RSA®

The Security Division of EMC

White paper

Business Success in a Dark Market: An Inside Look at How the Fraud Underground Operates

The fraud underground is a sophisticated criminal enterprise that operates much like a real-world business.

The business of online fraud has developed into a sophisticated underground criminal operation that continues to evolve everyday. Much like a real-world business, fraud "entrepreneurs" offer products and services for a profit, they fight to gain competitive advantage and market share, are continually innovating to improve their offerings and meet the needs of customers, and are affected by the laws of supply and demand.

Online fraud has changed from hackers trying to steal email passwords from America Online users to a far more menacing criminal enterprise, with bands of fraudsters working together to create schemes that dupe unsuspecting online users into divulging their personal details. And while the complexity and sophistication of online attacks continue to grow, even more alarming are their numbers and the loss to organizations and individuals.

This white paper will examine how the fraudster underground operates, the intricate supply chain that supports it, and how it continues to evolve.

Contents

I. Job Specialization

The fraudster underground is a marketplace for selling compromised credentials and tools and services used in the commission of fraud. Much like any free market, most fraudsters who participate in it are not "jacks of all trades," but specialize in offering specific technologies or services. A fraudster business typically falls into one of two categories: harvesting or cashing out.

Harvesting

Harvesting is the process of collecting credentials and personal information from online users. A harvester works to steal and collect compromised credentials with the intention of reselling them to other fraudsters to cash out. Harvesters leverage technical infrastructure and tools such as phishing kits, Trojans, ATM skimming devices, hosting services such as botnets, and advanced infection or spam delivery platforms to spread their attacks.

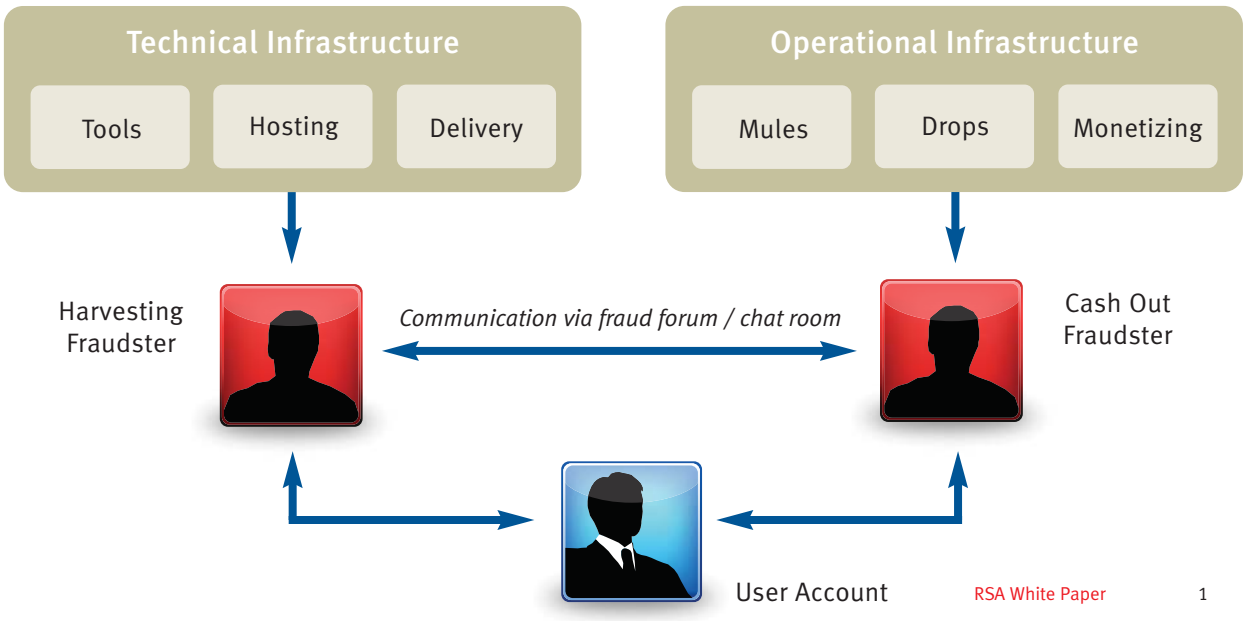
The technology and methods used to harvest credentials have evolved dramatically in the last few years, and continue to advance in order to circumvent established security measures of both organizations and consumers. The infrastructure being developed and used by harvesters today offers great scalability and a high degree of customization per specific target. The cost to deploy an attack has also decreased. For example, Zeus, the predominant Trojan in 2008-2009, sells for $1000. "Newbie" fraudsters can opt for cheaper Trojans such as Limbo, which sells for about $350 in the underground.

Harvesters do not actually steal money; they have no operational infrastructure to empty the compromised accounts. They steal credentials, and then provide them to others in the fraud ecosystem for a price: these fraudsters are most commonly known as cashiers. A typical transaction between a harvester and a cashier involves a set price per compromised account or, in some cases, per gigabyte of stolen data. Alternately, a revenue share system can be set up. In the early days of online fraud, harvesters claimed about half of the fraud proceeds; today, they settle for a mere 20 percent.

Cashier

The goal of a cashier is to develop the operational infrastructure and strategy to empty a victim's account without leaving any traces. While harvesters are focused mainly on technology development, cashiers are likely to practice in the service industry, offering services to enable other fraudsters to cash out credit cards and bank accounts. Cashiers utilize complex networks and often recruit bands of money mules to do the dirty work. A money mule is a person that receives funds into their accounts, withdraws the money, and sends it overseas to the fraudster, often through a money transfer provider. Mules can also be used to receive and reship goods that are purchased online with a stolen credit card or account.

The fraud ecosystem consists of harvesters who collect stolen data and cashiers who use the data to empty a victim's account.



Money mule recruitment networks and "mule herders" – managers who control the network of mules – are a specialized service offered for sale within the fraud underground. Many mule recruitment scams are sent through spam attacks that direct the user to websites that offer allegedly legitimate jobs to perform money transfers. People apply for a position described as a "money transfer agent" or "regional manager." In reality, honest people (and in some cases, dishonest people) are hired to become part of the fraud and money laundering cycle. They move cash that originates from compromised bank accounts, from one criminal to the other. Depending on the amount of money laundered, a mule will receive a small commission of the transferred amount.

Cashiers in the underground are also evolving phone fraud services to cash out accounts by taking advantage of inherent weaknesses in the Call Center. A new service uncovered by RSA shows fraudsters offering professional call services that can spoof any number in the United States and also offers cash out in multiple languages. The service costs USD$12.00 and allows phone numbers to be customized depending on the state where the account holder resides and enables fraudsters to accept incoming calls, posing as the genuine account holder.

In the real-world economy, buyers and sellers rely on each other. A buyer with a need requires a seller with a product or service to meet that need and a seller requires a buyer with a need in order to sell a product or service. Harvesters and cashiers depend on each other in much the same ways in order to conduct business in the underground. Harvesters need cashiers to buy the credentials they capture or to provide the services that enable them to cash out stolen accounts. Cashiers need harvesters to provide the products and services that enable them to get the credentials to cash out.

II. Innovation and Technology

As organizations continue to strengthen security and awareness of online threats within the general online user community increases, fraudsters are left to continue developing new ways to launch attacks. Through a combination of advanced technology, new distribution channels and social engineering techniques, fraudsters have continued to innovate in order to work around these challenges.

Phishing

As the "oldest" of the online threats, phishing – the process of attempting to acquire personal information from online users through communication such as email – is now the least successful and sophisticated. Despite its lack of sophistication and low returns, phishing still remains widely popular in fraudster circles because of its low execution cost and the fact that little technical knowledge is required to set up an attack. In fact, it has become such a commodity that fraudsters can buy phishing kits for just a few dollars that allow a phishing attack to be set up in mere minutes[1].

----- Forwarded Message ----
From: em kristin alexander@stola.com.br
Sent: Friday, October 24, 2008 10:01:10 AM
Subject: We need part-time manager

Dear Sir/Madam,

AutoPay Inc.looking for local branch adminitsrators in Uited States only!
You will work in your city, no trips, no relocation.
Vacancy: regional payment administrator (male and female) , salary: 2600-2800 per week.

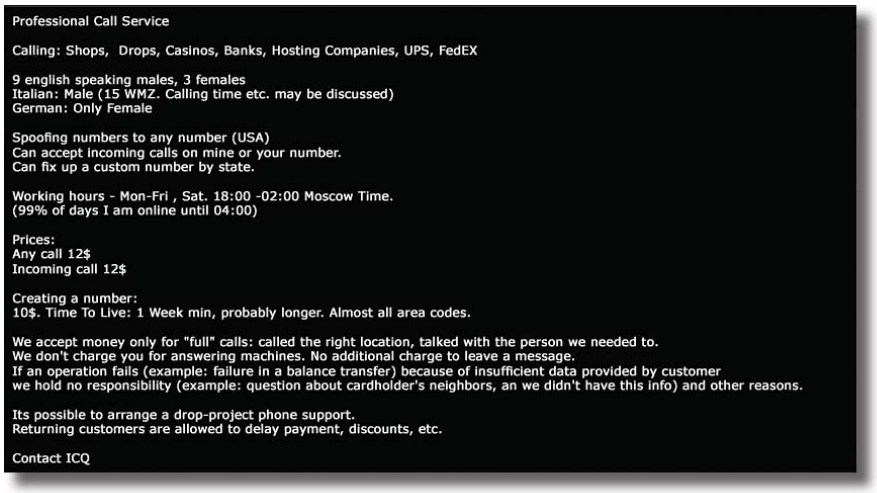
1)21 years and older,
2)2-3 hours per day (monday - friday),
3)education - any basic.

For more details mail to: autopayusa@aol.com

Sincerely, Leland Ramsey.
AutoPay Incorpotation.

A sample mule recruitment email. A good portion of mule recruitment is actually done on legitimate websites.

[1] Some fraudsters give away phishing kits for free, but they are usually developed with a "back door" where the author will also be given access to any credentials collected, unknown to the fraudster launching the attack.



A call service that operates in a local language on behalf of remote fraudsters

In 2008, the number of phishing attacks detected by the RSA Anti-Fraud Command Center grew an astounding 66% over the number of attacks detected in 2007. But because the lifespan of phishing attacks gets shorter and shorter, fraudsters have had to innovate and develop new ways to launch phishing attacks.

Fast-flux networks

Fast-flux networks are one of the methods that fraudsters are increasingly using to extend the life of a phishing attack. First used by the notorious group RockPhish, fast-flux is an advanced Domain Name Server (DNS) technique that utilizes a network of compromised computers, known as a botnet, to hide the true origin of the server (usually referred to as the "mother ship") that hosts phishing and malware websites. The botnet acts as an army of proxies, or middlemen, between the victim and the website. Exposing and shutting down attacks hosted on a fast-flux network is difficult as the server that is hosting the attack hides behind a cloud of these compromised computers, thus the IP address is constantly changing. Of the tens of thousands of phishing attacks identified by RSA in 2008, 44% of them were hosted on fast-flux networks.

Trojans

A Trojan is a form of malicious software ("malware") that typically resides on a user's computer as what appears to be a seemingly harmless program. Unlike phishing which is very "noisy" and can be easily identified by online users, a Trojan resides invisibly in the background, waiting on standby to facilitate unauthorized access to a user's computer system. Trojans typically record every SSL session – including both the user input and the information posted to the browser. Trojans such as Zeus and Limbo ride the original session of the website so there are no visible cues as to their existence. In other cases, they are capable of injecting additional HTML fields – for example credit card number and PIN code – in order to harvest supplementary data.

Trojans have been around for some time now and appear to finally be gaining attention in the mainstream. They are so prolific that it is estimated that 1 in 100 computers is infected with one[2] – and the rate is growing fast.

But Trojans are not just targeted directly at consumers anymore. Corporate environments are increasingly being targeted by online criminals as evidenced by incidents such as the growth of malware-related data breaches (see sidebar, page 4).

Trojan infrastructure has improved significantly in the last two years. Just like with phishing, Trojan kits are up for sale in the underground. These kits enable fraudsters to readily launch an attack and add new functionality on a whim. For example, in January 2009, RSA identified a fraud website coined the "Web Injection Shop" that sells HTML injections designed to steal information from online banking users. The injections are tailored fake HTML pages that match each bank's specific website design and can add new fields that would require a user to input credentials and other personal information. A sample product sold at this site is called "Balance Grabber" – a tool that copies out a bank account's balance field and sends the information to a drop server.

[2] Panda Labs: http://www.infoworld.com/d/security-central/anti-virus-vendor-id-theft-trojans-1-in-100-pcs-888

In addition, fraudsters are able to evade AV systems more easily and actually operate testing labs to test their Trojan builds against leading AV software. When a signature is developed to defend against the specific Trojan code, the fraudsters simply build a new variant. They set up their infrastructure with command and control servers that can automatically update Trojans 'in the wild' with new code as soon as it is detected.

Malware-related Data Breaches on the Rise

Malicious software, or malware, is increasingly being named as the cause of a number of high-profile data breaches within the past year. Malware is capable of infiltrating computer systems on the network and siphoning out masses of sensitive consumer and business data. Below is a list of several recent data breaches where malware was cited to be involved:

June 2009: Insurance giant, Aviva, announces a data breach potentially linked to a password-stealing Trojan.

February 2009: The Indian Ministry of External Affairs announces malware designed to track or take control of a user's actions has infected several hundred computers.

January 2009: Payment processor, Heartland Payment Systems, announces the largest data breach in U.S. history was due to unidentified malware that captured information on up to 100 million credit and debit cards.

March 2008: Supermarket retailer, Hannaford, announces more than 4 million credit and debit cards may have been exposed as the result of a Trojan secretly placed on their network.

Drive-by-downloads

Historically, phishing and Trojans have been recognized as two unique means of attack. However, the combination of phishing and Trojans working together is becoming more prevalent among fraudsters – a natural evolution that is driving propagation to a much higher degree. This is accomplished through what is known as a "drive-by download,"[3] and social engineering plays a key role in the success of these attacks.

A typical ruse used by fraudsters is to take a current topic or a popular celebrity that is in the news or of high interest to the general population. Fraudsters send emails to unsuspecting users directing them to view a video or read a news article. When users click on the link or the video, they are infected with a Trojan. In January 2009, RSA uncovered and shut down such an attack. It was a social engineering scam designed to lure people, via an email spam attack, to a fake news website designed to look like CNN.com. This fake web page included a link to what appeared to be a legitimate video. When visitors clicked to view the video, they received an error message asking them to install Adobe Flash Player 10. Instead they were actually launching a Trojan designed to capture their financial and personal information.

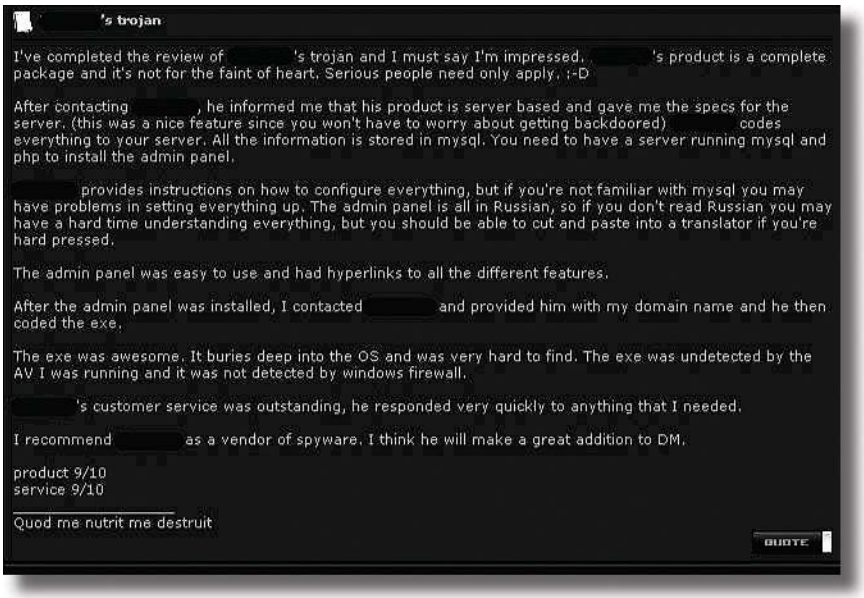
Man-in-the-browser Attacks

RSA has recently seen an increasing number of Man-in-the-Browser (MITB) Trojan attacks against financial institutions worldwide. A MITB attack enables fraudsters to perform unauthorized online transactions by hijacking a user's online session in real-time (sometimes referred to as session hijacking), and intercepting and changing the user's online transactions in real-time.

Unlike a phishing attack, where the user is directed to a fraudulent website, a Man-in-the-browser attack occurs when the user accesses the website of a targeted organization and initiates an online transaction – independent of being triggered by a prompt such as an e-mail or other notification. A Man-in-the-browser attack is harder to detect as it is done in the browser and closer to the user rather than on the traffic stream.

Man-in-the-browser attacks are slowly becoming a mainstream tool for fraudsters, especially in geographies where two-factor authentication is densely deployed, such as the European consumer banking and the US corporate banking markets.

[3] A program that is automatically downloaded to a user's consent without their consent or knowledge. The download can occur by simply visiting a website or viewing an email.



A Trojan reviewed in one of the fraud forums gets a rating of 9 out of 10 for product and service.

III. Customer Service and Loyalty

Organizations around the globe are committed to fostering brand loyalty and long-term relationships with their customers to ensure they will continue to buy from their business over a period of time. Several factors are relevant to building a good reputation including excellent customer service, quality, support, and satisfaction guarantees – all critical to ongoing success and repeat business.

Reputation

Fraudsters rely on very much the same model to develop customer loyalty and build their reputation in the underground. This is especially important as fraud forums and IRC channels are full of rippers, or fraudsters that engage in deals and then never complete their end of the trade. While keeping rippers out of the IRC channels is problematic, the forums have devised several methods to minimize the risk of dealing with rippers. One of these methods is to obtain a "Verified Vendor" status.

Verified Vendors are vendors with special status, who are pre-approved by the forum administrators. Much like the Better Business Bureau seal of approval communicates to consumers in the real market that a business is highly regarded, being elevated to "Verified Vendor" status is the forum's stamp of approval that a fraudster is legitimate and reliable. A "Verified Vendor" status automatically increases a fraudster's reputation, at least in that particular forum. In most forums that offer a vendor review service, there is a closed section where only Verified Vendors are allowed to offer their products or services for sale.

Product guarantees, free upgrades and support

Standing behind your product is important to building a base of repeat customers. In the real world, for example, this may be done by guaranteeing satisfaction with a product or service or offering money back or a replacement if something should go wrong.

Fraudsters offer similar guarantees to other fraudsters that purchase their goods and services. A harvester might offer a guarantee in the form of upgrades and support to a product. For example, fraudsters that sell Trojan kits offer free upgrades to their product, ensuring that the Trojan will not be detected by anti-virus engines. Fraudsters might also offer a guarantee in the form of replacement goods. For example, fraudsters that sell stolen credentials often guarantee the viability of their goods by offering replacement credentials if an account is not capable of being cashed out.

Customer service is crucial when Trojans are involved, as they often require some degree of technical expertise to install, upgrade and control. Most Trojan builders provide free customer support via email or chat.

IV. Marketing and Communication

Fraudsters rely on two main channels to communicate and market and sell their products – IRC chat rooms and forums. Both communication vehicles essentially share the same characteristics but also offer significant differences, as well, each with its own set of rules and procedures.

IRC chat rooms

IRC, or Internet Relay Chat, is a communication protocol which allows clients to connect to a server and participate in various chat rooms. The IRC protocol provides fraudsters with a host of capabilities including file transfer, secure private chats and the ability to moderate channels. The protocol also enables chat users to remain relatively anonymous.

The IRC chat room can be compared to a marketplace. In these rooms, fraudsters buy, sell, and trade anything that can be obtained via fraudulent methods – from online banking credentials to online gaming accounts. Those who offer the service "shout" on the main channel the type of products they are offering and what they expect in return. If someone is interested in one of the products, he approaches the seller via private chat to negotiate.

Just like in a marketplace, there is rarely any small-talk and the majority of the discussions are business-related. A fraudster that wants to launch a phishing attack can simply head to one of these channels to purchase the goods he requires.

Forums

If an IRC chat room can be compared to a marketplace, then the forums can be compared to a country club. These forums fit much better to the definitions of "community" and "organized crime," offering various exclusive services for its members. It is much more common to find small-talk in forums, as well as tutorials, discussions, and professional assistance. Due to the more organized nature of forums, they experience considerably less cases of "ripping" or scamming. Some forum members actually look down on users of the IRC channel, calling them "IRC kiddies."

In order to keep unwanted characters out, some forums are closed and require vouching by senior members for new fraudsters who apply to join. Several forums also require an "entrance fee" that is donated for the operation of the forum. This section will focus on the forums of the fraudster community, as their communal aspect is much more significant.

A requirement for most forums is that members must adhere to just one user name in order to build their reputation. A fraudster looking to sell goods must first undergo a rigorous review to prove he offers quality products and services and is reliable in order to confirm his legitimacy and prove he is not a ripper. Further services are offered, such as escrow services, to ensure that members' deals are completed in full.

Forums also offer non-business related talk regarding scene news, members and events. Tutorials for newcomers and public assistance are also commonly found in the forums. In many forums, there are also many amusing ads that fraudsters use to stand out and promote their services.

An ad promoting lists of stolen credit cards

V. Diversification

To survive in the underground and continue building a successful fraud business, fraudsters must diversify beyond developing new technology – they must diversify their business practices. This has become more evident over the last couple of years as we have seen fraudsters deploy new methods and tactics, develop new targets to attack, and take advantage of new channels to commit fraud and distribute malware.

Fraudster methods and tactics

Fraudsters continue to evolve their methods and tactics in an effort to find new ways to make money. Spear phishing, or whaling as it is commonly referred to, is one such method that is gaining traction among fraudsters. A derivative of traditional phishing attacks, whaling is a targeted form of phishing that is typically directed at senior level executives or a very specific entity.

The techniques fraudsters employ to conduct whaling attacks are very effective as demonstrated by a study conducted by the Intrepidus Group. Utilizing a number of mock phishing scenarios against tens of thousands of employees worldwide, the Intrepidus Group found that 23 percent of people will fall for whaling attack. Even more astounding, 60 percent of corporate employees who were susceptible to a targeted whaling attack responded to the emails within three hours on average.

RSA has witnessed the sale of certain information in the underground that suggests whaling is on the rise. For example, in the following post, a fraudster is seeking the email addresses of a company's CEO and top executives and is willing to pay $50 for them.

Fraud-as-a-service refers to the advanced supply chain operated in the underground and is another method on which fraudsters rely. Fraud-as-a-service gets its name from the Software-as-a-Service model, or SaaS, a software deployment model where a vendor develops, hosts, and operates an application over the Internet and the customer of the application, in turn, accesses and uses the application over the Internet. This model is very similar to the services that fraudsters operate in the underground, hence the name Fraud-as-a-Service.

A good example of Fraud-as-a-Service are hosted Trojan services which are available for sale in the underground, starting around $300. If a fraudster wants to launch a Trojan attack, he can get one that is already hosted on a bullet-proof server that will run for years. Most services provide some disaster recovery so if the server is down, the information collected will remain intact and the Trojan will continue to be distributed. The Trojan is already connected to an infection kit, which means as soon as the subscription service fee is paid, a fraudster needs to do little more than wait for credentials to be collected. Fraud-as-a-service offerings lower the barriers of entry even further for new fraudsters or experienced fraudsters seeking to make a career change.

Hosted Trojan services are available for sale in the underground, starting around $300.

New targets

Online fraud is still mainly associated with targeting financial institutions and their customers, capturing credentials such as credit card and bank account numbers, and the subsequent cash out of those accounts. However, fraudsters are increasingly identifying new targets to attack and seeking new types of information from those targets. Healthcare and insurance providers are two of the newest attack targets, as demonstrated by the following forum post.

The types of information that can be obtained from these organizations include a variety of personally identifiable information (PII) that can be used to commit fraud and identity theft. First, fraudsters can use PII to open new accounts online or create mule accounts for use in the cash out process of legitimate accounts. Second, fraudsters can use this information to raise the value of the credit card and bank account information available for sale in the fraud underground. For example, the average selling price for a U.S. credit card in the fraud underground is $1USD. But when that single card is sold with a full identity profile, which includes information such as the customer's billing address, Social Security number, mother's maiden name and date of birth, the price is inflated to $20USD[4].

Another new target is the enterprise as fraudsters seek to obtain new types of credentials to sell or exploit. While still in its infancy, online criminals are just starting to realize the potential benefits of enterprise fraud. RSA has witnessed many incidents of enterprise credentials being collected by Trojans. For example, RSA's fraud analysts have uncovered VPN and web mail account credentials within drop zones during the credential recovery process. Also, other high-profile recoveries have yielded FTP credentials collected through a Trojan. These credentials could be used by hackers to compromise legitimate sites with malicious code and drive-by downloads.

Online criminals are just starting to realize the potential benefits of enterprise fraud.

[4] Source: RSA Anti-Fraud Command Center

As the behavior and activities performed by online users change, fraudsters are ready to adapt their own strategies to maximize their profit. This is most evident in the explosive growth of social networking sites.

New channels of distribution

As the behavior and activities performed by online users change, fraudsters are ready to adapt their own strategies to maximize their profit. This is most evident in the explosive growth of social networking sites and the number of users that engage in social networking activities. Two-thirds of the world's Internet population visit social networking or blogging sites, accounting for almost 10% of all online time[5]. The heavy traffic and global reach of these sites have made them a prime target for exploitation by fraudsters. Today, nearly 20% of online attacks are targeted at social networking sites[6].

Through a combination of technology (mainly Trojans) and advanced social engineering tactics, fraudsters have been able to infect an infinite number of users with crimeware through social networking sites. While the scams are countless, one of the most common techniques works as follows: A Trojan embeds itself on a user's computer. When the user logs on to a social networking site, the Trojan automatically generates an invitation to everybody on the user's contact or "friends" list with an invitation to view a link or a video. Many people will accept the invitation as they feel they can trust the source (the social engineering). As a result of trying to run the file or software updates associated with it, they will get infected with a Trojan.

VI. Conclusion

Even though it is a criminal enterprise, the fraudster underground can draw the following comparisons to most legitimate businesses in operation today:

- **It's all about the money**. The bottom line is that no fraudster is assuming the high risk of getting caught without a handsome reward.
- **A division of roles**. Just as a legitimate business has marketing and sales, R&D, engineering and finance departments, each fraudster assumes a specific role – whether as a harvester or cashier.
- **Innovation and technology are essential**. Fraudsters must continually develop their technology to circumvent the advanced security solutions deployed by organizations and anti-virus protection used by consumers.
- **A good reputation brings back repeat business**. Like a legitimate business that thrives on reputation and brand loyalty, fraudsters with a demonstrated reputation are likely to be rewarded with more business.
- **Diversification is the key to success**. Fraudsters must diversify their business practices in order to win new business among other fraudsters while simultaneously offering products and services that effectively address the ever-changing behavior of the online users they target.

[5] Nielsen, "Global Faces and Networked Places," March 2009
[6] Breach Security Labs, "Web Hacking Incidents Database (WHID) 2009 Bi-Annual Report"

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

FUNDER WP 0909 H11934

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC