Taking Down a Botnet:
The Story Behind Rove Digital's Takedown

Ryan Flores – Forward Looking Threat Research
What is a takedown?
Figure 4. Evolution of KOOBFACE architecture as seen in our fourth paper.
Takedowns aren’t easy
ROVE Digital is an innovative company with experience in its field and great respect for its customers. It was established in 2002 and has been evolving rapidly since then.

The wide range of services of highest quality and professional co-operation with our partners that is based on trust and respect makes ROVE Digital the best choice one can make for the online business establishment and promotion.

Our products are powered by advanced software that allows simplifying and unifying the management of online services. Experienced customer support team can be reached at any time and is glad to answer all your questions related to ROVE Digital services.

People who work for ROVE Digital make up a strong goal-oriented team with the main priority to provide the best online services and online solutions ever available.

The customer-oriented philosophy of ROVE Digital combined with its cutting-edge technology is a guarantee of the ultimate success in online industry.

News

- 30.07.2009
  Znet online advertising system is based on the PPC (pay per click) model applied to the leading and widely used search engines, large

- 23.07.2009
  EntDomains, Inc, one of the world’s fastest growing domain name Registrar, launched Balder project several months ago.

- 27.06.2009
  The online advertising project ZMCT is live! From now on the powerful online advertising technologies are offered to those who want to
An IT company in Estonia

- “The most innovative IT company” in Estonia (2007)
- Among top 3 IT companies in Estonia (revenue)
- 2008: revenue > 9,000,000 USD.
- 2007: > 50 employees

ROVE DIGITAL
(Tamme Arendus)
### Servers in US

<table>
<thead>
<tr>
<th></th>
<th>Plan</th>
<th>Cost</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td><strong>$150.00 per month</strong></td>
<td></td>
<td>Intel Celeron 3.0Ghz, Maxtor 160Gb, 8Mb Cache, 512Mb DDR, 1000Gb Transfer</td>
</tr>
<tr>
<td>B</td>
<td><strong>$180.00 per month</strong></td>
<td></td>
<td>AMD Sempron 3400+, Maxtor 160Gb, 8Mb Cache, 1024Mb DDR, 1000Gb Transfer</td>
</tr>
<tr>
<td>C</td>
<td><strong>$220.00 per month</strong></td>
<td></td>
<td>P4 3.0GHz w/512K Cache, Maxtor 250Gb, 8Mb Cache, 1024Mb DDR, 1000Gb Transfer</td>
</tr>
<tr>
<td>D</td>
<td><strong>$250.00 per month</strong></td>
<td></td>
<td>P4 3.0GHz Dual-Core, WD 250GB w/8MB Buffer, 1024Mb DDR, 1000Gb Transfer</td>
</tr>
<tr>
<td>E</td>
<td><strong>$280.00 per month</strong></td>
<td></td>
<td>AMD Athlon 64 Dual-Core 3800+, WD 250GB w/8MB Buffer, 1024Mb DDR, 1000Gb Transfer</td>
</tr>
<tr>
<td>F</td>
<td><strong>$350.00 per month</strong></td>
<td></td>
<td>AMD Opteron Dual-Core 265, WD 250Gb HDD, 1024Mb DDR, 1000Gb Transfer</td>
</tr>
</tbody>
</table>
Rove’s “advertising” services

Nullor.com launched in 2002 has become one of the leading companies in the online advertising industry. We connect thousands of advertisers with millions of consumers. Our ultimate goal is to provide our customers with contemporary e-business and website technologies. We continue to balance the supply and demand from both of our advertisers and publishers by providing them with high-quality services and applying the latest technologies in order to increase their advertising value.

With years of professional knowledge and experience in the Internet advertising industry, Nullor.com employs the advanced and innovative technology to meet the needs of valuable advertisers and quality publishers.

Nullor.com aims to increase the benefits and revenue for our clients and members by bringing Internet advertising to a new higher level. We unite all advertising networks into one.

Are You A Brand Advertiser?

Extend your reach with diverse advertising and targeting options by applying performance-based advertising solutions. Sign up today and get advanced solutions to fit your advertising campaign.

Are You A Web Publisher?

Diversity and control your business by choosing Nullor.com. We expand advertising options and let your network revenues grow. Nullor.com will partner with you to meet your goals.

NEWS

28.02.2008
Nullor.com, rapidly growing Ad Network, announces that it has more than 10 million searches per month throughout its entire advertising network of targeted search. This rise in volume is due in part to the company’s broad advertiser base as well as having secure and reliable partners. Read more...

28.11.2007
Nullor.com, the developing advertising network, announces today a significant traffic increase for 2007 compared with 2006. Nullor.com site had nearly 20% overall traffic increase since last year.
Read more...
2002-2004 The Early Years

Malicious Activity
- Rented out servers to mainly cybercriminal customers for use as spambot command-and-control (C&C), data-stealing Trojan, phishing site, and Domain Name System (DNS) changer hosts

Infrastructure
- Rented servers in 3 data centers in New York (Pilosoft), San Francisco (Atrivo), and Estonia (Elion)
On the Radar

Malicious Activity

|| Used a spoofed Google Ads site that replaced the Google ads that DNS changer victims saw on legitimate sites

Infrastrucure

|| Rogue DNS servers hosted at Pilosoft seemingly disappeared in fall 2007 though these remained part of Rove Digital's infrastructure as back-end servers that did recursive DNS lookups

|| A nonprofit organization blacklisted the IP addresses of Rove Digital's spoofed Google Ads site

|| Deliberately waited months before spoofing the Google Ads site elsewhere in order to avoid suspicion and protect its operation
2009 A New Venture

Malicious Activity
- Directly entered the FAKEAV business

Geography: United States

Business Model: Decided to form its own FAKEAV affiliate program, Nelicash/NewlineCash

Contractors from Eastern European countries fulfilled most of its advanced coding and Trojan creation requirements

 Pirated movies

Created and spread adware

Started working with Clicksor for ad replacement
2010-2011

The Takedown

Malicious Activity

- Tried to enter the market for pirated movies
- Malicious operation was shut down
- Rove Digital employees were arrested
- Réseaux IP Européens (RIPE) froze Rove Digital’s IP domain ranges

Infrastructure

- Had a DNS botnet with more than 4M bots
- Had more than 100 servers in its infrastructure

Other Events

- Collaborative investigation among the Federal Bureau of Investigation (FBI), the Office of Inspector General (OIG), as well as Trend Micro and its industry partners ensued
Big Botnet Busts

- EstHost: Active since Nov 2011, Takedown date: Feb 2010
- CoreFlood: Active since Mar 2009, Takedown date: Mar 2011
- Rustock: Active since Sep 2008, Takedown date: Apr 2011
- Waledac: Active since Oct 2008, Takedown date: Feb 2010

Infected computers:
- 4 million
- 2 million
- 1 million
- <1 million
Operation Ghost Click: considered as the biggest cybercriminal takedown in history.
Rove Digital/Esthosts … ISP? Cybercrime hub?

An entrepreneurial professional CEO
So what’s it worth?

150,000 machines = 1,000,000 clicks per day

<table>
<thead>
<tr>
<th>earnings (USD)</th>
<th>keyword</th>
<th>clicks</th>
<th>CPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>35.48</td>
<td>facebook</td>
<td>4917</td>
<td>0.0072</td>
</tr>
<tr>
<td>33.64</td>
<td>dating</td>
<td>1244</td>
<td>0.027</td>
</tr>
<tr>
<td>16.43</td>
<td>free credit report</td>
<td>275</td>
<td>0.0598</td>
</tr>
<tr>
<td>15.7</td>
<td>ebay</td>
<td>911</td>
<td>0.0172</td>
</tr>
<tr>
<td>15.25</td>
<td>credit card processing</td>
<td>136</td>
<td>0.1122</td>
</tr>
<tr>
<td>15.24</td>
<td>direct tv</td>
<td>232</td>
<td>0.0657</td>
</tr>
<tr>
<td>14.09</td>
<td>malwarebytes</td>
<td>313</td>
<td>0.045</td>
</tr>
<tr>
<td>14.06</td>
<td>accept credit cards</td>
<td>105</td>
<td>0.1339</td>
</tr>
<tr>
<td>13.89</td>
<td>car insurance</td>
<td>63</td>
<td>0.2205</td>
</tr>
<tr>
<td>13.76</td>
<td>mcafee</td>
<td>87</td>
<td>0.1581</td>
</tr>
</tbody>
</table>

Total: 12933

Table 1. One-day earnings of a browser hijack botnet

4,000,000 machines = ?
THE PROBLEM
How DNS Works

Customer

www.mybank.com

DNS Server

www.mybank.com
Contrast to: Trojanized DNS + implications
By having the malware in their systems, users could be directed to any site at the whim of the cybercriminal.
CNN website (original)
CNN website (infected)
Porn?

Fake AV - Big Business
THE INVESTIGATION
Trend Micro has been monitoring these cybercriminal activities since 2006
Start of botnet activity by Esthost:

- **2005**: Trend Micro begins monitoring the company.
- **2008**: Trend Micro publishes a paper about the malicious activities of Esthost.
- **NOV 2008**: Its San Francisco datacenter was rendered inactive due to terminated internet connection.
- **AUG 2009**: ICANN revokes ESTdomains accreditation due to owner's conviction of credit card fraud.
- **2010**: Trend Micro publishes more findings on its Malware Blog.
- **NOV 2011**: Takedown.
We had a lot of flies on the walls of Rove.

Laughable security of Rove’s servers.**

100+ servers given .intra domains

looked at SMTP banners & DNS servers (often open resolvers)

DNS zone files transfers for domains of Rove.

All .intra domains, IPs and additions

Identify and follow the new domain names that got resolution from rogue dns

we got two hard drive of C&C servers.

**no password protection or encryption broken
<table>
<thead>
<tr>
<th>.intra</th>
<th>Port</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>portal2.intra</td>
<td>86400</td>
<td>IN</td>
<td>93.190.x.x</td>
</tr>
<tr>
<td>codecsoft3.intra</td>
<td>86400</td>
<td>IN</td>
<td>213.163.x.x</td>
</tr>
<tr>
<td>metaparser.intra</td>
<td>86400</td>
<td>IN</td>
<td>67.210.x.x</td>
</tr>
<tr>
<td>adsclick.intra</td>
<td>86400</td>
<td>IN</td>
<td>174.142.x.x</td>
</tr>
<tr>
<td>pharma1.intra</td>
<td>86400</td>
<td>IN</td>
<td>87.118.x.x</td>
</tr>
<tr>
<td>tds.intra</td>
<td>86400</td>
<td>IN</td>
<td>64.86.x.x</td>
</tr>
</tbody>
</table>

**Google Proxies**

<table>
<thead>
<tr>
<th>.intra</th>
<th>Port</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>gcachex1.intra</td>
<td>86400</td>
<td>IN</td>
<td>69.31.x.x</td>
</tr>
<tr>
<td>gcachex2.intra</td>
<td>86400</td>
<td>IN</td>
<td>67.210.x.x</td>
</tr>
</tbody>
</table>

**Fake AV sites**

<table>
<thead>
<tr>
<th>.intra</th>
<th>Port</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>billing.intra</td>
<td>86400</td>
<td>IN</td>
<td>64.28.x.x</td>
</tr>
<tr>
<td>billingproxy1.intra</td>
<td>86400</td>
<td>IN</td>
<td>78.159.x.x</td>
</tr>
<tr>
<td>billingproxy2.intra</td>
<td>86400</td>
<td>IN</td>
<td>68.198.x.x</td>
</tr>
</tbody>
</table>
Operation Ghost Click took down a long-running botnet with more than 4 million infected systems.
- Data centers got raided
- 200+ servers got seized
- Rogue DNS servers got replaced with ISC DNS
- Rove Digital’s office got raided
- Luxury cars, millions of USD, houses confiscated
- 6 arrests in Estonia
- RIPE blocked IP ranges
Vladimir Tsastsin

Tsastsin is the leader of the Rove Digital cybercrime ring. He was Esthost, EstDomains, and Rove Digital’s CEO. When he could no longer use his own name to register affiliate companies, he sought his family members’ help to sign formal letters in Estonia. Known as “scr” in the cybercrime underground, he was convicted of credit card fraud in Estonia in 2008.
Dmitri Jegorov

According to the online newspaper, Ekspress.ee, Jegorov had a criminal record as well. As a teenager, he allegedly tried to extort money from a local supermarket and even made a fake bomb but was easily arrested. Part of his role included recruiting new employees and registering several of Rove Digital’s shell companies in the United States. He can be considered a Rove Digital program manager. Known for using the alias “Dmitri Dimuskin,” he is also known as a pornography webmaster.
Timur Gerassimenko

Gerassimenko had his own company, Infradata, which provided services to Rove Digital. Also known as “hyper,” he dabbled in running pornography and malware-hosting sites (photo courtesy of Ekspress.ee).
Konstantin Poltev

Poltev was the spokesman for Esthost, EstDomains, and Rove Digital. He also headed Esthost and Cernel’s Abuse Department. In 2008, he publicly claimed on NANOG’s public mailing list that Esthost was a legitimate company. Also known as “kokach,” he was proclaimed EstDomains’s new CEO when the ICANN decided to revoke the company’s accreditation in 2008 due to “former CEO” Tsastsin’s conviction for credit card fraud in Estonia (photo courtesy of Ekspress.ee).
Valeri Aleksejev

Aleksejev calls himself a web developer on LinkedIn but avoids mentioning what company he works for. He allegedly wrote the code for a Rove Digital monitoring system for its rogue DNS infrastructure. He also appears to be one of the recipients of email alerts whenever the company encountered problems.
Not covered by the current complaints:
- FakeAv Business
- Affiliate Program
- Payment Service
Trend Micro provided the majority of the threat research in the takedown
Cybercrimes do not occur in isolation. Their reach and effects are far-extending.

Collaboration between
FBI, Estonian Police, Dutch Police,
Trend Micro,
RIPE, ISC, Qwest, Comcast, Bell Canada, AT&T, Neustar,
Spamhaus, Google, others
## Challenges

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Challenges</th>
</tr>
</thead>
</table>
| Crime        | • DNS knowledge,  
• knowledge how Websites work  
• knowledge how advertising work |
| Investigation| • Forensic skill (hard disks),  
• DNS skill ,  
• Pentesting skill set,  
• Internet forensics  
• Sandboxing and reverse engineering |
| Take down    | • Transnational nature of the crime  
(different police, different laws),  
• Number of players high (many DC owner, many ISP‘s)  
• confidentiality |
Did you lose your Internet last July 9?
Cyberpolice? – Which Cyberpolice

• Each country has own laws
• Each country has own law enforcement
• Cyberspace is global (even universal)
• Even within one state ist not clear if Cyber is internal affair or military
• Competition to use cyber defense for own advantage

Result: 1000 initiatives, tons of paper, but no progress
The Problem Continues

• Continuous development of TDSS/TDL4/Alureon rootkit
THANK YOU!
Google Search Fraud – Server Schema

1. DNS changer: Trojan victim types search queries
2. Spoofed site relays search query to a parser server
3. Search queries are parsed
4. Extracted keywords are compared with those in the cache server
5. If keywords are in the cache, user sees stored results
6. If keywords are not in the cache, search queries are forwarded to a load balancer
7. Load balancer forwards queries to one of the proxies
8. Proxy relays request to the real Google servers
9. Results are stored in the cache
10. Google servers send search results to user
11. User clicks search result
12. Parser detects the click on the search result
13. User is redirected to sites with foreign IP addresses
14. Traffic theft

End Result