FACEBOOK HACK HURRY WILL NOT WORK SOON.. (Pages: 1 2 3) TheTechNation	25	199	★★★★☆	Today 01:17 PM Last Post: VirtualDUDE
  [DEV] xDoS v1 Revision1 [DEV] ePixel	2	42	★★★★☆	Today 01:13 PM Last Post: LeGiIT
  Poll: [YouTube] Comment 4 Comment - More Views carl00s	4	30	★★★★☆	Today 01:10 PM Last Post: carl00s
 FUD Auto Spreader [Get More Bots/Servers] Working! (Pages: 1 2 3 4 ... last) nBlaiR	152	1	★★★★★	Today 01:09 PM Last Post: carl00s
 *{{{UPDATED TODAY}}}\$[L] Public Runtime crypter V1 Part -3 (Pages: 1 2 3 4 ... last)				



VipVince
I am Ownage.
★★★★★


Posts: 1,552
Joined: Apr 2008
Reputation: **46**
h4x\$: 2217.00






[New Topic](#) [Add Reply](#)

[LinkBack](#) [Thread Tools](#) [Display Modes](#)

03-20-2010, 07:55 AM

#1 (permlink)

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



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



MEMBERS LOGIN [input] [input] [ENTER]

OAD

- Name
- Price
- Stats
- Sign Up

Цены

Country	Price for 1k	
AU	300\$	Order now
DE	220\$	Order now
GB	210\$	Order now
IT	200\$	Order now
NZ	200\$	Order now
ES	200\$	Order now
US	110\$	Order now
BG	100\$	Order now
DK	100\$	Order now
FR	100\$	Order now
PT	100\$	Order now
NL	100\$	Order now
CA	80\$	Order now
JP	80\$	Order now
SE	70\$	Order now
BR	60\$	Order now
TR	60\$	Order now
NO	50\$	Order now

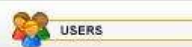
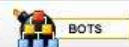
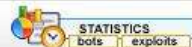
- Октябрь 26/2007
 Налетай на ES IT DE , идет
 хороший ладня.

- Октябрь 23/2007
 Введена принудительная
 проверка грузинских файлов
 на предмет полноты , если
 файл падает более чем 30%
 из тестируемых IT
 антивирусов , то загрузка
 данной задачи прекращается
 и рядом с ней появляется
 уведомление. Проверка
 файлов производится через
 приватный сервис.

- Октябрь 16/2007
 Налетай не скучай покупай
 живильсь и точнее мкс и
 оу.

- Август 30/2007

Lease (part of) an existing botnet



Global stats Rap. per time stats

Bot traffic Statistics for [redacted] generated on 2008/08/09

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.

Top 10 Countries:		Top 10 new countries today		Top 10 Countries order by bot's reports	
Country	Rating	Country	Rating	Country	Rating
Russia	7099 56%			Russia	626089 59%
United States	1641 13%			United States	163156 15%
Germany	1504 12%			Germany	63898 6%
Netherlands	492 4%			Brazil	24697 2%
Ukraine	237 2%			Ukraine	20728 2%
Brazil	196 2%			Spain	19229 2%
United Kingdom	152 1%			Netherlands	13215 1%
Spain	138 1%			United Kingdom	11816 1%
Belgium	126 1%			Taiwan	11541 1%
Turkey	101 1%			Turkey	10173 1%
Totally: 80		Country Rating totally: 0		Totally bot's reports: 1061892	

CHOOSE YOUR PROJECT

go!

MAIN

- [Manage projects](#)
- [Add project](#)
- [Change info](#)

PROJECT

- [Search by host](#)
- [Search by URI](#)
- [Global searching](#)
- [Online bots](#)

Hello,

Your last session: Tue Aug 5 06:16:31 2008

Active projects:

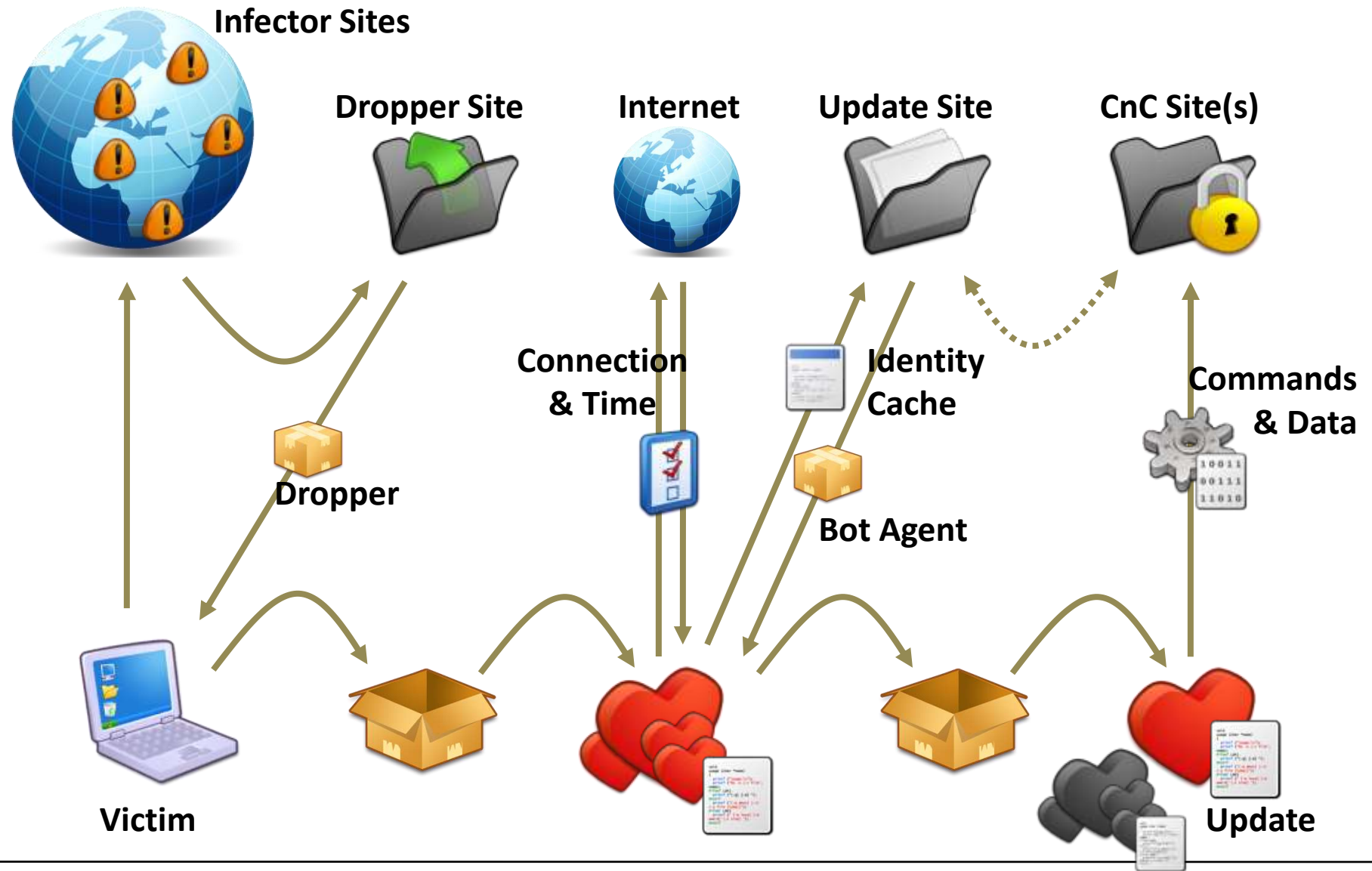
project	time end	price	bots	index time	size (mb)	action
[redacted]	14/1/2008	1	48 / 1	Tue May 13 00:18:43 2008	0.00	index
[redacted]	6/8/2008	1	1048 / 10000	Tue Aug 5 17:00:52 2008	0.00	index

- **"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.)





- **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



- **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



- **Access to executive target lists**
 - Easy, plenty of sellers.
 - Much of the information is publicly available



Lead 411 Companies People Enter Keywords Here

MY LEAD411 DAILY 411 EXECUTIVES COMPANIES EXCEL DOWNLOAD

Kansas City Power & Light (edit profile) ShareThis

Industries > Energy

Headquarters Recent Press Archives

<http://www.kcpl.com>
P.O. Box 418679
Kansas City, MO USA 64141
Phone:816-471-5275

[Free Trial](#): It's free to try our lead alerts and executive emails.

Executives LinkedIn

Dept	Executive	Title	Email @kcpl.com	Verified
Exe	Michael Chessee (ypard)	CEO	Not Available	07-30-09
	Chris Giles	VP Regulatory Affairs	Avail. Free Trial	04-26-10
	William Downey	President/COO/Pres Great Plains Energy	Not Available	07-30-09
	Kevin Bryant	VP Energy Solution	Avail. Free Trial	04-26-10
	Lon Wright	VP	Not Available	07-30-09
	Marcyn Rollason	VP Renewables/Gas Generation	Avail. Free Trial	07-30-09
	Mitch Krysa	Secretary	Avail. Free Trial	02-07-10
	Richard Spring	VP Transmission Services	Avail. Free Trial	04-26-10
	Scott Heidbrink	SVP Corporate Services	Not Available	07-30-09
	Terry Bassham	EVP Finance/Strategic Development/CFD	Not Available	07-30-09
	Todd Kobayashi	VP Strategy/Risk Management	Avail. Free Trial	07-30-09
	Bill Menae	Manager of Asset Management and Automation	Avail. Free Trial	07-30-09
	Curtis Blanc	Senior Director - Regulatory Affairs	Avail. Free Trial	04-24-10
	Greg Kindle	Manager of Economic Development	Avail. Free Trial	03-01-10

Our database is the lowest priced US Business Directory database on the web for only ~~\$199~~ \$149. That's over 130,000 Contact Listings Per Dollar!! [Buy Now!](#)

****We now have a version in [MS Access](#) for only \$199****

[See A Sample.](#)

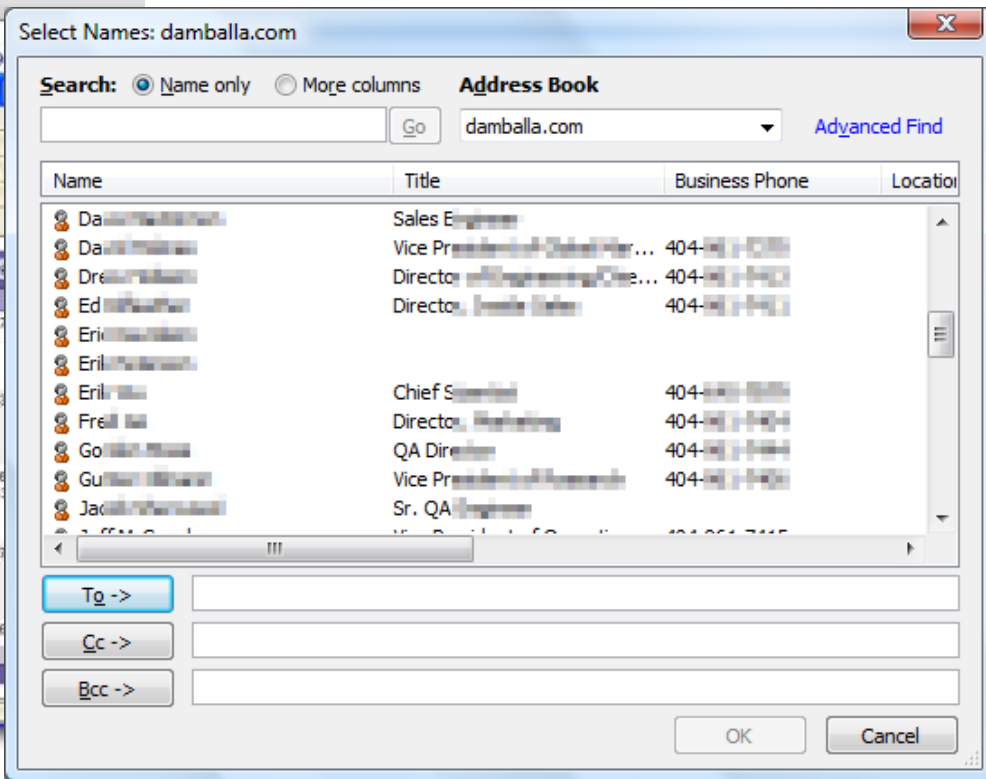
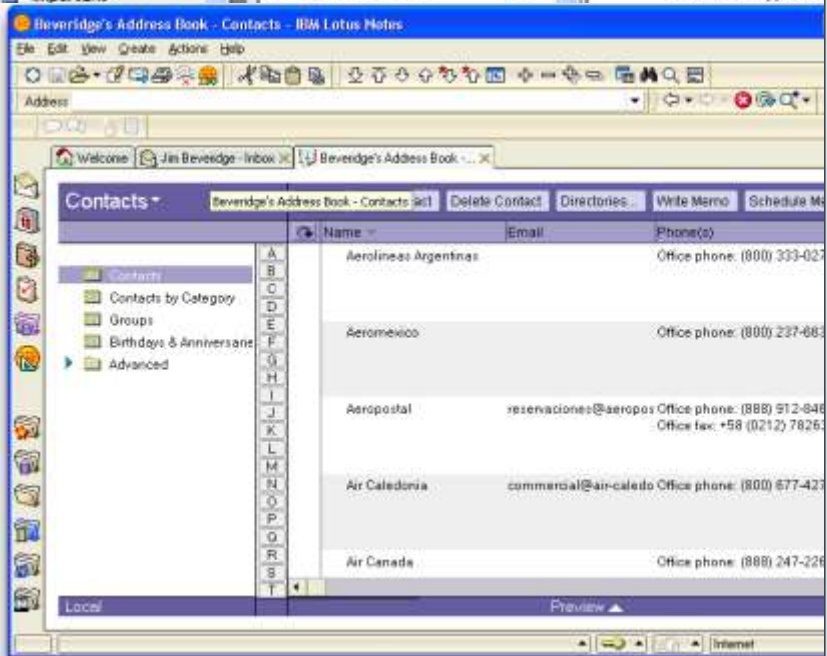
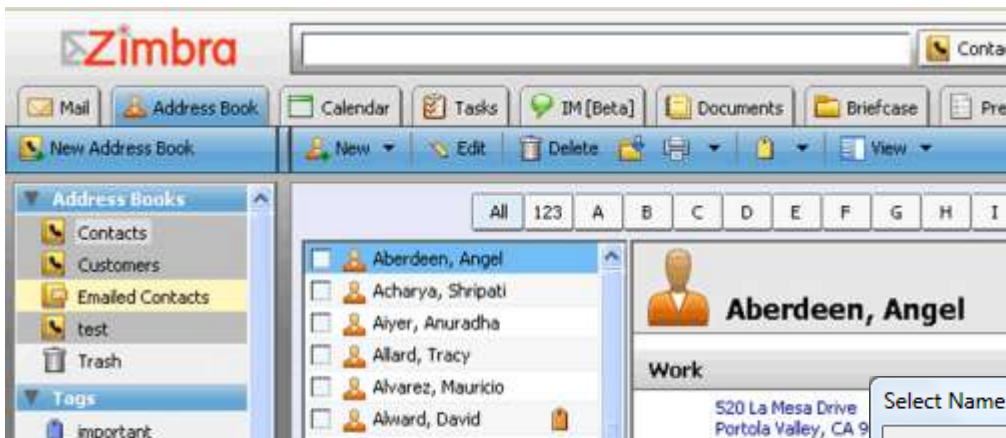
Approx. 20 Million Record Database Includes:

1. Company Name
2. Address
3. City
4. State
5. Zip
6. County
7. Contact Name
8. Contact Title
9. Contact Gender
10. Phone Number
11. Fax Number
12. Total Employees
13. Sales
14. WebSite Address
15. SIC Code - Description

- US Database - Approx 20,000,500 Businesses
- US Database - Approx 11,700 Unique SIC Codes
- US Database - Broken Up By State
- US Database - 1 Easy To Use Downloadable Zip File

Corporate Address Book Scraping

- Target corporate address books
 - Names, positions, email, phone, mobile,...



Lists of Leads – i.e. “Targets”

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Company Name	Address	City	State	Zip	County	WebSite	Phone	Fax	Contact	Contact Title	Gender	Employees	Sales	SIC Code - Category
2	Human Resources	112 State St # 660	Albany	NY	12207-2016	Albany	www.albanycounty.c	5184475510	5184475586	Robert Conway	Manager	Male	25	Unavailable	912103 - Government Offices-County
3	Albany Ear Nose & Throat	1375 Washington Ave # 1	Albany	NY	12206-1058	Albany	www.albanyent.com	5184721210		Debbie Elia	Manager	Female	36	7,164,000	801101 - Physicians & Surgeons
4	Albany Envelope	23 Winthrop Ave	Albany	NY	12203-1901	Albany	www.albanyenvelope	5184825481		Paul Seeney	Owner	Male	3	621,000	275202 - Printers
5	Albany Special Events	24 Eagle St # 402	Albany	NY	12207-1983	Albany	www.albanyevents.o	5184342032	5184260759	Dorothy Dack	Manager	Female	8	Unavailable	912104 - Government Offices-City, Village & Twtp
6	Bixby Crable & Stiglmeier	19 Dove St # 301	Albany	NY	12210-1389	Albany	www.albanyfamilylav	5184363404		Robert H Bixby	President	Male	5	835,000	811103 - Attorneys
7	Albany Fire Extinguisher Sale	18 Walker Way # 11	Albany	NY	12205-4991	Albany	www.albanyfire.net	5184563700	5184563979	Thomas Kretzler	Owner	Male	15	14,180,000	509903 - Fire Extinguishers (Wholesale)
8	First Assembly Of God	PO Box 8621	Albany	NY	12208-0621	Albany	www.albanyfirstag.or	5184383841	5184821394	Raymond A Sullivan	Religious Leader	Male	3	Unavailable	866107 - Churches
9	Albany Gastroenterology Cns	1375 Washington Ave # 1	Albany	NY	12206-1040	Albany	www.albanygi.com	5184384483		Karen Brimmer	Manager	Female	55	10,945,000	801101 - Physicians & Surgeons
10	Ginger Man	234 Western Ave	Albany	NY	12203-1322	Albany	www.albanygingerma	5184275963	5184271917	Michael Bryon	Owner	Male	20	800,000	581208 - Restaurants
11	Re/Max Premier	210 Washington Avenue	Albany	NY	12203-6339	Albany	www.albanyhome.coi	5188698500		Dave Evans	Owner	Male	50	6,700,000	653118 - Real Estate
12	Albany Housing Authority	200 S Pearl St	Albany	NY	12202-1834	Albany	www.albanyhousing.i	5186417500	5184450725	Steven Longo	Executive Director	male	Unavailable	Unavailable	953199 - Housing Authority
13	Kevin Cleary Government Rlt	39 N Pearl St	Albany	NY	12207-2785	Albany	www.albanyinsider.ci	5184632399					3	630,000	874301 - Lobbyists
14	Albany Institute-History & Art	125 Washington Ave	Albany	NY	12210-2296	Albany	www.albanyinstitute.r	5184634478	5184621522	Christine Miles	Executive Director	Female	30	2,363,000	841201 - Museums
15	Albany IVF Fertility & Gyn	349 Northern Blvd	Albany	NY	12204-1032	Albany	www.albanyivf.com	5184349759		Michelle Scrom	Manager	Female	25	4,975,000	801101 - Physicians & Surgeons
16	Albany Law School	80 New Scotland Ave	Albany	NY	12208-3494	Albany	www.albanylawjourn	5184452311	5184452315	Thomas Guernsey	Administrator	Male	135	Unavailable	822101 - Schools-Universities & Colleges Academic
17	Albany Management Inc	4 Computer Dr W	Albany	NY	12205-1697	Albany	www.albanymanagen	5184587113	5184587955	Karen E Laberge	President	Female	70	9,380,000	653118 - Real Estate
18	Hudson Valley Tile Marble	470 Central Ave	Albany	NY	12206-2279	Albany	www.albanymarble.ni	5184898989	5184898988	Rocky Orcluoli	President	Male	25	3,800,000	174301 - Tile-Ceramic-Contractors & Dealers

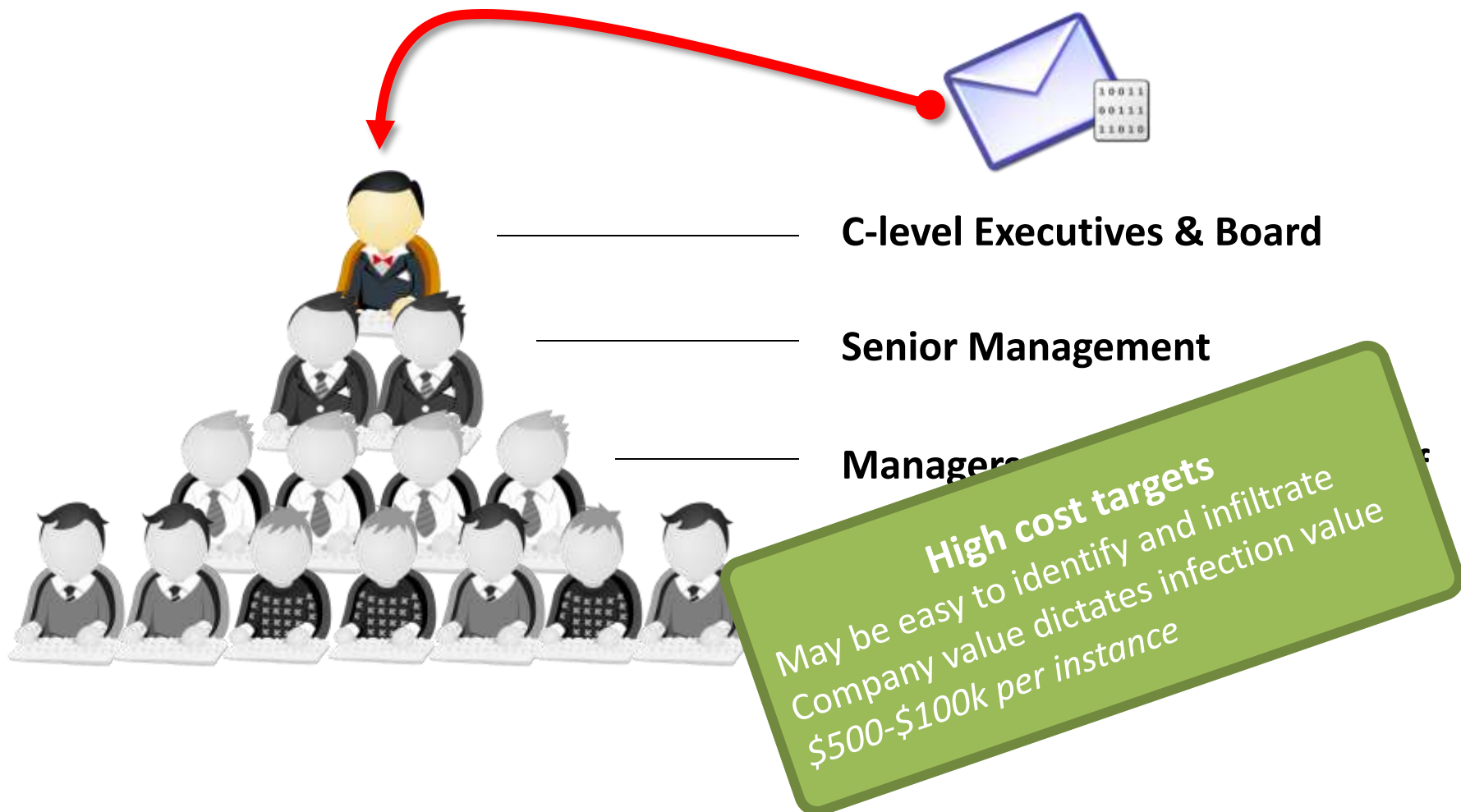
- **Lists available through black, gray and white markets**
 - Black = Acquired in underground forums & sellers
 - Gray = Sellers with clear or probable blackhat ties
 - White = Commercial leads vendors and public lists
- **Conveniently formatted for automated processing**
 - CVS and “standardized” file formats
 - Direct feed in to spam email tools
 - Ready for phishing template integration



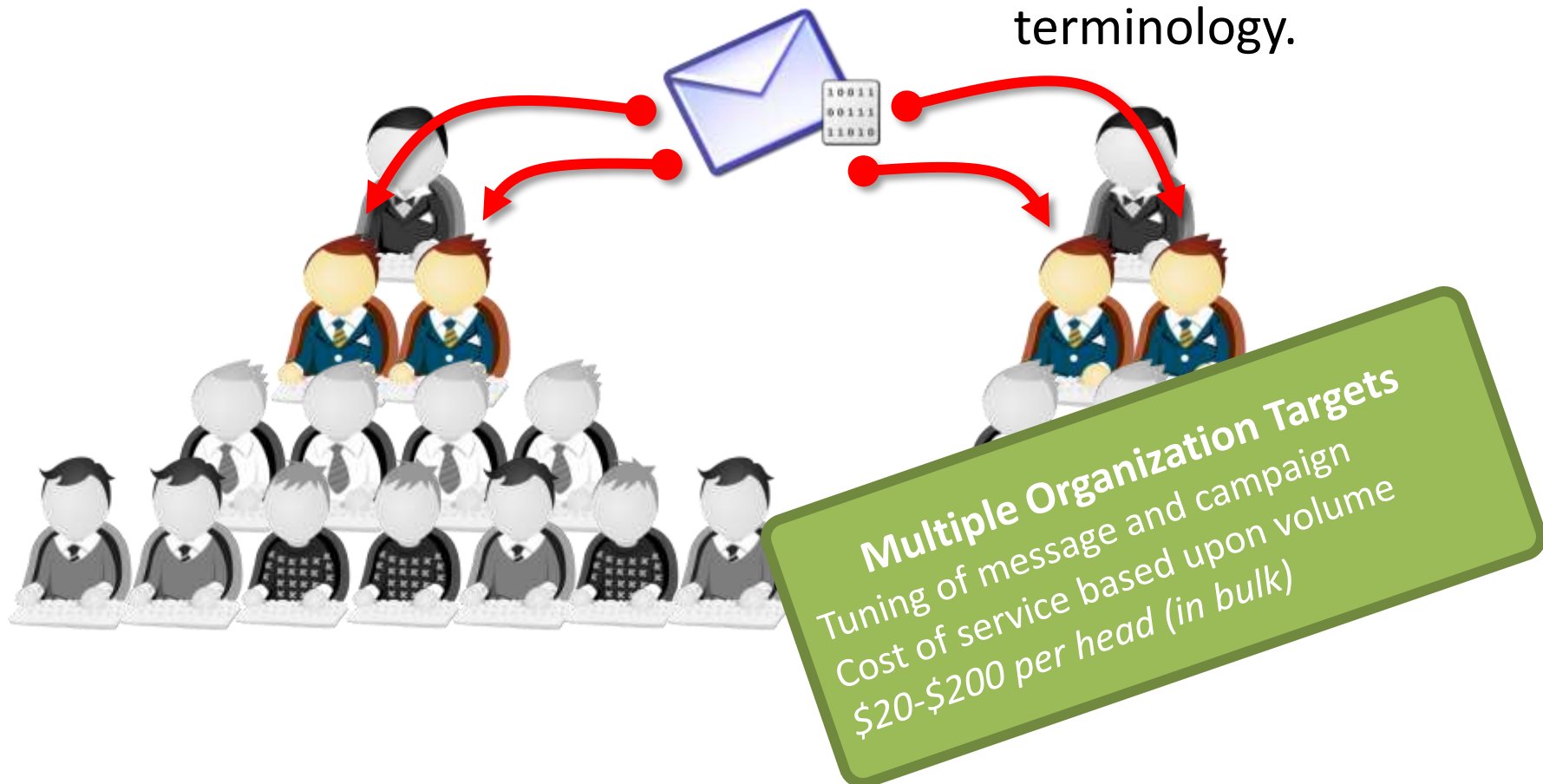
- **Email and/or malware delivery services**
 - Targeted at organizations, professions or whales
- **Botnet rendered services**
 - Targeted messaging (maybe broader than email)
 - Hosting of malware & infector components
 - Enumeration of target organization
 - Selling of existing botnet/agent access



- **Whaling** = Targeting the biggest & most visible executives

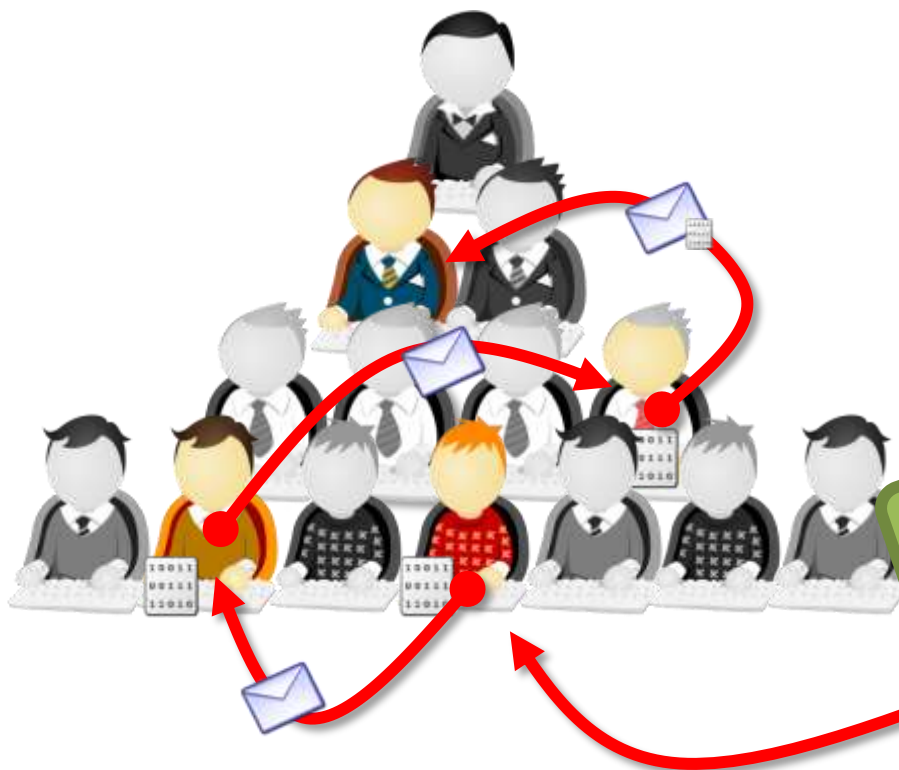


- **Horizontal Spear** = Targeting a specific role across similar industries using field-specific terminology.



- **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



Single Organization Target
Costly to perform – manual work
Cost of service based upon time
\$ unknown
Authenticity



Stroud

Powers

DOLLAR
A TRUE REPUBLICAN
N.C. HOUSE

Fletcher

Bate
CONC

NELSON *****
DOLLAR

DOLLAR
HOUSE

David Miner

HOUSE

Re-Elect

Donna
Stroud
FOR DISTRICT COURT JUDGE

to Representative

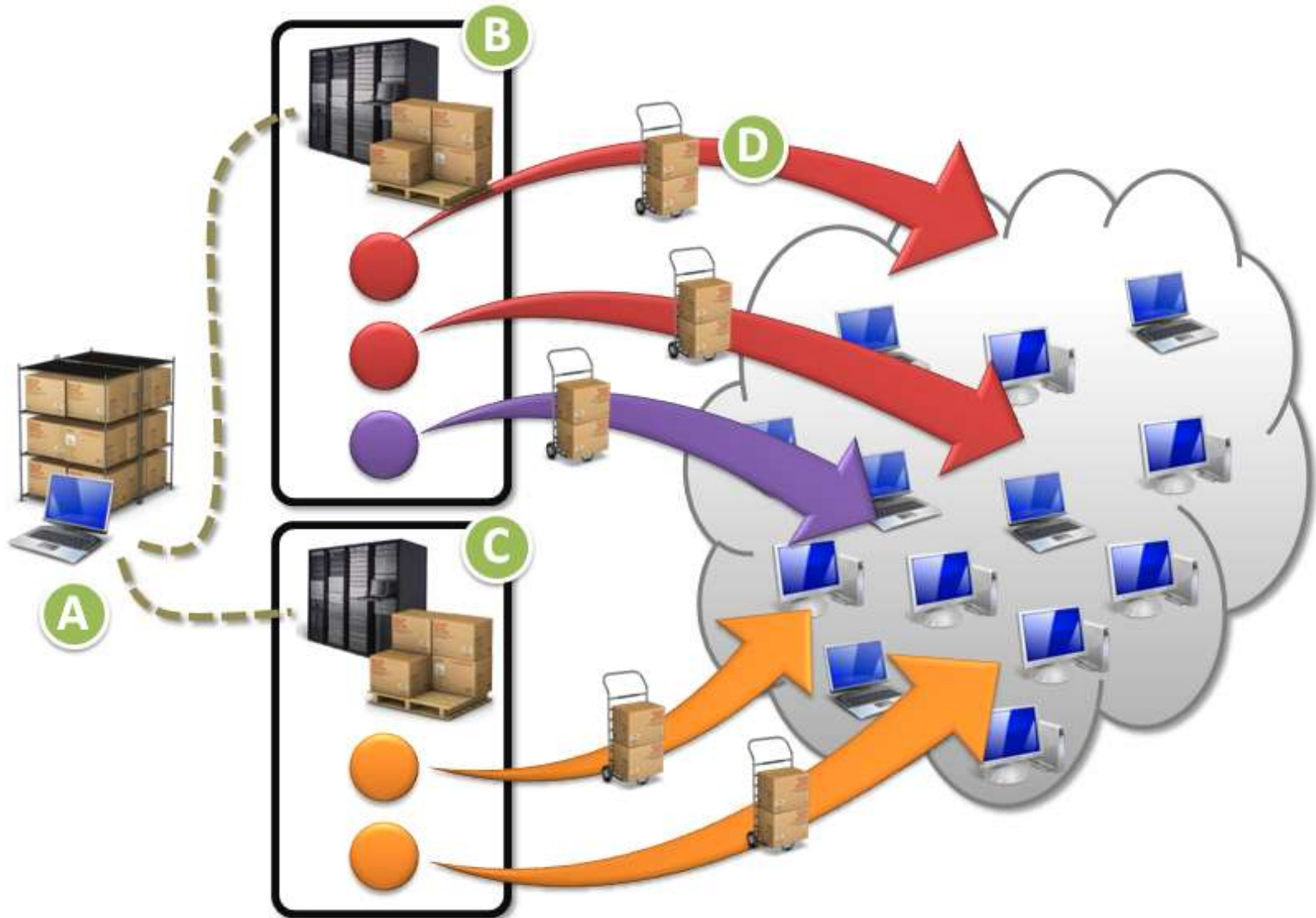
Bill
Fletcher
REPUBLICAN
MEMBER OF PUBLIC DISTRICTION
www.BillFletcher.com

Kris Bailey
Judge

Campaigns

- **Common myth of one botnet per botmaster**
 - Don't want to loose 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***





- **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



LoudMo
Get Paid Per Install

Username Password **LOGIN**

- Home
- Why Choose Us
- Products
- Payout Structure
- Signup
- Contact Us
- Blog
- Referral Program

LoudMo Pay Per Install Affiliate Program
★★★★★

FLV Direct Flash Video Player



0:00 / 0:51

Bookmark & Share
SHARE

TURN UP YOUR REVENUE

Get Paid Per Install

CLICK HERE TO SIGN UP NOW!

Affiliates, [Sign up Here!](#) | Need help? [Check the FAQ](#)

Looking to turn up your revenue?



Live Help is currently offline. We will return shortly.

Contact us

(866) 992-6734
info (at) loudmo.com

Welcome to LoudMo, the best install program on the net!

Loudmo's simple, easy to use installation and download products provide affiliates with the essential tools to make money from website traffic or with website content!

Loudmo's got the highest converting landing pages and one of the highest paying pay-per-install affiliate programs.

Our suite of download products below and our gateway creation wizard make it easy for affiliates to earn money. See what we have to offer.

- **Costs/earnings from campaign delivery**

Affiliate Web Marketing/Spam

0-800-288-2888
Toll Free: 1-800-288-2888
Customer Service Support

Home | My Account | Help Desk | About Us

Safe. Secure
The absolute security of your shopping is guaranteed by the most trusted internet security verification systems: Geotrust and McAfee.

100% Satisfaction Guaranteed or Money Back

Safe and Secure

- ✓ Reorder Discounts.
- ✓ No Waiting Rooms.
- ✓ W.H.O Approved Medication.
- ✓ Low Competitive Prices.
- ✓ Safe and Secure
- ✓ Qualified Medicines
- ✓ We Beat Any Price!

LOYALTY BONUSES! you can choose one of these deals

10% Cash Discount Bonus or **20% Free Product Bonus**

*Applies to all Reorders

Sildenafil Citrate Viagra Pills as low as \$0,99 You Save! GO	Tadalafil Tadalafil Pills as low as \$1,42 You Save! GO	Vardenafil Levitra Pills as low as \$1,42 You Save! GO
---	---	--

Ordering Made Simple [How to Order](#)

[Online](#) | [Phone](#) | [Chat](#)

Medications

Click here to login

Best Sellers | Categories

- Viagra | Sildenafil Citrate
- Tadalafil | Tadalafil
- Levitra | Vardenafil
- Soft Tabs
- Oral Jellies
- ED Sample Pack
- Isotretinoin | Isotretinoin
- Amoxicillin | Amoxicillin
- Azelaic Acid
- Levococixib

- **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

The 10 Worst Spammers

As at 18 July 2010 the world's worst spammers and spam gangs are:

-  **Canadian Pharmacy - Ukraine**
A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese web hosting.
-  **Leo Kuvayev / BadCow - Russian Federation**
Russian/American spammer. Does "OEM CD" pirated software spam, copy-cat pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus-created botnets and seems to be involved in virus distribution. Partnered with Vlad - aka "Mr. Green".
-  **Herbalking - India**
Massive affiliate spam program for snakeoil Body Part Enhancement scams. Also does replica luxury goods, pharma and porn. Spams via botnets, bulletproof hosting offshore and even sometimes uses fast flux hosting.
-  **Rove Digital - Estonia**
Botnets, malware, spam, phishing, DDoS, Inhoster, Camel, Rthost, Atrivo. What else needs to be said?

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%)

Message delivery services

Email Spam

SMTP send



Comment Spam



Webmail send



Advertisement Injection



Distributed hosting services

DNS & Fast-flux



Blackhat SEO



Web hosting



- **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 24

About	Prices	Contacts	Reviews
-----------------------	------------------------	--------------------------	-------------------------

▼ Sell iframe Traffic

Increase revenue from you 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.
- Weekly Payments. Webmoney, FET, PayPal.


▲ Buy iframe Traffic

Increase you 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,

1k users only 1\$





Kuzler Control Panel - [0] Connected



Server Rules Website

If: URL Contains (case sensitive) Then: Custom HTML SRC Delay: 0 No. of Times: 0

#	Contains	Then	Do Action	Delay	No. of Times
URL	google	Simple Redirect To	yahoo.com	0	0
Title	buy	Visible Iframe URL	www.YourLink.com	0	0
Inner Text	buy iphone	Invisible Iframe URL	www.YourCSLink.com	0	1
Inner Text	weight loss	Pop up URL	www.YourOfferLink.com	0	0
Inner HTML	Banner Code	Replace With	Your Banner Code	0	0
URL	facebook	Custom HTML SRC	<div align="center">Your Custom HTML SRC</div>	0	0

-  Edit Rule
-  Delete Selected
-  Delete Unselected
-  Delete All

Bind with (Optional) Icon (Optional) Add KB (Optional) Server Host / IP Port: 8888 Version: 1.0 Connect Add to Startup

Identity Laundering





- **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 \hat{A} 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...

STEP: (1) Receiver
Enter Receiver Information

The first thing to do is indicate to whom you're sending and where the money will be picked up.

To send us money, since we cannot handle Western Union payments in USA (for taxes reasons) please use the following details of our branch in Thailand:

First name : MAURO
Last name : SCIACCALUGA
Phone no. : +66800800390
City : BANGKOK
Country : THAILAND
Total Amount : \$87.99 / \$157.99 / \$197.99 (depending on the list you buy)

BUYLEADSEMAIL.COM Home About US Order NOW F.A.Q. Contact US

ORDER NOW!

- MEMBERS
- TESTIMONIALS
- OTHER SERVICES
- WEBSITE TEMPLATES
- AFFILIATE PROGRAM
- MARKETING SOFTWARE

REACH MILLIONS OPT-IN E-MAILS

Why E-mail Marketing?

Statistic shows:

- .025% - Banner Advertising
- .1% - Ip Messaging
- .25/30% - PopUp Advertising
- 2% - email Advertising

N. email	% Sales	Profit
50.000	.001	\$1,000
100.000	.001	\$2,000
200.000	.001	\$4,000

ALL EUROPE
177 million e-mails FOR ONLY \$197.99
ALERTPAY Buy Now

RUSSIA
38 million e-mails FOR ONLY \$157.99
ALERTPAY Buy Now

USA
117 million e-mails FOR ONLY \$157.99
ALERTPAY Buy Now

High Quality and Quantity at less cost in your

Fresh Account Store

HOME

Email Accounts

Facebook/Myspace

CONTACT

DeCaptcher - CAPTCHA bypass. Cheap and easy CAPTCHA solving

Fresh  **PRICE:**
YAHOO! **\$ 599**
100000 Accounts
Unique Ip
Exclusice accounts
Immediete delivery
>>>> [Buy](#)

Fresh  **PRICE:**
Hotmail **\$ 750**
100000 Accounts
Unique Ip
Exclusice accounts
Immediete delivery
>>>> [Buy](#)

OUR SERVICES

We will also provide quality services in

- Tagged Accounts
- Wayn/hi5 accounts
- Plenty of Fish accounts
- Friendster/bebo

Contact us to get any Custom accounts within 24 hours for \$100 per 1000 [Click here](#)

Forum

[Click here](#)

10k facebook Accounts

Special price >>>> \$ 599

10000 Myspace Accounts

Special price >>>> \$ 599

New [1000 Facebook blank Accounts \\$80](#)

New [1000 Myspace Accounts \\$80](#)

New [1000 Craigslist Accounts \\$80](#)

24 Hours Replacement Guarantee

1 Million YAHOO! Accounts

Contact us to get this 

Timeliness Matters

Fresh and (daily) validated accounts sold in batches. CSV-formatted for easy tool integration.

SATURDAY, MAY 22, 2010

Best Quality Craigslist Non-PVAs

CL NON PVA

- 500 CL Accounts \$60.00
- 500 CL Accounts \$60.00
- 1000 CL Accounts \$100.00
- 10000 CL Accounts \$800.00

[Buy Now](#)



POSTED BY TRUEPALS AT 11:47 AM

- **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...





Direct

- Hacker Forums
- Carder Forums



1¢

Reseller

- Buy/Sell in bulk
- Telemarketing lists



10¢

Proxy

- Affiliate schemes
- Vetting of lists
- Web forms



\$5



nick.barlow@leadx.co.uk | Company ID: 0001

- Links**
- Home
 - Reports
 - Purchase Orders
 - Buyers
 - Sellers
 - Opening Hours
 - Account Management
 - User Management
 - Bank Details

Home

Log Out

Activity Summary

Expenditure
 Leads Bought Today: 0
 Spend Today: £0.00
 5 Day Average: £0.00
 Spend For Month: £0.00

Orders
 Leads Ordered This Month: 0
 Leads Bought This Month: 0
 Percentage Of Order Complete: 0%

Revenue
 Leads Sold Today: 0
 Revenue Today: £0.00
 5 Day Average: £0.00



Balance
 £ 1844.11
 Your current average income exceeds your average spend.



General Line: 0844 871 4300
 Recruitment Line: 0844 871 4304

- Home
- About Us
- Buyers
- Sellers**
- Processes
- Contact Us
- Careers
- Login

The Digital exchange is now open

LeadX's mission is to provide a trading platform where virtually any digital goods can be traded.



Lead Exchanges

Matching buyers with sellers.
 Mixes with "work from home"
 Specialist and vetted exchanges

What is LeadX.com?

LeadX trades with brokers, insurers, lenders, banks and building societies. Every company has a percentage of customers they're unable to help, and rather than those potential customers go to waste LeadX provides an open market where leads can be bought and sold in real time, while still "hot".

Exchange Types

- Insurance**
Direct Insurers
- Lending**
Banks

What are the benefits to you?

[Benefits to Buyers](#)

[Benefits to Sellers](#)



Signup today

Leads ROBO
nothing compares...
The software that gather personal and business leads from all over internet

drive traffic on demand

home | Products | Features | FAQ's | Support | Contact Us

Products

LIMITED Time Offer, Upto 25% Discount on almost all Products!!

Leads ROBO

Leads Robo (US DNC Scrubber) JUMBO Pack (US+UK+Ca)
solution for your Telemarketing Leads requirement. It will pr
(B2C) & Business (B2B) Leads. All leads will atleast contain
and Phone Number. USA B2B leads will also have Email Add

- Remove DNCs from gathered list. List updated month
- Unlimited Leads Download. (All fresh)
- Auto-Next Option
- Text and comma separated formats

\$680 only --> [Buy Now](#)

Sell Identity Profiles
Grey-market for stolen and pilfered PII.
Purchase "leads" for other scams and activities

LEADPOINT™ Empowering Lead Generation

Call Us Toll-FREE
866.832.8158

BUY LEADS

SELL LEADS

ABOUT US

CONTACT US

CLIENT LOGIN

SIGN UP

What to Sell | How to Sell | Why it Works | Sign Up

Sell Leads

Maximize profits with LeadPoint!

- Mortgage Leads >
- Education Leads >
- Debt Leads >
- Automotive Leads >



EquiLeads

Username:

Password:

Type: Buyer Seller

Home | FAQs | Sample Leads | Pricing | Contact Us | **Join Now!**

- ✓ Fresh Leads Daily
- ✓ FREE To Join
- ✓ Cherry Pick System
- ✓ Bogus Lead Return
- ✓ Download To Excel



Fresh Quality Internet Leads
Our leads are fresh, accurate and backed by our 100% satisfaction guarantee. If you are not satisfied with the quality of a lead you buy from us, we will replace it immediately. Our leads have a high application ratio and a solid closing ratio, and we provide leads for many major industries.

Financial Services Prospects

- [Mortgages](#)
- [Life Insurance](#)
- [Loan Modifications](#)
- [Homeowners Insurance](#)
- [Healthcare Insurance](#)
- [Auto Insurance](#)
- [Car, Boat, and RV Loans](#)
- [Merchant Services](#)

Our Leads are 100% Guaranteed! Immediate replacement of leads is available!

Join Now!
Get The Leads You Want!



Affiliate Programs
Sell the previously acquired leads.
Automate submission of "vetted" leads.

[Sell Your Leads Here!](#)

[Join Our Affiliate Program](#)

[Click Here](#)

Consumer

Huge national Consumer database includes detailed demographic and geographic information

Qty	Price
1000	\$60.00
2500	\$146.25
5000	\$225.00
10000	\$350.00
25000	\$812.50
50000	\$1,500.00

Minimum Order: \$60.00

New Homeowner

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

Qty	Price
250	\$21.25
1000	\$82.90
5000	\$404.00
10000	\$788.00
25000	\$1,920.00
50000	\$3,745.00

Minimum

Business

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

Qty	Price
500	\$50.00
1000	\$97.50
2500	\$184.50
5000	\$250.00
10000	\$350.00
25000	\$750.00
50000	\$1,475.00

Minimum Order: \$50.00

New Mover

Consumers who have recently moved and to establish relationships with a wide range of business

Qty	Price
250	\$21.25
1000	\$82.90
5000	\$404.00
10000	\$788.00
25000	\$1,920.00
50000	\$3,745.00



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)

Pricing Schemes

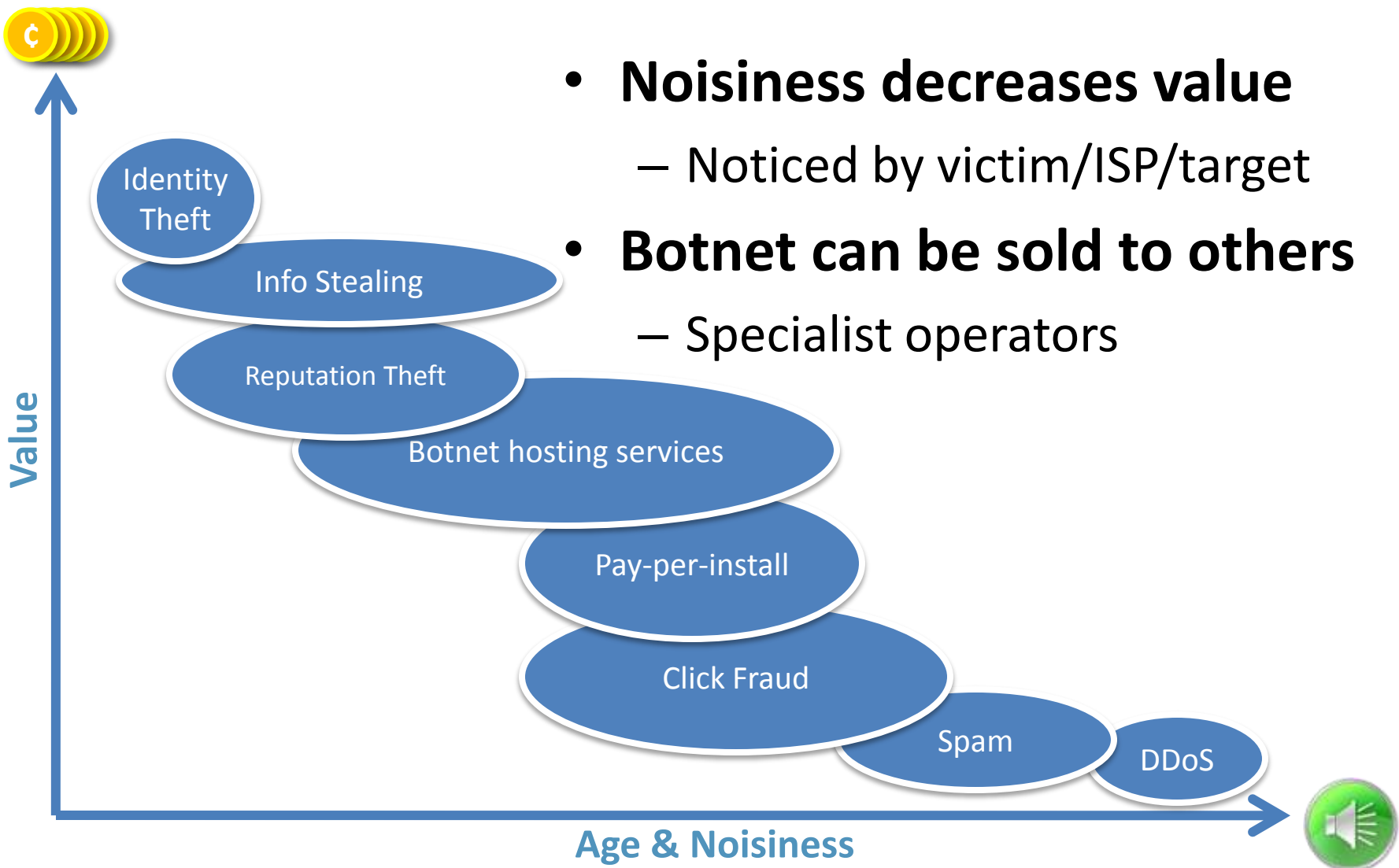
Quality, timeliness, details, clustering and volume all affect the value

The Aging Process



- **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%







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

- **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.



Increased Agent Robustness

Bot Agent

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



Updates

- * New (signed) config. 
- * New "locked" agent




DNS Services

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



CnC Servers & Drop Sites

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



Virtual Reputations



Spotlight
Videos
Games
Primetime
Community

ShaneKimChee DonJuan

A group of four avatars stands in front of a building with a blue awning and a sign that says "OPEN". The avatars are dressed in various casual clothing. Above the first two avatars are orange speech bubbles with their names "ShaneKimChee" and "DonJuan". Above the fourth avatar is a blue speech bubble containing a photo of a lion's face.

LuckLaster

A single avatar of a woman wearing a red cap, a black crop top, and brown pants stands in a virtual environment with some foliage.

scout

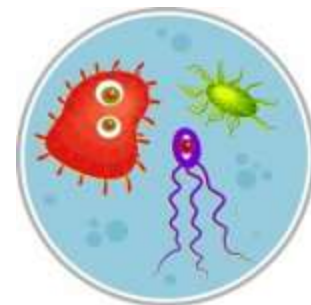
A single avatar of a man wearing a red shirt and dark pants stands in a virtual environment with a street lamp and a fence.

A single avatar of a woman stands in a virtual environment with a fence and a tree. Above her is a green speech bubble containing a photo of a SEGA Superstars game box.

Select Back



- **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



- **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.



- **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





- **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

- **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





- **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

- **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

Web: <http://www.damballa.com> Blog: <http://blog.damballa.com>