Trend Micro Incorporated
Research Paper
2012

OPERATION GHOST CLICK

The Rove Digital Takedown

By: Forward-Looking Threat Research Team

CONTENTS

Cybercrime is our common enemy.

– Konstantin Poltev, Esthost spokesman, October 13, 2008

INTRODUCTION

In the past few years, Trend Micro has been quietly cooperating with the Federal Bureau of Investigation (FBI), the Office of the Inspector General (OIG), and security industry partners in their attempts to take down the Estonia-based cybercriminal gang, Rove Digital. This collaboration was a huge success, as on November 8, 2011, law enforcement authorities seized Rove Digital's vast network infrastructure from different data centers in the United States and Estonia as well as arrested six suspects, including the organization's CEO, Vladimir Tsastsin.

Rove Digital is allegedly responsible for tens of millions of system infections with the aid of advanced Trojans and large-scale click-fraud schemes, resulting in hundreds of millions of dollars worth of damage and productivity loss for companies worldwide. Rove Digital allegedly used several shell companies based in the United States, Estonia, the Ukraine, Denmark, and other countries for their malicious activities; had an office in Tartu, Estonia; and was even touted as the "most innovative IT company" in that country in 2007 by a local newspaper.

This paper provides some information Trend Micro learned about Rove Digital since 2006. As early as 2006, Trend Micro learned that Rove Digital was spreading Domain Name System (DNS) changer Trojans and appeared to be controlling every step from infection to monetizing infected bots. We, however, decided to withhold publication of certain information in order to allow law enforcement agencies to take the proper legal action against the cybercriminal masterminds while protecting our customers. Now that the main perpetrators have been arrested and Rove Digital's network has been taken down, we can share more details regarding the intelligence we gathered about the operation in the past five years.

ROVE DIGITAL'S HISTORY

This section is intended to be just a brief overview of Rove Digital's history and is not intended to be complete. Certain details have been intentionally withheld. We do, however, highlight some points that we think are crucial to understanding Rove Digital's business.

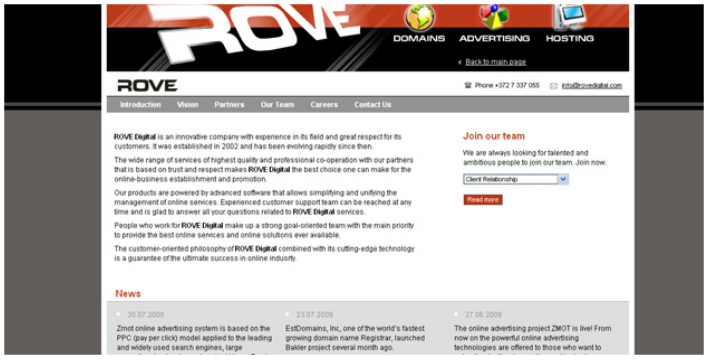


Figure 1. Rove Digital *site*

2002–2006: The Early Days

Rove Digital's history reportedly dates to as far back as 2002, perhaps even earlier. In this overview, however, we will focus on the DNS changer Trojans and FAKEAV variants it appears to have distributed.

From 2004 onward, it became more and more apparent that Esthost was allegedly involved in all types of cybercrime. Esthost was a daughter company of Rove Digital, which resold web-hosting services. Esthost had customers that used servers it rented from data centers based in San Francisco; New York; and its presumed home country, Estonia. These customers hosted command-and-control (C&C) servers for spam botnets, data-stealing Trojans, phishing sites, and DNS changer Trojans.

It was reported that when confronted about the abuse, Esthost claimed that all of the reported malicious activities involved bad customers against whom it was going to take action. Even if it may have taken some kind of action, however, the same kind of abuse seemed to crop up elsewhere with different Esthost-controlled IP addresses. This led many security researchers to believe that Esthost provided a safe haven for those who may engage in cybercrime.

At that time, Esthost's main ISPs allegedly included Atrivo in San Francisco, Pilosoft in New York, and Elion in Estonia. In 2005, Elion purportedly temporarily terminated all of its services to Esthost. San-Francisco-based web-hosting company, Atrivo, was allegedly aware of serious abuse originating from Esthost's customers but did not appear to take any action. An Atrivo representative on *Usenet* supposedly made the following significant written admission:

"If I had the ability… I would cut Esthost as a client… But, in doing so, it causes nearly a quarter if not half of the company's monthly revenue to be cut. That is not too good of a move nor reasonably possible."

Some believe this admission may have prompted Atrivo to shut down its operations three years later.

As early as 2005 and 2006, it was generally known that Esthost did not only provide services to many involved in cybercrime but that it was also directly involved in cybercrime. Moreover, there appeared to be considerable support that Esthost may have been responsible for spreading DNS changer Trojans and controlling a large infrastructure in order to monetize the bots it may have infected with the said Trojans.

DNS is the Internet protocol that resolves human-readable domain names into IP addresses that are assigned to computer servers on the web. Most Internet users automatically use their ISPs' DNS servers and are probably unaware that DNS even exists. DNS changer Trojans discreetly modify computers' settings so these will use foreign DNS servers set up by malicious third parties and translate certain domains into malicious IP addresses. As a result, victims are redirected to possibly malicious sites without their knowledge or consent.

It is not known when Esthost first started spreading DNS changer Trojans but a DNS changer Trojan was hosted on the domain, *winprotect.net,* in February 2005, a domain that appears to have been registered by a certain Peter Isson of Esthost. While *Whois* records of domain names are notoriously unreliable, we believe that in this case, only the name "Peter Isson" may have been fictitious (see Figure 2).

```
Domain Name: WINPROTECT.NET

Registrant:
ESTHOST
Peter Isson (domains@winmsn.com)
Tartu Peapostkontor, pk. 12
Tartu
,50001
EE
Tel. +372.5564764609

Creation Date: 28-Dec-2004
Expiration Date: 28-Dec-2006

Domain servers in listed order:
ns1.winprotect.net
ns2.winprotect.net

Administrative Contact:
ESTHOST
Peter Isson (domains@winmsn.com)
Tartu Peapostkontor, pk. 12
Tartu
,50001
EE
Tel. +372.5564764609

Technical Contact:
ESTHOST
Peter Isson (domains@winmsn.com)
Tartu Peapostkontor, pk. 12
Tartu
,50001
EE
Tel. +372.5564764609

Billing Contact:
ESTHOST
```

Figure 2. Whois *record details for the domain name,* winprotect.net

Starting 2005, it was believed that the DNS servers' infrastructure used *esthost.com* subdomains. For example, DNS servers were hosted on subdomains such as *dns1.esthost.com–dns52.esthost.com* and *apdns1.esthost.com–apdns32.esthost.com*. A central server that can update all of the said DNS servers at the same time was supposedly hosted on *dns-repos.esthost.com*, a back-end server for fake codec Trojans was supposedly hosted on *codecsys.esthost.com*, and a site that checked malware against several security vendors' detections was supposedly hosted on *virus.esthost.com* (see more examples in Table 1). Unless the esthost.com domain was hacked, only Esthost could add these very suggestive subdomains to its domain.

Table 1. *Some Esthost subdomains that were part of the company's large DNS infrastructure*

Subdomain	Description
apilosoft.esthost.com	Router at Pilosoft
banex[1–7].esthost.com	Back-end system for ad replacement and referral ID changes
codecsys.esthost.com	Back-end system for codec Trojan download sites
dns[1–52].esthost.com	DNS server
dns-repos.esthost.com	Back-end system for DNS servers
gaproxy.esthost.com	Proxy server for *Google* search hijacking
megatds.esthost.com	Traffic distribution system (TDS) that redirects DNS changer Trojan victims
metaparser1.esthost.com	Back-end system for *Google Ads* fraud
testdns1.esthost.com	Test DNS server
virus.esthost.com	System that checks security vendor detections against Rove Digital's malware
vpn1.esthost.com	VPN server in Pilosoft used to access the C&C server
xgallery[1–9].esthost.com	Landing pages that led to codec Trojans

The information above indicates that Esthost was most probably involved in cybercrime.

2007: "Virus Bulletin Conference" Talk

Pilosoft's owner was probably not pleased to discover that his company was identified as one of the hosts for some of Esthost's rogue DNS servers in a presentation made by Trend Micro during the "Virus Bulletin Conference" in Vienna in September 2007. By that time, Pilosoft was known to have already been leasing servers to Esthost for a couple of years. Pilosoft took some action and the Esthost rogue DNS servers it hosted seemingly disappeared from the web shortly after the "Virus Bulletin Conference" in fall 2007.

Rove Digital and Esthost appear to prefer building long-term relationships. They appeared to prefer a steady flow of ill-gotten rather than easy-to-obtain, short-term gains.

In fall 2007, Spamhaus, a nonprofit organization that sells anti-spam data feeds, blacklisted the IP addresses of a spoofed *Google Ads* site, which was supposedly part of Rove Digital's DNS infrastructure. This server appeared to replace *Google* ads with foreign ones on legitimate websites that DNS changer victims visited. Rove Digital seemed to have been surprised when Spamhaus took down the spoofed *Google Ads* site. Even if it was trivial to set up a new spoofed *Google Ads* site, as its core DNS changer infrastructure remained intact, Rove Digital did not do so. It supposedly did not set up a spoofed *Google Ads* site elsewhere until months later, thus likely forgoing a substantial amount of revenue. Instead of going for the quick buck, the company appeared to have opted to protect its operation by waiting until it felt comfortable spoofing the *Google Ads* site again.

2008: Ups and Downs

Esthost and EstDomains Go Down

In fall 2008, two of Rove Digital's daughter companies, Esthost and EstDomains, made headlines. The Internet Corporation for Assigned Names and Numbers (ICANN) decided to revoke the accreditation of registrar, EstDomains, after its owner, Vladimir Tsastsin, was convicted of credit card fraud in his home country, Estonia.

Atrivo shut down after its upstream providers allegedly decided not to engage in business with them due to public pressure from certain private parties. The vast majority of Esthost's servers were supposedly in Atrivo's data center. As such, Atrivo's downfall reportedly shut down more than 700 of Esthost's servers. Atrivo had purportedly been under pressure to get rid of Esthost as a customer since 2005 but never took steps until it was probably too late.

Shortly after Atrivo ran into serious business challenges in 2008, Rove Digital spokesman, Konstantin Poltev, posted messages on public forums as an apparent damage control attempt. In October 2008, Poltev even attended a North American Network Operators Group (NANOG) conference in Los Angeles to stress Esthost's legitimacy as a company. In fact, before the conference began, Poltev made some forward statements on NANOG's public mailing list:

"Cybercrime is our common enemy."

"I'll be around in the hotel bar should any law enforcement officer wish to arrest me. :)"

"Well, I'm right here in LA—if there's actual evidence, I have no doubt that law enforcement will act. However, I think this is highly unlikely."

Pilosoft Comes to the Rescue

When Atrivo, Esthost, and EstDomains shut down their operations, Rove Digital stopped offering web-hosting and domain-registration services. Rove Digital's rogue DNS network appeared to have suffered a major setback, as hundreds of its rogue DNS servers were suddenly taken offline, reducing its revenue from the DNS botnet to nothing.

After a couple of days, Rove Digital revived its rogue DNS network by using the New-York-based web-hosting company, Pilosoft. Pilosoft was already providing services to Rove Digital and its daughter company, Cernel, for a couple years and had been known for hosting rogue DNS servers until fall 2007.

Atrivo's shutdown appeared to have led Rove Digital to move the core of its rogue DNS C&C network infrastructure to Pilosoft's data center. Unlike Atrivo's data center, the new physical location was hidden from public view, which would make subsequent takedowns more difficult to achieve.

Rove Digital then allegedly acquired more than 100 servers in Pilosoft's data center though only a few purportedly used IP addresses that belonged to the service provider. Most of the rogue servers reportedly used the IP addresses of other networks that belonged to Rove Digital's shell companies such as Cernel and UkrTelegroup as well as to legitimate companies such as Tiscali and Tata Communications. These servers also had Internet access via legitimate companies such as Deutsche Telekom, Tiscali, and Tata Communications though apparently not via Pilosoft.

In actuality, however, their Internet traffic was supposedly first routed via a tunnel away from the New-York-based Pilosoft data center before it went to upstream providers. This tunneling trick probably threw researchers off Pilosoft's scent whenever they tried to check where the Internet traffic to and from Cernel was routed using standard tools such as *traceroute*. As a result, Pilosoft likely did not receive complaints about abuse originating from rogue DNS infrastructure because it did not visibly provide services to Rove Digital. This would also have allowed Rove Digital to contract other upstream providers whenever the need arose without making changes to its core infrastructure and with very little or even no downtime. Moreover, this would have enabled Rove Digital to use provider-dependent IP address ranges from legitimate web-hosting companies such as Tiscali, Tata Communications, and Level 3 Communications for servers in the Pilosoft data center.

We believe Rove Digital chose this particular setup to make takedown efforts harder to carry out.

2009: The Birth of the Nelicash Affiliate Program

In 2009, Rove Digital started an affiliate program called "NewlineCash," also known as "Nelicash," that apparently promoted the installation of DNS changer Trojans and FAKEAV malware in victims' systems, much like AviCash, Rashacash, and many of its other affiliate programs. Unlike the latter affiliate programs, which were probably outsourced to contractors in Russia and the Ukraine, Nelicash was more likely under Rove Digital's direct control.

Nelicash and its successors' management systems expanded even though their script coding appeared to be of poor quality. We believe that most of Rove Digital's advanced coding and Trojan creation requirements were developed by contractors from Eastern European countries. Even if Rove Digital's employees did not excel in writing computer code, they were able to develop novel ways to defraud advertising companies and advertisers on a grand scale and for long periods of time.

2010–2011: From Investigation to Takedown

The Rove Digital investigation—a close collaboration among the FBI, the OIG, as well as Trend Micro and industry partners—began in 2010. The thorough investigation led to the arrest of the main suspects and the takedown of Rove Digital's vast network infrastructure consisting of hundreds of servers in November 8, 2011.

TECHNICAL DATA

This section describes some of the technical data uncovered that supports Rove Digital's heavy involvement in cybercrime.

Tunneling into the Pilosoft Data Center

Atrivo's takedown in fall 2008 likely prompted Rove Digital to move the core of its rogue DNS infrastructure to Cernel's IP address space. Cernel was apparently one of Rove Digital's many shell companies. The new servers were hosted in Pilosoft's data center in New York although these were hidden from public view, making takedowns more difficult to achieve.

Rove Digital then reportedly had about 100 servers in the Pilosoft data center, which used provider-dependent IP addresses from legitimate companies such as Level 3 Communications, Tata Communications, and Tiscali as well as the IP address ranges of the organization's daughter companies, Cernel and UkrTelegroup. As such, using standard routing tools such as *traceroute* would not have identified Pilosoft as an upstream provider.

Rove Digital's servers were very likely physically located in Pilosoft's New-York-based data center. The different types of data indicated that Cernel, UkrTelegroup, as well as some Tiscali and Tata Communications Classless Inter-Domain Routing (CIDR) traffic was tunneled out of Pilosoft's data center first before going to upstream providers such as Tiscali, Tata Communications, and Deutsche Telekom.

Most domain names likely have correct DNS resolutions from rogue DNS servers because these only target a specific set of domain names. Botmasters aim to minimize the disturbance their victims experience so their bots' lifetimes could last longer. That is why their rogue DNS servers queried authoritative name servers in order to send correct DNS resolutions to their victims. Investigations, however, revealed that the back-end IP addresses that sent DNS lookups to authoritative name servers differed from the rogue DNS IP addresses of the front-end servers.

In 2009, it was discovered that the DNS lookups were made by a number of Pilosoft's IP addresses. These IP addresses were the same ones used by Rove Digital's front-end DNS servers until fall 2007. This meant that the DNS traffic was somehow routed from Cernel and UkrTelegroup's IP address ranges, to which the front-end DNS servers were affiliated, to that of Pilosoft. Later, Rove Digital's back-end servers also appeared to use Tiscali's IP addresses, along with those of Level 3 Communications, for a brief period of time. Note, however, that Level 3 Communications was one of the few providers that subsequently stopped providing services to Rove Digital's daughter company, Cernel. This data leads one to suspect that Rove Digital's servers in Pilosoft's data center used multiple virtual interfaces with IP addresses from different ranges and even varying Autonomous System (AS) networks.

Additional data confirmed this. For instance, different IP addresses Rove Digital used in different networks shared the same digital fingerprint. The IP addresses, *69.31.52.15* (Pilosoft AS), *93.188.161.110* (Internet Path Inc.–daughter company of Rove Digital formerly known as "Cernel"–AS), *77.67.83.121* (Tiscali AS), *64.86.5.122* (Tata IP address range), and *67.210.14.56* (Internet Path AS), had the same public Secure Shell (SSH) key. Even though a public SSH key is not a unique fingerprint per se, the similarity strongly confirmed that IP addresses from different networks were bound to interfaces of the same servers in Pilosoft's data center. The public SSH keys of the following 17 special IP addresses in various ranges were discovered to be the same as the SSH key of the Pilosoft IP address, *69.31.52.202*:

- *4.53.82.42*
- *63.218.110.34*
- *64.28.187.1*
- *64.86.5.1*
- *67.210.12.1*
- *67.210.14.1*
- *67.210.15.1*
- *67.214.159.2*
- *77.67.79.70*
- *77.67.83.1*
- *85.255.112.1*
- *93.188.160.1*
- *93.188.161.1*
- *93.188.166.1*
- *93.188.167.1*
- *213.109.72.1*
- *213.200.66.26*

Most of these IP addresses appear similar to those typically assigned to routers. All of these IP addresses may have belonged to the same router. Reportedly, a router in the Pilosoft data center had multiple interfaces that used IP addresses that belonged to several different Rove-Digital-controlled ranges.

Another interesting piece of data was the discovery of so-called *"Multi-Router Traffic Grapher (MRTG)* statistics." *MRTG* is a useful tool for system administrators who monitor traffic and server loads. *MRTG* graphs related to hundreds of Rove Digital servers, which could simply be loaded from a central management system even without authentication, reportedly showed the traffic from a Rove Digital router known as *"apilosoft"* to its upstream providers, including Deutsche Telekom, KDDI, Tata Communications, and Tiscali.

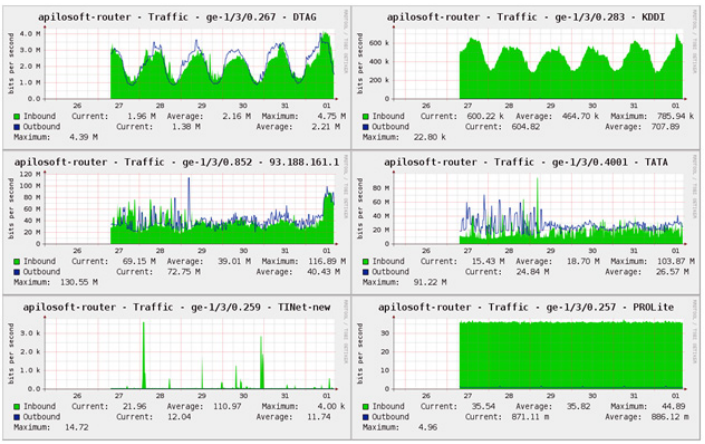


Figure 4. MRTG *graphs for a Rove Digital router's various interfaces*

Based on this information, it can be deduced that Rove Digital's servers, which used IP addresses that belonged to Cernel and UkrTelegroup's ranges as well as provider-dependent ranges from Tiscali and Tata Communications, were located in Pilosoft's data center. As shown in Figure 5, server traffic from Pilosoft's data center was routed through a tunnel in order to obscure the server's true physical location. As such, Pilosoft's involvement in Rove Digital's malicious undertakings was not detected when standard tools such as *traceroute* were used.

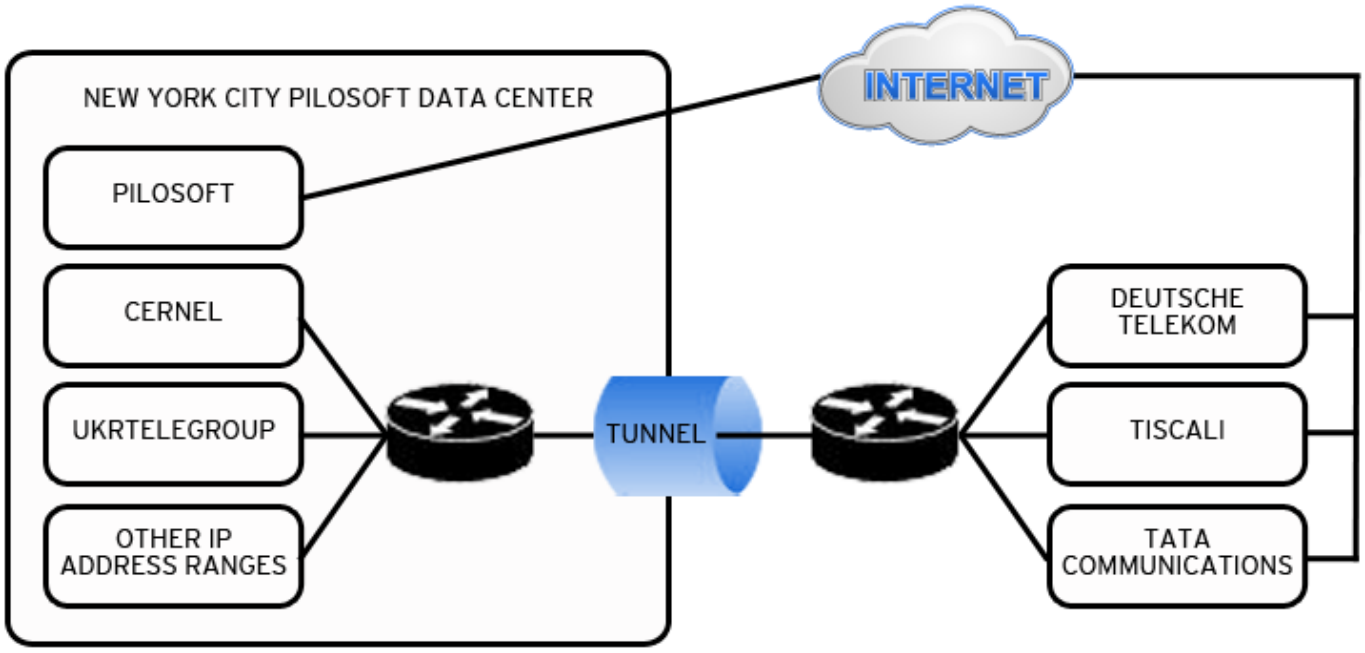


Figure 5. *Rove Digital's server traffic coming from Pilosoft's data center*

Another significant part of Rove Digital's infrastructure was apparently traced to a data center in Chicago.

FAKEAV Malware and the Nelicash Affiliate Program

Rove Digital reportedly often spread DNS changer Trojans along with FAKEAV malware. FAKEAV victims are tricked into buying applications that supposedly detect and remove malware from their systems but actually do not. The FAKEAV business is likely very profitable, as a single license can cost as much as US$100. In fact, we have seen that on some days, Rove Digital sold more than 600 FAKEAV licenses.

In 2005, DNS changer Trojans were bundled with a FAKEAV called *"SpySheriff."* It is not known whether *SpySheriff* was indeed a project of Rove Digital. In 2009 and 2010, however, there was considerable support that Rove Digital was likely spreading its own kind of FAKEAV malware. A schema of the Nelicash affiliate program in May 2009 (see Figure 6) was discovered in one of Rove Digital's main servers. This schema describes Nelicash's server setup.

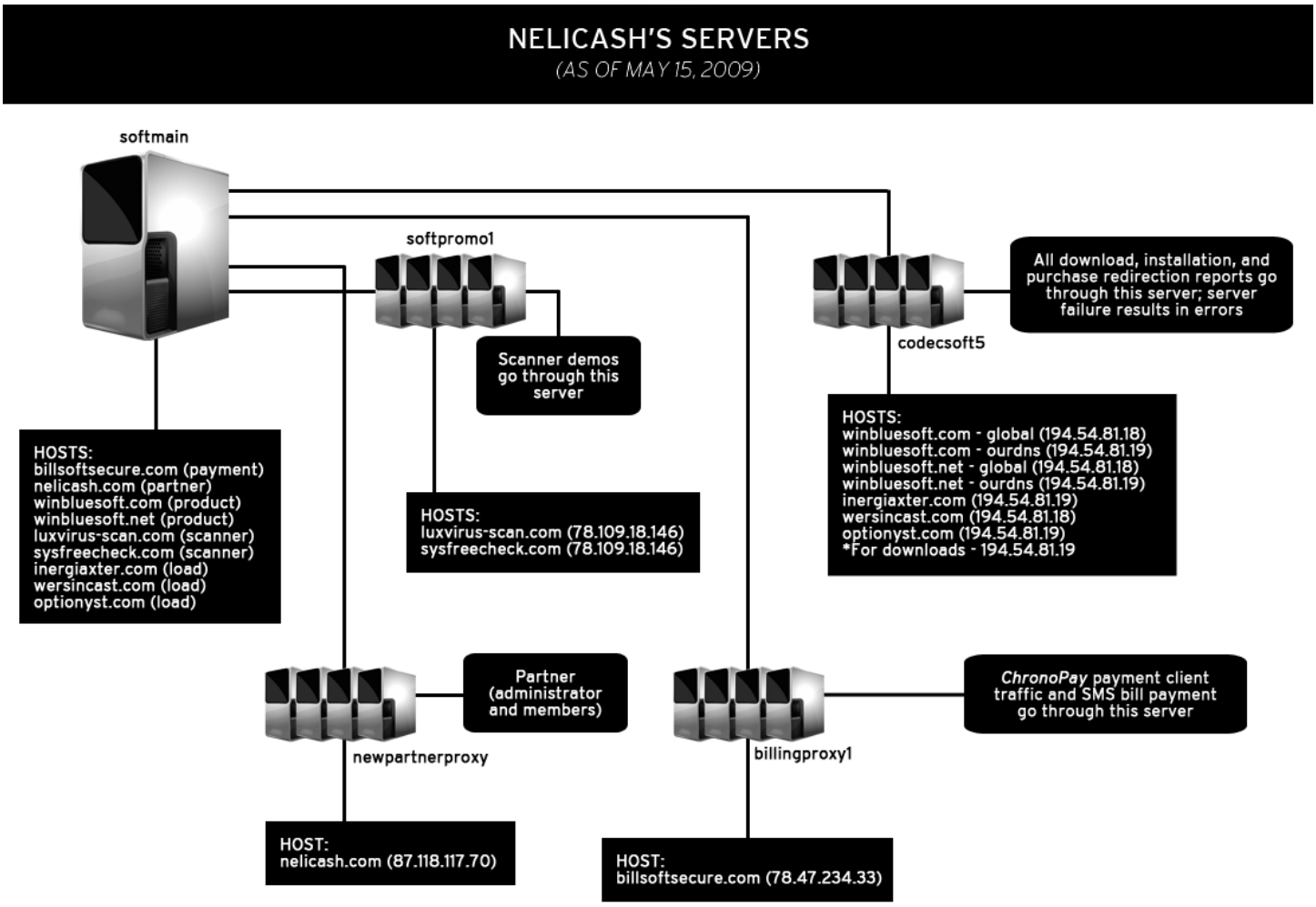


Figure 6. *Nelicash's FAKEAV affiliate program schema (English version)*

Examination of the original PDF and its metadata shows that it may have been written by a certain person known as "Vadim." Although there was reportedly a Rove Digital employee named "Vadim," nobody with such name was arrested on November 8, 2011.

Nelicash's schema appears to show that Rove Digital had a central server (i.e., *softmain)* that served as a back-end server for some of the company's proxy servers. Each of the company's proxy servers appears to have a particular function. *Newpartnerproxy* is, for instance, the site Rove Digital's partners can log in to in order to see their malware campaign statistics. The proxy server, *billingsproxy1,* on the other hand, connects to the *ChronoPay* payment and SMS billing systems. Finally, *softpromo1* displays fake infection warnings on affected users' systems. All of the proxies can be easily replaced by others in the event of termination. All of the important data appears to be stored in the back-end server. Consequently, the proxies could very well just be empty boxes containing hardly any forensic data and of little value for prosecution purposes.

In 2010, the Nelicash affiliate program reportedly used a central back-end system hosted in the Netherlands. Again, the setup comprised a central server with several front-end proxies. This time, however, the system was expanded to more than a dozen proxies in front of the back-end system. Some of the proxies hosted exploits from the *Eleonore Exploit Kit* while others hosted actual DNS changer Trojans and FAKEAV malware. The back-end server also hosted a management system called "*sm*," which was frequently accessed by IP addresses that belonged to Rove Digital's Tartu office and from its VPN servers worldwide. All of the proxies received their data from virtual hosts on the back-end server. Figure 7 shows that the back-end system, *sm*, was probably set up sometime in October 2009.

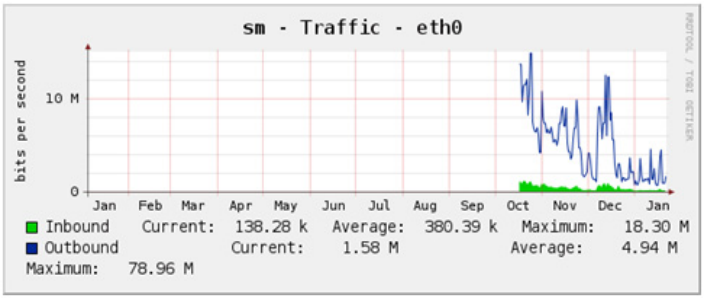


Figure 7. MRTG *graph of Nelicash's management system,* sm

Apart from Rove Digital's production system, it also had a development system called "*smdevel*" (see Figure 8).

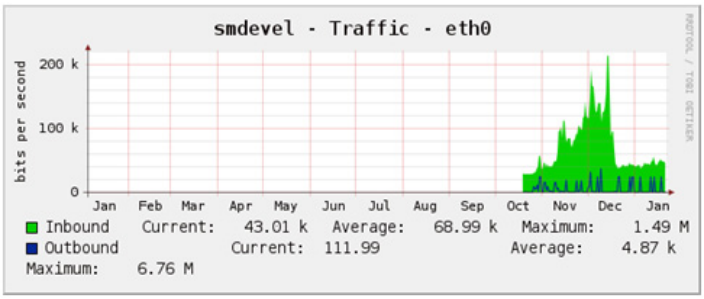


Figure 8. MRTG *graph of* sm's *development system,* smdevel

Rove Digital hosted exploit pages, malware sites, FAKEAV malware, and its central management system on a reverse proxy network. Each function was reportedly hosted on a different front-end system but all of the front-end servers appeared to be proxies that received data from the central back-end system located in the Netherlands.

In the FAKEAV business, it is important for the vendor to allow a certain number of refunds, as they risk getting penalized by major credit card companies for too many charge-backs from unsatisfied customers. Even worse, credit card companies can cancel their service provision. As such, Rove Digital set up a customer support system similar to those of other FAKEAV vendors (see Figure 9). When dissatisfied buyers of Rove Digital's FAKEAV request for charge-backs, they were asked to fill up a form on *trustpaycards.com* explaining why.

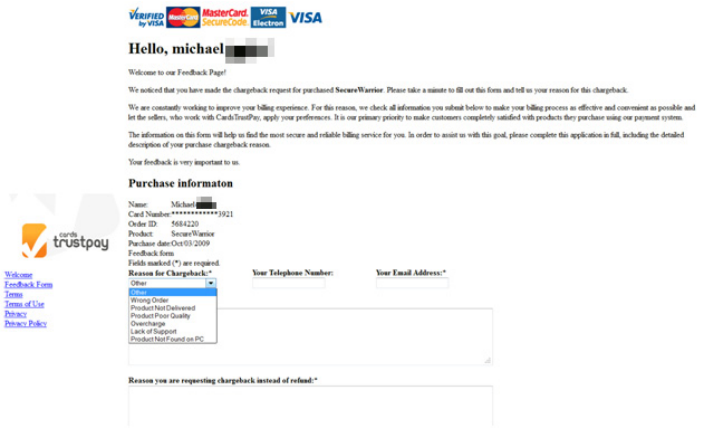


Figure 9. *Rove Digital site where unsatisfied FAKEAV buyers can request for charge-backs*

On another site hosted on Nelicash's proxy network, there was reportedly a customer support system where Rove Digital's employees can reply to emails from FAKEAV victims (see Figure 10). Rove Digital likely carefully addressed complaints so as to dissuade victims from demanding their money back.

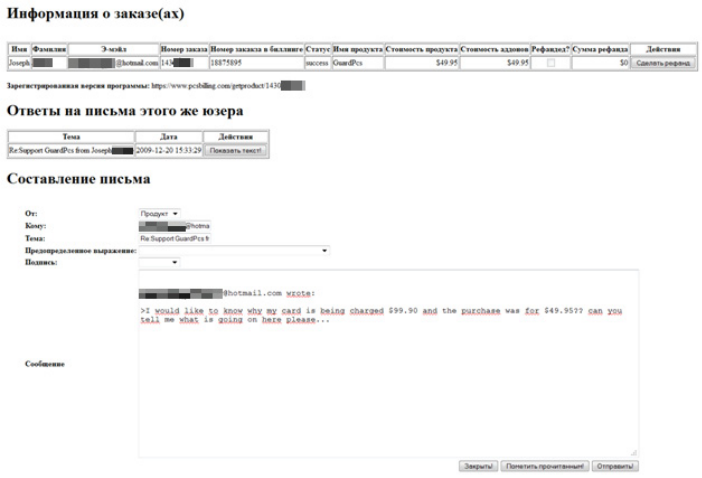


Figure 10. *Email reply from a Rove Digital employee to an unsatisfied FAKEAV buyer*

A test order that was submitted by an individual named Vadim who was apparently not among those who were arrested on November 8, 2011 was also discovered (see Figure 11).

Figure 11. *Test order Vadim submitted*

A test order submitted by Dmitri Jegorov from the Tartu office using what appeared to be his private *Gmail* account was also discovered (see Figure 12). Jegorov was among those arrested on November 8, 2011.

Figure 12. *Test order Jegorov submitted*

Rove Digital apparently promoted various FAKEAV brands. FAKEAV constantly needed to change names, as negative reviews about these appeared in *Google* searches. The following FAKEAV brands are reportedly related to Rove Digital:

- *AntiAdd*
- *AntiAID*
- *AntiKeep*
- *AntiTroy*
- *APCprotect*
- *BlockKeeper*
- *BlockProtector*
- *BlockScanner*
- *BlockWatcher*
- *IGuardPc*
- *KeepCop*
- *LinkSafeness*
- *ProtectPcs*
- *REAnti*
- *RESpyWare*
- *SafeFighter*
- *SafetyKeeper*
- *SaveArmor*
- *SaveDefender*
- *SaveKeeper*
- *SecureFighter*
- *SecureKeeper*
- *SecureVeteran*
- *SecureWarrior*
- *SecurityFighter*
- *SecuritySoldier*
- *ShieldSafeness*
- *SiteAdware*
- *SoftBarrier*
- *SoftCop*
- *SoftSafeness*
- *SoftSoldier*
- *SoftStrongHold*
- *SoftVeteran*
- *SysDefence*
- *SystemFighter*
- *SystemVeteran*
- *SystemWarrior*
- *TheDefend*
- *TrustCop*
- *TrustFighter*
- *TrustSoldier*
- *TrustWarrior*
- *Winbluesoft*
- *Winiguard*

Monitoring System

In August 2009, a Trend Micro sales engineer discovered log files of a Rove Digital monitoring system that were partially indexed by Google's crawlers. As such, anyone could download the log files, as these did not require any password for access. These log files appeared to belong to a Rove Digital system that monitored its network infrastructure's vital systems. It contained email and SMS alerts that were sent out to various Rove Digital employees every time there was an issue, again confirming the company's deep involvement in cybercrime.

DNS CHANGER TROJANS

DNS changer Trojan proliferation was reportedly one of Rove Digital's main activities. DNS changer Trojans discreetly modify systems' settings so these will use foreign DNS servers. These DNS servers can be set up by malicious third parties and translate certain domains into malicious IP addresses. As a result, unwitting victims are redirected to possibly malicious sites. Cybercriminals use a variety of methods to monetize their DNS changer Trojan botnets, including hijacking search results, replacing the ads victims see on legitimate sites, and pushing additional malware.

Rove Digital reportedly owned the largest DNS changer Trojan botnet that has been in existence since at least 2005. A crucial server of Rove Digital, *dns-repos.esthost.com,* could seemingly update all of its rogue DNS servers at once by simply changing some configuration files. On *dns-repos.esthost.com,* a text file called *"domains.txt"* allegedly contained all of the domain names that resulted in resolutions. About 14,000 domains appeared to have gotten rogue DNS resolutions, including the following:

- Major search engine domains such as *Google, Yahoo!, Bing,* and *Ask.com*
- Advertising companies' domains such as *Google Ads, Overture,* and *DoubleClick*
- Software update domains of vendors such as Microsoft and Adobe as well as of major security vendors
- C&C domains for malware such as TDSS Trojans
- Pornography domains
- Dating site domains
- Name server domains of web-parking service providers
- Some high-traffic domains such as *wikileaks.org*

Rove Digital apparently also tried to hijack several domains to see if these would convert well.

The name servers of web-parking service providers reportedly received rogue resolutions as well. Web-parking service providers park domain names that are not actively used. These domains generally do not have any content. However, due to the enormous volume of parked domain names, companies can profit off them by displaying ads visitors who happen to land on parked domains may be interested in. Because some web-parking name servers received rogue DNS resolutions for DNS changer Trojan victims, millions of parked domain names were allegedly hijacked.

We did not see much supporting data that Rove Digital used DNS changer Trojans to steal victims' identities. In fact, the only incident wherein we saw an apparent login credential theft involved users of *vkontakte.ru, Facebook's* Russian equivalent. This showed that Rove Digital did not shy away from targeting Russian-speaking Internet users. Not targeting Internet banking users was probably a deliberate choice, as attempts to redirect online banking sessions to foreign sites would likely have drawn much more law enforcement attention.

Rove Digital's DNS changer Trojan victims would not have been able to correctly resolve domain names in order to update their Microsoft OSs or security software. This meant that for a long time, they did not have the latest software patches and were, therefore, vulnerable to malware and exploit attacks. It is thus likely that their systems could be easily infected with other malware. Rove Digital would have monetized secondary malware infections by hijacking their C&C domain names. This reportedly started in 2005 when domain name, *toolbarpartner.com,* got rogue resolutions. This domain name pointed to a C&C server related to the infamous *Googkle.com* mass infection. *Googkle.com* malware used *toolbarpartner.com* to install new Trojans in victims' systems. Rove Digital apparently knew about this and hijacked the update URL that was regularly loaded by *Googkle.com* malware victims. Automated *toolbarpartner.com* clicks turned into automated clicks on Rove-Digital-chosen ads.

A more recent example featured TDSS Trojan C&C domains. TDSS Trojans are advanced Trojans used to install other malware in victims' systems, for browser hijacking, and for stealing ad clicks. Rove Digital's rogue DNS server's reportedly hijacked TDSS C&C domains in order to steal the clicks that TDSS Trojans already stole.

Rove Digital actually used TDSS Trojans to spread DNS changer Trojans. It apparently defrauded some of its TDSS partners by resolving TDSS domains to IP addresses under its own control.

Hijacking Search Results

Hijacking search results is a particularly lucrative and easy way to capitalize on legitimate search engines' success. This is why rogue DNS servers have been resolving key search engine sites such as *Google*, *Yahoo!*, *Bing*, and *Ask.com* to foreign IP addresses for years.

For DNS changer Trojan victims, a search still works as usual. However, whenever they click a search result or a sponsored link, they are instead directed to a foreign site so Rove Digital could monetize their clicks. The infrastructure needed to hijack search results was rather large (see Figure 13).

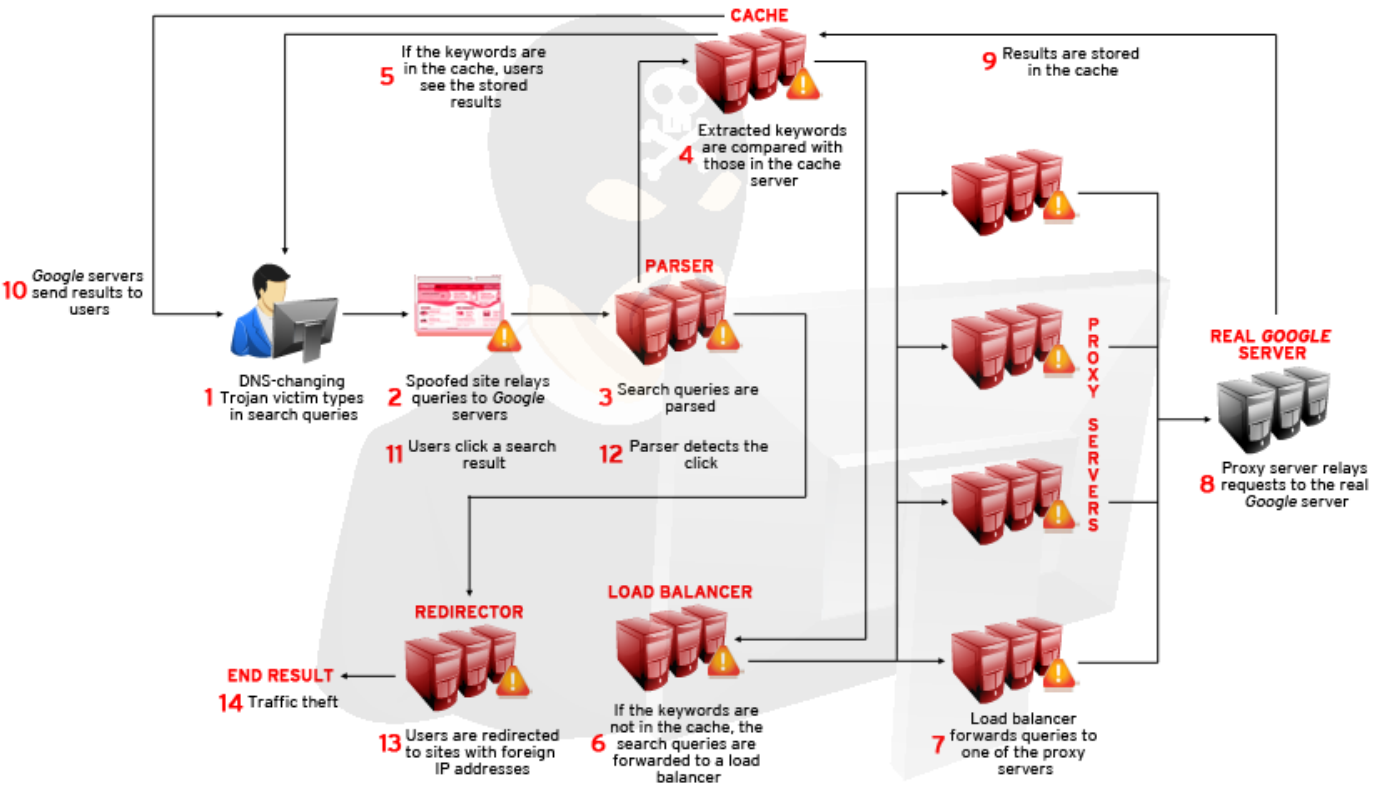


Figure 13. *Rove Digital's infrastructure for hijacking search results*

Replacing Site Ads

Another lucrative use of rogue DNS servers is ad replacement. DNS changer Trojan victims who visit legitimate sites such as *nytimes.com* or *amazon.com* thus see foreign ads on these pages instead of legitimate ones. Rove Digital earns money from ad impressions and clicks while the site owner loses money, as he/she does not get paid for ads that were actually intended to be shown to users. This advertising trick worked very well for Rove Digital in that its DNS changer Trojan victims would not be able to see that the ads have been replaced. Even the sites' layout looks fine and is not affected (see Figure 14).

Figure 14. Amazon.com *as seen by a DNS changer Trojan victim*

In the beginning, Rove Digital allegedly replaced legitimate ads with graphic ads promoting male-organ-enhancement pills. This tactic, however, caught victims' attention, as they saw the same kind of explicit ads everywhere.

Soon after, Rove Digital reportedly contracted a Canadian company called "Clicksor" to deliver ads promoting a wide variety of products and services. In this case, Rove Digital had to pose as a real advertising company via the establishment of daughter companies (see Figure 15). Clicksor should have realized there was something wrong with the impressions and clicks it obtained from these companies.

Figure 15. *Site of one of Rove Digital's daughter companies*

Rove Digital reportedly spread DNS changer Trojans via various social engineering techniques and the exploitation of legitimate sites that promoted special video content though these required users to download and install special codecs in order to view the promised videos. These codecs were apparently Trojans that altered users' DNS settings and, in many cases, also installed rootkits.

In recent years, DNS changer Trojans increasingly spread via the exploitation of legitimate sites. Table 2 shows the statistics for the *Eleonore Exploit Kit* that a Rove Digital affiliate uses to spread DNS changer Trojans. As shown, about 13% of visitors' systems were successfully infected with DNS changer Trojans using the *Eleonore Exploit Kit*.

Table 2. Eleonore Exploit Kit *statistics for one of Rove Digital's affiliates*

Exploit	Infection Count as of October 1, 2010		Infection Count as of October 23, 2010	
None	151,400	86.66%	178,567	86.98%
JAVA TC	3,258	1.86%	12,598	6.14%
JAVA SMB	4,749	2.72%	3,874	1.89%
HCP	1,737	0.99%	415	0.20%
PDF COLLAB	1,908	1.09%	1,679	0.82%
PDF PRINTF	179	0.10%	202	0.10%
PDF FONT	1	0.00%	0	0.00%
FLASH 9	496	0.28%	291	0.14%
PDF LIBTIFF	5,844	3.34%	6,679	3.25%
QUICKTIME	0	0.00%	1	0.00%
Hacking attempt	8	0.00%	0	0.00%
Hacking attempt	3,541	2.03%	0	0.00%
IEPEERS	195	0.11%	111	0.05%
Hacking attempt	23	0.01%	0	0.00%
Hacking attempt	28	0.02%	0	0.00%
MDAC	1,306	0.75%	863	0.42%
Hacking attempt	0	0.00%	0	0.00%
Hacking attempt	0	0.00%	0	0.00%
FLASH 10	9	0.01%	10	0.00%

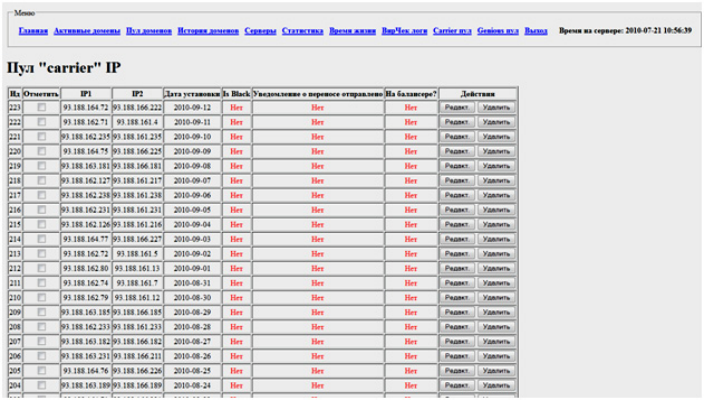
The following table lists the number of victims whose systems were apparently infected by DNS changer Trojans after visiting legitimate websites on a certain day in December 2010. The statistics, however, are for a single affiliate only.

Table 3. *Number of DNS changer Trojan victims of a Rove Digital affiliate*

Referer	Infection Count
ads.mbrgames.com	1,969
www.codecguide.com	1,612
www.doubleviking.com	840
www.ftv.com	446
twitter.tempointeraktif.com	314
www.pr-inside.com	205
ssl.ftv.com	199
www.download.hr	151
–	87
zeus.flexserving.com	82
www.lesopia.net	64
multibrands.me	63
codecguide.com	38

The Rove Digital management system reportedly displayed planning details for the deployment of new rogue DNS servers. Each day, it spread a new DNS changer Trojan hard-coded with a unique pair of rogue DNS IP addresses. So, given a DNS changer Trojan victim, Rove Digital would be able to know which day his/her system was infected by looking at which rogue DNS server he/she used for domain name resolutions.

Rove Digital also purportedly continuously monitored if the DNS changer Trojans it spread were detected by security companies. Log files of a script that periodically checked for vendor detections were reportedly discovered. Trojans that were already being detected by vendors were apparently no longer used to infect other victims' systems. These were replaced by so-called "clean" or still-undetected DNS changer Trojans.


Меню

Главная | Активные домены | Пул доменов | История доменов | Серверы | Статистика | Время жизни | BinCheck логи | Carrier пул | Generic пул | Выход | Время на сервере: 2010-07-21 10:56:39

Пул "carrier" IP

Ид	Отчистить	IP1	IP2	Дата установки	Is Black	Уведомление о переносе отправлено	На балансере?	Действия
223		93.188.164.72	93.188.166.222	2010-09-12	Нет	Нет	Нет	Редакт. Удалить
222		93.188.162.71	93.188.161.4	2010-09-11	Нет	Нет	Нет	Редакт. Удалить
221		93.188.162.235	93.188.161.235	2010-09-10	Нет	Нет	Нет	Редакт. Удалить
220		93.188.164.75	93.188.166.225	2010-09-09	Нет	Нет	Нет	Редакт. Удалить
219		93.188.163.181	93.188.166.181	2010-09-08	Нет	Нет	Нет	Редакт. Удалить
218		93.188.162.127	93.188.161.217	2010-09-07	Нет	Нет	Нет	Редакт. Удалить
217		93.188.162.238	93.188.161.238	2010-09-06	Нет	Нет	Нет	Редакт. Удалить
216		93.188.162.231	93.188.161.231	2010-09-05	Нет	Нет	Нет	Редакт. Удалить
215		93.188.162.126	93.188.161.216	2010-09-04	Нет	Нет	Нет	Редакт. Удалить
214		93.188.164.77	93.188.166.227	2010-09-03	Нет	Нет	Нет	Редакт. Удалить
213		93.188.162.72	93.188.161.5	2010-09-02	Нет	Нет	Нет	Редакт. Удалить
212		93.188.162.80	93.188.161.13	2010-09-01	Нет	Нет	Нет	Редакт. Удалить
211		93.188.162.74	93.188.161.7	2010-08-31	Нет	Нет	Нет	Редакт. Удалить
210		93.188.162.79	93.188.161.12	2010-08-30	Нет	Нет	Нет	Редакт. Удалить
209		93.188.163.185	93.188.166.185	2010-08-29	Нет	Нет	Нет	Редакт. Удалить
208		93.188.162.233	93.188.161.233	2010-08-28	Нет	Нет	Нет	Редакт. Удалить
207		93.188.163.182	93.188.166.182	2010-08-27	Нет	Нет	Нет	Редакт. Удалить
206		93.188.163.231	93.188.166.211	2010-08-26	Нет	Нет	Нет	Редакт. Удалить
205		93.188.164.76	93.188.166.226	2010-08-25	Нет	Нет	Нет	Редакт. Удалить
204		93.188.163.189	93.188.166.189	2010-08-24	Нет	Нет	Нет	Редакт. Удалить

Figure 16. *Rove Digital's plan for deploying new rogue DNS servers*

Apparently, as shown in part by Rove Digital's log file for February 18, 2010, a TDSS Trojan it spread was no longer clean at 13:40. This Trojan was already being detected as a piece of malware. As such, Rove Digital replaced the binary with an undetected Trojan at 14:40.

THE TAKEDOWN

"... if there's actual evidence, I have no doubt that law enforcement will act. However, I think this is highly unlikely."

– Konstantin Poltev, Esthost spokesman, October 13, 2008

On November 8, 2011, the coordinated effort of the FBI, the OIG, and the Estonian Police Force took down Rove Digital's network infrastructure. This was probably one of the biggest cybercrime ring takedowns ever. The Internet Systems Consortium (ISC) based in Redwood City, California, replaced Rove Digital's rogue DNS servers in Pilosoft's data center with legitimate ones that correctly resolved user requests. This was necessary because suddenly taking down the rogue DNS infrastructure could cause millions of Rove Digital victims to lose Internet access.

A court appointed the ISC to provide DNS services to Rove Digital's DNS changer Trojan victims for 120 days. At the same time, Réseaux IP Européens (RIPE), the regional Internet registry that allocates IP addresses in Europe, complied with a Dutch Police order to freeze Rove Digital's European IP address ranges. These steps likely prevented Rove Digital's accomplices who were not arrested on November 8, 2011 from moving the rogue DNS infrastructure to another location and continue to exploit the company's large pool of DNS changer Trojan victims. RIPE apparently decided to comply with the order of the Dutch Police, a truly historic step that will serve as a precedent for future cases. On the other hand, the RIPE Network Coordination Centre (NCC), an independent nonprofit organization of users of IP ranges, decided to fight RIPE's decision in court. As of this writing, there has been no resolution of the case.

The Rove Digital takedown was complicated, as many different parties were involved and a lot of work was necessary. When these types of takedown and related arrests are made public, people often wonder why it takes so long. In this instance, suffice it to say that the Rove Digital matter was indeed very complicated; involved a large infrastructure; was international in scope; and required input, coordination, and support from many parties.

Trend Micro provided relevant information to investigators related to Rove Digital's huge and ever-changing infrastructure, which was spread worldwide. The ISC, an industry partner, also played an important role in replacing Rove Digital's rogue DNS servers with legitimate ones on the night the suspects were arrested and its infrastructure was taken down. Ultimately, the enforcement agencies had to perform much of the vital work needed to support any successful arrest and prosecution.

Figure 18. *Bits of abuse gallery*

THE SUSPECTS

All of the suspects but one have been arrested and charged with wire fraud conspiracy, computer intrusion conspiracy, wire fraud, and computer intrusion. The leader, Vladimir Tsastsin, was charged with money laundering as well. If successfully convicted, all of them can face up to tens of years in prison.

This section provides brief profiles of the Rove Digital employees.

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.

Andrey Taame

The only suspect who appears to remain at large. We believe Taame lives in Russia and was probably a Rove Digital contractor for an extended period of time. He has been described as the "brains" behind the technical aspects of the DNS changer botnet monetization. He allegedly designed Rove Digital's huge network, which hijacked *Google* searches, and acted as middleman so the company could sell the traffic its DNS changer Trojan victims generated to legitimate companies. He also ran companies such as Rbtechgroup.com, Onwa Ltd., Lintor Ltd., Crossnets, and Uttersearch.

Anton Ivanov

Ivanov was a Rove Digital programmer. Like the other suspects, he also appears to have received email alerts whenever Rove Digital encountered infrastructure problems.

Disclaimer: The information contained in this research paper was obtained using industry-recognized open source research techniques, which rely on publicly available information.

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud