The Business of Cybercrime
A Complex Business Model

Focus Report Series

January 2010

A Trend Micro White Paper | January 2010

I. *Executive Summary*

As online crime has grown more prevalent, consumer confidence has plummeted. Unlike the old days when hackers created viruses to be mischievous, modern-day malware authors create threats primarily to make a profit. As the "Underground Economy" has grown and flourished, cybercriminals have developed new methods for tricking victims into downloading Trojans. These scams are amazingly lucrative, with profits totaling in the millions per year. Many perpetrators hail from Eastern Europe where cybercrime is rampant and considered business as usual. Canadian pharmacy spam, rogue antivirus (AV), and others are part of a well-organized business model based on the concept of affiliate networking. In the case of cybercrime, products sold via affiliate marketing are anything but legitimate—such as click fraud and credit card details—lucrative but also illegal.

Hundreds of affiliates operate "pay-per-install" or "installs for cash" programs in which a criminal organization enlists an army of workers to drive traffic to malware-serving websites. Workers are paid a commission for every "install achieved". Trend Micro security researchers documented one affiliate who generated $300,000 from rogue AV installs in only one month. Installs receive different valuations according to location and residential broadband customers in the U.S. and Western Europe are popular targets.

The pay-per-install business model often mimics the business world. A hierarchy based on levels of involvement keeps crime bosses hidden and each affiliate group has a structure that consists of "departments" with each handling a variety of functions. For example, affiliates are recruited just like in the business world, lured by the promise of beautiful women, fancy cars, and luxury goods. Criminal organizations also hire technically savvy programmers to develop sophisticated malware ranging from data-stealing Trojans to rogue AV software. Most are rewarded handsomely, compared to usual wages in their area.

Just as legitimate companies hire search engine optimization (SEO) firms to market online, so too do criminal affiliates—referred to as blackhat SEO. Web users visit these sites and contract malware via drive-by download or by clicking on a video, resulting in a Trojan infection. In addition to sophisticated marketing programs, pay-per-install businesses have established customer support centers to help rogue AV customers. Deceived customers—thinking they paid for legitimate AV software—call in to these centers for "help" with their systems.

Within the area of finance, pay-per-install organizations operate sophisticated, well-hidden, financial transactions using legitimate merchant accounts and receiving actual credit card payments. Ironically, cybercriminals also excel at security. In addition to proactively developing new binaries to evade pattern-based antivirus detection, some Russian websites offer malware scanning. These criminal organizations also spend a great deal of time and money building redundant systems and architectures. The Russian Business Network (RBN), one of the largest, most sophisticated botnet syndicates, and others have learned from coordinated disconnections of bulletproof hosting providers, that engaging smaller hosting providers spread out globally is a better way to diversify operations.

By some accounts the bad guys are winning. At this point, consumers do not play an active role so most crimes go unreported. Law enforcement is actively involved but efforts are fragmented. Also, "bad actors" that support cybercrime are notoriously difficult to track down and shut down.

Many stakeholders are interested in reducing the impact of global cybercrime; however, no one organization can make a significant impact against cybercrime by itself. Ad hoc efforts work only partially and are typically short-lived. Instead, a coordinated, multi-stakeholder approach is required to share information and strategies. For example, the Conficker Working Group, the Anti-Phishing Working Group, FIRST (Forum of Incident Response and Security Teams), and regional CERTs (Community Emergency Response Teams) help participants network and learn the latest strategies while developing relationships that help fight cybercrime throughout the world.

Recent large-scale cybercriminal wins, such as the Heartland data breach in early 2009, create a critical need for adaptable security techniques and technologies that deliver better protection. Antivirus software alone is insufficient; however, reliable security software with a web reputation support, such as the Trend Micro™ Smart Protection Network™ infrastructure, provides more effective protection to fight cybercrime.

II. *The Growth of Cybercrime*

Unfortunately for consumers, cybercrime appears to be the new normal for anyone who uses the Internet to work, send email, shop or just read the news—a large majority of the developed world. Cybercrimes are crimes committed on a computer network, especially the Internet, to steal a person's identity, sell contraband, stalk persons, or disrupt operations with malevolent programs or malware. As online crime grows more prevalent and increasingly more sophisticated, consumers are beginning to react. Consumer confidence worldwide is at abysmal levels due to rampant, unchecked criminal activity on the Internet. According to European news site, V3.co.uk**,** nearly three-quarters of UK consumers believe that the recession has put them at greater risk of identity theft and related crimes, according to the latest biannual Security Index Report from UNISYS. The Security Index Report, which measures the level of security concern among respondents, rose 20 per cent from a figure of 125 a year ago to 150 in 2009.[i]

According to the latest biannual Security Index Report from UNISYS, the level of security concern among respondents rose 20 per cent from a figure of 125 a year ago to 150 in 2009.

According to the 2008 Internet Crime Report, published by the Internet Crime Complaint Center (IC3), from January 1, 2008 through December 31, 2008, 275,284 complaints were filed online with IC3. This figure represents a 33.1 percent increase compared to 2007 when 206,884 complaints were received.ii In addition, the number of websites hosting malicious software is rising rapidly according to recent statistics from Dasient, a group of former Googlers who have banded together to offer services that help websites prevent malware infection. According to Dasient, more than 640,000 websites and about 5.8 million pages are infected with malware, which is nearly double an estimate that Microsoft provided in April 2009. At the same time, the Google blacklist of malware infected sites has more than doubled in only one year, registering as many as 40,000 new sites in one week. Dasient identified more than 52,000 web-based malware infections, bringing the total to more than 72,000 unique infections logged by the company since it launched its malware analysis platform earlier this in 2009.[iii]

THE BUSINESS OF CYBERCRIME

Unlike the old days when hackers created viruses to be mischievous and to "show they could," modern-day malware authors create threats primarily to make a profit. As the "Underground Economy" has grown and flourished into a multi-billion dollar industry, cybercriminals have developed new methods for tricking Internet users. Popular examples include "Canadian pharmacy" spam, which accounts for an amazing majority of spam volume. Pharmacy spam leads unsuspecting users to fake websites that supposedly sell pharmaceuticals but are usually instead made up of a shifting hyperlink in a spam message generated by one of the world's biggest botnets.

Perhaps most prevalent today in the world of cyber scams is rogue antivirus software, which encompasses several classes of scam software—usually with limited or no benefit—and sold to consumers via unethical marketing practices. Queries for normal search terms lead unsuspecting parties to legitimate websites that have been compromised as part of a plot to manipulate search engines. When pre-determined keywords are searched, victims encounter fake web pages—some of which have been booby-trapped with malicious content—that redirect to a scareware page that may read something like this:

"Your computer is running slower than normal, maybe it is infected with viruses, adware or spyware."

One is then prompted to download fake antivirus programs. Rogue antivirus programs are usually Trojans or other malware disguised as files to protect a computer.

This selling approach is designed to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user. Cybercriminals may also use spam to convince persons that a virus has infected their computer, suggesting that they download (and pay for) antivirus software to remove it. Usually the virus is entirely fictional and the software is non-functional or malware. According to the Anti-Phishing Working Group (APWG), the number of rogue antivirus (AV) packages in circulation rose from 2,850 to 9,287 in the second half of 2008. In the first half of 2009, the APWG identified a 583 percent increase in rogue AV programs.[iv]

These cybercriminal ventures are amazingly lucrative, with profits now totaling in the millions per year. Most perpetrators appear to come from a particular region - Russia, Estonia, and the Ukraine. Cybercrime is rampant in these countries where a deep seated mentality exists in which cybercrime is considered business as usual. This part of the world creates the majority of the world's spam and interviews with known spammers suggest they do not understand why the rest of the world sees spam as a nuisance—to them it is simply business. In some ways this perceived cultural indifference may stem from the fact that life in these countries is more difficult and spartan than in the West. Some of these hardworking technical gurus see cybercrime as a way to equalize the world's wealth so they do not feel particularly guilty about bilking the wealthy of their hard-earned dollars.

III. *An Organized Business Model*

Canadian pharmacy spam, rogue AV, and other cyber scams are often part of an intricate, highly sophisticated and highly organized business model based on the concept of affiliate marketing. Affiliate networks are essentially a way to distribute and sell products using multilevel marketing (MLM) techniques. Products are sold using independent distributors who build and manage their own sales force by recruiting, motivating, supplying, and training others to sell products. The distributors' compensation consists of their own sales and a percentage of the sales of their sales group. In an MLM structure, payouts occur at two or more levels—the worker and the person managing the worker receive a portion of the proceeds. One of the best known examples of a legitimate, successful MLM company is Amway, which sells a variety of health and beauty products. In the case of cybercrime, products sold via MLM techniques are anything but legitimate—click fraud, credit card details, rogue AV, fake pharmaceuticals—all lucrative, yet all very much illegal.

There are hundreds of affiliates that exist in Russia, the Ukraine, Estonia, and elsewhere in Eastern Europe that operate “pay-per-install” or “installs for cash” programs.

There are hundreds of affiliates that exist in Russia, the Ukraine, Estonia, and elsewhere in Eastern Europe that operate “pay-per-install” or “installs for cash” programs in which a criminal organization enlists an army of workers to drive traffic to malware-serving websites. These workers are then paid a commission for every “install achieved.” By using affiliate marketing, crime leaders distribute tasks and responsibilities amongst a wide network of workers, increasing their reach and their ability to touch consumers. Additionally, these networks separate the criminal organizations, or brains of the operation, from the day to day work to minimize the risk of being found liable for the crime.

Pay-per-install

Zango, a software company that ceased operations in 2009, sponsored one of the first known affiliate programs, providing users access to its partners' videos, games, tools and utilities in exchange for viewing targeted advertising placed on their computers. Zango’s business strategy was a model for how these programs worked. From 2002 through 2005, Zango’s applications were distributed via various affiliates and although the affiliates were legally required to obtain user permissions prior to software installation, many failed to do so causing millions of alleged, illegal, non-consensual installs. Many other affiliates notified users only via the end user license agreement (EULA), resulting in millions more arguably legal but essentially non-consensual installs. Zango viewed their products and services as legitimate but some security researchers deemed its business practices questionable and classified some of its software as adware and spyware.

Trend Micro security researchers report that they documented an affiliate who generated $300,000 from rogue AV installs in only one month.

Zango software displayed pop-up ads while a user was surfing the Internet. It was also often bundled with other free software, some of which was considered adware. The applications were often difficult to uninstall, requiring the user to download an additional uninstall application or to use an adware removal tool. Zango was embroiled in various disputes with the FTC and faced legal challenges due to its questionable business practices.

Affiliates continue to operate in much the same manner, using spam and other techniques to lure consumers into downloading malware, such as data-stealing Trojans or bot software. If a user clicks through, a site could keep track of each click by unique affiliate ID and the affiliate receives a commission for each click. Although this may not seem like a lucrative way to make a living, Trend Micro security researchers report that they documented an affiliate who generated $300,000 from rogue AV installs in only one month.

Installs receive different valuations depending on the targeted party's country. For example, U.S. installs presumably generate a higher rate of compensation than installs received from Vietnam because U.S. targets generally have more money to exploit. In addition, from a botnet perspective, U.S. installs of data-stealing malware, for example, offer better bandwidth capabilities for siphoning off banking information or other sensitive data leaked over the Internet. For this reason, residential broadband customers in the U.S. and Western Europe are popular targets of pay-per-install campaigns.

Business Not As Usual

One of the most fascinating aspects of the pay-per-install model is how much it mimics the real business world. Affiliate programs are headed by a criminal organization, although it is almost impossible to track all those involved — an intentional strategy to keep crime bosses concealed. Each affiliate group or program is structured much like a regular company in that there are different "departments" or groups that handle different functions.

For example, a company named "Innovative Marketing" from the Ukraine was accused of spreading massive scareware campaigns. When the U.S. District Court for the District of Maryland approved the FTC's request to stop the company's activities, it was discovered that the company had more than 600 employees in offices and with subsidiaries in India, Poland, Canada, the U.S. and Argentina. Operations included customer call centers, technical support, a professional website and LinkedIn profiles for key employees. It is estimated that Innovative Marketing was receiving 4.5 million orders in 11 months time, totaling $180 million.[v]

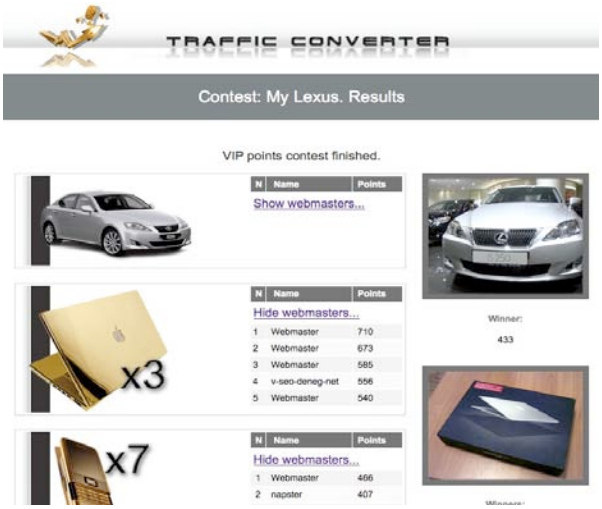

Figure 1: Example of contest used to lure new affiliates

Also, just like in the legitimate business world, a great deal of time and energy is spent recruiting affiliates. Pay-per-install opportunities and programming jobs are advertised on underground websites and alluring ads of beautiful women, fancy cars, electronics, luxury vacations, and promises of high pay are used to entice people to join (see Figure 1). The affiliates even hold sales conferences to profile their programs, share ideas, and brainstorm strategies.

Trend Micro security researchers have observed advertisements for these conferences on underground websites in Russia. Researchers have also observed underground programmers' posts that display a portfolio of criminal ads and malware designs—essentially a criminal's resume.

Criminal organizations hire these technically savvy programmers to develop sophisticated malware ranging from data-stealing Trojans to rogue AV software (see Figure 2). Most are rewarded handsomely, compared to typical wages in their region. These programmers continually create new malware binaries to evade new antivirus signatures—an ongoing effort that resembles the legitimate business of antivirus software development.

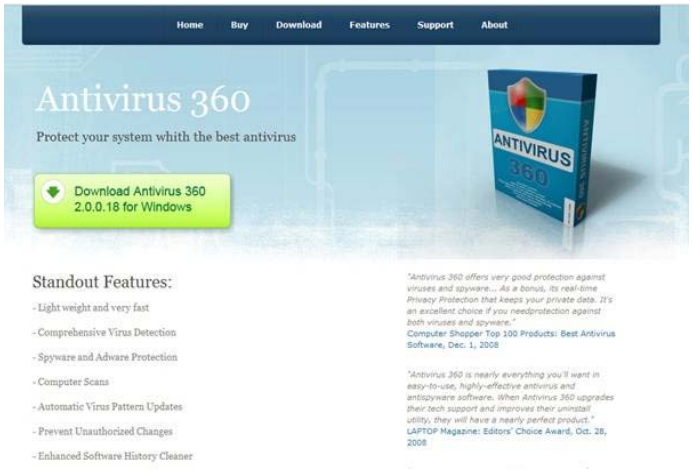

Figure 2: Slick, professional-looking rogue AV

Trend Micro Security Researcher, Paul Ferguson, tracked an underground programmer from Russia who was specifically hired to create Apache web server modifications to guard against law enforcement or antivirus companies that might try to attribute malicious activity to that web server. The programmer was developing a sophisticated method of running through compromised hosts on the Internet so IP addresses being used were hidden. The programmer was well compensated, especially compared to what he would have earned as a legitimate programmer in Russia.

Marketing

Just as legitimate companies hire search engine optimization (SEO) firms to favorably position their products and services online, so too do criminal affiliates. Blackhat SEO and fake blog scraping are used as part of social engineering schemes to drive traffic to compromised websites. Once there, individuals either contract malware by mistake via drive-by download or are induced to click on a video or other enticement, which often results in a Trojan infection.

For example, Trend Micro researchers observed several recent blackhat SEO campaigns that demonstrated incredible skill and speed. In the aftermath of actress Farrah Fawcett's death, cybercriminals achieved top rankings in search engines for search terms containing her name within only four hours of the first announcement of the news. These poisoned search results led to rogue antivirus downloads (see Figure 3). The cybercriminals behind this attack have also skillfully hitchhiked on additional, recent, high profile news like Kanye West's

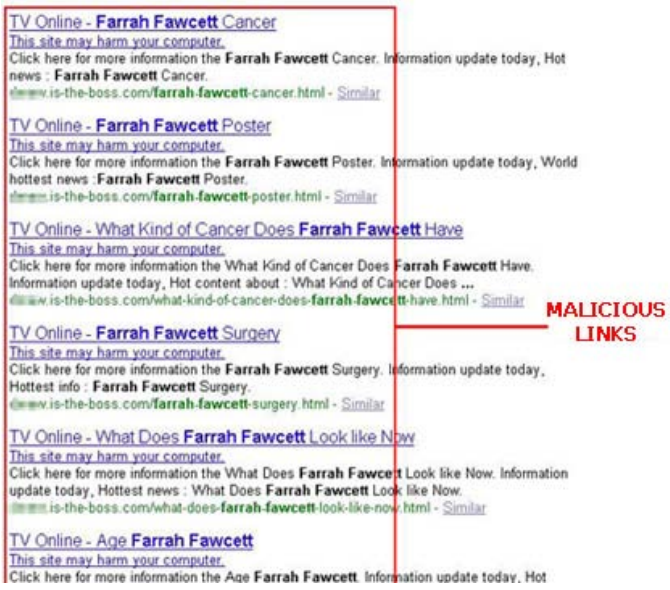

Figure 3: Blackhat SEO searches for Farrah Fawcett

infamous interruption on the MTV VMA awards and the death of Yale student Anne Le. In addition to online marketing, many pay-per-install networks advertise using Russian spam and on Russian language sites with names like "BigCashforYou," or "installsforcash," or "Iframesforcash."

Customer Service

In addition to sophisticated marketing programs, evidence exists that pay-per-install businesses have established customer support centers to help their rogue AV customers. Duped customers—thinking they have paid for legitimate AV software—call in to these centers for "help" with their systems. According to captured VoIP records from a tech support group working for a rogue AV vendor, consumers were calling in and complaining that "Trend Micro will not let me install your security program." The supposed tech support employee explained to the worried "customer" that his PC could not support two antivirus programs running at the same time and then carefully explained how to uninstall Trend Micro's software. The user's response was a grateful thank you and a claim that his system was running even faster! He also mentioned that the new program was finding viruses that Trend Micro had failed to discover.

Pay-per-install businesses have established customer support centers to help their rogue AV customers.

Unfortunately for this individual and all others, these findings are, of course, false—generated by the rogue AV software to appear it is working. This example portrays one aspect of the sophistication of affiliates' operations and how they prey on users' fears.

Finance

Pay-per-install organizations operate sophisticated, well-hidden financial transactions. Many hold active, legitimate merchant accounts for processing transactions and receive payments from credit card companies. These organizations frequently use WebMoney, an electronic money and online payment system. Interestingly, WM Transfer Ltd. is the owner and administrator of the WebMoney Transfer Online Payment System, which conducts all WebMoney transfers, and WM Transfer Ltd. is a legal corporate entity located in Belize, Central America. Belize is the location where the well-known, Russian Business Network (RBN) has been known to always have conducted its money laundering efforts.

Security

Ironically, cybercriminals excel at security. In addition to proactively developing new malware binaries to evade detection by antivirus companies, certain Russian websites now offer automated malware scanning as a service to help malware continue to fly under the radar of pattern-based detection. This service, called "The Anti Virustotal" (a play on the name of an award-winning legitimate service called "Virustotal") offers scanning against 18 well-known AV products. The service is supposedly updated daily and files can be uploaded directly or pulled from a URL and the scanning process can be scheduled to run every few hours. Subscribers even receive detection status reports that help them reengineer their malware the moment their files show up as being detected by AV vendors.

Ironically, cybercriminals excel at security.

In addition to securing their malware, these criminal organizations spend a great deal of time and money building redundant systems and architectures. As IP blacklisting has become mainstream, some of the larger cybercriminals organizations have grown more adept at diversifying operations after several high profile shutdowns. One of the most notable and far-reaching incidents occurred in November 2008 when the plug was pulled on San Jose-based McColo Corporation—known as one of the world's most disreputable hosting providers. With suspected links to the RBN in St. Petersburg, McColo was believed to have hosted some of the command and control (C&C) infrastructure for several of the world's largest identified botnets, which were controlling hundreds of thousands of zombie PCs involved in email spam, spamvertising, malware, child porn, credit card theft, fraud, and get-rich-quick scams. As a "bulletproof" hosting provider, McColo was known to be unresponsive to complaints about its hosted sites, collecting a premium from criminal operators for turning a blind eye when notified of infractions.

Thanks to the efforts of a rogue band of "good-guy" security researchers who regularly collect data on malicious Internet activity, McColo was finally disconnected from the Internet when years of investigation culminated in a complete shutdown, eliminating an unbelievable 50 to 75 percent of the world's junk email in a single day.

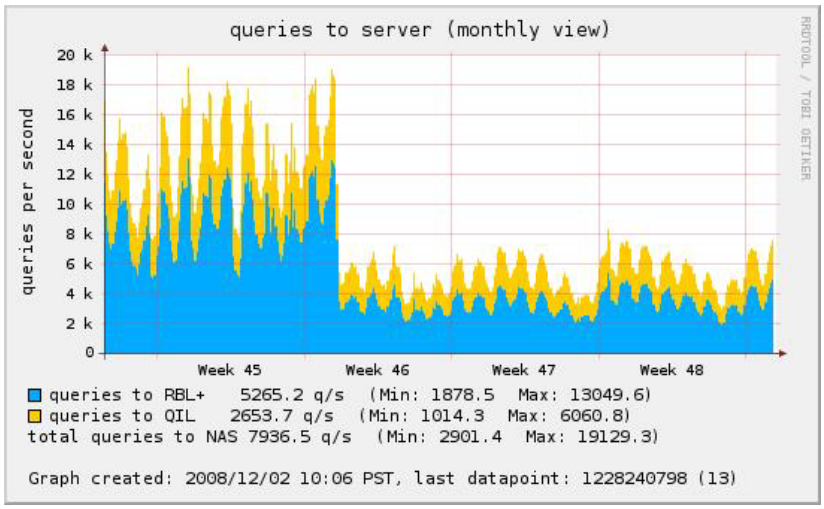

Figure 4: Trend Micro spam counts—note the drop at week 45 where the McColo shutdown occurred

Researchers had alerted McColo's upstream Internet service providers (ISPs), Global Crossing and Hurricane Electric, of the purported criminal activities occurring at McColo. After reviewing details of the investigation, the ISPs immediately shut down McColo's Internet connections.

According to Advanced Threats Researcher, Paul Ferguson, "Trend Micro Email Reputation Services (ERS) detected a 40 percent drop in spam activity immediately following termination of McColo's connectivity." *See Figure 4*.
The RBN and others learned from the McColo incident and today use smaller hosting providers spread out globally in an attempt to diversify operations. In this way they can blend in with Internet noise around the world, making it tough to track the servers and almost impossible to take down, especially because rack space is shared with other, legitimate businesses.

Bad Guys Are Winning?

By some accounts the bad guys are winning. At this point in time, most consumers do not play an active role in fighting cybercrime as most crimes go unreported. Mostly their role is restricted to recouping their own individual financial losses, regaining control of lost identities and reclaiming hijacked bank accounts. Law enforcement is actively involved in fighting cybercrime but efforts are fragmented and spread out over the globe. The role of law enforcement is also strictly limited by prosecutorial discretion, separate jurisdictions, politics, and inadequate technical resources.

One of the greatest challenges is trying to take down the "bad actors" that support cybercrime. "Bad actors" are a small number of network and hosting service providers and domain registrars that supply the infrastructure needed to host the technology that drives cybercrime—drive-by downloads, botnet command-and-control servers, stolen data drop sites, and DNS numbers. In most cases, the motivation is purely financial—"bad actors" profit handsomely from their work with The Underground.

Bad actors are a small number of network and hosting service providers and domain registrars that supply the infrastructure needed to host the technology that drives cybercrime.

Although most "bad actors" have been identified and are fairly well-known, they are also somewhat unstoppable due to legal, economic, and technical issues. For example, Eastern Bloc hosting providers openly promote email spam services, ICQ-based spam, and spam hosting since they know they are well outside the jurisdiction of any law enforcement in these countries.[vi] In addition, most cybercriminals today know that bulk domain registration for hosting malicious websites or pages is best handled in China because the Chinese do not typically suspend known malicious domains. For this reason, cybercriminals are currently burning through .cn domain registration at record speed.

"Bad actors" are highly skilled at responding quickly to ISP shutdowns and server blacklisting. Failover processes have been automated using malware designed for resiliency and high availability. For example, security researchers discovered that the Srizbi botnet contained a failover domain name mechanism that would activate if the main Srizbi control servers were shutdown. Each Srizbi bot PC would periodically connect to a newly generated domain name until a new C&C server was contacted. Anyone with access to the domain name generation algorithm could then register domains in advance of the bots connecting to seek out a new C&C server.[vii]

Most network and hosting service providers and domain registrars are concerned about their reputations and try to respond if upstream ISPs complain about malicious activity. Protecting consumers, however, is expensive and not particularly profitable. These companies do not make enough money to set up and manage a support staff solely for handling abuse complaints.

Current Efforts

There are many stakeholders interested in reducing the impact of global cybercrime. These include law enforcement, the security industry, academia, policy organizations, Internet service providers, domain registrars, other researchers, and of course, victims.

A good example of an organized effort toward fighting cybercrime is the Conficker Working Group, a task force comprised of security researchers, Internet service providers, domain name registries, universities, law enforcement agencies, and other cross-industry stakeholders. The group was formed recently to combat the Conficker worm, which is believed to have originated with the same Russian/Ukrainian cybercriminal operation believed to be behind many other profitable criminal operations such as the RBN, Atrivo/Intercage, McColo, the Storm botnet, the Waledac botnet, rogue antivirus campaigns, and other criminal activities.

Additionally, the Anti-Phishing Working Group (APWG) created an initiative that includes civilian network operators and researchers who have volunteered to try to bridge the cybercrime data-sharing gap between public law enforcement, private network security, investigative intelligence, network measurement and experimentation, and related policy. The APWG hosts an annual counter e-crime operations summit, which helps participants network and learn the latest strategies while developing relationships that help fight crime throughout the world.

Figure 5: Examples of regional CERTs

An organization named FIRST (Forum of Incident Response and Security Teams) also provides a global forum to share information. Membership in FIRST enables incident response teams to more effectively respond to security incidents and to develop proactive methodologies to fight cybercrime. FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations to collaborate in incident prevention. FIRST also stimulates rapid reaction to security incidents and promotes information sharing among members and the community at large. Currently FIRST has more than 200 members, spread over Africa, the Americas, Asia, Europe, and Oceania.

Local and regional groups are also being formed to combat cybercrime. One of the best examples is the network of CERTs (Community Emergency Response Teams) composed of local groups devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems. CERTs in this country are funded primarily by the U.S. Department of Defense and the Department of Homeland Security, along with several federal civil agencies. Other countries also sponsor CERTs, such as the Netherlands (CERT.NL), Estonia (CERT.EE), and Australia (AusCERT). Some companies have even founded their own CERT teams, such as Adobe and CISCO *(see Figure 5).*

A Recent Win

After a recent FBI sting operation led to the dismantling of an international cybercrime ring, J. Keith Mularski, a special agent who works in the Federal Bureau of Investigation's Cyber Division, says that when it comes to fighting cybercrime, the bad guys may still hold a technological upper hand but the good guys are getting better. He believes that increasing transnational police cooperation is turning the tide against digital criminals. "We're not far behind," says Mularski, who spent several years trying to crack a crime network that was selling stolen credit card numbers, bank numbers, and personal log-in information to online buyers. The website, DarkMarket.ws, was eventually dismantled last October after a German radio network disclosed news of the sting operation on-air. In an interview with CNET, Mularski commented "I wouldn't say that we're winning the battle but I expect to see great strides in the near term."[viii]

Coordinated Multi-Stakeholder Approach

No one organization can make a significant impact against cybercrime alone. Ad hoc efforts work only partially and are typically short-lived. Instead, a coordinated, multi-stakeholder approach is required to share information and strategies. Stakeholders must share clear, concise records of threat information that pinpoint the “who, what, why, where, and how” of attacks with detailed information and desired actions. Through collaboration between law enforcement, network and hosting service providers, and domain registrars, domains can be suspected, and large-scale takedowns and remediation can help stop cybercriminals upstream. Criminal charges and arrests are also desired outcomes but much more difficult to achieve at this time. Some of these efforts have been building momentum; however, more cooperation is needed amongst the disparate groups of stakeholders.

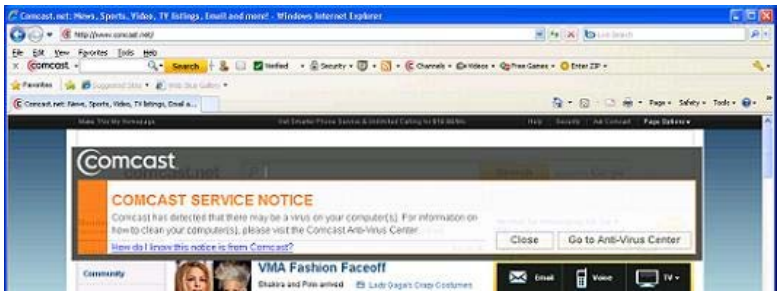

Figure 6: Comcast Constant Guard sends a "Service Notice" to customers who have been detected to have downloaded bot software

A standardized way of reporting security incidents is one strategy that could dramatically help efforts. Malware and incident reporting help the security community correlate data points that can then be sent out to other security researchers, law enforcement, ISPs, and domain registrars to put cybercriminals on the defensive. Finger-pointing is non-productive and each country or organized group should first concentrate on cleaning up cybercrime regionally before a true, international concerted effort can occur.

An example of a successful, small-scale effort that could be used as an example for other ISPs is Comcast’s recent decision to make a targeted effort to eliminate botnet viruses through a new initiative called “Constant Guard” *(see Figure 6)*. Constant Guard is the end result of several years of work to create a comprehensive approach toward protecting Comcast customers from sophisticated online threats. Constant Guard involves several components, including a Customer Security Assurance (CSA) team of security experts to proactively respond to customer

complaints related to spam, bots, and viruses. All Comcast customers will also receive security software as a standard part of their service, as well as a web portal that provides security tips, alerts, and tools.[ix]

IV. *Looking Ahead*

As the digital underground economy grows more profitable, cybercriminals will continue to create malware for profit. Most recently, the Ukrainians have made a name for themselves in their development of increasingly sophisticated Trojan banker malware. Because consumer protections are better established and more stringent compared to corporations, cybercriminals are increasingly turning to larger, less protected enterprise targets.

The most recent large-scale data breach occurred last year involving Heartland Payment Systems, one of the five largest payment processors in the U.S. The breach occurred when cybercriminals managed to sneak a keystroke logger onto the company's credit card processing system. Heartland serves 250,000 business locations and conducts more than four billion business transactions per year.[x] In most instances, breaches occur because security protections are too lax or are missing entirely. This creates a critical need for adaptable security techniques and technologies that deliver better protection for all users. Antivirus software alone is insufficient; however, reliable security software with a web reputation component provides more effective protection.

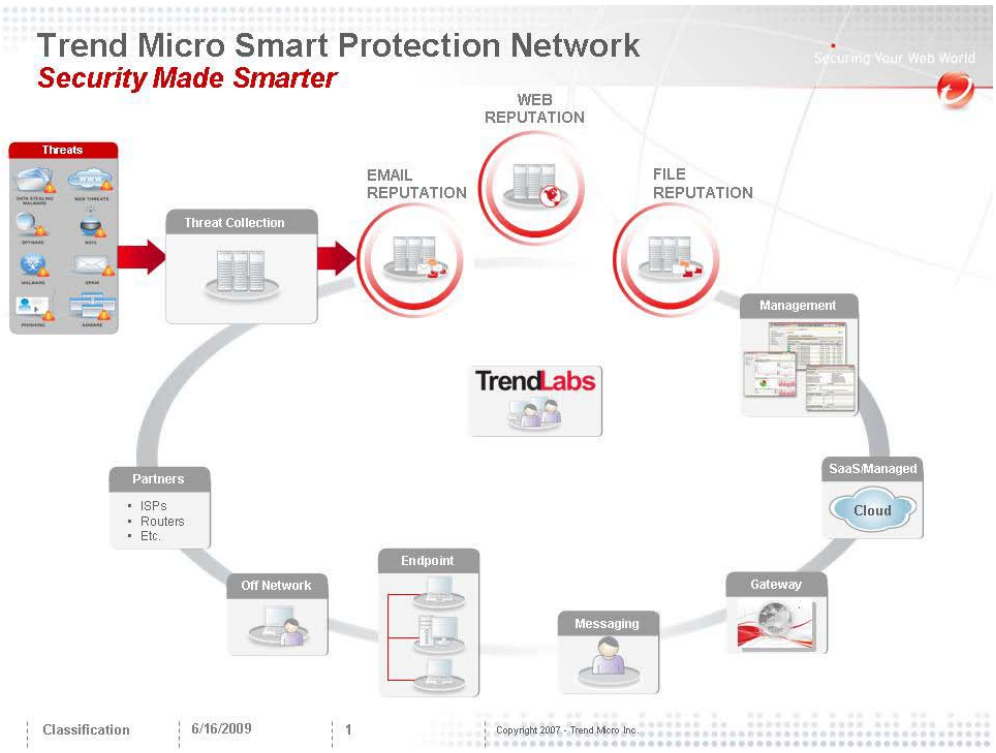

Figure 7: Trend Micro's Smart Protection Network

For example, Trend Micro's Smart Protection Network is a next generation, cloud-client content security infrastructure designed to protect users from web threats while reducing the network and system impact, and the reliance on

conventional pattern file downloads. By incorporating in-the-cloud reputation, scanning, and correlation technologies, the Trend Micro Smart Protection Network reduces reliance on conventional pattern file downloads. Leveraging both internal expertise in delivering leading content security solutions and real-time feedback from customer environments, the Trend Micro Smart Protection Network correlates information from multiple vectors to deliver comprehensive web threat protection. The Trend Micro Smart Protection Network is used in on-site and hosted web, messaging, and endpoint security solutions to protect companies and end-users from threats that compromise information and severely damage a company's or an individual's reputation *(see Figure 7).*

Trend Micro also provides a client-server solution called OfficeScan™ that protects desktops, laptops, servers, storage appliances, and smart phones—on and off the network—with a blend of world-class anti-malware and in-the-cloud protection from the Smart Protection Network. New File Reputation frees endpoint resources by moving pattern files into the cloud. And Web Reputation blocks access to malicious websites.

V. *Conclusion*

As cybercrime skyrockets and consumers and businesses face the prospect of losing money and sensitive data to pay-per-install affiliates, a new approach is required to fight the criminal organizations behind these attacks. To date, ad hoc efforts have been only partially effective and usually provide short-lived results. Instead, a coordinated global response involving multiple stakeholders must occur to stem the rising tide of cybercrime. Security companies, researchers, law enforcement, educators, government officials, Internet service providers, domain registrars, and even consumers must band together to identify malware, eliminate bad actors, share information, and disrupt the operations of pay-per-install affiliate programs. Malicious business activities require improved documentation and reporting with a free exchange of information to promote a better understanding of these criminal operations and their effects on innocent individuals. In addition, adaptable security techniques and technologies are needed to deliver better protection for all users. Antivirus software alone is insufficient; however, reliable security software with a web reputation component provides more effective protection.

References

[i] Phil Muncaster, "Soaring Online Crime Hits Consumer Confidence," *V3.co.uk*, April 20, 2009, http://www.v3.co.uk/vnunet/news/2240628/consumer-online-fears-grow

[ii] "2008 Internet Crime Report, *IC3*, December 2008, http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf.

[iii] Elinor Mills, Web-based Malware Infections Rise Rapidly, Stats Show," *CNET News.com*, October 27, 2009, http://news.cnet.com/8301-27080_3-10383512-245.html?part=rss&subj=news&tag=2547-1_3-0-20.

[iv] *Wikipedia*, http://en.wikipedia.org/wiki/Scareware.

[v] Francois Paget, "Mafia-style Cybercrime Organizations," *GovernmentSecurity.org*, October 19, 2009, http://www.governmentsecurity.org/global-security-news/mafia-style-cybercrime-organizations.html

[vi] Alex Lanstein, "Exposing Bad Actors Sites that Support Cybercrime," *ComputerWorld,* October 8, 2009, http://www.computerworld.com/s/article/print/9139141/Exposing_Bad_Actor_Sites_That_Support_Cybercrime?taxonomyName=Network+Security&taxonomyId=142

[vii] Ibid.

[viii] Charles Cooper, "To catch a (cyber) thief. It's not easy." *CNETNews.com*, April 22, 2009, http://news.cnet.com/8301-10787_3-10225278-60.html

ix Sebastian Rupley, "Comcast to Put Botnet Cops on the Security Beat," Gigaom, October 11, 2009, http://gigaom.com/2009/10/11/comcast-to-put-botnet-cops-on-the-security-beat/

x Richard Adhikari, "Cyber Thieves Hit Payment Processor Heartland," InternetNews.com, January 21, 2009, http://www.internetnews.com/security/article.php/3797551

TREND MICRO INCORPORATED

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800-228-5651
phone: 1 +408-257-1500
fax: 1 +408-257-2003
www.trendmicro.com

TREND MICRO™