“You know, you can do this just as easily online.”
Who is behind this?
# Yesterday’s Bad Guys

<table>
<thead>
<tr>
<th>Blaster.B</th>
<th>Nestky / Sasser</th>
<th>CIH</th>
<th>29-A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeffrey Lee Parson</td>
<td>Sven Jaschan</td>
<td>Chen Ing-Hau</td>
<td>Benny</td>
</tr>
</tbody>
</table>
Today’s Bad Guys

Spam

James Ancheta

Phishing

Andrew Schwarmkoff

Spam

Jeremy Jaynes
Jeanson James Ancheta

Plead guilty to four felony charges of violating United States Code Section 1030, Fraud and Related Activity in Connection with Computers

Penalty:
57 months in prison
Adam Botbyl

The government claimed that the crime could have caused more than $2.5 million in damages.

Penalty:
26 months in prison
Cameron Lacroix

Plead guilty to hacking into the cell-phone account of celebrity Paris Hilton and participated in an attack on data-collection firm LexisNexis Group that exposed personal records of more than 300,000 consumers.

Penalty:
11 months in a Massachusetts juvenile detention facility
Ehud Tenenbaum

Admitted to cracking US and Israeli computers, and plead guilty to conspiracy, wrongful infiltration of computerized material, disruption of computer use and destroying evidence.

Penalty:
Six months of community service (in 2001)

August 2009:
Pleaded guilty to a single count of bank-card fraud for his role in a sophisticated computer-hacking scheme that federal officials say scored $10 million from U.S. banks.
A Real Case
Завершена разработка АвтоОплата на сайте WWW.SOCKS.BZ
Теперь вам нет необходимости оплачивать тарифный план или стучать в аську если вам нужно пару соксов - при чисте всего değil.

**NEWS**

WWW.SOCKS.BZ
The “Infected Team”

MPack
Dream Downloader
Limbo

Total Investment: 1,500$
The “Infected Team”

![Image of a spreadsheet showing infected team data]
The “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: \(0.40 \times 70,300 \times 30 = 843,600\)
The “Infected Team”

Who’s paying the “Infected Team”?
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? SnapInstall is 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, SnapInstall 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 offering 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!

Quality Content - Great Alternative to Traditional Advertising Media

SnapInstall 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, screen savers, new widgets - the list continues to grow and go on and on... SnapInstall easily allows you to offer an alternative advertising media to your
Hello! The ability to earn on the computers connected to the Internet opportunity, and working with it.

1. Very good aspect that is not.
2. The statistics in real time!
3. We pay for the unique down loaders.
4. Rapid server, which are located.
5. Since we can work any Website.
6. By advetram we give FREE a.
7. We employ "TrafficBestUp".
8. Very friendly support to resolve something is not working.
9. By paying a convenient way transfer. To pay by bank transfer.
10. We load absolutely innocently.

If you do not find the information, please contact us!

Our Support: 380-785-762 14

spywareDollars.com объединяется с KlikSoftware.com для увеличения кол-ва продаж:

1. Зарегистрироваться на KlikSoftware.com
2. Стать клиентом в ICS 154-577-459, сдать свой ID в KlikSoftware.com
3. Нам выдают еще либо iFrame решение для продаж софта и увеличение цены за продажу с стандартных 15$ до 20$ (только на продукт RazeSpyware)
Rogueware Infected Computers → 3.50%
Computers worldwide → 1 billion (Forrester)

35,000,000 infected computers / monthly

35 million computers ≠ 35 million users
Let’s take just half: 17.5 million people
Phishing victims (Gartner) → 3.30%

557,500 rogueware buyers / monthly
Rogueware Average Price → $59.95

$59.95 \times 557,000 = $34,621,125 \text{ PER MONTH}

$415,453,500 \text{ PER YEAR}
<table>
<thead>
<tr>
<th>Id</th>
<th>Имя</th>
<th>Продукт</th>
<th>Комментарий</th>
<th>Default</th>
<th>Статус</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>antivirusxp08.net</td>
<td>(16) Antivirus XP 2008 New</td>
<td>(16) основной</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>antivirusxp2000.net</td>
<td>(16) Antivirus XP 2000 New</td>
<td>(16) спамеры (was &quot;для sp32&quot;)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>antivirusxp-00.net</td>
<td>(16) Antivirus XP 2000 New</td>
<td>(16) top20, кроме sp32 и спамеров</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>antivirusxp-08.net</td>
<td>(16) Antivirus XP 2008 New</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>av2008.net</td>
<td>(16) Antivirus XP 2000 New</td>
<td>(16) common</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>avxp-2008.net</td>
<td>(16) Antivirus XP 2008 New</td>
<td>(16) common</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>online-security-guide.com</td>
<td>(16) Antivirus XP 2000 New</td>
<td>(16) top20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>ap2008.com</td>
<td>(16) Antivirus SP 2008 New</td>
<td>02-09-08, для топов</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>antivirxp.net</td>
<td>(16) Antivirus XP 2000 New</td>
<td>02-09-08 для бала</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>antivirus00.com</td>
<td>(16) Antivirus XP 2000 New</td>
<td>09-09-08 основной для всех</td>
<td>[*]</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>antivirus-online-08.com</td>
<td>(16) Antivirus XP 2008 New</td>
<td>Для спамеров, 01-09-08</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>online-antivirus-09.com</td>
<td>(16) Antivirus XP 2000 New</td>
<td>Для даны, 03-09-08</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
$81,388 USD in 6 days!
<table>
<thead>
<tr>
<th>TransactionType</th>
<th>Settled</th>
<th>Merchant</th>
<th>FirstName</th>
<th>LastName</th>
<th>Email</th>
<th>CreditCard</th>
<th>Merchant Amount</th>
<th>Total Amount</th>
<th>IP</th>
<th>TID</th>
<th>Affiliated</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>michelle</td>
<td></td>
<td><a href="mailto:m202092@comcast.net">m202092@comcast.net</a></td>
<td>3713...1063</td>
<td>$48.95</td>
<td>$49.95</td>
<td>187.157.186</td>
<td>46916819</td>
<td>396123</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Juana</td>
<td></td>
<td><a href="mailto:s_06@hotmail.com">s_06@hotmail.com</a></td>
<td>5121...3350</td>
<td>$48.95</td>
<td>$49.95</td>
<td>61.171.10.22</td>
<td>46917674</td>
<td>396126</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Peter</td>
<td></td>
<td><a href="mailto:1992@gmail.com">1992@gmail.com</a></td>
<td>4063...9884</td>
<td>$48.95</td>
<td>$49.95</td>
<td>193.125.107</td>
<td>46921875</td>
<td>396130</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Steve</td>
<td></td>
<td><a href="mailto:ave@verizon.net">ave@verizon.net</a></td>
<td>4264...9385</td>
<td>$48.95</td>
<td>$49.95</td>
<td>220.233</td>
<td>46928554</td>
<td>396133</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>rosemarie</td>
<td></td>
<td><a href="mailto:aaros301@aol.com">aaros301@aol.com</a></td>
<td>4744...9411</td>
<td>$48.95</td>
<td>$49.95</td>
<td>16.105</td>
<td>40973570</td>
<td>396166</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Robin</td>
<td></td>
<td>aol.com</td>
<td>47920...0892</td>
<td>$48.95</td>
<td>$49.95</td>
<td>200.203</td>
<td>46976483</td>
<td>396170</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Zachary</td>
<td></td>
<td><a href="mailto:ber@yahoo.com">ber@yahoo.com</a></td>
<td>4862...6716</td>
<td>$48.95</td>
<td>$49.95</td>
<td>192.96</td>
<td>46989064</td>
<td>396183</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Kimberly</td>
<td></td>
<td>earthlink.net</td>
<td>4606...1468</td>
<td>$48.95</td>
<td>$49.95</td>
<td>63.87</td>
<td>46990599</td>
<td>396184</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Kristin</td>
<td></td>
<td><a href="mailto:erstone@netzero.net">erstone@netzero.net</a></td>
<td>4540...1583</td>
<td>$48.95</td>
<td>$49.95</td>
<td>106.30</td>
<td>46991211</td>
<td>396185</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Toni</td>
<td></td>
<td>cox.net</td>
<td>4147...0461</td>
<td>$48.95</td>
<td>$49.95</td>
<td>169.193</td>
<td>46998371</td>
<td>396187</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Andor</td>
<td></td>
<td><a href="mailto:e@connet.nl">e@connet.nl</a></td>
<td>5413...5594</td>
<td>$48.95</td>
<td>$49.95</td>
<td>191.79</td>
<td>46998627</td>
<td>396188</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>stefano</td>
<td></td>
<td><a href="mailto:ilo@tiscali.it">ilo@tiscali.it</a></td>
<td>3752...1065</td>
<td>$48.95</td>
<td>$49.95</td>
<td>35.61</td>
<td>47003256</td>
<td>396190</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>WALTER</td>
<td></td>
<td>msn.com</td>
<td>5401...1019</td>
<td>$48.95</td>
<td>$49.95</td>
<td>126.200</td>
<td>47008022</td>
<td>396191</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>nicole</td>
<td></td>
<td><a href="mailto:np@navy.mil">np@navy.mil</a></td>
<td>5155...5443</td>
<td>$48.95</td>
<td>$49.95</td>
<td>245.64</td>
<td>47008636</td>
<td>396192</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Aram</td>
<td></td>
<td>poptonline.net</td>
<td>5466...5712</td>
<td>$48.95</td>
<td>$49.95</td>
<td>143.26</td>
<td>47011793</td>
<td>396196</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>Timothy</td>
<td></td>
<td><a href="mailto:mw@v.net">mw@v.net</a></td>
<td>3732...1003</td>
<td>$48.95</td>
<td>$49.95</td>
<td>87.99</td>
<td>47013819</td>
<td>396197</td>
</tr>
<tr>
<td>AUTH_ONLY_CAPTURED</td>
<td>Settlement</td>
<td>Spyaway</td>
<td>albert</td>
<td></td>
<td><a href="mailto:m200072@comcast.net">m200072@comcast.net</a></td>
<td>5911...3855</td>
<td>$48.95</td>
<td>$49.95</td>
<td>75.110</td>
<td>47018075</td>
<td>396198</td>
</tr>
<tr>
<td>DECLINED</td>
<td>Pending</td>
<td>Spyaway</td>
<td>jeff</td>
<td></td>
<td>mchsi.com</td>
<td>4121...2422</td>
<td>$48.95</td>
<td>$49.95</td>
<td>155.210</td>
<td>396200</td>
<td>396200</td>
</tr>
<tr>
<td>DECLINED</td>
<td>Pending</td>
<td>Spyaway</td>
<td>jeff</td>
<td></td>
<td>mchsi.com</td>
<td>4121...2422</td>
<td>$48.95</td>
<td>$49.95</td>
<td>155.210</td>
<td>396200</td>
<td>396202</td>
</tr>
<tr>
<td>#</td>
<td>Nickname</td>
<td>Payout</td>
<td>Searches</td>
<td>Clicks</td>
<td>Avg. Bid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>------------</td>
<td>--------</td>
<td>----------</td>
<td>--------</td>
<td>----------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Sowmya</td>
<td>3,156.7</td>
<td>2865</td>
<td>4652</td>
<td>0.6830</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Webmaster</td>
<td>2,395.3</td>
<td>181601</td>
<td>40782</td>
<td>0.0867</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><a href="http://www.gopaychaa.com">www.gopaychaa.com</a></td>
<td>841.1</td>
<td>10632</td>
<td>1708</td>
<td>0.4925</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Webmaster</td>
<td>773.7</td>
<td>132403</td>
<td>117510</td>
<td>0.0056</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Webmaster</td>
<td>752.7</td>
<td>120564</td>
<td>117365</td>
<td>0.0054</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Webmaster</td>
<td>699.9</td>
<td>113798</td>
<td>110119</td>
<td>0.0064</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Webmaster</td>
<td>682.4</td>
<td>1326306</td>
<td>107834</td>
<td>0.0053</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Aaah kala Moorah ekkai!</td>
<td>557.7</td>
<td>13078</td>
<td>21</td>
<td>0.0054</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Webmaster</td>
<td>499.1</td>
<td>1006598</td>
<td>88762</td>
<td>0.0056</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Webmaster</td>
<td>487.3</td>
<td>1823</td>
<td>405</td>
<td>1.2031</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Webmaster</td>
<td>457.8</td>
<td>955013</td>
<td>82365</td>
<td>0.0056</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Webmaster</td>
<td>422.0</td>
<td>500715</td>
<td>66055</td>
<td>0.0064</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Webmaster</td>
<td>415.1</td>
<td>574296</td>
<td>64563</td>
<td>0.0064</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Aoiyge eloidal</td>
<td>399.4</td>
<td>1721</td>
<td>282</td>
<td>1.1031</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Webmaster</td>
<td>387.0</td>
<td>1435</td>
<td>410</td>
<td>0.9459</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Webmaster</td>
<td>385.3</td>
<td>534593</td>
<td>60145</td>
<td>0.0064</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Webmaster</td>
<td>383.1</td>
<td>530881</td>
<td>60157</td>
<td>0.0064</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Webmaster</td>
<td>378.0</td>
<td>756</td>
<td>415</td>
<td>0.9138</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Webmaster</td>
<td>376.7</td>
<td>816963</td>
<td>69576</td>
<td>0.0054</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Please Input the Login Information

Login
Password
Enter

Forgot your password? | Sign UP

Klikvip.com users come from these countries:

- Belarus: 28.0%
- Russia: 24.9%
- Ukraine: 18.2%
- United States: 5.9%
- Armenia: 5.4%
KLIK DOCTOR РЕКОМЕНДУЕТ!

- ПОДАРОК С ПРОДАЖ
- ЕЖЕДНЕВНЫЕ ВЫПЛАТЫ
- САМЫЕ СОВременные решения
- Уникальные условия препаратам

WWW.KLIKDOCTOR.COM
Malware figures
Malware figures

Rogueware Samples in 2008

Q1 08, 1086
Q2 08, 13609
Q3 08, 22534
Q4 08, 54986
OH, #@@*!

Social network
Now following you:
- Blue Ghost
- Yellow Ghost
- Red Ghost
1,000,000 malicious links indexed by Google
3,000,000 legitimate search terms hijacked
Targeted users looking for instructions (E.g. How to loosen a tension belt)
Served 100 new MSAntiSpyware2009 binaries in 24 hours
Comments on Digg.com leading to Rogueware

- 500,000+ comments leading to Rogueware
- Comments targeted news submission title and content
Twitter trending topics lead to Rogueware

- Messages (tweets) targeting trending topics on Twitter.com
- 27,000 tweets per 24 hours
- 60 unique samples detected over 72 hour period
Rogueware exploits Wordpress vulnerability to facilitate Blackhat SEO attack

- Affected Ned.org and TheWorkBuzz.com
- Targeted a security vulnerability in an old version of Wordpress
- Redirected all links to point to Rogueware servers
What do you think about iPhone
http://ambersurman2.123bemy...
6 minutes ago from web

achatz461
Dale Osterlag
News results for natal youtube

Project Natal Microsoft YouTube! - 1 day ago
LALATE has 3 YouTube videos of Microsoft's Project Natal from E3 today. Project Natal's introduction at E3 came during Microsoft's Monday press conference....
LALATE - 1224 related articles »

Project: natal youtube. All about Project natal youtube!!! 
He resolutely denied these rumors project natal youtube hunting all over Moscow she woke Sony project natal youtube told her what she had done...
14 hours ago -

natal youtube - AOL Video 
Watch natal youtube videos free online at AOL Video.
video.aol.com/category/natal-youtube - 95k - Cached - Similar pages -

Project: Natal Youtube 3 
Jun 1, 2008 ... Project Natal Youtube 3. Project NATAL V.. Project Natal Video 2. PROJECT NATAL V.. Project Natal Video 1. Left 4 Dead 2 E....
news.lalate.com/celebrity/home.html?task=videodirectlink&id=748 - Similar pages -
Conclusion
Thanks!

Luis Corrons
luis.corrons@pandasecurity.com

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