The Underground Economy

CS 161: Computer Security
Prof. Vern Paxson

TAs: Devdatta Akhawe, Mobin Javed & Matthias Vallentin

http://inst.eecs.berkeley.edu/~cs161/

April 26, 2011
Announcements

• Matthias back on May 5
  – Send him email for office hour appointments

• Reminder: Final exam in F295 Haas
  – (not Haas Pavilion!)
  – IEEE will provide breakfast munchies

• Course Summary/Review lecture on Thurs
  – TLS, certs, crypto requested by several
  – Possible other topics: DNSSEC, XSS/CSRF
  – … ?
Termed **Bullet-proof hosting**

**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 website 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.
**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!

<table>
<thead>
<tr>
<th>MINI PLAN</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume disc</td>
<td>400 MB</td>
</tr>
<tr>
<td>Domains</td>
<td>1</td>
</tr>
<tr>
<td>Traffic *</td>
<td>Unlimited</td>
</tr>
<tr>
<td>FTP-access</td>
<td>there is</td>
</tr>
<tr>
<td>MySQL database</td>
<td>there is</td>
</tr>
<tr>
<td>Control panel</td>
<td>there is</td>
</tr>
<tr>
<td>COST</td>
<td>4 000 rub. / 1 month.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STARTER PLAN</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume disc</td>
<td>500 mb</td>
</tr>
<tr>
<td>Domains</td>
<td>3</td>
</tr>
<tr>
<td>Traffic *</td>
<td>Unlimited</td>
</tr>
<tr>
<td>FTP-access</td>
<td>there is</td>
</tr>
<tr>
<td>MySQL database</td>
<td>there is</td>
</tr>
<tr>
<td>Control panel</td>
<td>there is</td>
</tr>
<tr>
<td>COST</td>
<td>5 000 rub. / 1 month.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS PLAN</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume disc</td>
<td>1000 mb</td>
</tr>
<tr>
<td>Domains</td>
<td>7</td>
</tr>
<tr>
<td>Traffic *</td>
<td>Unlimited</td>
</tr>
<tr>
<td>FTP-access</td>
<td>there is</td>
</tr>
<tr>
<td>MySQL database</td>
<td>there is</td>
</tr>
<tr>
<td>Control panel</td>
<td>there is</td>
</tr>
<tr>
<td>COST</td>
<td>7 000 rub. / 1 month.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PREMIUM PLAN</th>
<th></th>
</tr>
</thead>
</table>
Fighting Bots / Botnets, con’t

• Approach #2: seize the domain name used for C&C
  – This is what’s currently often used, often to good effect …
• … Botmaster counter-measure?
  – Each day (say), bots generate a large list of possible domain names using a Domain Generation Algorithm
    • Large = 50K, in some cases
  – Bots then try a random subset looking for a C&C server
    • Server signs its replies, so bot can’t be duped
    • Attacker just needs to hang on to a small portion of names to retain control over botnet
• This is becoming state-of-the-art … (not yet widely used)
• Counter-counter measure?
  – Behavioral signature: look for hosts that make a lot of failed DNS lookups (research)
The Problem of Botnets

• Constitute the *Great Modern Threat* of Internet security: *Generic Platform For Badness*

• Why botnets rather than worms?
  – Greater control
  – Less emergent
  – Quieter
  – Optimal flexibility

• Why the shift towards valuing these instead of seismic worm infection events?
  $$ \textit{Profit} $$

• How can attackers monetize botnets?
Monetizing Botnets

• General malware monetization approaches:
  – Keylogging: steal financial/email/social network accounts
  – Ransomware
  – *Transaction generators*
    • Malware watches user’s surfing …
    • … waits for them to log into banking site (say) …
    • … and then injects *additional* banking transactions like “send $50,000 to Nigeria” …
    • … and alters web server replies to *mask the change in the user’s balance*
Monetizing Botnets, con’t

• Monetization that leverages scale
  – DDoS (extortion)
  – Spam
  – *Click fraud*
  – Scam *infrastructure*
    • Hosting web pages (e.g., phishing)
    • Redirection to evade blacklisting/*takedown* (DNS)

• Which of these cause serious pain for infected user?
  – *None*. Users have *little incentive* to prevent (*⇒* externality)
How FBI, police busted massive botnet
12m zombie machines run by 3 admins

By John Leyden

Posted in Malware, 3rd March 2010 15:56 GMT

Analysis More details have emerged about a cybercrime investigation that led to the takedown of a botnet containing 12m zombie PCs and the arrest of three alleged kingpins who built and ran it.

As previously reported, the Mariposa botnet was principally geared towards stealing online login credentials for banks, email services and the like from compromised Windows PCs. The malware infected an estimated 12.7 million computers in more than 190 countries.

The Mariposa Working Group infiltrated the command-and-control structure of Mariposa to monitor the communication channels that relayed information from compromised systems back to the hackers who run the botnet. Analysis of the command system laid the groundwork for the December 2009 shutdown of the botnet, as well as shedding light on how the malware operated and provided a snapshot of the current state of the underground economy.
The botmasters made money by selling parts of the botnet to other cybergangs,

Netkairo finally regained control of Mariposa and launched a denial of service attack against Defence Intelligence using all the bots in his control. This attack seriously impacted an ISP, leaving numerous clients without an Internet connection for several hours, including several Canadian universities and government institutions.
Once again, the Mariposa Working Group managed to prevent the DDP Team from accessing Mariposa. We changed the DNS records, so the bots could not connect to the C&C servers and receive instructions, and at that moment we saw exactly how many bots were reporting. We were shocked to find that more than 12 million IP addresses were connecting and sending information to the C&C servers, making Mariposa one of the largest botnets in history.

alleged lieutenants “Ostiator” and “Johnyloleante” have been charged with cybercrime offences. More arrests are expected to follow.

Under Spanish law suspects are not named at this stage of proceedings. Pedro Bustamante, senior research advisor at Panda Security, said: “Our preliminary analysis indicates that the botmasters did not have advanced hacking skills.

"This is very alarming because it proves how sophisticated and effective malware distribution software has become, empowering relatively unskilled cyber criminals to inflict major damage and financial loss." ©
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
Список доступных аккаунтов

Сервис по продаже аккаунтов аукциона eBay.

Добрые юзеры аукциона 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 субъективно.

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$
allBots Inc.

Social Networking Bots

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

Winsock (Multi-threaded) Bots
Click here for 30+ MySpace Bots

Become an Affiliate and Start Earning Now

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

<table>
<thead>
<tr>
<th>Social Networks</th>
<th>Buy Now</th>
<th>$180.95-</th>
<th>$140.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySpace Accounts Creator with Picture Uploader, Profile &amp; Layout Manager</td>
<td>PayPal</td>
<td>$180.95-</td>
<td>$140.00</td>
</tr>
<tr>
<td>MySpace Accounts Creator (Winsock)</td>
<td>PayPal</td>
<td>$360.95-</td>
<td>$320.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Social Networks</th>
<th>Buy Now</th>
<th>$120.95-</th>
<th>$95.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>YouTube Accounts Creator</td>
<td>PayPal</td>
<td>$120.95-</td>
<td>$95.00</td>
</tr>
<tr>
<td>Friendster Accounts Creator</td>
<td>PayPal</td>
<td>$120.95-</td>
<td>$95.00</td>
</tr>
<tr>
<td>Hi5 Accounts Creator</td>
<td>PayPal</td>
<td>$120.95-</td>
<td>$95.00</td>
</tr>
<tr>
<td>TagWorld Accounts Creator</td>
<td>PayPal</td>
<td>$120.95-</td>
<td>$95.00</td>
</tr>
</tbody>
</table>

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
Marketplace Ads for Services

Percentage of Labeled Data

Cashier Available
Cashier Wanted
Confirm Available
DoS Available
Phisher Wanted
Confirm Wanted
Carder Wanted
Phisher Available
Carder Available
DoS Wanted

Ad Type (Services)
Marketplace Ads for Goods

Ad Type (Goods)

Percentage of Labeled Data
Marketplace Ads for Goods, con’t
The Underground Economy

• Why is its emergence significant?

• Markets enable efficiencies
  – *Specialization*: individuals rewarded for doing a single thing particularly well

• Lowers barrier-to-entry
  – Only need a single skill
  – Some underground market activities are legal

• Competition spurs innovation
  – Accelerates *arms race*
  – Defenders must assume a more pessimistic threat model

• Facilitates non-$ Internet attacks (political, nation-state)
  – Provides actors with cheap attack components
  – Provides stealthy actors with plausible cover
The Underground Economy, con’t

• What problems do underground markets face?

• Markets only provide major efficiencies if they facilitate deals between strangers
  – Susceptible to infiltration

• Depending on marketplace architecture, can present a target / single point of failure

• By definition, deals are between crooks
  – Major issue of betrayal by “rippers”
Pay-Per-Install (PPI)
Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

Контакты:
- 560869831
- 556055303
- info [at] installs4sale.net

Приемущества:
- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миры стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Договоритесь по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!
Goldinstall Rates for 1K Installs for each Country.

<table>
<thead>
<tr>
<th>Country</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTH</td>
<td>13$</td>
</tr>
<tr>
<td>US</td>
<td>150$</td>
</tr>
<tr>
<td>GB</td>
<td>110$</td>
</tr>
<tr>
<td>CA</td>
<td>110$</td>
</tr>
<tr>
<td>DE</td>
<td>30$</td>
</tr>
<tr>
<td>BE</td>
<td>20$</td>
</tr>
<tr>
<td>IT</td>
<td>65$</td>
</tr>
<tr>
<td>CH</td>
<td>20$</td>
</tr>
<tr>
<td>CZ</td>
<td>20$</td>
</tr>
<tr>
<td>DK</td>
<td>20$</td>
</tr>
<tr>
<td>ES</td>
<td>30$</td>
</tr>
<tr>
<td>AU</td>
<td>55$</td>
</tr>
<tr>
<td>FR</td>
<td>30$</td>
</tr>
<tr>
<td>NL</td>
<td>20$</td>
</tr>
<tr>
<td>NO</td>
<td>20$</td>
</tr>
<tr>
<td>PT</td>
<td>30$</td>
</tr>
<tr>
<td>LR</td>
<td>6$</td>
</tr>
</tbody>
</table>
The partnership program «Earning4u» is the easiest way to earn money. All you need to do to start working with us is register.

You will earn from $6 (Asia) to $180 (USA) per 1000 installs. You can view all prices in the «Rates» section.

Key Features

Thanks to an individual approach to each client when you work with our system you have:
- Online statistics updated in real time
- A 24-hour support service ready to answer all your questions
- Absolutely no shaving and total independence of your statistics from other system users
- Stable weekly payments on virtually all payment systems: Fethard, WebMoney, Wire, e-gold, Western Union (WU), MoneyGram, Anelik and ePassporte, and PayPal.
PAY PER INSTALL AFFILIATE PROGRAMS

Affiliate Program Newsletter Get new programs via email
Insert your Email Address: Subscribe

Best Pay-Per-Install affiliate program reviews. ActiveX affiliates.

Make money with these BEST AFFILIATE PROGRAMS

Best Pay-per-install affiliate programs on the net. Earn money with any traffic, these ActiveX affiliates will convert anything and make you rich. Payments are up to $1.50 per install. You usually distribute installation of toolbar and making cash. You can also make loads of money with content sites such as movies, games, mp3 and protect your content with Content Gateways which are paying most, to unlock the content user needs to install simple adaware application and than he can get content for free.

JOIN MAKE MONEY FORUM
Learn How to make money with PPN Gateway Free guide to teach you how to make $7000 per day

CLICK HERE TO VISIT OUR BEST SPONSOR.

WE WORK Even when you sleep!
One of the best PPI programs. Up to $180 per 1000 Installs.

Last 10 Reviews
- CPALead - November/13/2010
- SexSearch - October/31/2010
- LoudMo - October/28/2010
- SexSearch - October/19/2010
- SexSearch - October/18/2010
- ioXes - October/12/2010
- Earning4u - September/09/2010
- Earning4u - August/30/2010

Pages: [0] [1] [2] [3] [4]
Infiltration

[Diagram showing the infiltration process:

1. Clients receive fake AV and Spambot.
2. PPI Affiliate distributes the PPI Service.
3. Target Host is compromised.
4. Infiltration opportunity]

Downloader
Install
Payment
The majority of the world’s top malware appeared in PPI downloads.

Table 2: FireEye’s top 20 malware families observed in their MAX Cloud network on the April–June 2010 time
PPI distribution of malware during August 2010
Spam & Spam Profit
Modern Spam Operations

• To make the issues concrete, let’s take a tour of a modern “spambot”
  = Botnet primarily used for sending spam

• Goal is to get a sense of:
  – Botnet construction
  – Email spam-sending process
  – Arms-race issues

• Note: not comprehensive
  – E.g., there’s also blog spam, social network spam, etc.
Welcome to Storm!

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

Operated using "bulletproof hosting"
Spam “Campaign” Mechanics

Botmaster

HTTP proxies

HTTP

Proxy bots

TCP

Workers
Campaign Mechanics: Harvest

Botmaster

HTTP proxies

HTTP

Proxy bots

TCP

Workers
Campaign Mechanics: Spamming

- Botmaster
- HTTP proxies
- HTTP
- Proxy bots
- TCP
- Workers
Synthetic diversity aims to thwart content-based anti-spam filtering.

Figure 2: Snippet of a spam template, showing the transformation of an email header from template (top) to resulting content (bottom). The \texttt{\textbackslash b}-symbol indicates line continuations. Bold text corresponds to the formatting macros and their evaluation.
<table>
<thead>
<tr>
<th>MACRO</th>
<th>SEEN LIVE</th>
<th>FUNCTIONALITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0)</td>
<td>✓</td>
<td>Spam target email address.</td>
</tr>
<tr>
<td>(A)</td>
<td>✓</td>
<td>FQDN of sending bot, as reported to the bot as part of the preceding C&amp;C exchange.</td>
</tr>
<tr>
<td>(B)</td>
<td></td>
<td>Creates content-boundary strings for multi-part messages.</td>
</tr>
<tr>
<td>(Cnum)</td>
<td>✓</td>
<td>Labels a field’s resulting content, so it can be used elsewhere through (V); see below.</td>
</tr>
<tr>
<td>(D)</td>
<td>✓</td>
<td>Date and time, formatted per RFC 2822.</td>
</tr>
<tr>
<td>(E)</td>
<td></td>
<td>ROT-3–encodes the target email address.</td>
</tr>
<tr>
<td>(Fstring)</td>
<td>✓</td>
<td>Random value from the dictionary named string.$^2$</td>
</tr>
<tr>
<td>(Gstring)</td>
<td>✓</td>
<td>Line-wrap string into 72 characters per line.</td>
</tr>
<tr>
<td>(Hstring)</td>
<td></td>
<td>Defines hidden text snippets with substitutions, for use in HTML- and plain-text parts.</td>
</tr>
<tr>
<td>(I)</td>
<td>✓</td>
<td>Random number between 1 and 255, used to generate fake IP addresses.</td>
</tr>
<tr>
<td>(Istring)</td>
<td></td>
<td>Produces quoted-printable “=” linewrapping.</td>
</tr>
<tr>
<td>(K)</td>
<td></td>
<td>IP address of SMTP client.</td>
</tr>
<tr>
<td>(M)</td>
<td>✓</td>
<td>6-character string compatible with Exim’s message identifiers (keyed on time).</td>
</tr>
<tr>
<td>(N)</td>
<td></td>
<td>16-bit prefix of SMTP client’s IP address.</td>
</tr>
<tr>
<td>(Ostring;num)</td>
<td>✓</td>
<td>Randomized message identifier element compatible with Microsoft SMTPSVC.</td>
</tr>
<tr>
<td>(Pnum$_1$[-num$_2$];string)</td>
<td>✓</td>
<td>Random string of num$_1$ (up to num$_2$, if provided) characters taken from string.</td>
</tr>
<tr>
<td>(Qstring)</td>
<td></td>
<td>Quoted-printable “=” linewrapping.</td>
</tr>
<tr>
<td>(Rnum$_1$–num$_2$)</td>
<td>✓</td>
<td>Random number between num$_1$ and num$_2$. Note, special-cased when used with (D).</td>
</tr>
<tr>
<td>(Ustring)</td>
<td></td>
<td>Randomized percent-encoding of string.</td>
</tr>
<tr>
<td>(Vnum)</td>
<td>✓</td>
<td>Inserts the value of the field identified by (Cnum).</td>
</tr>
<tr>
<td>(W)</td>
<td></td>
<td>Time and date as plain numbers, e.g. “20080225190434”.</td>
</tr>
<tr>
<td>(X)</td>
<td></td>
<td>Previously selected member of the “names” dictionary.</td>
</tr>
<tr>
<td>(Ynum)</td>
<td>✓</td>
<td>8-character alphanumeric string, compatible with Sendmail message identifiers.</td>
</tr>
<tr>
<td>(Z)</td>
<td>✓</td>
<td>Another Sendmail-compatible generator for message identifiers.</td>
</tr>
</tbody>
</table>

Table 2: Storm’s spam-generation templating language.
Campaign Mechanics: Spamming

- Botmaster
- HTTP proxies
- HTTP
- Proxy bots
- TCP

Campaign Mechanics: Spamming

- Botmaster
- HTTP proxies
- HTTP
- Proxy bots
- TCP
Campaign Mechanics: Reporting

Botmaster

HTTP proxies

HTTP

Proxy bots

TCP

SPAM
Welcome to Storm! What can we sell you?
Anatomy of a modern Pharma spam campaign

Spammer

Paid commission

Spam emails

Bulk email sender

Open proxies/botnet

Other recipients

Email with link

Impotent? Curious?

Clicks on link

Email recipient

redirects

Affiliate program

Commission (up to 40%)

Viagra/affordable pharmacy site

Sale made

Typical value $50-100?

Shipped to customer

VGR100

Generic pills (Sildenafil citrate)

Non-US supply (India, Mexico etc.)
Patent expired
Mere cents per pill = massive markup

Diagram by Stuart Brown
moderntimeisrubbish.co.uk
Life As A Spammer …

• From a research study where we infiltrated Storm and measured its use for spamming:
  – Modern spam campaigns can send 10s of billions of spams using mailing lists of 100s of millions of addresses
  – 3/4 to 5/6 of all spam delivery attempts fail before the message is even sent to the receiver’s server …
    • … due to heavy & effective use of black-listing
  – It takes around 20,000 “postcard” spams to get one person to visit the postcard site
    • 1 in 10 of the visitors will click to download the postcard
  – It takes around 12,000,000 Viagra spams to get one person to visit the site and make a purchase (~$100)
  – Even given those low rates, huge volume ⇒ profitable