Global Information Assurance Certification Paper

There's No Going it Alone: Disrupting Major Cyber Crime Rings (a Case Study)

GIAC (GSEC) Gold Certification

Author: John Garris, jgarr@sans.leemail.me
Advisor: Robert Vandenbrink
Accepted:

Abstract

The identification and eventual disruption of a sophisticated criminal enterprise, requiring on-the-fly problem solving and groundbreaking international collaboration, offers a model of how an international cooperative effort can succeed. The efforts that ultimately brought down Rove Digital, an Estonian-based criminal operation that compromised millions of computers, provides just such an example. The approach taken by law enforcement from several countries, coupled with the important roles played by security researchers, can be built upon to address burgeoning threats that can only be tackled cooperatively.

1. Introduction

On July 8th, 2015, Vladimir Tsastsin pled guilty to charges relating to his development and long-term management of a criminal enterprise that conducted a complex, highly profitable Internet fraud scheme involving millions of compromised computers located in over 100 countries. Tsastsin's guilty plea helps bring to a close the United States' prosecution of six Estonian nationals, including Tsastsin, who had been extradited to the United States from Estonia following extensive coordination and notable cooperation between the two governments. A seventh individual indicted by the U.S. Government, Andre Taame, remains at-large (USAO-SDNY, 2015).

The telling of this law enforcement success story would be entirely deficient, however, if the central role played by a large number of cybersecurity researchers and IT Security organizations were absent or relegated to footnotes. The partnerships amongst private sector individuals and organizations, alongside the efforts of law enforcement agencies from several countries, were critical in assessing and identifying this complex fraud scheme and bringing about its eventual demise. Not only did this effort require a significant amount of skill and committed willingness to work cooperatively, a multi-disciplinary approach was vital in formulating and executing a strategy to minimize the disruption to more than four million victims of these crimes (the number of victims was much higher when measured over the lifespan of this criminal operation) (Trend Micro, 2012).

One particularly impressive aspect of this coalition is that it worked cooperatively for approximately five years. This largely informal coalition was central to developing the information needed to successfully execute arrest and search warrants simultaneously in Estonia and the United States. In his press conference announcing the arrests of the six Estonians, Mr. Preet Bharara, United States Attorney for the Southern District of New York, noted the critical investigative work of the NASA OIG, FBI, and the Estonian Police and Border Guard Board, as well as the National High Tech Crime Unit of the Dutch National Police Agency. Mr. Bharara made a point of highlighting the many private sector partners that were part of the overall effort, including Georgia Tech University, Internet Systems Consortium, Mandiant, National Cyber-Forensics and

Training Alliance, Neustar, Spamhaus, Team Cymru, Trend Micro, University of Alabama at Birmingham, and members of a group of subject matter experts known as the DNS Changer Working Group (DCWG) (USAO-SDNY, 2011).

An accurate recounting of the many contributions by the specific cybersecurity organizations recognized by Mr. Bharara in his 2011 press conference is constrained by the limited amount of publicly available reporting produced by some of these participants. However, viewed in a different light, the limited information published by these individuals and groups is noteworthy in itself. The fact that such a large grouping of participants, many with commercial profit making pressures, either published little with regards to their involvement, or fastidiously withheld key information at critical junctures in the investigation, is evidence that participants placed larger community concerns above self-interest. Given the growing torrent of reporting on a wide range of cybersecurity events over the course of the past several years, the fact that the vast majority of cybersecurity organizations conduct themselves so responsibly may oftentimes be lost amidst the clatter over the most recent high-profile intrusion event.

2. Background

The IT Security firm Trend Micro reported noting a significant number of malware infections that involved the systematic altering of the DNS resolutions of infected systems staring in 2005. Over the subsequent five years, Trend Micro worked cooperatively with several public and private organizations investigating these activities. Trend Micro's Forward-Looking Threat Team was able to piece together a fairly comprehensive picture of the mechanisms and key organizational structures comprising the larger criminal enterprise behind these activities (Trend Micro, 2012). According to their research paper on the matter, Trend Micro found that a collection of companies, primarily registered in Estonia, were central to the larger criminal activities responsible for infecting approximately 10 million systems over several years. The principal company, or at least the one chosen as the moniker for the overall criminal efforts, was Rove Digital. Rove Digital's roots have actually been traced back to many other companies, notably Esthost, EstDomain, and Cernel. While fully active, these accredited

domain registrars directly supported "Bullet-Proof" hosting services via data centers largely based in New York, San Francisco, and Estonia. In addition to domain registration, Esthost's customers used their hosting services to run any number of criminal activities, such as command-and-control servers for botnets, phishing sites, malware dump-sites, and DNS changer Trojans. As Esthost's hosting services gained popularity with various criminal elements, their infrastructure and overall operations grew significantly (Trend Micro, 2012). This growth in activity was along several fronts, to include DNS registrations, and a growing wave of malicious activities via various ISPs. These operations were vital to the rapid growth of a global network of infected personal use computers primarily through tricking individuals into downloading and installing fake anti-virus software, as well as fake video codec software. The infection of personal computers was a significant source of revenue for Rove Digital, but more importantly, it was a means to build what would become an extensive network of compromised systems. Those infected systems would become central to a highly lucrative fraud scheme to hijack advertising revenue (Trend Micro, 2009).

2.1. Rove Digital – Clear Warning Signs

As noted earlier, Rove Digital (Rove) grew out of a wide range of criminal activities supported by the various services hosted under Esthost, EstDomains and related front companies. Although it did not appear to be actively used as a corporate entity relating to Internet-based criminal activity until around 2005, Ravelli's (2009) earlier research found that the formal incorporation of Rove occurred in Tartu, Estonia, in 2002. The documentation of incorporation notes that Rove's business would center on software development, and the initial capitalization claimed at the time of incorporation was 10,000,000 EEK (Note: the Euro replaced the Estonia Kroon (EEK) in 2011). Before Rove's illegal activities were widely revealed, its growth and financial success were noted publicly in Estonian news outlets. For one, *Äripäev* Business Daily, an Estonian news service specializing in reporting on Estonian business topics, listed Rove as the "Estonian IT company of the year in 2007" (Ravelli, 2009). Clear indications that Rove's founder had a proclivity for criminal activity is evident in Tsastsin's 2008 criminal conviction by Estonian criminal courts. This conviction stemmed from an earlier arrest

of Tsastsin by Estonian authorities for a credit card fraud and money laundering scheme where fictitious refunds were made to credit cards and those refunds withdrawn via ATMs. Ultimately, Tsastsin was found guilty by an Estonian court of committing these crimes and was sentenced to time he had already served since his initial arrest (Estonian Public Broadcasting, 2014). Looking at this setback from Tsastsin's perspective, it is likely that the more troubling aspect of his conviction was the temporary disruption dealt to Rove's burgeoning operations. As noted in their July 25, 2013, pre-sentencing brief to the U.S. Circuit judge overseeing the trial of the Rove defendants, a lead Southern District of New York Assistant U.S. Attorney prosecuting this case noted that based on Tsastsin's 2008 conviction, the Internet Corporation for Assigned Names and Numbers ("ICANN") "…revoked EstDomains' accreditation as a registrar, meaning that any IP address or domain name registered through EstDomains, for all practical purposes, would not exist on the Internet" (NY Southern Dist Court, 2013).

Although Rove would experience an additional setback in 2008 through the loss of a U.S. based ISP, these events proved only temporary impediments for Tsastsin. Once the U.S. and Estonian criminal investigation got underway, it became clear Tsastsin had been busy working to overcome the damage of his conviction by shifting Rove's assets under a newly formed corporate body. As related in the Southern District of New York U.S. Attorney's request to Estonian Authorities for assistance, "Rove Digital" was acquired by Tamme Areudus OÜ (Incorporated) on September 19, 2008. This acquisition was obviously a method to paper-over the true ownership of Rove, as Tamme Areudus lists the address of "Lai 6, Tartu, Estonia," as their headquarters -- the same address as Rove. If the timing of the transfer and location of the new business entity were not proof enough this was all a sham orchestrated by Tsastsin in light of his 2008 conviction, all the major board members of Tamme Areudus Inc were Tsastsin's close relatives (NY Southern Dist Court, 2010).

2.2. Continued Adaptation and Sleights of Hand

By way of framing the major architectural features of the enterprise, it's useful to understand Rove's key touchpoints for Internet access. Through their extensive research of Rove and its related companies, Trend Micro was able to stitch together an

impressively detailed overview of the key infrastructure used to further and grow Rove's profitable criminal activities. According to Trend Micro, one of Rove's key Internet Service Providers (ISP) included Atrivo, located at the time in San Francisco, CA. Another important ISP for Rove was Pilosoft, located in New York. Rove's principal Estonia based ISP was Elion (Trend Micro, 2012). A very helpful overview of Rove's framework for their click-fraud operations can be seen in the graphic developed by Trend Micro, found in Appendix A.

Atrivo, also known as "Intercage," eventually became infamous within the cybersecurity community for hosting all manner of malicious activities. In its earlier years of operation, one of its largest customers was the "Russian Business Network (RBN)," known for being a preferred hub for many cyber criminals. As Atrivo drew more unwanted attention from cybersecurity practitioners and law enforcement, RBN began to disperse its operations to other ISPs in an apparent risk reduction move (Krebs, 2008). In his article on Atrivo, Krebs (2008) reported that different portions of Atrivo's business operations specialized in particular services for their highly suspect customer base. For example, Atrivo's "Hostfresh" provided routing through Hong Kong and China. With the departure of RBN, it appears Atrivo became increasingly dependent on Rove's business, as even around the time RBN was migrating their business operations elsewhere the security firm iDefense identified Atrivo as being one of the single largest hosts of malicious activity on the Internet (Krebs, 2008).

The hue and cry of the cybersecurity community continued to build to the point Atrivo's upstream service providers took notice and began to distance themselves from Atrivo. Shortly after the security company HostExploit published detailed evidence that approximately 78 percent of Atrivo's hosted services where clearly of the malicious variety, the upstream providers of Global Networks, Bandcon, and WVFiber, ceased business with Atrivo. At this point, Atrivo's only remaining upstream provider was Pacific Internet Exchange (PIE). Spamhaus, a nonprofit cybersecurity company specializing in subscription based anti-spam data feeds, had been collecting extensive information on Atrivo for some time as well, and continued to observe hostile activity emanating from Atrivo after PIE was the only remaining upstream provider. Spamhaus'

engagement, benefiting from the heft of its reputation in the cybersecurity community, appears to have been the knock-out blow for Atrivo. Not long after Spamhaus placed PIE on its blocklist in 2008, PIE dropped Atrivo, essentially causing Atrivo to go dark (Hruska, 2008).

Despite 2008 being a challenging year for Rove operations, with Tsastsin's conviction, ICANN's revocation of EstDomain's listings, and loss of Altivo's services, Tsastsin and his staff displayed the ability to adapt and innovate. Now that Rove's Pilosoft based operations were elevated in relative importance, Tsastsin had to work to preserve this critical asset. Apparently learning from their experiences via Altivo's closure, they developed methods to help them lower their profile while still growing their highly profitable illicit click-fraud business. According to Trend Micro's reporting (2012), Rove's principal approach to lowering their profile, and to help obfuscate the importance of their Command & Control (C&C) servers and DNS infrastructure hosted at Pilosoft, was to use VPN tunneling. Rove used VPNs within their networks to tunnel their suspect traffic away from Pilosoft before it went to Pilosoft's upstream providers, thus avoiding one fatal flaw in Rove and RBN's earlier use of Altivo. It should also be pointed out that Trend Micro's study of Rove developed evidence that Elion, Rove's Estonia-based ISP, had rebuked Rove earlier, so Rove's options for reliable ISP access were not limitless (Trend Micro, 2012).

Through Rove's extensive use of VPN tunneling, Pilosoft appears to have received few complaints associated with Rove's malicious DNS infrastructure. Thus, Rove was able to buy themselves additional time as security researchers attempted to identify the critical nodes controlling a growing amount of DNS Changer related activity. Perhaps more importantly, this sleight-of-hand provided Rove access to a vital veneer of legitimacy by giving them the flexibility to contract with other mainstream providers, such as Level-3 Communications. These sources of dependable bandwidth were needed to reliably leverage the millions of infected systems Tsastsin manipulated via Rove C&C servers physically hosted at Pilosoft (Trend Micro, 2012).

True of most any relatively young company, Rove's financial success was largely dependent on growing market share and establishing viable avenues for revenue

generation. With the disruption of his Atrivo based operations, Tsastsin appears to have been forced to take note of the pitfalls associated with the unwanted attention inherent in being the proprietor of Bullet Proof hosting services. It's unclear precisely what Rove digital's long-term strategic business plans were, or whether or not Tsastsin seriously used such management tools. What is clear is that Rove's early revenue generation efforts were diversified and included the infection of millions of personal computers with DNS Changer malware (Note: DNS Changer allows attackers the ability to alter the routing of traffic to and from a victimized system). Rove's diversified operations shifted steadily towards more specialization, namely towards click-fraud operations (Trend Micro, 2009).

Spamhaus took note of the DNS Changer malware related activity of Rove at least as early as 2007 when one of Rove's spoofed Google Ads sites appeared on Spamhaus' list of sites to block. This site proved to be just one small piece of an extensive DNS infrastructure that was constructed and manipulated to steal advertisement revenues by directing unwitting victims to ads Rove controlled (Spamhaus, n.d.). As noted in Trend Micro's assessment of Rove's evolving operations (2012), Rove very quickly shifted much of their core operations, most significantly the C&C servers used to manage their click-fraud efforts, to Pilosoft hosted services not long after Altivo's demise. By leveraging the extensive botnet they had developed through the infection of millions of systems with the DNS Changer malware, they had the means for generating large volumes of online fraudulent advertisement activity. This botnet also provided a very effective approach for avoiding detection by the major online advertisement companies (Trend Micro, 2012). After all, given that the victims whose systems comprised Rove's botnet were unwitting to the fact their traffic was being hijacked, their day-to-day Internet activities would be very difficult to distinguish from legitimate user generated advertisement activity.

2.3. Rove's Click-Hijacking – a Windshield Tour

According to Trend Micro's research, Rove had the largest botnet in existence for several years. This network, controlled principally via the C&C structure hosted at Pilosoft, was reasonably well engineered. The thoughtfulness of the architects of Rove's

C&C systems is evident in their apparent ability to manage all their rogue DNS servers through one or two configuration files. This span of control allowed Rove to serve up altered traffic to systems infected with DNS Changer so that they could redirect the results for major search engines such as Google, Yahoo, and Bing. Impressively, Rove was believed to have been able to manipulate the millions of infected systems they controlled so they could serve up altered search results and DNS resolutions for approximately 14,000 unique domains (Trend Micro, 2012). The results of the multinational investigation revealed Rove's capabilities to have been even greater.

In order to more fully appreciate Rove's click-fraud operations, it is useful to view the activity from the perspective of one of the millions of victims whose system was infected with DNS Changer malware. In the indictment of Tsastsin and six of his crew filed in U.S. Circuit Court, the Assistant U.S. Attorney describes a number of examples of how a victimized user's online activities were hijacked via Rove's DNS Changer malware. Broadly, the fraud involved the hijacking of selected portions of a user's Internet activities, notably search results. When an infected user searched for a particular word or phrase using a major on-line search engine, such as Yahoo.com, the results presented to the victim would be altered so as to provide results that when clicked on would generate revenue for Rove through one or more of its advertising contracts. This hijacking activity encompassed both user-generated searches, as well as for sponsored links (US Dist Court –SDNY, 2010).

Specific examples in the indictment also include advertisement replacement fraud, which required a more sophisticated approach than simply substituting legitimate search results for those crafted by Rove. In this more subtle approach, Rove would render the majority of a requested webpage to a victim accurately, but replace specific advertisements found on that webpage with their own. For example, when a DNS Changer victim requested the Wall Street Journal on May 31, 2010, the majority of the Wall Street Journal webpage would be rendered accurately. In actuality, the legitimate website would be presenting an American Express advertisement for their "Plum Card." The altered results received by an individual using a system infected with DNS Changer, at least on May 31, 2010, would display an advertisement for "Fashion Girl LA" where

the "Plum Card" advertisement was intended to appear (US Dist Court –SDNY, 2010). Even simple views of this altered page, referred to as "impressions" in on-line advertisement parlance, would generate revenue for Rove. More revenue would be generated when users actually clicked on content for advertisement that Rove controlled. Individually, these impressions and clicks on links and images sponsored by various advertisers were frequently only fractions of pennies. However, as seen through the lens of law enforcement's eventual insight into Rove's financials, those pennies and fractions of pennies certainly added up.

3. Where's a Cop When You Need One?

To quickly recap, the collective efforts of an informal alliance of cybersecurity professionals had succeeded in amassing a fairly detailed picture of much of Rove's evolving network of criminal activities. These efforts eventually succeeded in temporarily disrupting Rove's operations, most notably through the shuttering of Atrivo. However, Rove quickly adapted and their subsequent illegal activities only grew. It became clear to many of these security professionals that the active involvement of law enforcement was becoming increasingly important as a potential avenue for targeting Rove's ever more expansive and sophisticated operations.

The affidavit submitted on March 1st, 2012, to the U.S. District Court of the Southern District of New York (USDC-SDNY) in support of a search warrant to be executed on the premises of Pilosoft for specific Rove servers offers interesting insight into U.S. law enforcement's formal engagement in this matter. The affidavit notes the central role of "numerous private-sector researchers" and a "NASA Agent" in the development of the facts used to support the application for the search of Pilosoft (US Dist Court –SDNY, 2010). Interestingly, the involvement of NASA can be found in the earliest court filings supporting the investigation and eventual conviction of Tsastsin and his crew. Affidavits submitted to support applications for several search warrants filed in the USDC-SDNY during the course of U.S. law enforcement's investigation of Rove point to October 14, 2009, as the date when U.S. federal law enforcements efforts started in earnest. Regularly noted in most of the affidavits submitted by the FBI agents

investigating Rove is the foundational statement, "I have discussed this investigation in detail with a Special Agent of the Office of the Inspector General of the National Aeronautics and Space Administration (the "NASA Agent"), and have learned the following:" (US Dist Court –SDNY, 2010). The active involvement of the FBI in the investigation of such significance seems obvious. Why then is a NASA agent playing such a prominent role in kicking-off and pushing forward U.S. law enforcement's investigation of a criminal enterprise that, at least at that time, controlled the largest malicious botnet in existence?

A review of the many filings with the U.S. Circuit Court in support of the U.S. Government's case reveals the prominent role played by the NASA Office of the Inspector General appears to have stemmed from two aspects of the case. First, the NASA agent so widely referenced in court documents obviously played a very significant role in conducting the nuts and bolts of the investigation. This can be seen in how frequently he personally submitted affidavits in support of search warrant applications and protective orders, or was referenced in the affidavits of others. The court documents also show that without the rich competencies and extensive capabilities of the FBI, as well as the support of cybersecurity researchers, the U.S. case would have likely never succeeded. The second reason for NASA's prominence in the facts of the investigation is potentially much more relevant to public-private cyber security efforts in the future. It appears NASA, at least very early on in the investigation, was the only source of solid information regarding the adverse effects of Rove's DNS Changer infections. In the application to execute the search warrant at Pilosoft, NASA is offered as the only clear victim, including estimates of monetary loss, of Rove's deliberately diffused and obfuscated activities. In his affidavit requesting court approval for the warrant, the FBI agent reports that on October 26, 2009, the NASA Agent conducted searches of NASA's database for computer security incidents and found, at the time, 65 NASA systems that were infected with malicious software controlled from Rove's C&Cs hosted at Pilosoft (US Dist Court –SDNY, 2010).

In order to better understand the triggers for law enforcement's engagement in this matter, it's useful to appreciate how complaints and information are typically triaged

by investigative agencies and U.S. Attorney Offices as a means to prioritize the use of limited resources. This prioritization, as logic would lead most to assume, attempts to factor in traditional measures of significance, such as victim loss and broader societal effects. In fact, this recurring triage of complaints and issues is so central to day-to-day law enforcement operations that methodologies have been memorialized. The core methodology for U.S. Attorneys to assess whether or not to accept or decline cases is found in the Department of Justice U.S. Attorneys' Manual (U.S. DoJ, n.d.). As the investigation of Rove continued to build upon the earlier work of computer security researchers, the scale and impact of Rove operations would have eventually met the threshold of nearly any U.S. Attorney's office. However, the initial evidence of NASA's victimization seems to have provided a very useful foundation for U.S. law enforcement to justify the initial resource investments needed to aggressively pursue this case.

Perhaps the more telling evidence of NASA's role in law enforcements' efforts to target Rove comes from Tsastsin himself. As he was fighting both Estonian criminal charges and extradition to the U.S. from his Estonian jail cell, Tsastsin went on something of a public relations push. During an interview by a reporter from the Estonian daily *Pealinn*, Tsastsin said he could trace his plight back to the fact his software, which he was arguing caused no true harm, had been found on NASA systems. He told the reporter when referring to the genesis of his current plight, "the initiative came from NASA" (Estonian Public Broadcasting, 2014). Ironically, Tsastsin's extensive efforts to avoid detection through VPN tunneling and other obfuscation techniques began to unravel when just 65 NASA systems were hijacked into Rove's botnet of over 4 million systems. Tsastsin apparently just didn't appreciate the risk that entailed it at the time. Actually, given the size and dynamic nature of his operations, neither her nor his staff likely even took notice.

Law enforcement's involvement brought important authorities to the longer standing efforts of security researchers, such as the ability to seek and execute search and arrest warrants. Law enforcement's involvement also provided previously unavailable tools to gain insight regarding the money flows into and out of Rove and its many front companies. These uniquely governmental authorities and tools, including subpoenas and

letters rogatory, were also very important in developing a clearer picture of Rove's various assets. Although the true origins of the catchphrase "Follow the money," popularized in the motion picture "*All the President's Men,*" is questioned by scholars (Safire, 1997), that catchphrase has been widely embraced by law enforcement as a tried and true method for zeroing in on even the most complex of fraud schemes. Armed with subpoenas, warrants and assistance from Estonian and Dutch law enforcement, the growing cadre working the Rove case were now equipped to truly "follow the money."

Referenced earlier, the previously sealed 43-page indictment filed by the U.S. Attorney's Office for the Southern District of New York is a rich source for understanding the key aspects of the U.S. Government's case against Tsastsin et al. Understandably, the indictment was originally sealed at the request of the U.S. Attorney's Office as a precautionary step to help preclude alerting their targets before they could be arrested in Estonia. Given the targets were all located overseas, another key aspect of the indictment is that it would serve as an important foundation for subsequent requests for assistance to Estonian authorities. Without an indictment, important aspects of the Multilateral Assistance Treaty between the U.S. and Estonia would be unavailable to U.S. law enforcement (MLAT, 2000). Most noteworthy is the sheer amount of information in the indictment, as it foreshadowed the strong merits of the U.S. Government's case.

An indictment must be written in a clear and concise manner so as to provide only the essential information necessary to address the individual charges being brought by the prosecutor (U.S. DoJ, n.d.). Thus, despite its length and the large number of charges outlined therein, the indictment essentially represents short summaries of the information thought necessary for a judge to meaningfully assess the charges listed. With that in mind, Appendix B offers an eye-opening sampling of Rove's financial transactions during 2009 and 2010. Extracted from the indictment, Appendix B represents how the Government supported several of its charges, specifically counts 7 through 27. These transactions provide a keyhole view of Rove's impressive revenue stream, as well as a sense of the size of its operation through some of the payments Tsastsin made to ISPs. The Rove accounts referenced include those provided by JP Morgan Chase, New York ("The Manhattan Data Center-Chase Account"); the Furox-USD account in Denmark to

the "Chicago Data Center"; and a corporate account for Onwa held in Cyprus, another of Tsastsin's front companies. After viewing this snapshot of financial transactions, there is little wonder how the Government was able to assert a minimum figure of $14 million in illicit gains and assets that would be subject to seizure and forfeiture in the case against Tsastsin et al (US Dist Court –SDNY, 2010). In actuality, the illicit wealth amassed by Tsastsin far exceeded $14 million. A strong indicator of that can be found in the Assistant U.S. Attorney's memorandum to the court in opposition to pretrial motions filed by the attorneys for several of the Rove defendants. In countering the defense's argument that the search conducted on Rove's Pilosoft assets was overly broad, the Government's attorney framed her argument, in part, by referencing an interesting assertion made by the defense, "…whereas the affidavit alleged approximately $25 million in fraud, the agents seized documents relating to all $1.2 billion of assets managed by the target company." (US Dist Court – SDNY, 2015). In this case of course, Rove is "the target company."

3.1 The Takedown.

The cooperative efforts of Estonian, U.S. and Dutch law enforcement continued to build upon the work of the security researchers who had brought forward their concerns regarding Rove's extensive criminal activities. The investigation not only developed a growing understanding of the contours of Rove's financials, the tentacles of Rove's business operations, previously obscured by their use of VPN tunneling and numerous front companies, came into much clearer view as well.

Guided by a key discovery uncovered through Trend Micro's earlier research, the FBI executed a search warrant on Pilosoft targeting records associated with IP address 69.31.87.98. This IP address was leased at the time to a company called SBP Group, which was found to be yet another front company used by Tsastsin. However, this server proved to be critical in expanding law enforcement's understanding of Rove's operation (US Dist Court –SDNY, 2010). This server was found to be the primary mechanism used by Rove to control traffic to the immense number of domains Rove was regularly hijacking (Trend Micro, 2012). As outlined in the U.S. Government's request for assistance from Estonian authorities, the subsequent analysis of this server showed it

hosted a program used to re-route the traffic of millions of infected users to approximately 19,900 domains. Conveniently, at least from the perspective of building the case against Tsastsin et al., was the email traffic found on the server. These emails reflected back and forth conversations between the defendants regarding how they regularly handled the day-to-day challenges of managing such a large global operation (US Dist Court –SDNY, 2010).

In preparation for the takedown of the Rove enterprise, U.S. law enforcement laid the groundwork by obtaining court orders to freeze Rove's many assets, to include numerous systems required to operate that enterprise. As seen in a request for a protective order filed by the Southern District of New York's U.S. Attorney's office leading up to the take down operations, Rove's overall operations had demonstrated impressive growth and complexity. In addition to listing a few thousand IP addresses owned by Rove at the time, the post-indictment protective order listed Rove's forfeitable property maintained by the following providers: Colosecure, Chicago, IL; ThePlanet, Houston, TX; Multacom Corp, Canyon, CA; Layered Technologies, Plano, TX; GlobalNet Access, Atlanta, GA; as well as seven other locations (US Dist Court –SDNY, 2011).

On November 8th, 2011, U.S. and Estonian law enforcement personnel executed coordinated search and arrest operations at multiple locations within the U.S. and Estonia. Six of the seven indicted defendants, Vladimir Tsastsin, age 31, Timur Gerassimenko, age 31, Dmitri Jegorov, age 33, Valari Aleksejev, age 31, Konstantin Poltev, 28, and Aanton Ivanov, 26, were arrested and taken into custody in Estonia by the Estonian Police and Border Guard. (USAO-SDNY, 2011).

The extensive international coordination and successful simultaneous execution of numerous search and arrest warrants in multiple time zones and international jurisdictions was an impressive accomplishment by any measure. However, the groundbreaking cooperation and creativity demonstrated to minimize the impact on millions of victims, whose Internet access would effectively cease when the takedown occurred, was quite impressive as well.

John Garris, jgarr@sans.leemail.me

Initiated largely through the initiative of a supervisory FBI agent, the DNS Changer Working Group (DCWG) was formed through the participation of an ad hoc group of cybersecurity professionals who were familiar with the widespread impact Rove's DNS Changer malware infections had had. The DCWG was formed primarily to try and mitigate and remediate the adverse effects that the takedown of Rove's DNS servers would have on the approximately 4 million systems infected at the time of the planned law enforcement operations (Todd, 2012). As described in the DCWG website, it is an ad hoc group of subject matter experts that includes members from organizations such as Georgia Tech, Internet Systems Consortium, Mandiant, National Cyber-Forensics and Training Alliance, Neustar, Spamhaus, Team Cymru, Trend Micro, and the University of Alabama at Birmingham (DCWG, n.d.).

The court order transferring temporary control of the core Rove infrastructure seized at Pilosoft, NY, and Colosecure, IL, to the Internet Systems Consortium (ISC) provides useful insight into the legal framework used to grant ISC temporary authority to take any and all steps reasonably necessary to administer the "Replacement DNS Servers." In crafting the order approved by the judge, the U.S. Attorney's Office of the Southern District of New York, took care to request ICS be granted the authorities necessary to, "…identify computers that are infected with malicious DNS Changer software (The DNS Changer Malware) by collecting the IP addresses that query the Replacement DNS Servers, the network ports associated with those requests, and the date and time of those requests…" Of note, the court order also set important limitations in that ICS could not capture any content of the victims' communications. Another important constraint was that the receivership and its underlying authorities had a finite lifespan. In the case of ICS' receivership, it was ultimately set to expire on July 9th, 2012 (US Dist Court –SDNY, 2012). Shortly after the Rove takedown and arrest of Tsastsin et al., the DCWG took over the day-to-day monitoring of the "Replacement DNS Servers," operated by ICS under authority of the court order.

DCWG members regularly assessed the traffic related to the millions of DNS Changer infections and provided input for possible mitigation strategies. The DCWG's efforts complemented a media campaign the FBI launched to increase awareness of DNS

Changer infections, to include information on how to remediate those infections (Todd, 2012). Using the approximate baseline of 4 million systems infected with DNS Changer at the time of Rove's demise, and the last set of data reported by DCWG, these remediation efforts appear to have been largely successful. According to the DCWG website's daily count of unique IP addresses of systems infected with DNS Changer, the count was down to 303,867 by June, 11th, 2012 (DCWG, n.d.). Viewed less optimistically, the fact that over 300 thousand systems remained infected despite all these efforts highlights the challenges of pushing proper security hygiene to individual users.

4. Conclusion

This case study demonstrates how, faced with a persistent and consequential cybersecurity challenge, a coalition of individuals and organizations from the public and private sectors can successfully navigate past the challenges that often serve as impediments for such efforts to succeed.

In her analysis of public-private collaboration in cybersecurity partnerships, Germano (2014) found that public-private partnerships were essential in addressing national and global cybersecurity threats. Germano's (2014) examination of this issue identified five primary barriers to successful partnerships necessary to address these threats. Those barriers include: (1) issues surrounding trust and control of incident response; (2) questions about obligations regarding disclosure and exposure; (3) the evolving liability and regulatory landscape; (4) challenges faced in the cross-border investigation of cybercrime; and (5) cross-border data transfer restrictions that impede the ability of companies to respond nimbly to cyberthreats and incidents (p. 3). The Rove takedown effort successfully overcame at least three of these traditional barriers.

The shear duration and ultimate success of the collaborative efforts to extinguish Rove's activities speaks volumes with regards to the trust that obviously existed among the participants. The fact that law enforcement was a recipient of much of the early information developed by security professionals may have helped, as it side-stepped many of the restrictions to sharing information derived from search warrants and other legal process. Trust was likely enhanced in the eyes of law enforcement by the fact

security researchers were responsibly restrained with regards to what they published through critical phases of the criminal investigation. Also, the FBI's innovative and open approach to mitigating down-stream effects that would occur after the takedown of Rove's DNS network likely helped continue to engender trust with private sector participants.

Traditional disclosure concerns associated with victimized corporations wrestling with both remediation of the incident and considerations of adverse publicity were not as pronounced in Rove. The losses NASA OIG was able to tally with regards to DNS Changer infections after being approached by cybersecurity researchers was very useful in moving past loss thresholds applied when assessing the potential value of law enforcement's engagement. As noted by Germano (2014), cyber investigations are inherently complex, and some of that complexity often stems from the need to navigate international jurisdictional considerations. Fortunately for U.S. law enforcement, Tsastsin and his crew physically resided in Estonia, a country with a ratified Multi-lateral Assistance Treaty with the U.S. That is not to imply the coordination and negotiation with Estonia was not deliberative and procedurally involved. However, the fact that a ratified treaty between the U.S. and Estonia existed was extremely helpful. Contrast the successful outcome of the Rove investigation with so many other criminal investigations where the subjects are believe to be residing in Russia, China, or other countries with whom the U.S has no such treaty. As a final point to support the preceding observation, Andre Taame, a Russian citizen, is the only member of Rove indicted by the U.S. who remains at-large.

References

A Cybercrime Hub. (2009). Trend Micro Inc. -- Threat Research. White Paper. Retrieved from http://www.trendmicro.co.uk/media/wp/cybercrime-hub-whitepaper-en.pdf

DNS Changer Working Group – About/Contact Information (n.d.). Retrieved from: http://www.dcwg.org/aboutcontact/

Estonian National Pleads Guilty In Manhattan Federal Court To Charges Arising From Massive Cyber Fraud Scheme That Infected Millions Of Computers Worldwide. USAO-SDNY. Department of Justice. (2015). Retrieved from http://www.justice.gov/usao-sdny/pr/estonian-national-pleads-guilty-manhattan-federal-court-charges-arising-massive-cyber

Germano, Judith. (2014). Cybersecurity Partnerships: A New Era of Public-Private Collaboration. The Center on Law and Security. New York University School of Law. Retrieved from: http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf.

Hruska, Joel. (Sep 23, 2008). Bad seed ISP Atrivo cut off from rest of the Internet. Ars Technica. Retrieved from http://arstechnica.com/security/2008/09/bad-seed-isp-atrivo-cut-off-from-rest-of-the-internet/

Krebs, Brian. (Aug 28, 2008). Report Slams U.S. Host as Major Source of Badware. Washington Post. Retrieved from http://voices.washingtonpost.com/securityfix/2008/08/report_slams_us_host_as_major.html

Krebs, Brian (2015). Cybercrime Kingpin Pleads Guilty. Krebs on Security. Retrieved

John Garris, jgarr@sans.leemail.me

from http://krebsonsecurity.com/2015/07/cybercrime-kingpin-pleads-guilty/

Mutual Legal Assistance – Treaty Between the United States of America and Estonia. Signed April 2nd, 1998; ratified Oct 20th, 2000.

New York Southern District Court. Re: U.S. v. Tsastsin et al. Case No. 1:11-cr-00878. SDNY USAO Briefing Memo to the Court "Re: *United States* v. *Valeri Aleksejev*, S2 11 Cr. 878 (LAK)," dtd: July 25, 2013. Retrieved via Public Access to Court Electronic Records (*PACER*).

New York Southern District Court. Re: U.S. v. Tsastsin et al. Case No. 1:11-cr-00878. Indictment. "*United States v. Vladimir Tsastsin, Andre Taame,…"* dtd: Nov 1st, 2011. Retrieved via Public Access to Court Electronic Records (*PACER*).

New York Southern District Court. Re: U.S. v. Tsastsin et al. Case No. 1:11-cr-00878. Request for Assistance to the Central Authority of Estonia in the Investigation of Computer Intrusion Activity in the United States by Rove. dtd: Dec 6th, 2010. Retrieved via Public Access to Court Electronic Records (*PACER*).

New York Southern District Court. Re: U.S. v. Tsastsin et al. Case No. 1:11-cr-00878. Post-Indictment Protective Order. "Re: *United States* v. *John Doe 1, et a;"* dtd: Nov 3rd, 2011. Retrieved via Public Access to Court Electronic Records (*PACER*).

New York Southern District Court. Re: U.S. v. Tsastsin et al. Case No. 1:11-cr-00878. Affidavit in support of a search warrant for the premises of Pilosoft, 55 Broad St., New York, New York, as it pertains to IP Address 69.31.87.98, dtd: March 1st, 2010. Retrieved via Public Access to Court Electronic Records (*PACER*).

New York Southern District Court. Re: U.S. v. Tsastsin et al. Case No. 1:11-cr-00878.

John Garris, jgarr@sans.leemail.me

"Government's Memorandum of Law In Opposition to the Pretrial Motions of Defendants Timur Gerassimenko, Dmitri Jegorov and Konstantin Poltev", filed: Feb 4th, 2015. Retrieved via Public Access to Court Electronic Records (*PACER*).

New York Southern District Court. Re: U.S. v. Tsastsin et al. Case No. 1:11-cr-00878. Letter Rogatory from the U.S. Department of Justice to the Central Authority of Estonia. Subject: "Request for Assistance in the Investigation of Computer Intrusion Activity in the United States by ROVE DIGITAL, TAMME ARENDUS OÜ…". dtd: December 6th, 2010. Retrieved via Public Access to Court Electronic Records (*PACER*).

Operation Ghost Click – The Rove Digital Takedown. (2012). Trend Micro Inc. Research Paper. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_rove_digital_takedown.pdf

Public-private effort against cyberattacks could become a model for online safety. Pittsburgh Post-Gazette. (Nov 18, 2012). Retrieved from http://www.post-gazette.com/businessnews/2012/11/18/Public-private-effort-against-cyberattacks-could-become-a-model-for-online-safety/stories/201211180217

Ravelli, Erich. "Rove Digital - Finally Gone?" *InfoSecurity*. N.p., 6 Sept. 2009. Retrieved from http://www.arvutikaitse.ee/rove-digital-kas-loplikult-lainud/

Register of Known Spam Organizations (ROKSO): Rove Digital - The Spamhaus Project. (n.d.). Retrieved from http://www.spamhaus.org/rokso/evidence/ROK8745/rove-digital/main-info

Safire, William. "Follow the Proffering Duck." *New York Times*. 3 Aug 1997. Retrieved

John Garris, jgarr@sans.leemail.me

from http://www.nytimes.com/1997/08/03/magazine/follow-the-proffering-duck.html

US Case Against International Clickjacking Defendant May Be Compromised. Estonian Public Broadcasting. (2014, April 25). Retrieved from http://news.err.ee/v/scitech/1a7eb606-eedd-47d1-83b6-d7c67b54e232

U.S. Department of Justice. (n.d.). United States Attorneys' Manual. Section 9-27.230 – Initiating and Declining Charges—Substantial Federal Interest. Retrieved from http://www.justice.gov/usam/usam-9-27000-principles-federal-prosecution#9-27.230

U.S. Department of Justice. (n.d.). United States Attorneys' Manual – Criminal Resource Manual. Section 214 – Drafting Indictments and Informations. Retrieved from http://www.justice.gov/usam/criminal-resource-manual-214-drafting-indictments-and-informations

United States Attorney's Office – Southern District of New York. (2011). Manhattan U.S. Attorney Charges Seven Individuals with Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business [Press release]. Retrieved from http://oig.nasa.gov/press/pr2012-A.pdf

Appendix - A
Rove's Approach to Search Hijacking

Graphic of Rove Digital's infrastructure for hijacking the search results of its victims. (Source: Trend Micro's whitepaper "Operation Ghost Click – Rove Digital's Takedown)

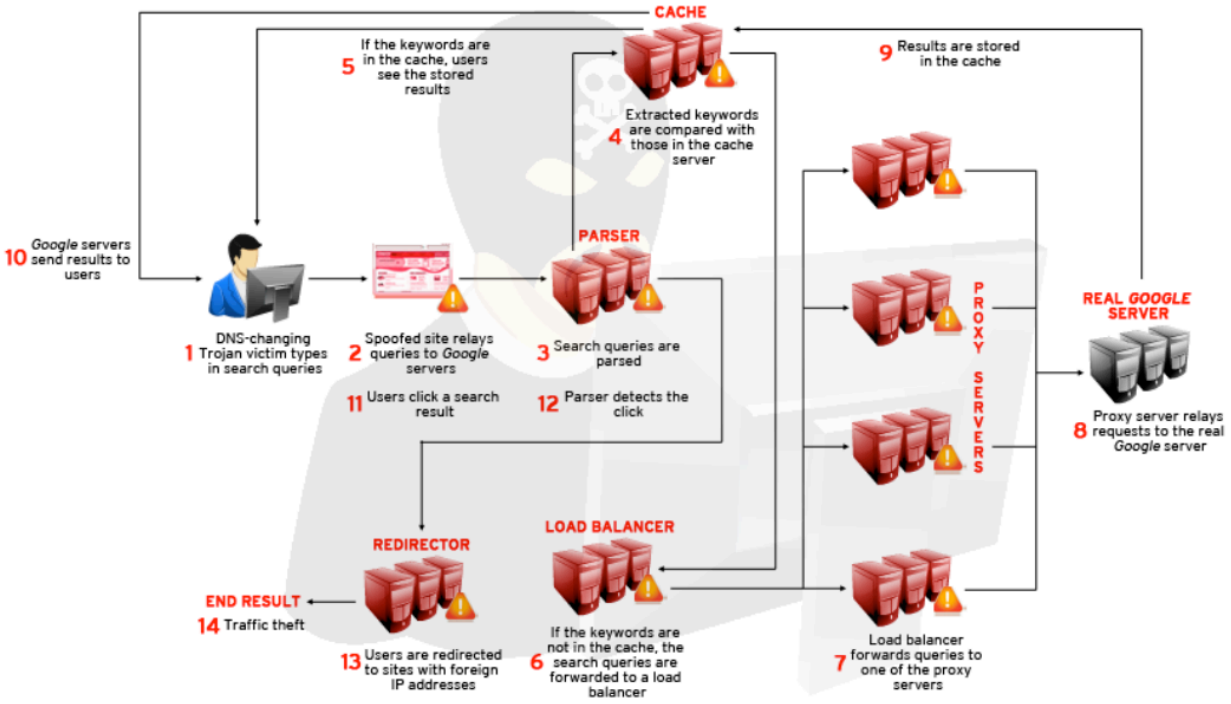

Figure 13. *Rove Digital's infrastructure for hijacking search results*

John Garris, jgarr@sans.leemail.me

Appendix - B
A Glimpse into Rove's Financials

Spreadsheet used in Nov 1, 2011 (then sealed) indictment of Tsastsin et al
(Source: U.S. District Court Southern District of New York)

Case 1:11-cr-00878-LAK Document 4 Filed 11/01/11 Page 30 of 43

COUNT	DATE	WIRE TRANSFERS FROM ACCOUNT IN THE NAME OF:	AMOUNT OF WIRE TRANSFER (USD)	TO ACCOUNT IN THE NAME OR FOR THE BENEFIT OF:
7	3/13/2009	Rove Digital	41,814.00	Chicago Data Center
8	4/3/2009	Rove Digital	25,060.71	Manhattan Data Center
9	5/5/2009	Rove Digital	17,397.20	Chicago Data Center
10	5/14/2009	Rove Digital	24,048.00	Manhattan Data Center
11	5/20/2009	Furox	750,000.00	Charles Schwab & Co.
12	6/5/2009	Rove Digital	11,346.00	Chicago Data Center
13	7/29/2009	Rove Digital	10,621.00	Chicago Data Center
14	9/18/2009	Rove Digital	23,646.00	Chicago Data Center
15	11/28/2009	Furox	780,000.00	Onwa (Cyprus)
16	1/20/2010	Furox	150,000.00	Onwa (Cyprus)
17	2/11/2010	Furox	160,000.00	Onwa (Cyprus)
18	3/11/2010	Furox	210,000.00	Onwa (Cyprus)
19	5/6/2010	Furox	500,000.00	Onwa (Cyprus)
20	6/2/2010	Furox	30,100.00	M.H.V.
21	6/28/2010	Furox	300,000.00	Onwa (Cyprus)
22	7/19/2010	Furox	120,000.00	Onwa (Cyprus)
23	9/7/2010	Furox	140,000.00	Onwa (Cyprus)
24	9/21/2010	Furox	100,000.00	Onwa (Cyprus)
25	12/14/2010	Furox	180,000.00	Onwa (Cyprus)
26	12/21/2010	Furox	33,332.58	Chicago Data Center
27	12/23/2010	Furox	91,000.00	Onwa (Cyprus)

(Title 18, United States Code, Sections 1957 and 2.)

John Garris, jgarr@sans.leemail.me