The Business of Cybercrime

Luis Corrons
PandaLabs Technical Director
The Business of Cybercrime

Agenda

1. Malware figures
2. Who is behind this?
3. Web Attack Toolkits
4. A Real Case
5. Underground Shopping Cart
6. Where to buy?
Malware figures
Malware evolution

Malware detected per year

Source: PandaLabs
Malware evolution by type

New malware by type in 2007

- Trojans: 75%
- Spyware / Adware: 14%
- Worms: 10%
- Rest: 1%

Source: PandaLabs
Malware evolution by type

Source: PandaLabs
Who is behind this?
Yesterday’s Bad Guys

Blaster.B

Nestky / Sasser

CIH

29-A

Jeffrey Lee Parson

Sven Jaschan

Chen Ing-Hau

Benny
The Business of Cybercrime

Today’s Bad Guys

Spam

Phishing

Spam

James Ancheta

Andrew Schwarmkoff

Jeremy Jaynes
Web Attack Toolkits
Web Attack Toolkits

Malware server

Payment methods: VISA, Mastercard, American Express

Targeted websites: YouTube, News, Media

Malicious servers: HTTPS, HTTPS, HTTPS
**MPack**

**Secure your computer from viruses**

**Crippling malware attack strikes in Italy**

Researchers claim hundreds of sites compromised

Shaun Nichols in California, vnunet.com 10 Jun 2007

Italy is suffering from a barrage of remote attacks launched from hundreds of compromised websites, security experts have warned.

Researchers at Symantec reported that attackers have injected 'iframe' tags within the HTML files on compromised sites.

**Wednesday, June 20, 2007**

**Massive Embedded Web Attack in Italy**

The Web is abuzz with news stories regarding the MPACK web exploitation kit installed on over 10,000 mostly Italian based sites, and in the spirit of previous analyses of malicious URLs here’s an overview of the strategy of the attack, the outcome, and IPs in question, thus the ones that should get blacklisted or CYBERINT applied for further juicy details on the severity of the attack.

The strategy of the attack

Picture yourself in the position of a malicious

...
**MPack**

- Tracking Mpack for 2 months (April & May 2007):
  - 41 different servers with Mpack running
  - 366,717 web pages “iframed”
  - More than 1 million users infected (1,217,741)
## MPack v0.90 stats

### Attacked hosts (total - uniq)

<table>
<thead>
<tr>
<th>Host</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE XP ALL</td>
<td>114721</td>
</tr>
<tr>
<td>QuickTime</td>
<td>2175</td>
</tr>
<tr>
<td>Win2000</td>
<td>7033</td>
</tr>
<tr>
<td>Firefox</td>
<td>12885</td>
</tr>
<tr>
<td>Opera7</td>
<td>1271</td>
</tr>
</tbody>
</table>

### Traffic (total - uniq)

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total traffic</td>
<td>159073</td>
</tr>
<tr>
<td>Exploited</td>
<td>44804</td>
</tr>
<tr>
<td>Loads count</td>
<td>17408</td>
</tr>
<tr>
<td>Loader's response</td>
<td>38.85%</td>
</tr>
</tbody>
</table>

### Efficiency

Efficiency: 10.94% - 12.37%

### Browser stats (total)

<table>
<thead>
<tr>
<th>Browser</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSIE</td>
<td>4</td>
<td>0%</td>
</tr>
<tr>
<td>Opera</td>
<td>1</td>
<td>0%</td>
</tr>
</tbody>
</table>

### Modules state

- **Statistic type**: MySQL-based
- **User blocking**: ON
- **Country blocking**: OFF

### Country stats

<table>
<thead>
<tr>
<th>Country</th>
<th>Traff</th>
<th>Loads</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>RU - Russian federation</td>
<td>112793</td>
<td>12653</td>
<td>11.22%</td>
</tr>
<tr>
<td>UA - Ukraine</td>
<td>16666</td>
<td>1670</td>
<td>10.02%</td>
</tr>
<tr>
<td>IT - Italy</td>
<td>7045</td>
<td>593</td>
<td>8.42%</td>
</tr>
<tr>
<td>GE - Georgia</td>
<td>5775</td>
<td>673</td>
<td>11.65%</td>
</tr>
<tr>
<td>BY - Belarus</td>
<td>5419</td>
<td>657</td>
<td>12.12%</td>
</tr>
<tr>
<td>KZ - Kazakstan</td>
<td>3098</td>
<td>376</td>
<td>12.14%</td>
</tr>
<tr>
<td>US - United states</td>
<td>1117</td>
<td>50</td>
<td>4.48%</td>
</tr>
<tr>
<td>AZ - Azerbaijan</td>
<td>1060</td>
<td>128</td>
<td>12.08%</td>
</tr>
<tr>
<td>MD - Moldova, republic of</td>
<td>683</td>
<td>101</td>
<td>14.70%</td>
</tr>
</tbody>
</table>
IcePack

Login
IcePack
**IcePack**

**Operating System**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>% of Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>266</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>190</td>
</tr>
<tr>
<td>Windows 2010</td>
<td>182</td>
</tr>
<tr>
<td>Other</td>
<td>74</td>
</tr>
<tr>
<td>Windows 2013</td>
<td>63</td>
</tr>
<tr>
<td>Windows 7</td>
<td>43</td>
</tr>
<tr>
<td>Mac OS</td>
<td>23</td>
</tr>
<tr>
<td>Linux</td>
<td>26</td>
</tr>
<tr>
<td>Windows 95</td>
<td>2</td>
</tr>
<tr>
<td>Windows NT 4</td>
<td>1</td>
</tr>
</tbody>
</table>

*2017 NIST report*
### IcePack

#### Browser

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
<th>Malware Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 4.0</td>
<td>2000</td>
<td></td>
</tr>
<tr>
<td>Internet Explorer 7.0</td>
<td>578</td>
<td></td>
</tr>
<tr>
<td>Firefox 3.0</td>
<td>435</td>
<td></td>
</tr>
<tr>
<td>Opera 9.23</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>Mozilla 5.0</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>Opera 9.19</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>Opera 9.21</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>Opera 9.20</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>Opera 9.02</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>Mozilla 4.0</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>Firefox 1.5.8</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>Opera 9.08</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Opera 9.07</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Opera 8.59</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>Opera 9.01</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Internet Explorer 5.5</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Internet Explorer 5.01</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Firefox 2.0</td>
<td>13</td>
<td></td>
</tr>
</tbody>
</table>
The Business of Cybercrime

**IcePack**

<table>
<thead>
<tr>
<th>Language</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanish</td>
<td>5</td>
</tr>
<tr>
<td>English</td>
<td>5</td>
</tr>
<tr>
<td>British</td>
<td>2</td>
</tr>
</tbody>
</table>

This table shows the distribution of languages used in IcePack-related activities. The percentages indicate the majority language for each category.
**IcePack**

**Referrers**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Value</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ware.com</td>
<td>9</td>
<td>75%</td>
</tr>
<tr>
<td>net.com</td>
<td>2</td>
<td>16%</td>
</tr>
<tr>
<td>index.php</td>
<td>1</td>
<td>0%</td>
</tr>
</tbody>
</table>

**FTP import**

**FTP checker**
The Business of Cybercrime

**IcePack**

**iFramer**

**Country blocking**
The Business of Cybercrime

FirePack

Table of browser statistics:
- Browser 1:下载次数:0, 通过次数:0, 成功率:0%
- Browser 2:下载次数:0, 通过次数:0, 成功率:0%
- Browser 3:下载次数:0, 通过次数:0, 成功率:0%

Table of operating system statistics:
Traffic Pro

The Business of Cybercrime
# The Business of Cybercrime

## Neosploit

### Total Stats

<table>
<thead>
<tr>
<th>Username</th>
<th>Traffic</th>
<th>Redirect</th>
<th>Total</th>
<th>Loads</th>
<th>Total</th>
<th>Loader hits</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active users</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user1</td>
<td>15483</td>
<td>3686</td>
<td>215</td>
<td>4417</td>
<td>23806</td>
<td>1778 (11.483%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td></td>
<td>610</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>610</td>
<td>7 (2.034%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>10 (10.191%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td></td>
<td>593</td>
<td>1394</td>
<td>134</td>
<td>1199</td>
<td>6669</td>
<td>520 (13.201%)</td>
<td>78 (5.595%)</td>
</tr>
<tr>
<td></td>
<td>1256</td>
<td>110</td>
<td>4</td>
<td>1099</td>
<td>4832</td>
<td>377 (15.366%)</td>
<td>62 (4.336%)</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td><strong>Passive users</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>
The Business of Cybercrime

And many more…

- E-corepack
- Nuclear traffic
- Multi exploits pack
- Nuclear Malware Kit
- Prime Exploit System
- Web-Attacker
- SmartPack
A Real Case
The Business of Cybercrime
The Business of Cybercrime

Infected Team

- **Proxy**
  - 5 - $2.5
  - 1,000 - $300

- **DDoS**
  - 1 hour - $20
  - 24 hours - $100
  - Major projects starting at $200
  - 10 minutes for free!
Infected Team

- Spam: < 192,000,000 e-mail addresses

- USA (home users) – 117,000,000
  - US$150 / million messages
- USA (enterprises) – 4,000,000
  - US$150 / million messages
- Western Europe (home users) – 45,000,000
  - US$130 / million messages
- Western Europe (enterprises) – 902,256
  - US$130 / million messages
- Russia (home users) – 20,700,000
  - US$100 / million messages
- Russia (enterprises) – 5,000,000
  - US$120 / million messages
The Business of Cybercrime

Infected Team

- Personal cryptor ($15, updates $5)
- ABLoader ($60, builder $500)
- RooT iFrame ($25 Russian, $50 English)
- SpamPHP Script ($2)
- FTPCheckIframe ($25)
The Business of Cybercrime

Infected Team

MPack
Dream Downloader
Limbo

Total Investment:
1,500$
Infected Team

The Business of Cybercrime
Infected Team
### Infected Team

#### Command Log

<table>
<thead>
<tr>
<th>USFRID</th>
<th>IP</th>
<th>COUNTRY</th>
<th>COMMAND</th>
<th>PARAMS</th>
<th>TIME</th>
<th>STATUS INV</th>
</tr>
</thead>
<tbody>
<tr>
<td>68001</td>
<td>09122006_133409</td>
<td>BR</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68002</td>
<td>16122006_232056</td>
<td>CO</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68003</td>
<td>13122006_190851</td>
<td>BR</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68004</td>
<td>09122006_190113</td>
<td>BR</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68005</td>
<td>06102006_235052</td>
<td>CZ</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68006</td>
<td>12122006_110213</td>
<td>--</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68007</td>
<td>17122006_173406</td>
<td>AR</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-13 07:59:55</td>
<td>1</td>
</tr>
<tr>
<td>68008</td>
<td>16122006_115609</td>
<td>US</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68009</td>
<td>15122006_112727</td>
<td>JP</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68010</td>
<td>14122006_204558</td>
<td>US</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-13 02:22:02</td>
<td>2</td>
</tr>
<tr>
<td>68011</td>
<td>16122006_224721</td>
<td>--</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68012</td>
<td>16122006_213950</td>
<td>PH</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68013</td>
<td>17122006_072205</td>
<td>US</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:43</td>
<td>0</td>
</tr>
<tr>
<td>68014</td>
<td>11122006_065005</td>
<td>US</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:42</td>
<td>0</td>
</tr>
<tr>
<td>68015</td>
<td>16122006_154842</td>
<td>--</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:42</td>
<td>0</td>
</tr>
<tr>
<td>68016</td>
<td>17122006_134950</td>
<td>US</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:42</td>
<td>0</td>
</tr>
<tr>
<td>68017</td>
<td>16052006_214929</td>
<td>--</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:42</td>
<td>0</td>
</tr>
<tr>
<td>68018</td>
<td>17122006_101726</td>
<td>--</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:42</td>
<td>0</td>
</tr>
<tr>
<td>68019</td>
<td>12122006_173342</td>
<td>CO</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:42</td>
<td>0</td>
</tr>
<tr>
<td>68020</td>
<td>09122006_040213</td>
<td>CL</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 23:45:20</td>
<td>1</td>
</tr>
<tr>
<td>68021</td>
<td>08122006_021173</td>
<td>--</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 20:51:42</td>
<td>0</td>
</tr>
<tr>
<td>68022</td>
<td>15122006_234931</td>
<td>BR</td>
<td>RUN</td>
<td>http</td>
<td>2007-03-12 01:48:02</td>
<td>0</td>
</tr>
</tbody>
</table>
Infected Team

Win32.exe = Trojan downloader

Installed:
Spammer Trojan
Rogue AntiSpyware
The Business of Cybercrime

Infected Team

Rogue AntiSpyware

Commissions paid per installation:

- $0.40 USA, Canada
- $0.20 UK, France, Germany, Italy, Spain, Belgium, Luxembourg, Monaco
- $0.05 Austria, Denmark, Finland, Sweden, Norway, The Netherlands
- $0.01 China, Korea, Japan
The Business of Cybercrime

Infected Team

Let’s do some maths

China, Korea, Japan: $0.01 \times 70,300 = $703
Finland, Norway…: $0.05 \times 70,300 = $3,515
UK, France…: $0.20 \times 70,300 = $14,060
USA, Canada: $0.40 \times 70,300 = $28,120

And the same numbers in 30 days...

China, Korea, Japan: $0.01 \times 70,300 \times 30 = $21,090
Finland, Norway…: $0.05 \times 70,300 \times 30 = $105,450
UK, France…: $0.20 \times 70,300 \times 30 = $421,800
USA, Canada: $0.40 \times 70,300 \times 30 = $843,600
Infected Team

Who’s paying these Rogue AntiSpyware installations?
The Business of Cybercrime

WaveRevenue: the best performing program to boost your revenue

WaveRevenue is an affiliate Toolbar that pays you each time a surfer installs our Toolbar on his computer.

Let WaveRevenue turn your traffic into cash!

Free content

Get free content and get paid! Put our free quality content:
* Adult videos
* Funny movies
* Animated smiley

And get paid for it! Our content is constantly updated to keep your visitors happy.

Encoding tool

Upload and bundle your own content in one click!
Games, movies, applications, everything is possible with our unique online encoding tool.

Active X

Active X Content Protection
Protect specific sections, pages or your entire website.
With our high converting Active X

Get started now and Quit your 9-5 Rat Race. Let WaveRevenue work for your
Money, Quality Product and Real Money.
Welcome To TopInstalls

TopInstalls provides dynamic bundling and distribution services to dozens of third-party applications to end users worldwide. With TopInstalls, companies can experience extremely fast growth, almost overnight, and create a strong and lasting web presence — something that normally takes months or years and hundreds of thousands of dollars.

Contact us to know how we can help increase your distribution and reach.
The Business of Cybercrime
The BUSINESS of Cybercrime

The DAYS when you had to work hard for your money are over.
This is the way to enjoy life again.
Get started now and Quit your 9-5 Rat Race.
Let MatCash work for your Money.
Quality Product and Real Money.
1. We pay you for every install $0.40 per install!
2. A unique way to change your sites appearance

SIGN UP NOW!
The Business of Cybercrime

Июнь 20/07
 Если вы думаете начать попробовать в плане количества, вы пугаетесь в виду
предъявления 22 часов

Июнь 05/07
 Если накопленные дозы
этого и прочих проблем,
запуск снова заработал в
штатном режиме, со дня на
день уменьшается прогона,
так что за последние годы
в картинку и скорость
загрузки и такие вещи.

Май 06/07
 Если вам надо начать
загрузка нейтральной
скорости загрузки, пишите в
сообщение, сделаем больше.

Общие положения, правила и FAQ:

- Все загрузки чистые т.е. параллельно ничего не грузится.
- Загрузки производятся разом с сервером, который сносится после успешного запуска
вашей задачи.
- В "кись" не присоединяют страны, на которые указаны нерабочие страны.
- Загружаются только те страны, которые указаны в задаче.
- "Страна" определяется по инструкциях.
- Если указано "ALL" грузятся все страны и цена загрузки расценивается отдельно по каждой стране.
- За загрузку вы платите 0.2$ за РЕ и 0.03
- Цена на загрузки могут иногда незначительно зависеть за этим следите сами.
- Как такового понятия "кись" не существует, у каждой страны свои цены и если страна меньше
не указана в глобал то цена 30$/1к
- Деньги снимаются со счета по факту скачки и загрузки ако на машине измерена.
- При оставке на холоде $5 и меньше загрузки останавливаются.
- Минимум нет, но можно грузить хоть 3шт хоть 10к указав лимит в задаче.
- Для начала крайне рекомендуется протестировать свой файл 30-100 раз для проверки оттока.
- Претензия по УЖЕ сделанной загрузке не принимаются, грузите новый вариант или сделайте
тест чтобы проверить качество.
- После создания задачи ее надо активировать нажатием на ссылку в поле статуса, аналогичные
методы задачу можно просматривать.
- После задачи "получилось" показывает сколько ботов счила задачу, обычно оно немного больше
поскольку "получилось" значит всего 1-3 бота, некоторые боты могут не закончить задачу.

Go
The Business of Cybercrime

SNAPINSTALLS
MAKING PAY-PER-INSTALL REVENUE A SNAP!

INCREASE REVENUE TO YOUR SITE IN A SNAP!
Simply SIGN UP, place our FREE CONTENT on your site, and start getting paid the highest pay-per-install on the planet!

Highest & Fastest Payouts in the World!
Did you know that most pay-per-install programs only pay for countries they want to? SnapInstalls pays for every major country in the world! We believe in paying the highest and realistic rate we can offer to our PARTNERS over the long-term. Depending on whether you're a software-developer, or web-master or a distributor, SnapInstalls believes in counting accurately and paying on time every pay period. Did you also know that other programs promote being the highest paying companies in the market, but when it comes to their reporting and getting paid, they cut back on the total amount of installs; so they don't have to pay you for what you delivered!!! Therefore, not only are they relying on faulty advertising, they are also reducing their actual payout by increasing the discrepancy between what you delivered and what they are counting. BUT NOT HERE AT SNAPINSTALL - WE BELIEVE IN PAYING YOU FOR EXACTLY WHAT YOU DELIVERED!

Sign Up Now!

Quality Content - Great Alternative to Traditional Advertising Media
SnapInstalls believes in high quality content, and is constantly rotating and adding new offers into the system. We stay current with market trends and needs and do our very best to make sure this FREE content is available to you and your website audience. Your audience or user-base will be extremely satisfied when have the ability to choose between search products, games, screensavers, new widgets - the list continues to grow and go on and on...
SnapInstall easily allows you to offer an alternative advertising media to your

Pricing Rates
SnapInstall Payouts

<table>
<thead>
<tr>
<th>Region</th>
<th>Payout</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>$0.30</td>
</tr>
<tr>
<td>Canada &amp; United Kingdom</td>
<td>$0.10</td>
</tr>
<tr>
<td>International</td>
<td>$0.05</td>
</tr>
</tbody>
</table>

Sign Up Now!
The Business of Cybercrime
The Business of Cybercrime

Hello! The ability to earn on the internet is a dream of many. We live in the 21st century, and many have computers connected to the internet and the desire to earn money on the internet! We offer you the opportunity, and working with us you will get:

1. Very good exploit that is not "kill" the traffic and you can freely him posted on their sites.
2. The statistics in real time!
3. We pay for the unique downloading.
4. Rapid service, which are located in different Data-Centra. The possible loss of traffic:
5. Since we can work any Webmaster-infection as a cause, and newcomer.
6. By advertisement we give FREE abusing scalability hosting + expander and dorogenerator!
7. We employ "TrafficExpander" - that is, unique traffic you can send where you please.
8. Very friendly support to respond to you in any matter of interest to you and help you understand if something is not working.
9. By paying a convenient way for you: E-passports, Web Money, Othercard, Gold, Western Union, bank transfer. To pay by bank transfer andWestern Union minimum payment of $ 1,000, the other $ 100.
10. We load absolutely innocent soft!

If you do not find the information that interests you, on the site, you can contact our customer support.

Our Support: 380-766-762 ICO - iframebiz.com
Traffic-Converter.biz - is the best tool over the entire Web to convert your traffic into cash! Our price policy allows you to get the maximal profit by selling your traffic. Unique tariffing algorithm determines the maximum price of your traffic accordingly to its quality. You can send any amount of traffic since we do not have the maximum and minimum restrictions. All payments to you will be processed at proper time. Our scripts are 100% accurate that provides you with exact stats. Bi-weekly payments to WM or Fethard.

Registration closed, please contact support for details.
ICQ:452033813
TRAFFIC STRATEGIES
Learn how to maximize your Revenues by getting the highest converting traffic!
The Business of Cybercrime
Underground Shopping Cart
Underground Shopping Cart

– Web Attack Toolkits

• MPack
  – US$700
  – DreamDownloader + US$300
  – Adding new exploit + US$50-150
  – Avoid AV detection + US$20-30

• IcePack
  – Lite: US$30
  – Platinum: US$400

• FirePack
  – US$3,000

• Traffic Pro
  – US$40

• Ecore
  – Bundle US$590 (for a domain / ip with ecore installed).
  – Domain / additional ip US$490
  – Help for the installation US$15
Underground Shopping Cart

– Malware

• Keylogger Teller 2.0
  – Typical keylogger; it uses stealth techniques and is quite complete: US$40

• Webmoney Trojan
  – It captures Webmoney accounts: US$500 (the first 100 will obtain it for US$400!)

• WMT-spy:
  – Another Trojan to obtain WebMoney accounts, but cheaper than the previous one
  – Trojan  US$5
  – Updates  US$5
  – Builder  US$10

• SNATCH TROJAN:
  – It steals passwords and has rootkit functionalities:  US$600

• Limbo:
  – Banking Trojan, keylogger, etc.  US$1,000

• Pinch:
  – Very complete Trojan.  US$30
  – Update:  US$5
Underground Shopping Cart

- Joiner and encryption

  - **Polaris**
    - Polymorphic encryption for your executables  US$20

  - **Freejoiner**
    - Hides your executables joining them with other files  US$30 + US$5 per update

  - **My joiner**
    - Other joiner belonging to the creator of Pinch  US$10

  - **Pity Joiner**
    - Just another joiner  US$7
Underground Shopping Cart

– Other Tools

• FTP checker
  – Program to validate stolen FTP accounts. US$15

• Dream Bot Builder
  – Floods servers US$500 + US$25 per update
Underground Shopping Cart

- Spam

  - Spam Hosting: $200
  - Dedicated spam server: $500
  - +10,000,000 Mails per day: $600
  - SMS spam (per message): $0.2
  - ICQ (1,000,000): $150

Mailing lists for spam: (US$)

<table>
<thead>
<tr>
<th>ACCOUNTS</th>
<th>USA</th>
<th>GERMANY</th>
<th>RUSSIA</th>
<th>UKRANIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000,000</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>3,000,000</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>5,000,000</td>
<td>300</td>
<td>300</td>
<td>300</td>
<td>-</td>
</tr>
<tr>
<td>8,000,000</td>
<td>500</td>
<td>500</td>
<td>500</td>
<td>-</td>
</tr>
<tr>
<td>16,000,000</td>
<td>900</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>32,000,000</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Underground Shopping Cart

– Accounts

• FTP accounts:
  – US$1 per account

• ICQ numbers:
  – From US$1 to US$10 (depending on the ICQ number)

• RapidShare premium accounts:
  – 1 month - US$5
  – 2 months - US$8
  – 3 months - US$12
  – 6 months - US$18
  – 1 year - US$28

• Online Shop accounts
  – (megashop.ru, bolero.ru, cup.ru, etc. ALL RUSSIAN) - US$50 each

• 50MB of Limbo Trojan logs
  – US$30 (contains email accounts, bank account numbers, credit card numbers, etc. A percentage is guaranteed)
Underground Shopping Cart

– Already finished?

• Credit Cards
  – VISA / MASTERCARD
    1 - 10 cards  US$2 (per card)
    10 - 100 cards  US$1.5 (per card)
  – AMEX
    1 - 10 cards  US$2.5 (per card)
    10 - 100 cards  US$2 (per card)

• Passports:
  – Black and white:  US$2
  – Color:  US$5
Where to buy?
- отображение размера логов
- поиск по логам
- архивация логов
- фильтрация по стране
- возможность посылки логов на email
- статистику по заражениям
- просмотр сграбленных emails
- дачу заметок выбранным пользователям
- время последнего захода
- отображение в постраничном виде (скажем по 200 записей на страницу)
- возможность грабить все в один файл (по желанию)
- сортировка логов по разным критериям
- удаление всех логов

Данные команды скачиваются с хостинга через определенный интервал времени и выполняются; в админке можно видеть статус команды для определенного пользователя - скачана\скачана но не выполнена\выполнена.

Билд - 500 w mz
ICQ [удалено]
Кому интересно, могу дать посмотреть тестовую админку.
<table>
<thead>
<tr>
<th>Name</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORDER</td>
<td>crack for SSSS - 11.06.2007 23:52:16</td>
</tr>
<tr>
<td>aleksiva</td>
<td>Need to crack programme RENTAL 5 <a href="http://pisoft.ru/dl/prokat50.exe">http://pisoft.ru/dl/prokat50.exe</a> reward</td>
</tr>
</tbody>
</table>

Message: 4
Joined: 11.06.2007
Status: offline
The Business of Cybercrime

<table>
<thead>
<tr>
<th>Name</th>
<th>Communication</th>
</tr>
</thead>
</table>

Communication : 1  
Joined : May 28, 2007  
Status : offline

- 1000 + free ordering
- 2000 - 0.4 wmz
- 5000 - 0.6 wmz
- 10000 1.1 WMZ
- 15000 2 WMZ
- 25000 3 WMZ
- 50000 6 WMZ
- 100000 11 WMZ
- 200000 15 WMZ
- 500000 20 WMZ
- 1000000 34 WMZ
- 2000000 53 WMZ

Criteria spam:
1) Very rapid delivery of messages.
2) Permanent customers discounts.
3) Can be delivered to your base, at the option of (sex, country, region, age).
4) Ability to send in a given time, you at the dates specified intervals lists (the time zone).

References can be found here: https://forum.zloy.org/showthread.php?t=30691
Knocking at ICQ: 369-336

# The Business of Cybercrime

<table>
<thead>
<tr>
<th>Name</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>fekthi</td>
<td>Service sales CC! ! ! - 09.06.2007 20:53:51</td>
</tr>
<tr>
<td></td>
<td>I wish to invite you to board with cvv2 Usa, (Walid - 90-95%). there VISA - MC PRICE :</td>
</tr>
<tr>
<td></td>
<td>1-10 cards - $ 2 (per unit)</td>
</tr>
<tr>
<td></td>
<td>10-100 cards - $ 1.5 (each)</td>
</tr>
<tr>
<td></td>
<td>DISCOVER-AMEX</td>
</tr>
<tr>
<td></td>
<td>1-10 cards - $ 2.5 (each)</td>
</tr>
<tr>
<td></td>
<td>10-100 cards - $ 2 (per unit)</td>
</tr>
<tr>
<td></td>
<td>Nevalid change within 3 days!</td>
</tr>
<tr>
<td></td>
<td>STANDING POKUPATELYAM DISCOUNTS! ! !</td>
</tr>
<tr>
<td></td>
<td>We guarantee the sale only in one hand and a high validity. if we can make a selection in the state, bin etc. ! !</td>
</tr>
<tr>
<td></td>
<td>pounding in ICQ : 498-007-015</td>
</tr>
<tr>
<td></td>
<td>Write to OFF-line. Answer 🤗</td>
</tr>
<tr>
<td>Name</td>
<td>Communication</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Keksik</td>
<td>Scanning passports and not only ... - 09.06.2007 0:15:36</td>
</tr>
<tr>
<td></td>
<td>There are scans passports. All questions ICQ 177303)</td>
</tr>
<tr>
<td></td>
<td>Prices 5 $ 2 $ colored black white</td>
</tr>
<tr>
<td>Posts</td>
<td>11</td>
</tr>
<tr>
<td>Joined</td>
<td>May 10, 2007</td>
</tr>
<tr>
<td>Status</td>
<td>online</td>
</tr>
<tr>
<td>Name</td>
<td>Communication</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Selling scans paspartov ...</td>
<td>03.04.2007 1:42:46</td>
</tr>
</tbody>
</table>

Post:Terminal

Message: 7
Joined: 03.04.2007
Status: offline

There paspartov scans are available:
USA, Russia, Ukraine, England, Australia, New Zealand, Nigeria, Shvedtsii, China, Kazakhstan

Added some countries Drive license:
Australia
Germany
Lithuania
Norway
Russia
Thailand
Ukraine
England
USA
Estonia
Sweden
70 Mage 70 Warrior 70 Shaman 70 Warlock all full epic

Seller of this item? Sign in for your status

Starting bid: US $27,000.00
PayPal account required

Your maximum bid: US $_________
(Enter US $27,000.00 or more)
Get $10 back on this item Apply

End time: 2 hours 40 mins (Feb-18-08 07:54:44 PST)
Shipping costs: Free
Other (see description)
Service to United States
Ships to: United States
Item location: McKeesport, PA, United States
History: 0 bids

You can also: Watch This Item
Get mobile or IM alerts | Email to a friend

Listing and payment details: Show
The Business of Cybercrime
Thanks!

Luis Corrons
luis.corrons@pandasecurity.com

PandaLabs Blog:
http://www.pandalabs.com