

Botnets

Ramin Sadre

Botnets

- Collection of compromised/hijacked machines (bots, zombies) under control of an attacker (botmaster)
- Many different ways to compromise machines for a botnet
 - Malware = software containing a virus or worm
 - A worm = virus that spreads to other computers
 - Drive-by-download = User visits compromised website that exploits a vulnerability in the browser
 - Attacks against weakly protected systems, e.g. password dictionary attacks
 - ...

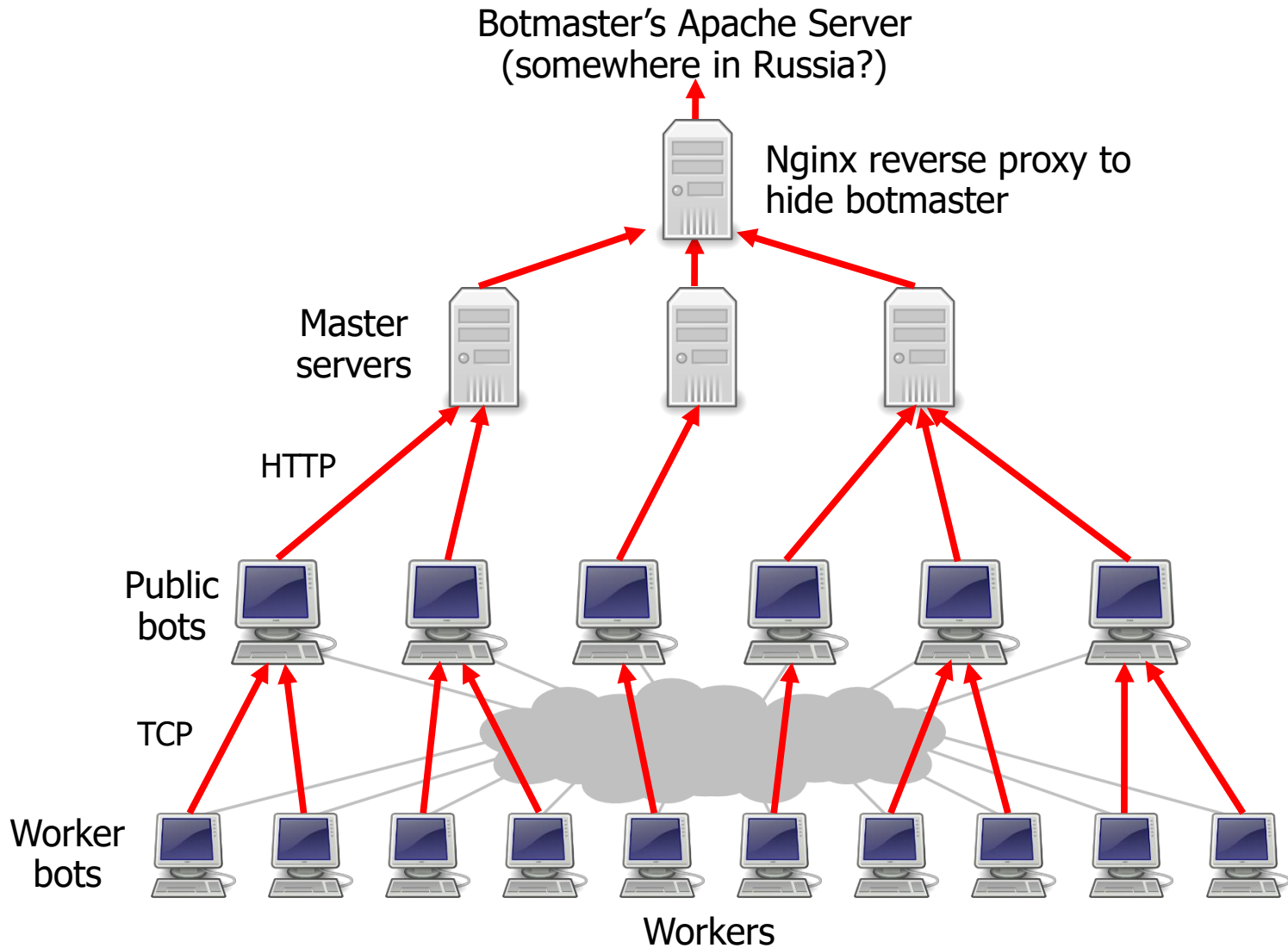
Command and Control

- Once a machine has been “recruited” for a botnet it is ready to receive instructions from the botmaster
 - Commands
 - Updates
 - The bot software can also transfer information from the infected machine to the botmaster (passwords etc.)
- Botmaster operates a *Command-and-Control* server that communicates with the bots

Command and Control (2)

- Challenge for botmaster: Operate a C&C server...
 - without revealing the botmaster's identity
 - without raising alarms of admins/users who monitor the traffic of their machines
 - in a flexible way. If the C&C server is discovered and shut down by the police or the ISP, the bots should be able to find a new C&C server
- Lots of ways to design a C&C infrastructure
 - Topology: Star, hierarchical, p2p
 - Communication: Encrypted, stealthy (hidden)
 - Protocols: HTTP, IRC,...

Storm Botnet (2007)



Adapted from Kanich et al.

Storm Architecture

- Used for spamming
- Infection of Windows computers through malware (exe-file distributed through e-mail attachments)
- “Worker bots” = computers that request jobs (spam, DDoS) from the masters servers and execute them
- “Public bots” = infected computers that are externally accessible
- Encrypted P2P protocol (Overnet) to find other nodes (not used for data exchange, only for location information)
- Small number of “master servers”
 - Compromised computers hosted in data centers
 - Nginx reverse proxy server, hide the top-level server of the botmaster
 - Likely managed by botmaster directly

Storm Architecture (2)

- To find the master servers, bots resolve a domain name (e.g. evil-master.com)
- IP address of domain name is rapidly changed, pointing to a compromised computer (several times per hours; “Fast Flux DNS”)
 - This technique was originally invented for load balancing (sending clients to different servers)
- Very resilient architecture
 - Layered
 - Peer to peer: decentralized, harder to get down than the old IRC channel approach

What can you do with a botnet?

- Type of commands in Storm botnet:
 - Activation
 - Harvest e-mail addresses from host
 - Spamming
 - DDoS
 - Sniff passwords
 - ...

Fighting botnets

1. Prevent infection with bot malware. Hard 😞
2. Take down C&C server. Hard because of the botnet architecture 😞
3. Intrude the botnet and send switch-off command
 - Was successful in the past but modern botnets use encryption and authentication
4. Seize the domain names used by the botnet
 - Was quite successful in the past
 - Modern botnets generate large lists (50k) of possible domains using a deterministic algorithm known by all bots
 - Bots try randomly subset from that list
 - Botnet can only be stopped if all domain names on the list seized

→ Leads to a possible bot detection method: hosts that make a lot of failed DNS queries are suspicious

Attack Economy

Market

- People are willing to pay for
 - Spam services
 - Accounts, credit card numbers,...
 - DDoS attacks
 - Click fraud
 - Votes on social networks
 - ...

Selling accounts/credit card numbers/...

BuyAccs.com

BUY BULK ACCOUNTS AT BEST PRICES

[Russian Version](#) [English Version](#)

If you need quality **bulk accounts**, you've come to the right place. You can get your accounts **immediately** after your payment - there is no need to wait.

All the accounts are provided in **any format** you like. Just use our **[free account converter](#)** to get them in the way you need.

Special rates are applied if you purchase less than 1000 accounts.

We accept Paypal, Perfectmoney and Webmoney.

Please, review our [terms and conditions](#) before purchasing any accounts.

[Earn Money Selling Accounts](#)

[Buy Yahoo Accounts](#)

[Buy Twitter Accounts](#)

[Buy Hotmail Accounts](#)

[Buy Tumblr Accounts](#)

[Buy Facebook Accounts](#)

For sale

Provider	Quantity	Price for 1000 accounts
Gmail.com USA PVA	1360	1K-10K: \$100 10K-20K: \$100 20K+: \$100
Yahoo.com USA PVA	6793	1K-10K: \$130 10K-20K: \$130 20K+: \$130
Hotmail.com USA PVA	9058	1K-10K: \$120 10K-20K: \$120 20K+: \$120
Hotmail.com Aged	13142	1K-10K: \$15 10K-20K: \$14 20K+: \$13
Hotmail.com POP3	5417	1K-10K: \$10 10K-20K: \$9.5 20K+: \$9
Hotmail.com Basic	7075	1K-10K: \$8 10K-20K: \$7.5 20K+: \$7
Yahoo.com	96461	1K-10K: \$14 10K-20K: \$13 20K+: \$12
Yahoo.com USA	31975	1K-10K: \$20 10K-20K: \$20 20K+: \$20
Yahoo.com Basic	40826	1K-10K: \$10 10K-20K: \$9.5 20K+: \$9

News

23 Mar 2015

New arrivals! Just added **Netcourrier.com** and **Seznam.cz** accounts with **POP3** enabled.

02 Mar 2015

Just added **Tinder PVA** accounts.

06 Dec 2014

You can now pay in **EUR** for any accounts. Choose **Paypal EUR** option during checkout.

24 Nov 2014

WMZ payments are **available** again.

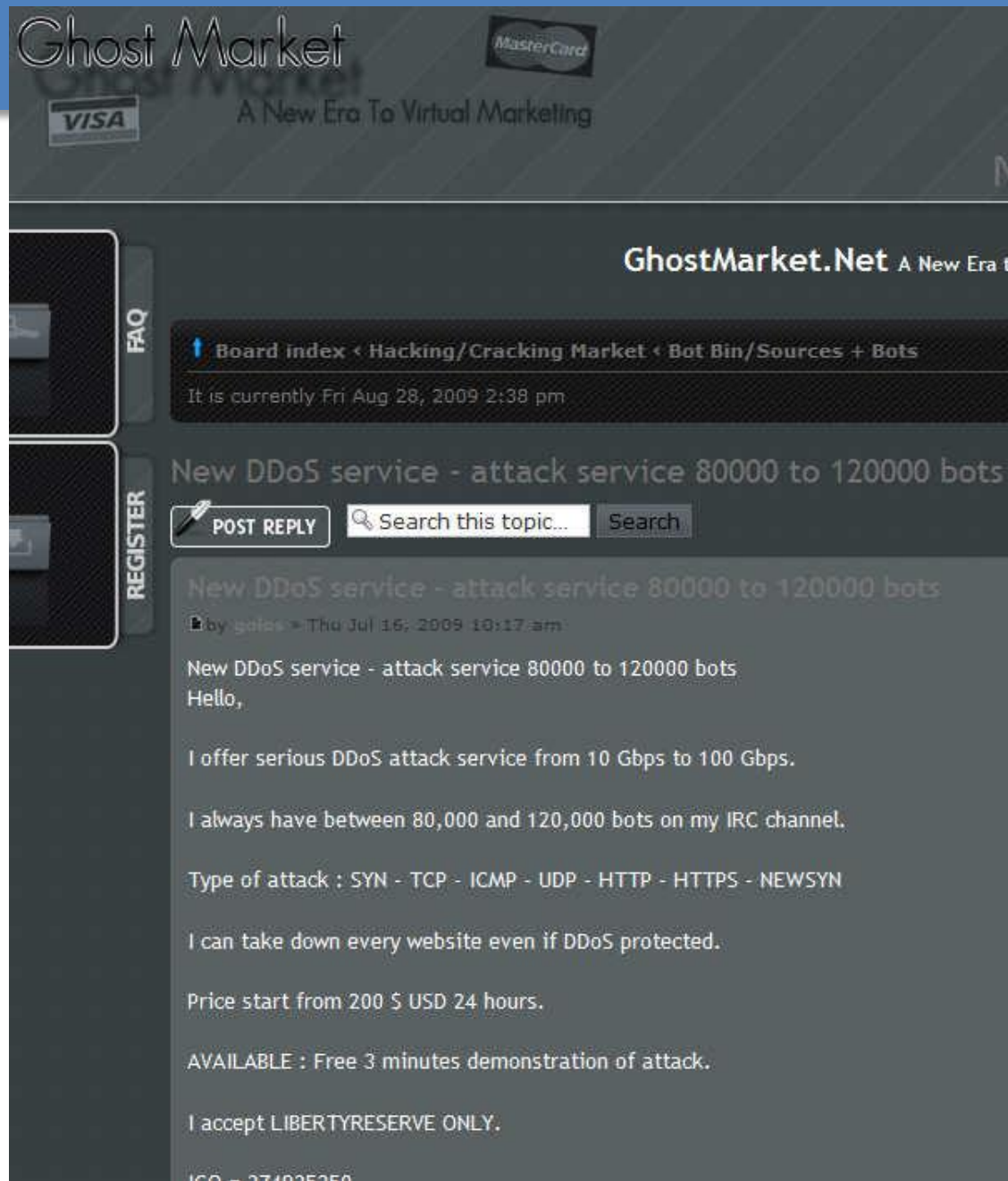
23 Nov 2014

Important! **Yahoo.com Basic** accounts can be used with **POP3 only!** Please, **do NOT** buy them if you intend to use Web interface!

31 Oct 2014

You can see **account samples** before purchase. Just choose the accounts you need, and **we will show you what you will get** before you pay!

DDoS



The screenshot shows the GhostMarket website, which has a dark theme. At the top, the site's name "Ghost Market" is displayed in a stylized font, with "A New Era To Virtual Marketing" below it. Logos for Visa and MasterCard are visible in the top right corner. On the left side, there are navigation links for "FAQ" and "REGISTER". The main content area features a breadcrumb trail: "Board index < Hacking/Cracking Market < Bot Bin/Sources + Bots". Below this, a timestamp indicates the current time is "Fri Aug 28, 2009 2:38 pm". The primary focus is a forum post titled "New DDoS service - attack service 80000 to 120000 bots". The post includes a "POST REPLY" button and a search bar. The text of the post describes a DDoS attack service, listing various attack types (SYN, TCP, ICMP, UDP, HTTP, HTTPS, NEWSYN) and claiming the ability to take down websites even if they are DDoS protected. The price is stated as starting from 200 \$ USD for 24 hours, and a free 3-minute demonstration is offered. The post concludes with the statement "I accept LIBERTYRESERVE ONLY." and a partially visible IP address "192.168.1.1".

Ghost Market
A New Era To Virtual Marketing

MasterCard
VISA

GhostMarket.Net A New Era t

Board index < Hacking/Cracking Market < Bot Bin/Sources + Bots

It is currently Fri Aug 28, 2009 2:38 pm

New DDoS service - attack service 80000 to 120000 bots

POST REPLY Search this topic... Search

New DDoS service - attack service 80000 to 120000 bots

by golos » Thu Jul 16, 2009 10:17 am

New DDoS service - attack service 80000 to 120000 bots
Hello,

I offer serious DDoS attack service from 10 Gbps to 100 Gbps.

I always have between 80,000 and 120,000 bots on my IRC channel.

Type of attack : SYN - TCP - ICMP - UDP - HTTP - HTTPS - NEWSYN

I can take down every website even if DDoS protected.

Price start from 200 \$ USD 24 hours.

AVAILABLE : Free 3 minutes demonstration of attack.

I accept LIBERTYRESERVE ONLY.

192.168.1.1

Rent a Botnet

JETBOTS

Automating WebKind [fast cash manahawkin nj](#)

Jet Bots

Featured ▾

Contact Us

PRODUCTS

NikeStore Shoe Bot

Kik Auto Message Bot

Google Plus Voter Bot

Google Plus Circles Adder Bot

Custom Software Development
Services

Custom Bot Development Services

Instagram Liker Commenter
Follower Bot

Instagram Follower Unfollower Bot

Finishline Auto Purchaser Bot

Footlocker Auto Purchaser Bot

Jet Bots

Products Overview

All of our Bots use enhanced Winsock Technology meaning they are not the usual bots you see everywhere. These bots are up to **50 times faster** than the regular bots and are much much stable in comparison as well.

Massive Package Discount: [Contact us](#), for your custom package.

Common Features

- Enhanced Winsock Technology
- Easy to use GUI
- Advanced PP Technology to process requests faster
- Multi Threading that further speeds up the bot
- Chaining – Enables the bot to run unmonitored on a given list of accounts
- Proxy Feature
- Auto-Proxy Switching Feature
- Multi-computer License

Search Website

GO

CUSTOM SOFTWARE!

Get a
FREE
Quote Today!

STAY TOUCHED TO THE
MARKET

Enter your email address to receive
notifications of seasonal discounts,

Booters

- Booter = DDoS as a service (often called “stresser”)
- *Booters - An Analysis of DDoS-as-a-Service Attacks*
Santanna et al., 2014

“Of the 14 Booters from which we purchased attacks, 5 Booters did not perform the UDP-based attacks that we ordered: 3 of those did not send any traffic, and 2 surprisingly generated a handful of TCP packets. The 9 remaining Booters performed as requested, however, and generated more than 250 GB of traffic.”

Booters: Example

Snowball Booter



xlloyd

[Account Settings](#)
[Support Center](#)
[My Attack Logs](#)
[Logout](#)



Dashboard



Stresser



Friends / Enemy



Down Or Not (Coming Soon!)



Resolvers



IP Logger



Geolocation



TOS

Stresser

Welcome to Snowball Booter.

Stresser Panel

Host

Enter Victims IP Here.

Port

Enter Port Here (80/3074)

Time

Enter Seconds Here. Your Max Is: 1500 Seconds

Method

– select option –

Booters: Example 2

The screenshot shows the 'Service' page of the DownThem booter control panel. The interface includes a sidebar menu with options like 'Home', 'Service', 'Subscription plan', 'Buy blacklisting', and 'Account info'. The main content area features a 'Service' dashboard with statistics for Servers (3), Online (3), Sessions (215366), In Progress (0), Users (2378), Online (1), and Plans (5). Below this, there are sections for 'Server Info' (with fields for IP address, Port, Interval time, and Method), 'Status log' (showing attack logs), 'Utilities' (with buttons for Notes, IP Logger, and Methods help), and 'Stop Operation' (with a field for Server IP to stop). At the bottom, there are five input fields for Cloudflare, To IP address, Skype, Geo location, and Down or not, each with a 'Resolve' or 'Check' button.

Not Secure | downthem.org/booter

K Sinkhole CDET Known booters MOL UDP_Pot Blockchain

DownThem Settings | Support | Logout

MENU

Home

Service

Subscription plan

Buy blacklisting

Account info

Service

Servers 3

Online 3

Sessions 215366

In Progress 0

Users 2378

Online 1

Plans 5

Server Info

Server IP address [Clear](#)

192.168.1.1

Port [Clear](#)

80

Interval time [Clear](#)

60

Method

CHARGEN

Start operation

Status log

[Clear status log](#)

Awaiting start..

[2018-07-19 15:24:04] Attack starting in 3, 2, 1.. Started!

[2018-07-19 15:24:04] Attack Successfull

Utilities

Notes

IP Logger

Methods help

Stop Operation

Server IP to stop

192.168.1.1

Stop

Cloudflare

Hostname

Resolve

To IP address

Hostname

Resolve

Skype

Username

Resolve

Geo location

IP address

Resolve

Down or not

Website URL

Check

Chat? - Offline