MegaD C&C's crafted response to "GET /"

```
HTTP/1.0 200 OK Server: Apache/1.3.37
Content-Type: text/html; charset=iso-8859-1

<html>
  <head>
    <title>  test page  </title>
  </head>
    <body>
      <a href='http://www.microsoft.com/'>microsoft.com</a>
    </body>
</html>
```

test page

microsoft.com.

doretorza.com/ - Cached

test page

microsoft.com.

www.doretorza.com/ - Cached

test page

microsoft.com.

selementusaks.org/ - Cached

test page

microsoft.com.

kildamindak.net/ - Cached

test page

microsoft.com.

www.kildamindak.net/ - Cached

test page

microsoft.com.

216.32.90.186/

Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

Categories: Botnets, Browsers, Data theft, Exploit code, Firefox......

Tags: Operation, Supercomputer, Malware, Worm, Ryan Naraine

150 TalkBacks
ADD YOUR OPINION

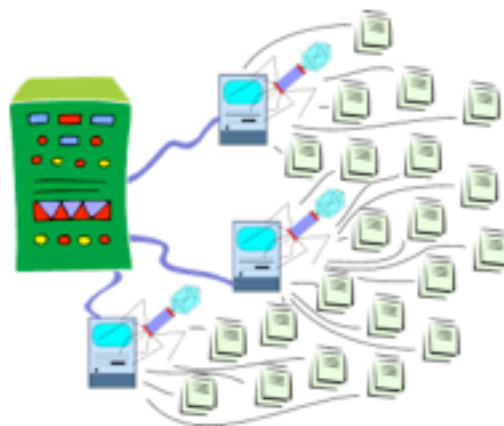SHARE | PRINT | E-MAIL | WORTHWHILE? **+97** 115 VOTES

Nearly nine months after it was first discovered, the Storm Worm Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power to rival the world's top 10 supercomputers

> " The [Storm] botnet reportedly is powerful enough as of September 2007 to force entire countries off the Internet, and is estimated to be capable of executing more instructions per second than some of the world's top supercomputers. However, it is not a completely accurate comparison, according to security analyst James Turner, who said that comparing a botnet to a supercomputer is like comparing an army of snipers to a nuclear weapon

If that made you catch your breath a bit, read on...

> " At certain points in time, the Storm worm used to spread the botnet has attempted to release hundreds or thousands of versions of itself onto the Internet, in a concentrated attempt to overwhelm the defenses of anti-virus and malware security firms. According to Joshua Corman, an IBM security researcher, "This is the first time that I can remember ever seeing researchers who were actually afraid of investigating an exploit."

(PRNG). Storm generates OIDs using its own PRNG given by the recurrence:

$$I_{i+1} = (a \cdot I_i + b \bmod 2^{32}) \bmod m$$

with $a = 1664525$, $b = 1013904223$, $m = 32767$, and the initial value I_0 is based on the system clock. The generator appears to be based on a well-known linear congruential PRNG described in the *Numerical Recipes*

Location	Hallmarks
Germany	Random OIDs with lower 10 bytes constant. Floods the Storm network aggressively with thousands of fake node IPs.
Iran	Random OIDs biased to upper half of space (first bit always set).
Sweden	Random OIDs biased to upper half of space (first bit always set). Does not appear in routing tables of any other peers.
France	One fixed OID, relatively passive crawler, appears to just be sampling Storm.
East Coast, US	257 OIDs evenly distributed in ID space behind one IP, port number used as upper two bytes of the OID.
East Coast, US	Uniform random OIDs, both a Storm implementation and crawler behind the same IP, does not report other peers.
West Coast, US	Random OIDs biased to upper half of space 100:1. Does not report IPs in response to queries.

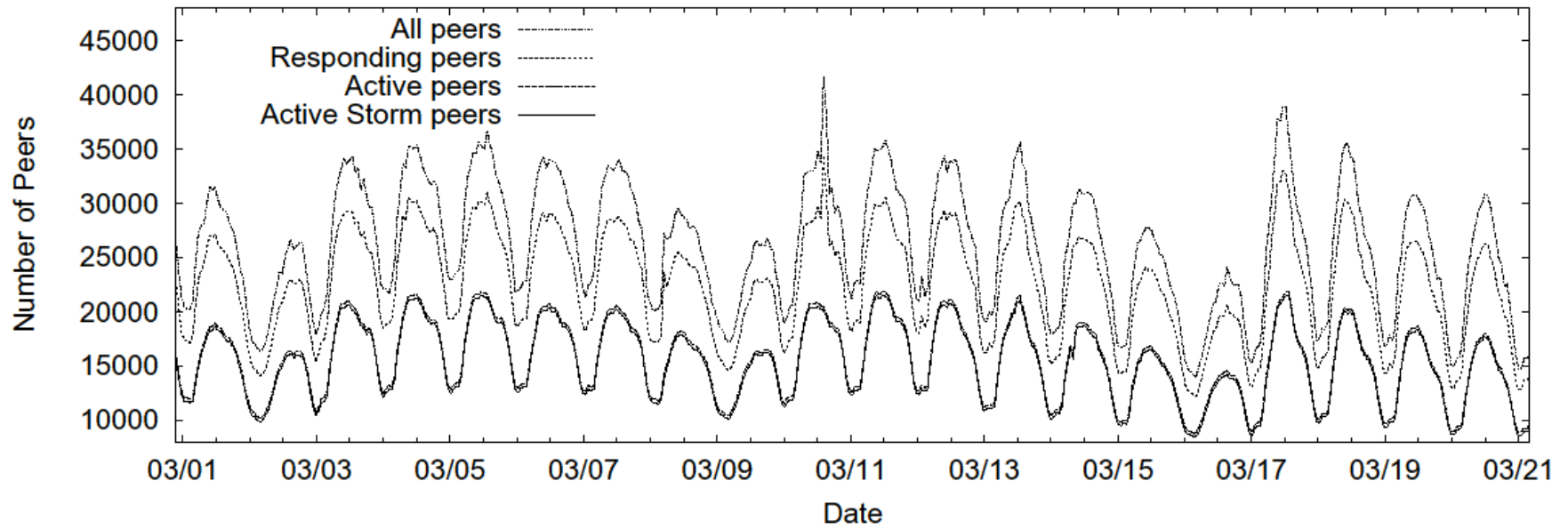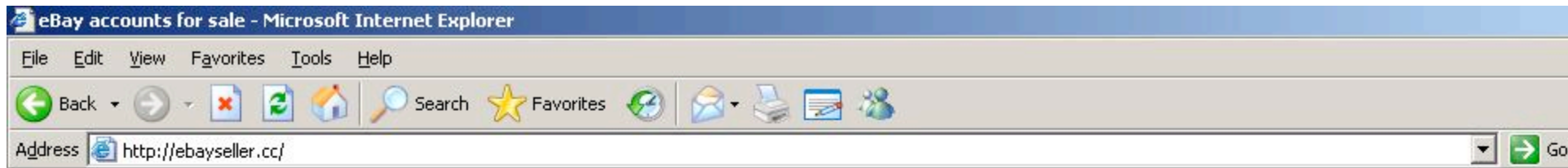Table 2: Other parties participating in the "encrypted" Storm network on April 4, 2008.

Figure 2: Estimates of the size of the Storm botnet using different notions of liveness over the first three weeks of March 2008 Note that the y-axis does not begin at zero to better separate the curves.

Список доступных акков

Сервис по продаже аккаунтов аукцыона eBay.

Добрые юзеры аукцыона eBay предлагают вашему вниманию свои аккаунты.
Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки.
Все аккаунты с доступом к мылу холдера.

Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете.
Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.

Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субьективно.

Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.

Оплата по WM.
Перед покупкой следует обязательно ознакомиться с FAQ.
По работе с товаром не консультирую.
Работа через гарант сервис приветствуется.

Мои цены:

seller/баер акк до 10 фидов = 5$
seller/баер акк 10-25 фидов = 10$
seller/баер акк 25-50 фидов = 15$
seller/баер акк более 50 фидов = 25$

My Documents

ProAgent ¥2.0 Public Edition — □ ✕

Send Menu
- ☑ Send Passwords
- ☑ Send CD-Keys
- ☑ Send KeyLog
- ☑ Send System Information
- ☑ Send Address Book
- ☑ Send URL History
- ☑ Send Processes Log

Options
- ☐ Give a fake error message
- ☐ Melt server on install
- ☑ Disable AntiVirus Programs
- ☑ Clear Windows XP Restore Points
- ☐ Protection for removing Local Server

Server Icon
You can choose any icon for server

📁 Choose Icon

Bind with File
☐ Bind with File

You can bind server with any files you want

📁 Select File To Bind

Notification
Your e-mail address which you will to receive information from ProAgent.

E-Mail: bomberman@yahoo.com   Test

Decryptor   Remove Server

About   💲 Buy Undetectable   Help

Create Server

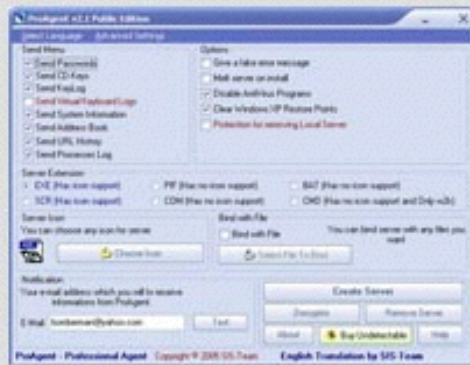**ProAgent - Professional Agent**   Copyright © 2005 SIS-Team

Recycle Bin

Start   ProAgent   9:56 AM

ProAgent v2.1

SIS – Products

Purchase Program

Customer Support Department

Commercial Programs

Freeware Programs

Custom Special Programs

New Generation Software Solutions...

- ProAgent Spy Software is one of the most powerful monitoring and surveillance applications available today.

- It is an ultimate solution for monitoring spouses, children, employees, or anyone else!

- ProAgent records all typed keystrokes, all active window texts, all visited web sites, usernames, passwords and more and sends e-mail reports to your e-mail address that you specified when creating the server, completely hidden!

- ProAgent can work in all kind of networks, it doesn't matter if the PC is behind a firewall or behind a router or in a LAN, ProAgent works in all of these conditions without any problems.

Click here to purchase **ProAgent v2.1** Special Edition...

Click here to download **ProAgent v2.1** Public Edition

New Products

SIS-IExploiter v2.0

SIS IExploiter

ProAgent v2.1

PRO AGENT

AntiDote v1.2

SIS-Downloader

Virtual Keyboard

allBots Inc.

Social Networking Bots

GOOD News!!! We have something more for you! Yes, we have just integrated **CAPTCHA Bypasser** in all of our bots.

Winsock (Multi-threaded) Bots

Become an **Affiliate** and **Start Earning Now**

Click here for 30+ MySpace Bots

Accounts Creator
(You Just Need To Type In The CAPTCHAs To Create Accounts)

Social Networks

MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager	PayPal Buy Now	~~$180.95~~	$140.00
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock)	PayPal Buy Now	~~$360.95~~	$320.00
YouTube Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
Friendster Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
Hi5 Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
TagWorld Accounts Creator	PayPal		

Friend Adders, Message Senders, Comment Posters & Others
(All Bots Work In A Conventional Manner, They Gather Friend IDs/Names And Send Friend Requests, Messages, Comments Automatically)
Chaining Feature Is Available On All Bots for All Networks Except Facebook

Advertisement

i have boa wells and barclays bank logins....

have hacked hosts, mail lists, php mailer send to all inbox
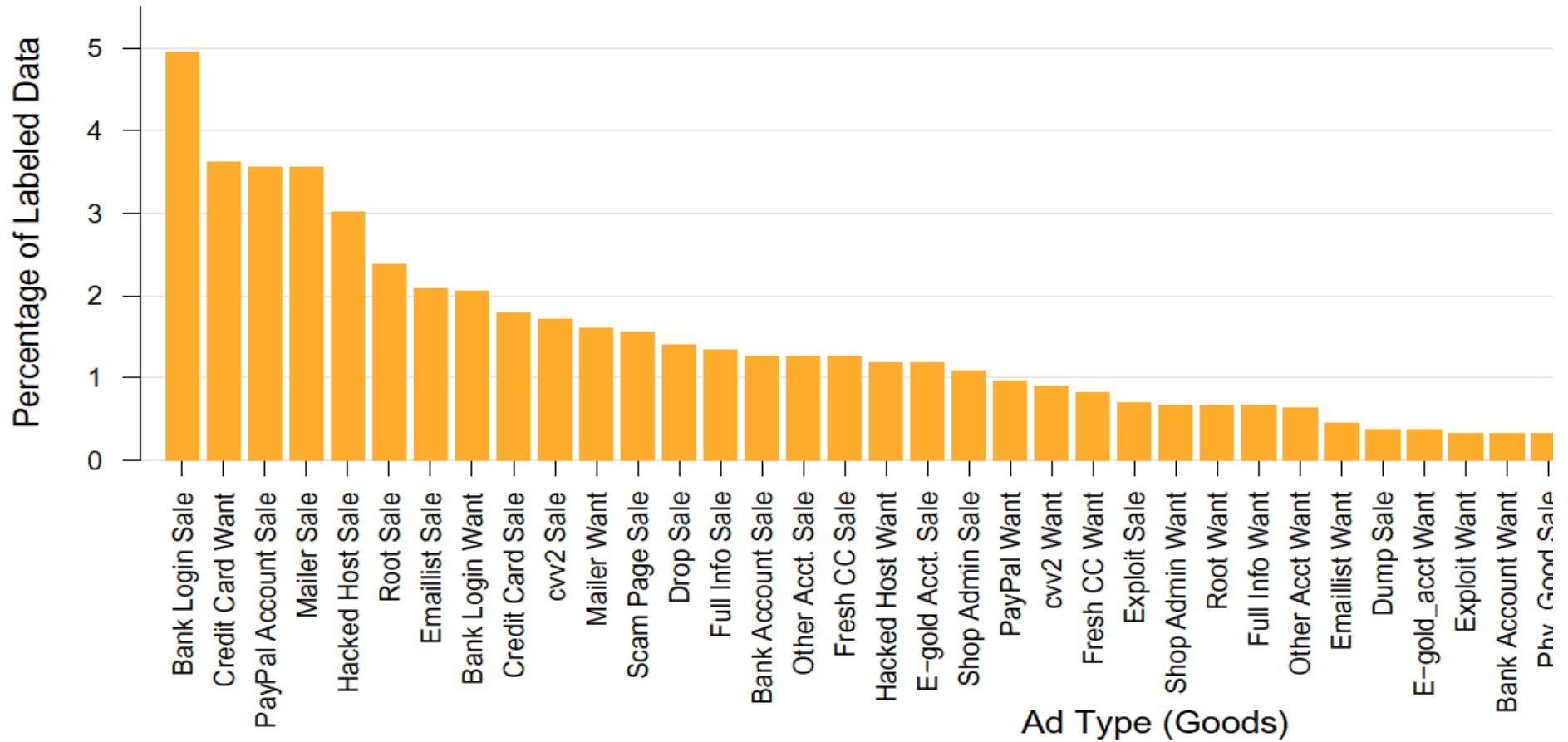
i need 1 mastercard i give 1 linux hacked root

i have verified paypal accounts with good balance...and i can cashout paypals

OrAcLe	I NEED INBOX MAILER ..HOW MUCH IS IT?
OrAcLe	i REQUIRE IT
<ehmo>	yop
OrAcLe	?
OrAcLe	IS IT TO ALL INBOX?
<ehmo>	5$
<ehmo>	hm
OrAcLe	WILL YOU PLS ACCEPT $3
<ehmo>	many people selling for 3
<ehmo>	ask him
OrAcLe	WHO?
<ehmo>	dono
OrAcLe	hm?
OrAcLe	bRO...I REALLY WANNA BUY 4RM YOU
<ehmo>	ok
OrAcLe	Already uploaded i hope
<ehmo>	yes
OrAcLe	Ok..what's ur egold acct ?
<ehmo>	give me a second
OrAcLe	Ok..i wait

OrAcLe	Ok..i wait
OrAcLe	Please make sure that it is the account that you intend to spend to.
OrAcLe	Amount: 5.00 US Dollars' worth of Gold
OrAcLe	From: [elided] (Anthrax De Oracle)
OrAcLe	Is this info correct?
OrAcLe	Ok..i send now
OrAcLe	e-metal. payment confirmation: Batch [elided]
OrAcLe	Paid To: [elided] (Filialka)
OrAcLe	Memo:
OrAcLe	
OrAcLe	Actual payment weight = 0.007704 oz. (0.239626 grams)
OrAcLe	Equivalent USD amount of this payment: $5.00
OrAcLe	Applicable Conversion factors:
OrAcLe	1 oz. troy = 31.1034768 grams
OrAcLe	Gold exchange rate = 649.00USD/oz
OrAcLe	The e-metal payment was successful
OrAcLe	Your batch number for confirmation is [elided]
OrAcLe	Thank you for using e-gold.
OrAcLe	SENT
— —	I'm SELLING Usa AOL Fulls Info CC also - Uk/Eu Full info - with unique algo.. !
	.5.Payment Only E-GOLD

Marketplace Ads for Goods

Marketplace Ads for Services
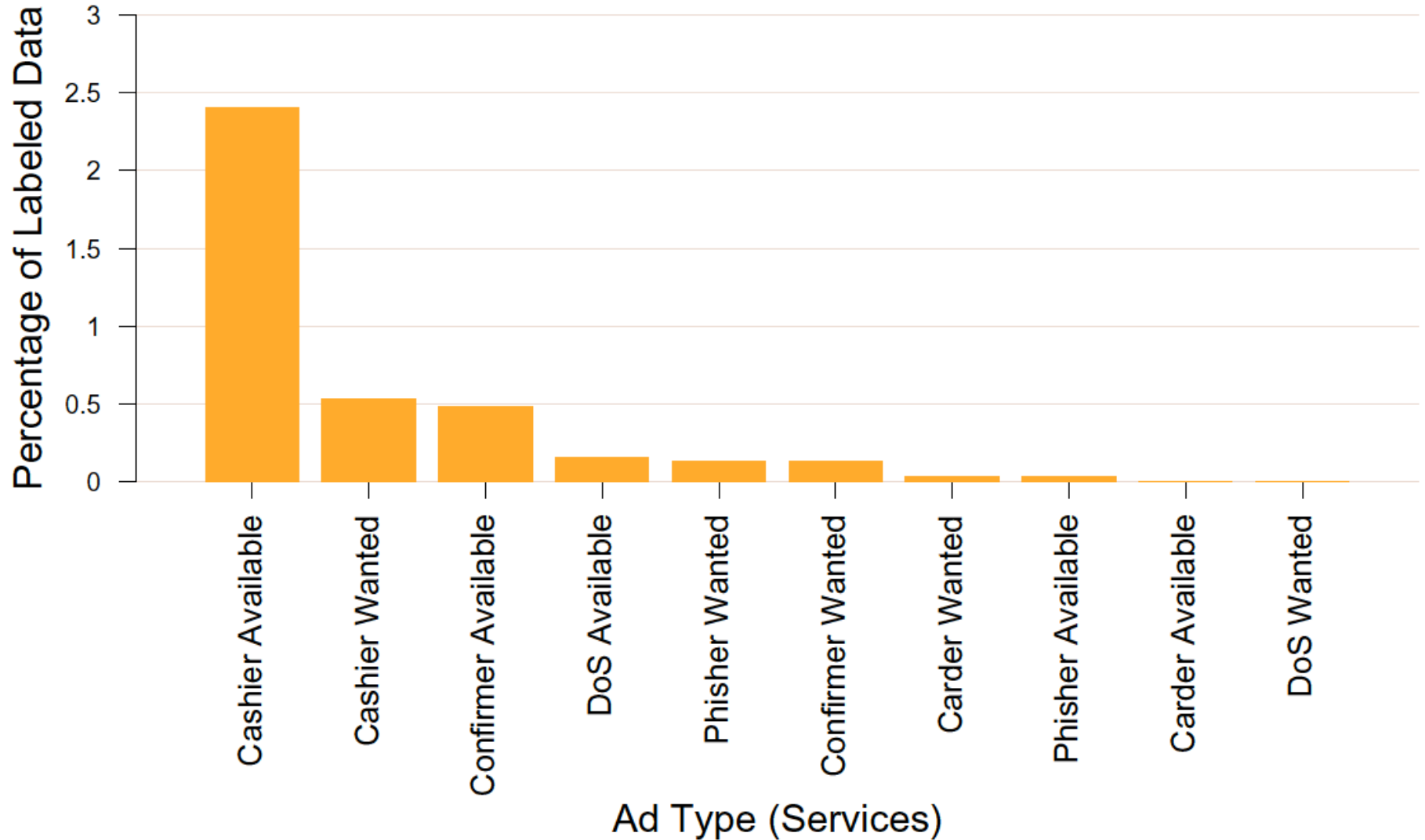
Study programs:

Study programs:

[0] INTRODUCE - BASICS - 1-2÷ - 50$

Security in the network, configuring the system to work.
Proxies, TOR, Proxy, Socks, VPN (+ double))

Working Dedicated Server
Want to know how get this yourselft? +15$

Credit/Debit card (CC) payments in internet
Where to get this and how make money on this

AntiFraud, Verified by Visa, Master Card security Code.

[1] HELLO WORLD or SKYPE CARDING - 2-3h - 75$

for those who passed the basic.

Skype Carding. The first practical experience, bringing a steady income, it is recommended for those who passed basic course on security in the network.

Material for the work included:

Credit Card USA (no VBV/MCSC)
Dedicated Server USA
DoubleVPN for security in network

Invest 10$/day. Get 100-150$.

Advice: sell skype accounts not only on one board, try to sell this on RU-boards

Result: You learn SKYPE carding, get an account with a balance $ 50 (live long), you can immediately sell on the forum for 7-8$, or you can try to sell it to other (legal) sites for 30-40 $.

[2] How to get your own DROPS for STAFF and TRANSFERS 4-6h – 250$

*for those who passed the basic

Drop - person who takes the bank transfer to his bank account, then sends money you or stuff (product: a laptop, for example) to his address, then sends to you.

Sooner or later anybody think about this.
Your own drop project its very good business.

Material for the work included:

Drop project (used)
+want to make your own? +150$
Forums, jobs, posting boards
DoubleVPN for security in network

Advice: its not too hard get drops and its good business for you, when you control drops you can get 50/50 staff (carder makes 2 notebook on your drop, one for you and for carder) and 60% from bank transfer amount, take it!

Result: Making drop project, posting on forums with intersting leged and get your own QUALITY DROPS READY FOR WORKING ON YOU, then you can give him to carder (50/50) or to bank transfers (60%).

[3] SCAM (Phishing) 4-6h - 200$

for those who passed the basic

WESTERN UNION

MONEY TRANSFER

Phishing is the criminally fraudulent process of attempting to acquire money!

Literate phishing in internet
For example on dating site.

Material for the work included:

Foto and video (model; woman) for scum.
+want to know how to get your own? **+50$**
Dating site, Social Networks, Chats
DoubleVPN for security in network

Advice: not many people know about that more than half of potential victims punched "new wife" on GOOGLE, if you writing you love to cook - sign up online cooks and share recipes))

Result: Getting acquainted with the victims, and quality PHISHING them for WESTERN UNION, main legends for phishing, learn all about anti-scam and stop-phishing, and how to bypass fraud tests;)

[4] Poker PS, FTP, BF, BU 5-7÷ – 300$

for those who passed the basic

Poker Stars.com

Poker - interesting game, you can make money in game always, when you gaming on stolen money;) (ñ)

Material for the work included:

Credit Card (AU/CA/EU)
Dedicated Server
DoubleVPN for security in network

Scans and calls for additional payments

Advice: In poker, everyone should find his own way, where and how to take more $

Result: Make your own deposit in poker from stolen credit card (max 600 euro) and take money for this (you can sell for 15% from balance) on forum, or you can game on this money or cashout them, there are many pitfalls that i'll show you, and most importantly you'll know how the casino anti-fraud politics and most importantly gain the necessary knowledge to move next and get your own way in poker.

[5] CC-Shop-Track (Shopping) 6-8h - 350$

for those who passed the basic

Shopping on the Internet on stollen bank cards, so to store the goods sent to drop (without police:))

Material for the work included:

Credit Card / Enroll
Verified DROP (50/50)
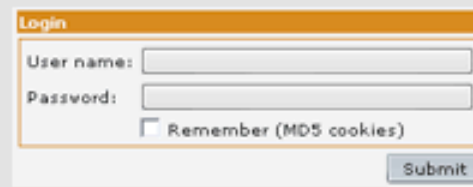Dedicated Server
DoubleVPN for security in network

Scans and calls for additional payments

Advice: many pitfalls! should be patient and be immediately ready to proring, scans the ID and CC, and even photos HOLDER'a (credit card holder) about the computer (a new practice in the NL).

Result: SEND YOUR FIRST (Notebook, camera, ring) on drop and get money for it, and get detailed information about shoping on stolen CC on USA or DE, that, where to find drops, about shops and their search, anti-fraud policies and circumvent potential problems, as well as many stumbling blocks in this business.

[6] Botnet or how to get my own bank accounts. 12-18h - 500$

for those who passed the basic
experienced PC user

Login	
User name:	
Password:	
	☐ Remember (MD5 cookies)
	Submit

Trojan - virus, programm, that helps you to get your own bank accounts, paypal, credit cards, poker accounts, ebay, admin accounts of shops and so on.

A botnet is a serious thing, it's not Skype carding)) Bank accounts, credit cards, shops, MoneyBookers, Bet office, poker, Ebay, Enroll - all this you get with Bank Trojan, Trojan are all sorts of public nice triple ZeuS, I remember in my memory was limbo and adrenaline and SpyEye, from privat mbo and 76, must always start somewhere in order to get results and not necessarily to invest 15k in a new Zeus of the author, can be found in public for free 1.2 or 1.3, forums often spread builder, that's only 90% of them are infected with other viruses and your admin panel, along with Troy obscured As soon as you let go LOADS.

Material for the work included:

Zeus Trojan (bank trojan). *WE DON'T SELL BUILDER*
Injects Pack (>200 injects)
VPS Hosting for trojan (1 month)
DoubleVPN for security in network

Advice: invest in a triple can be infinitely better to hone a particular topic, of course the most money its auto-transfers:)

Result: Mak Trojan, will go a few thousand loads and get the combat botnet, which You will have your own logs (bank accounts), will introduce the basics of cryptography, where are get loads, also learn to write injections, and be able to earn money on this.

Individual counseling from $ 20. No Antenatal clinics :-)

GOOD DAY, GOOD MOOD AND GOOD BUSINESS [!]

CASH PARADISE UNIVERSITY ICQ:
JABBER: