Client: PASS $!0@
Client: NICK [NIP]-IBM6N4SKA
Client: USER YSNARFAL "ask0.org" "FCK" :YSNARFAL

Client: JOIN #mipsel %#8b

Server: :[NIP]-IBM6N4SKA!YSNARFAL@114-30-XXX-XX.ip.adam.com.au JOIN
:#mipsel

Server: :leaf.4714.com 332 [NIP]-IBM6N4SKA #mipsel :.silent on .killall
.lscan .rlscan .esel [US],[FR],[IT],[GB],[ES],[DE] rejoin 10800 10800

Server: :leaf.4714.com 333 [NIP]-IBM6N4SKA #mipsel DRS 1228994845

Server: :leaf.4714.com 353 [NIP]-IBM6N4SKA @ #mipsel :[NIP]-IBM6N4SKA

Server: :leaf.4714.com 366 [NIP]-IBM6N4SKA #mipsel :End of /NAMES list.

```
.visit              - flood URL with GET requests
.scan                   - scans a random range for vulnerable routers/modems
.rscan          - scans a CIDR range for vulnerable routers/modems
.lscan                  - scans the local subnet for vulnerable routers/modems
.lrscan                 - scans a range in the local subnet for vulnerable routers/modems
.split          - splits the workload of a scan thread into two threads
.sql            - scans for vulnerable MySQL servers and attempts to make them download and run URL
.pma            - scans for vulnerable phpMyAdmin and attempts to make them download and run URL
.sleep              - makes the bot sleep for the given time
.sel                    - ???
.esel                   - skip next part if locale is not X
.vsel                   - skip next part if version is not X
.gsel                   - ???
.rejoin [delay]         - cycle the channel after delay
.upgrade                - download new bot from the distribution site
```

It appears that Netcomm NB5 ADSL modems are not the only devices affected by this bot.

Modems with similar hardware configurations (unknown brands) from Italy, Brazil, Ecuador, Russia, Ukraine, Turkey, Peru, Malaysia, Columbia, India and Egypt (and likely more countries) also seem to be affected, and are spreading the bot.

Introduction:

The NB5 was a popular ADSL/ADSL2+ modem-router, produced by Netcomm circa 2005. The NB5 is based on the Texas Instruments TNETD7300, featuring a 32bit RISC MIPS 4KEc V4.8 processor, 2MB of flash ROM, 8MB of RAM, Ethernet + USB connectivity, and runs an embedded Linux distribution.
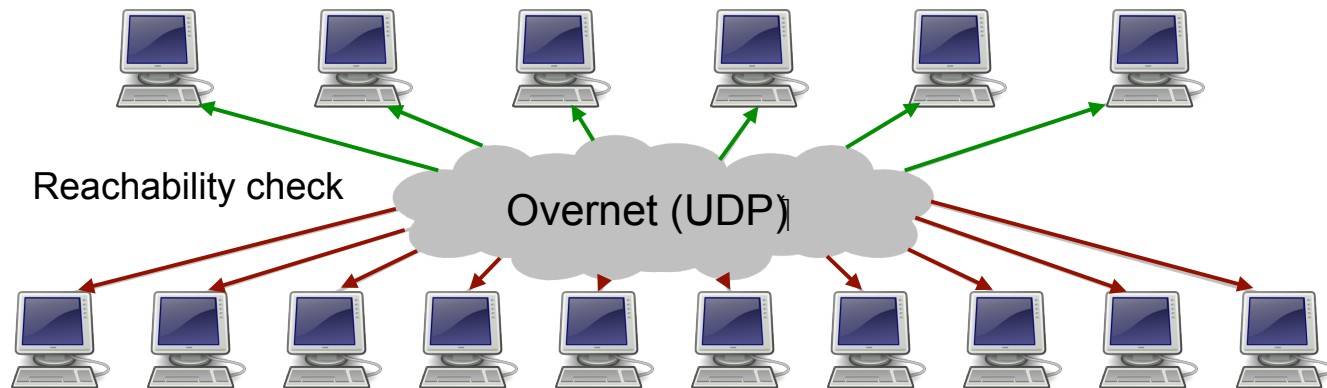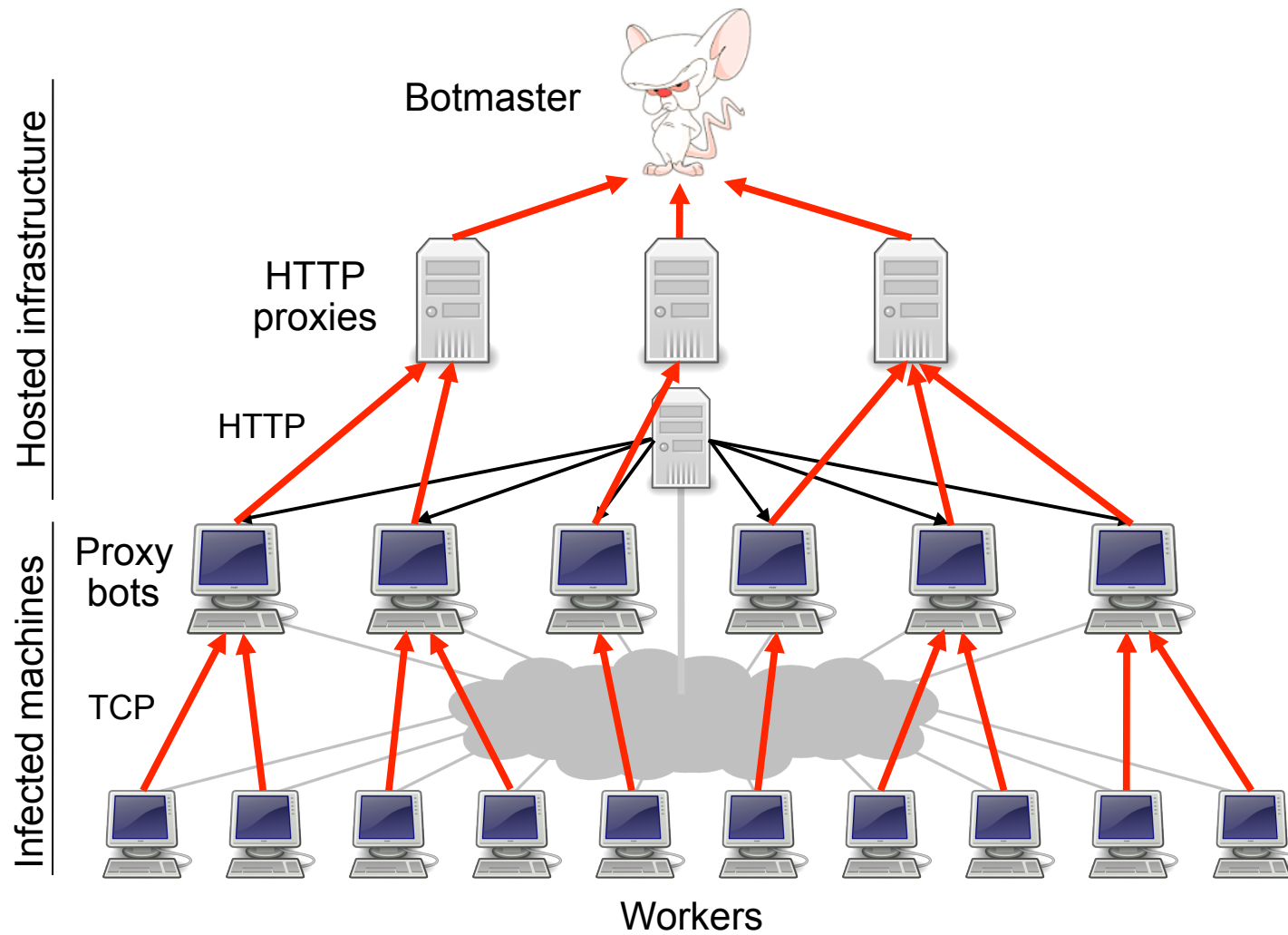
Welcome to Storm!

AwesomePostcard.Com

http://█████████████/ ▾ ▶ G ▾ Google 🔍

AWESOMEPOSTCARDS
http://www.awesomepostcards.com

Your download will start in 5 seconds.
If your download does not start, <u>click here</u>

Done

Would you like to be one of our newest bots?

Just read your postcard!

(Or even easier: just wait 5 seconds!)

The Storm botnet

Reachability check

Overnet (UDP)

The Storm botnet

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   SHARE | PRINT | E-MAIL | WORTHWHILE? **+97** 115 VOTES
ADD YOUR OPINION
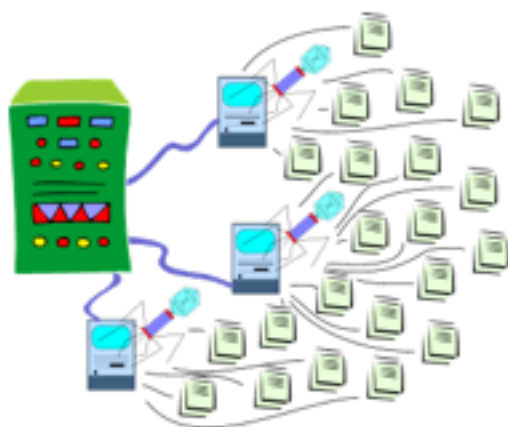
Nearly nine months after it was first discovered, the Storm Worm Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

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."

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.

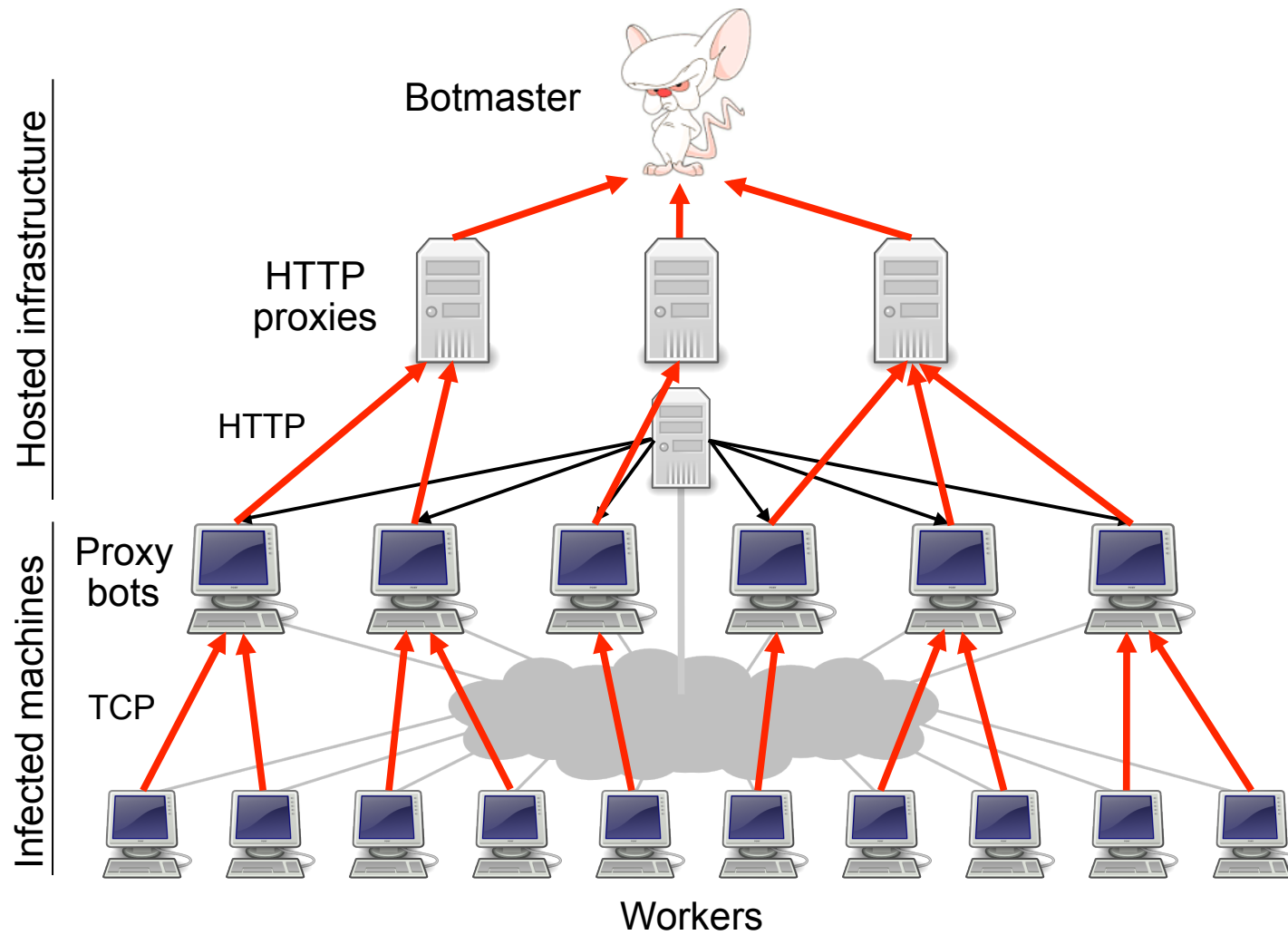Table 2: Other parties participating in the "encrypted" Storm network on April 4, 2008.
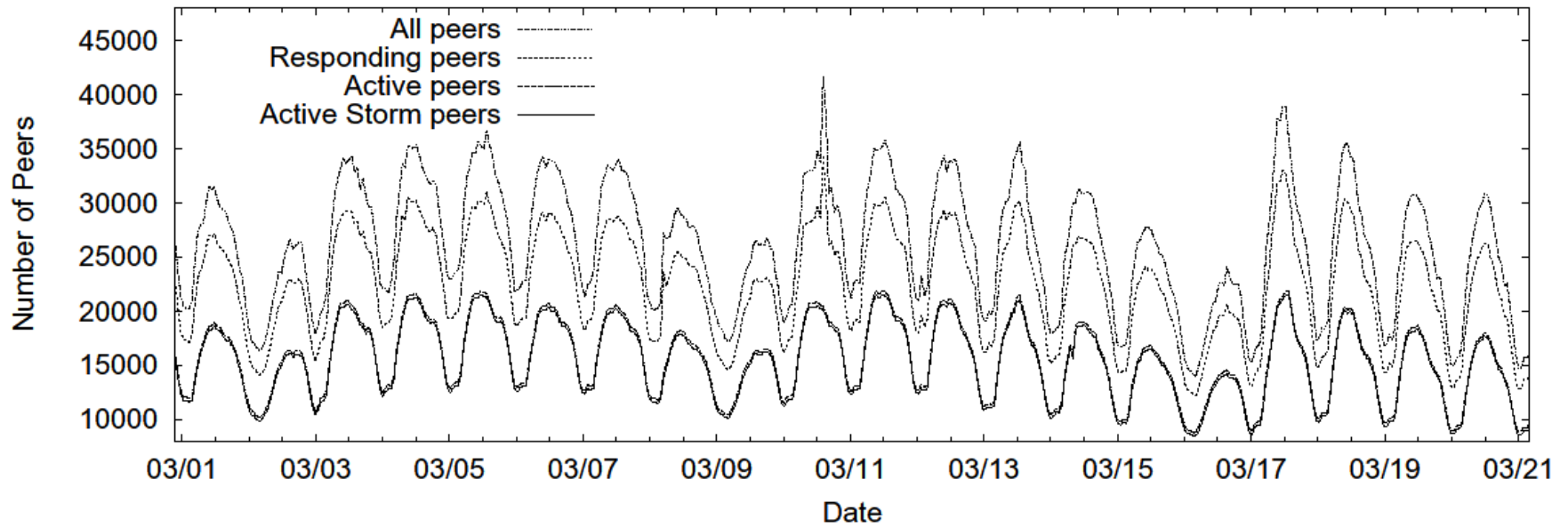
Figure 2: Estimates of the size of the Storm botnet using different notions of liveness over the first three weeks of March 2008 Note that the y-axis does not begin at zero to better separate the curves.

The Storm botnet

GooHost.ru
## Reliable and quality hosting

Тел.: +7(495) 542-39-87, icq: 418396204

Menu

- Hosting Plans
- Email Mailing
- Website Design
- FAQ
- Dedicated server
- Domain Registration
- Payment
- Contact

Hosting Plans

We offer a complaint-resistant hosting to host your sites, which are specified in mass mailings.

We decided to bring visitors to your web site through unsolicited mass emails? Wonderful idea! You certainly expect a boom visits. But! As in any ointment and then not pass without a spoon of tar ... Alas, but your wonderful site, shortly after the start of spam mail, will be closed due to flood of complaints from postal services. Is there a way to avoid these problems? Of course! Our complaint-resistant hosting simply ignores any complaints, all postal services, and you can be rest assured about the performance of their sites - they will not be closed. And you get new customers, expand their business and increase their sales and revenue, thanks to spam mailing lists.
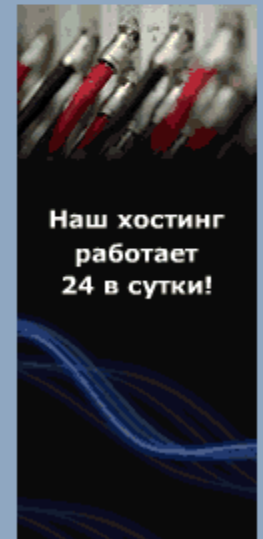
Наш хостинг работает 24 в сутки!

Internet

Obuzoustoychivy hosting is more expensive than usual, but you will have the full guarantee that your site no one ever closes, it will always be available to your customers!

MINI PLAN	
Volume disc	400 MB
Domains	1
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	4 000 rub. / 1 month.

STARTER PLAN	
Volume disc	500 mb
Domains	3
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	5 000 rub. / 1 month.
BUSINESS PLAN	
Volume disc	1000 mb
Domains	7
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	7 000 rub. / 1 month.
PREMIUM PLAN	

Bulletproof Hosting - Never Get Shut Down Again !

Reliable Bullet Proof Web Hosting

-Email Marketing Service

Enter your Domain Name:

www. [   ] [.com ▲▼] (Submit) Check Available

☑ .com ☑ .net - Bullet Proof Domain $100/Year

Hosting Plans:

Partners:

◆Sun.

AMD⏚

Cisco

Microsoft
CERTIFIED
Partner

Red Hat Linux

3 Day Free

SILVER PLAN
- Bullet Proof Hosting A
- 50MB Web Space
- 10GB Monthly Bandwidth
- Static Pages Only
- FTP Account
- 99.8% Uptime
- $299.95/month

New Price $**199.95**/month
More... ——— **Order Now**

GOLDEN PLAN
- Bulletproof Hosting B
- 50MB Web Space
- 10GB Monthly Bandwidth
- PHP/CGI/ASP Supported
- FTP Account
- 99.8% Uptime
- $399.95/month

New Price $**299.95**/month
More... ——— **Order Now**

Bullet Proof Hosting

Bullet Proof Domains

Bullet Proof Server

Reseller

BP URL

Contact Us

Sitemap

Bulletproof hosting and dedicated servers

Hosting is our business, what you're hosting is your business! Keep your website safe with 100% bulletproof hosting.

Bulletproof hosting plans for any requirement

Bulletproof without compromises

Host anything
We allow any kind of content and software, no questions asked.

Completely anonymous
We don't require any of your personal information from you, payments to us are completely anonymous through bitcoin.

Bulletproof
No abuse complaints or takedown requests will get through to you, your hosting is safe at any time.

Dedicated Network
All of our servers have their own network connection, you won't have to share your bandwith with anyone else.

Multiple Locations
We have a multiple different locations available, all of equally excellent quality.

Automatic Setup
We realize that time is money, server setup is completely automatic and ready within just minutes of ordering!

Low Prices
We have the lowest prices amongst all **real** bulletproof hosting providers.

Money Back Guarantee
If you're not satisfied with our services within the first 3 days of ordering, ask for a refund and we will refund you in full, no questions asked.

Bulletproof hosting plans for any requirement

VPS Basic	VPS Pro (BEST VALUE)	Dedicated One	Dedicated Two (PRO)
Bulletproof	Bulletproof	Bulletproof	Bulletproof
2GB Ram	4GB Ram	Amd 8 Core FX	Intel Xeon Processor E5-2697 (12 Core)
CentOS 6, CentOS 7, Fedora, Windows	CentOS 6, CentOS 7, Fedora, Windows	16GB Ram	32GB Ram
Free cPanel	Free cPanel	CentOS 6, CentOS 7, Fedora, Windows	CentOS 6, CentOS 7, Fedora, Windows
1 IP Address	2 IP Address	Free cPanel	Free cPanel
Dedicated 10 Mbit UP / DOWN	Dedicated 10 Mbit UP / DOWN	3 IP Addresses	3 IP Addresses
Basic DDoS protection	Basic DDoS protection	Dedicated 100 Mbit UP / DOWN	Dedicated 100 Mbit UP / DOWN
Storage 200GB	Storage 200GB	Professional DDoS protection	Professional DDoS protection
Unlimited Bandwidth	Unlimited Bandwidth	Storage 2TB	128GB SSD OS Dedicated
Full root access	Full root access	Unlimited Bandwidth	Storage 2TB
		Full root access	Unlimited Bandwidth
			Full root access
$199 (per month)	**$249** (per month)	**$499** (per month)	**$599** (per month)
ORDER NOW	ORDER NOW	ORDER NOW	

Intel Xeon inside™

Samsung SSD activated

Security Fix
Brian Krebs on Computer Security

About This Blog | **Archives** | **Security Fix Live: Web Chats** | **E-Mail Brian Krebs**

RECENT POSTS

- **E-Banking on a Locked Down PC, Part II**
- **ChoicePoint Breach Exposed 13,750 Consumer Records**
- **President Obama on Cyber Security Awareness**
- **Mozilla Disables Microsoft's Insecure Firefox Add-on**
- **PayChoice Suffers Another Data Breach**

Entries By Category
- **Cyber Justice**
- **Economy Watch**
- **Fraud**
- **From the Bunker**
- **Latest Warnings**
- **Misc.**
- **New Patches**
- **Piracy**
- **Safety Tips**

Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (**Note**: A link to the full story on McColo's demise is available here.)
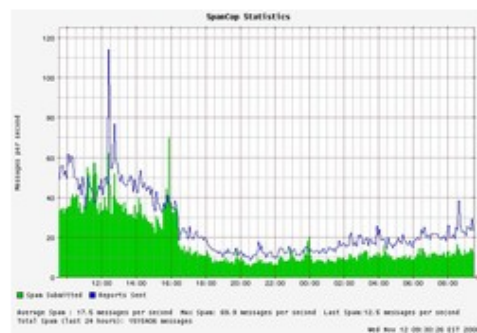
Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

> In the afternoon of Tuesday 11/11, IronPort saw a drop of almost 2/3 of overall spam volume, correlating with a drop in IronPort's SenderBase queries. While we investigated what we thought might be a technical problem, a major spam network, McColo Corp., was shutdown, as reported by The Washington Post on Tuesday evening.

Spamcop.net's graphic shows a similar decline, from about 40 spam e-

Retail Fraud Rates Plummeted the Night McColo Went Offline

One month after the shutdown of hosting provider McColo Corp., spam volumes are nearly back to the levels seen prior to the company's take down by its upstream Internet providers. But according to one noted fraud expert, spam wasn't the only thing that may have been routed through the Silicon Valley based host: New evidence found that retail fraud dropped significantly on the same day.

It is unclear whether the decrease in retail fraud is related to the McColo situation, but in speaking with **Ori Eisen**, founder of 41st Parameter, he said close to a quarter of a million dollars worth of fraudulent charges that his customers battle every day came to a halt.

Eisen, whose company provides anti-fraud consulting to a number of big retailers and banks, told me at least two of the largest retailers his company serves reported massive declines in fraud rates directly following McColo's termination.

"It stopped completely that night," Eisen said, referring to a drop in fraudulent activity linked to purchases of high-value merchandise with stolen credit and debit cards on Nov. 11, the day McColo was shut down. "Yet, it will come back after [the scammers] erect their new infrastructure."

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/

http://installs4sale.net/   Google

Google   Search ·   ·   ·   · M ·   Sidewiki ·   Bookmarks·   Translate ·   AutoLink · »

Installs4Sale.net

Installs4Sale.net - надежный сервис по
загрузкам, достойный доверия

КОНТАКТЫ

560869831
550525933

info [at] installs4sale.net

ПРИЕМУЩЕСТВА

→ Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миксы стран по вашему выбору.

→ Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.

→ Договорится по всем ценам и получить индивидуальные условия вы можете в службе

Wire

E-PASS

WebMoney

The PPI Eco-system

Clients

Fake AV Spambot Keylogger

❶

PPI
Service

❹

❷

PPI
Affiliate

❸

Target
Host

Downloader
Install
Payment

Gangsta Bucks.com
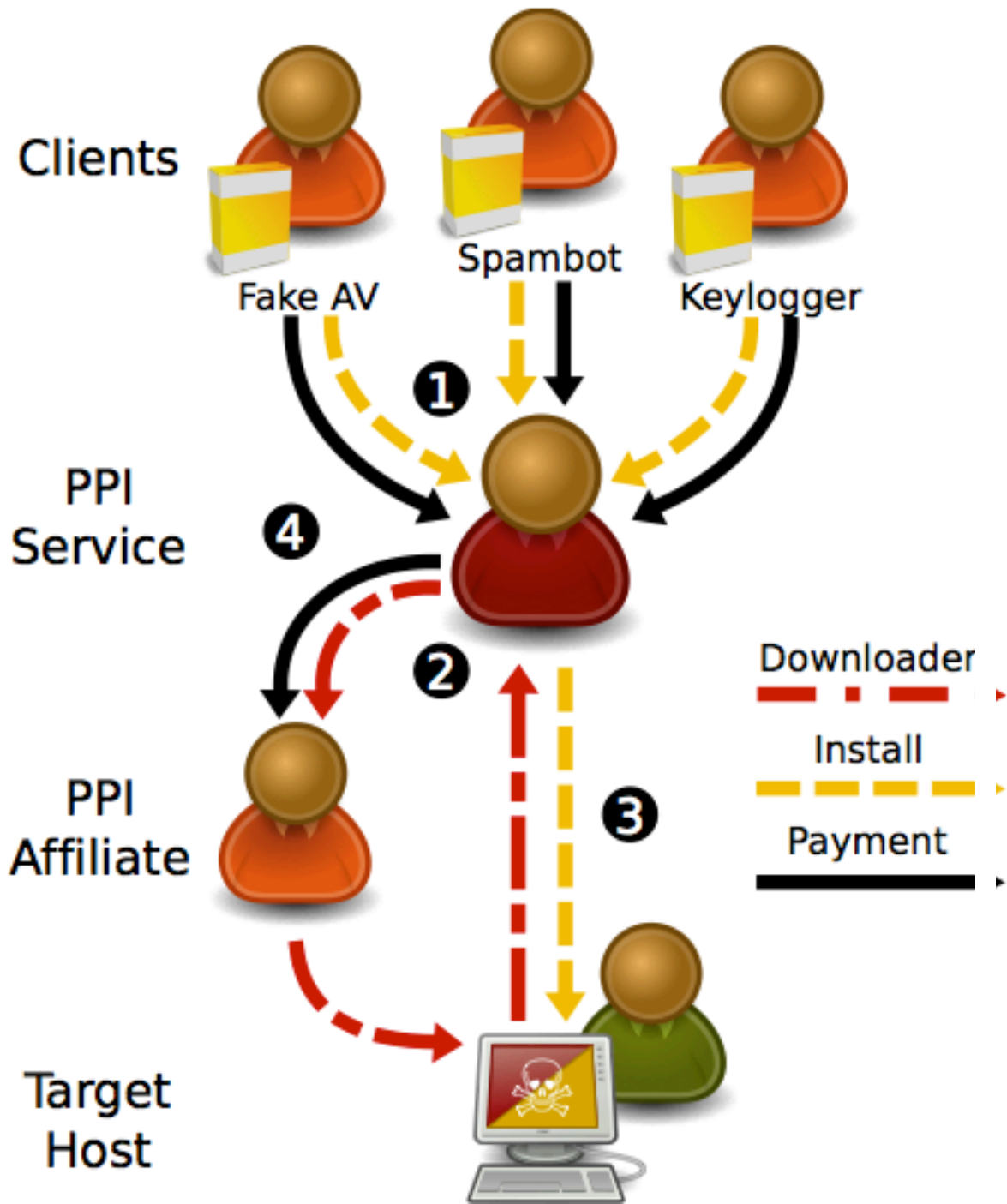
Statistic

Home   Conditions   Registration   Tariffs   Contacts

An individual approach to everyone

Guaranteed weekly payouts

Round-the-clock support

Detailed statistics

User-friendly software

GangstaBucks.com - it pays on time! We pay for all installs!

Join our ranks and by tomorrow you could get your first payout!

Gangsta Bucks.com

WebMoney

➔ Договорится по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!

➔ Мы отслеживаем уникальность инсталов и их чистоту перед продажей.

УСЛОВИЯ

➔ Мы работаем строго по предоплате. Допускается частичная оплата постоянным клиентам на большие объемы.

➔ Мы не несем ответсвенности за то что у вас по каким-то причинам отстувуют загрузки. Если вы не видите инсталов с первых минут мы можем проистановить отгрузку до выяснения обстоятельств.

ТАРИФЫ

		Все цены указаны за 1000 уникальных загрузок
GB (Англия)	150$	
DE (Германия)	150$	
USA (США)	130$	
IT (Италия)	120$	
Микс (US,CA, AU, GB)	100$	
CA (Канада)	100$	
Микс (Европа)	40$	
Азия	10$	

Репутация: 4 [−2/+6]

Место свободно   Место свободно   Место свободно   Место свободно
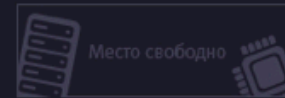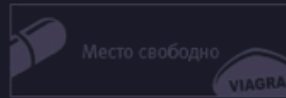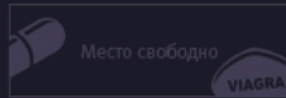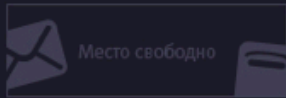
Продам инсталлы MIX

NEW TOPIC   POST REPLY   Список форумов SpamDot -> Трафик, загрузки, ботнеты

Автор	Сообщение

Umbro
Member

Зарегистрирован:
29.12.2007
Сообщения: 216

Добавлено: Вт Янв 26, 2010 9:48 am   Заголовок сообщения: Продам инсталлы MIX   Оценить: 0   QUOTE

Приветствую всех!
Greetings to all!
В связи с неожиданным переизбытком, продам не нужные инсталлы.
Due to overstock I am selling unneeded installs.
Цена : 60 вмз за 1к
Price: $60 WMZ for 1k
Оплата: оплата вперед, без протекции.
Payment: In advance, with no escrow.
География: микс мира, практически без азии.
Geography: A mix of countries, with virtually no Asia.
Что грузится: грузится на бота только мой граббер и ВАШ спамбот (ничего кроме спамботов не гружу принципиально)
Loads: Only my grabber and your spam bot is being loaded (nothing but spam bots allowed)
Получение: оплачиваете и через 10 минут я запускаю Ваш ехе на прогруз.
Delivery: You pay and I start running your exe in 10 minutes.
Качество: исходя из того, что я написал выше, я не гружу ничего кроме своего граббера и вашего спамбота, загрузки не дохнут и я никого не выгружаю со временем, не гружу по 2 ехе на 1 бота. Хотя о качестве я думаю отпишут те, кто брал у меня уже инсталлы.
Quality: As stated above, nothing else is loaded besides my grabber and your spambot, loads do
Контакты: **not die, and I do not overutilize resources, or load 2 exe per bot. Inquire with others who have already purchased installs**
icq: 312-456, когда стучитесь, просьба сообщать ваш ник и что вы с форума по поводу инсталлов.

Всем спасибо, приятного дня.

vatinkes πύργους

Verify Your Registration

* Enter the code shown: _____ More info

This helps prevent automated registrations.

Please enter the code you see below. what's this?

Qualifying question

Just to prove you are a human, please answer the following math challenge.

Q: Calculate:

$$\frac{\partial}{\partial x}\left[4 \cdot \sin\left(7 \cdot x - \frac{\pi}{2}\right)\right]\Bigg|_{x=0}$$
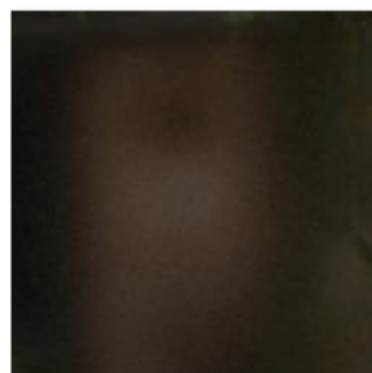
A: _____

mandatory

Note: If you do not know the answer to this question, reload the page and you'll get another question.

Figure 2: Difficult but correctly transcribed examples from the internal street numbers dataset.
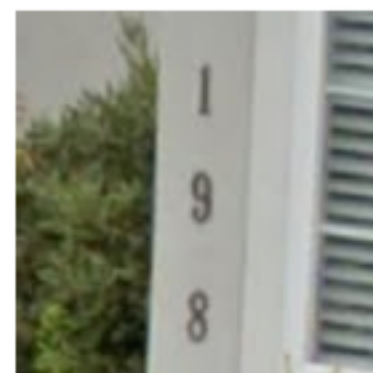
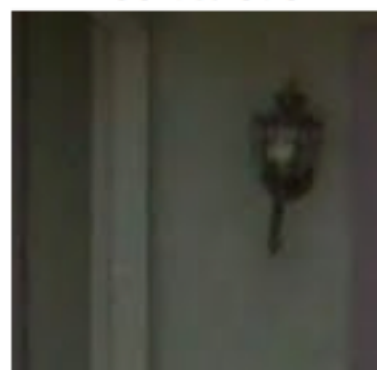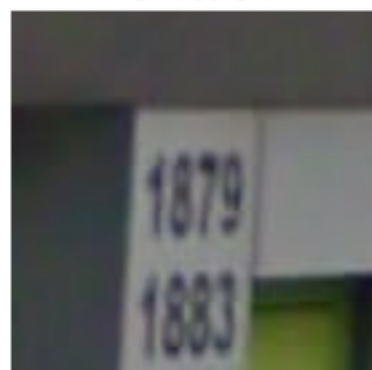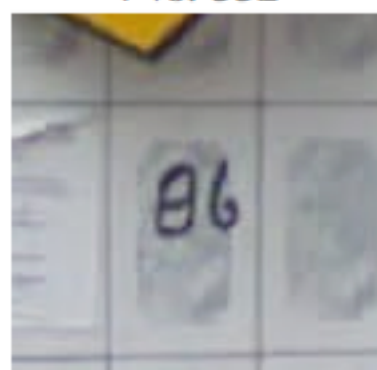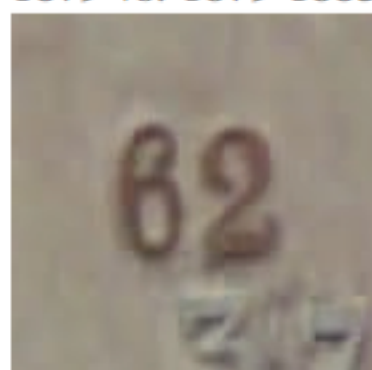|			
100 vs. 676	1110 vs. 2641	23 vs. 37	1 vs. 198
4 vs. 332	2 vs 239	1879 vs. 1879-1883	228 vs. 22B
96 vs. 86	1844 vs. 184	62 vs. 62-37	1180 vs. 1780
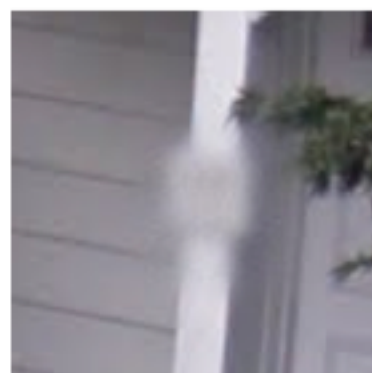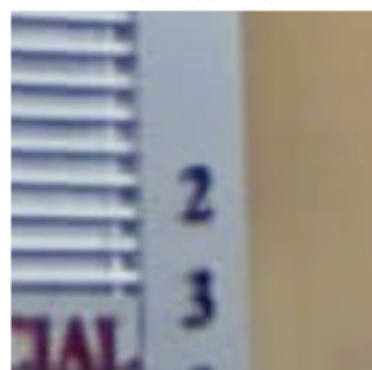
Figure 3: Examples of incorrectly transcribed street numbers from the large internal dataset

Figure 4: Examples of images from the hard CAPTCHA puzzles dataset.

Asirra

Asirra is a human interactive proof that asks users to identify photos of cats and dogs. It's powered by over **two million photos** from our unique partnership with Petfinder.com. Protect your web site with Asirra — free!

Please click on the images that show cats:

adopt me   adopt me   adopt me   adopt me

adopt me   adopt me   adopt me   adopt me

adopt me   adopt me   adopt me   adopt me

Score Test

http://www.google.com/

Q▾ Google

Google

Web   Images   Videos   Maps   News   Shopping   Gmail   more ▾

iGoogle | Search settings | Sign in

Google™

"crack captcha"

crack captcha php

Advanced Search
Language Tools

| Google Search | I'm Feeling Lucky |

Advertising Programs - Business Solutions - About Google

©2009 - Privacy

http://www.google.com/search?hl=en&source=hp&q=%22crack+captcha%22&aq=f&oq=&aqi=g1   Google

NY Times   Google News   Daily▾   Weather   294   United   Traffic   Papers   HN09   IMC   Google Maps   RSS (1)▾   Movies▾   BART▾   Wikis▾   Calories   Blog

"crack captcha" – Google Search

Web   Images   Videos   Maps   News   Shopping   Gmail   more ▼   Search settin

Google   "crack captcha"   Search   Advanced Search

Web   ⊞ Show options...   Results **1 - 10** of about **17,700** for "**crack** captcha". (0.17 seconds)

Captcha solving   Sponsored Link
www.decaptcher.com   Cheap captcha solving Cheap programs for advertisement

Using the advertisement in blogs, social networks, etc significantly increases the efficiency of the business. Many services use pictures called CAPTCHAs in order to prevent automated use of these services.

Solve CAPTCHAs with the help of this portal, increase your business efficiency now!

Follow these steps:
    Register   .
    Login and follow the link inside to load funds to your account.
    Your request will be processed ASAP.

You pay for correctly recognized CAPTCHAs only
The price is $2 for 1000 CAPTCHAs. We accept payments from $10.

If you use a third-party software the price could be different, contact the software vendor for more information.

Hi! I want to bypass captcha from my bots. Bots have different IPs. Is it possible to use your service from many IPs?
We have no restrictions about IP: with DeCaptcher you can bypass CAPTCHA from as many IPs as you need.

Hi. I need to crack captcha. Do you provide a captcha decoders?
DeCaptcher CAPTCHA solving is processed by humans. So the accuracy is much better than an automated captcha solver ones

Language	Example	AG	BC	BY	CB	DC	IT	All
English	one two three	51.1	37.6	4.76	40.6	39.0	62.0	39.2
Chinese (Simp.)	一 二 三	48.4	31.0	0.00	68.9	26.9	35.8	35.2
Chinese (Trad.)	一 二 三	52.9	24.4	0.00	63.8	30.2	33.0	34.1
Spanish	uno dos tres	1.81	13.8	0.00	2.90	7.78	56.8	13.9
Italian	uno due tre	3.65	8.45	0.00	4.65	5.44	57.1	13.2
Tagalog	isá dalawá tatló	0.00	5.79	0.00	0.00	7.84	57.2	11.8
Portuguese	um dois três	3.15	10.1	0.00	1.48	3.98	48.9	11.3
Russian	один два три	24.1	0.00	0.00	11.4	0.55	16.5	8.76
Tamil	ஒன்று இரண்டு மூன்று	2.26	21.1	3.26	0.74	12.1	5.36	7.47
Dutch	een twee drie	4.09	1.36	0.00	0.00	1.22	31.1	6.30
Hindi	एक दो तीन	10.5	5.38	2.47	1.52	6.30	9.49	5.94
German	eins zwei drei	3.62	0.72	0.00	1.46	0.58	29.1	5.91
Malay	satu dua tiga	0.00	1.42	0.00	0.00	0.55	29.4	5.23
Vietnamese	một hai ba	0.46	2.07	0.00	0.00	1.74	18.1	3.72
Korean	일 이 삼	0.00	0.00	0.00	0.00	0.00	20.2	3.37
Greek	ένα δύο τρία	0.45	0.00	0.00	0.00	0.00	15.5	2.65
Arabic	ثلاثة اثنين واحد	0.00	0.00	0.00	0.00	0.00	15.3	2.56
Bengali	এক দুই তিন	0.45	0.00	9.89	0.00	0.00	0.00	1.72
Kannada	ಒಂದು ಎರಡು ಮೂರು	0.91	0.00	0.00	0.00	0.55	6.14	1.26
Klingon	✓ ‹ ‹	0.00	0.00	0.00	0.00	0.00	1.12	0.19
Farsi	سه دو یک	0.45	0.00	0.00	0.00	0.00	0.00	0.08

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.