



The Security Division of EMC

Report

Special RSA Online Fraud Report: What to Expect in 2009 and Beyond



Online fraud is a non-stop threat to organizations around the globe, and cybercriminals have no intention of slowing down the pace. In fact, they continue to improve their technology, launch increasingly sophisticated attacks, and use

advanced social engineering techniques to dupe online users into falling for scams. Also, global conditions, such as the receding economy and vulnerabilities in the financial markets, are likely to have an impact on the evolution of cybercrime.

The RSA Anti-Fraud Command Center has developed a list of the top trends in global online fraud it expects to see develop within the next 12 – 18 months. The RSA Anti-Fraud Command Center is on the forefront of new threat detection and fraud intelligence and offers an experienced team of fraud analysts who work 24x7 to shut down fraudulent sites, deploy countermeasures, and conduct extensive forensic work to catch online criminals and prevent future attacks. The RSA Anti-Fraud Command Center works on a global scale and has established direct, open channels with over 9,000 ISPs, registrars and web hosting companies around the world, as well as dozens of law enforcement agencies and CERTs.

To date, the RSA Anti-Fraud Command Center has:

- Shut down over 140,000 online attacks¹
- Reduced rates of online fraud in over 140 countries
- Reduced the average lifespan of a phishing attack to a median of just five hours

This white paper will review recent online fraud tactics, many discovered or witnessed by RSA, and provide a series of predictions for online fraud trends RSA expects to see in the next 12 – 18 months.

The use of fast-flux botnets will increase

In 2008, RSA saw the development of several “bullet-proof” fast-flux network hosting services which were both deployed and provided for a fee for use by other online criminals. And within those fast-flux networks, the RSA Anti-Fraud Command Center observed that online criminals were using them to launch both phishing and Trojan attacks and other malicious content such as money mule recruitment sites.

Fast-flux is an advanced 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 fast-flux networks is difficult as the content servers that host the phishing and malware sites are hidden behind a cloud of compromised machines, causing a constant rotation of IP addresses, and thus avoiding detection.

Fast-flux networks are becoming increasingly popular in the online fraud community for two main reasons:

- Scalability. An attack using a fast-flux botnet is easy to set up. Service providers in the fraud community provide the infrastructure to launch the attack (i.e., fraudsters can rent a botnet and a content server for a nominal monthly fee). An online criminal just needs to establish a new domain and start spamming.
- Stability. Fast-flux networks are long-lasting and can be easily reused. The core infrastructure is considered very stable since the content servers are “hidden” behind the proxies and are theoretically harder to detect.

In 2008, 44% of the phishing attacks detected by the RSA Anti-Fraud Command Center were hosted on fast-flux networks. Over the next year, RSA expects to see a steady increase in the use of these hosting services for phishing attacks and other malicious content such as Trojan infection points, Trojan drop points, and mule recruitment sites. RSA also anticipates that the transition to fast-flux networks will move past the early adopter stage and become a more mainstream hosting method used by online criminals.

¹ Statistic provided as of March 2009

Trojan functionality and infrastructure will improve

The advanced stealth technology and other features of financial Trojans already exist. Trojans can now steal a wide variety of online credentials and assets and remain undetected for a considerable amount of time – as evidenced by the repository of stolen credentials stolen by the Sinowal Trojan discovered by RSA in October 2008. The Sinowal Trojan maintained one of the most advanced and reliable communication infrastructures which allowed it to gather and transmit information for almost three years. In that time, more than 500,000 compromised credentials were collected.

RSA predicts a rapid improvement in Trojan functions and infrastructures in the coming year. In terms of functions, RSA fraud analysts have already started to see various Trojan plug-ins available for sale in the underground. An example of such a plug-in is the “balance grabber,” named as such because it automatically grabs the balance of an account and delivers that information along with the compromised credentials to a fraudster’s drop zone. This saves online criminals the time required to login to an account to check account balances and credit limits.

While functions will improve, RSA believes a primary focus over the next 12 months will be on improving the Trojan infrastructure. Similar to phishing websites, most Trojan hosting servers can still be easily detected and shut down, but this is changing. RSA expects the Trojan hosting infrastructure to evolve as online criminals will use both fast-flux networks for infection and/or drop domains and other alternatives such as the private networks similar to that used by the Sinowal Trojan.

These private networks are under the control of Trojan herders and introduce rotating servers that mirror each other and a wealth of domains and IP addresses. In addition, some Trojans that lose communication with the “mother ship” are capable of searching the Internet for new command and control (C&C) domains, based on a pre-defined formula for creating new domain names. Through automated searching, infected machines are able to recover and communicate with new C&C domains, even when the original “mother ship” is not available.

Finally, in 2008, RSA detected several software toolkits that were sold within the fraud underground that enable online criminals to create new Trojan variants within seconds. With slight modifications to the Trojan binary file, a new file can be created each time an infection campaign is launched.

This makes the Trojan appear as a new file when scanned by anti-virus engines, providing some “breathing space” before detection. The ability to create new binary files with the click of a mouse makes these Trojans undetectable for a longer period of time as no new variant is similar to its predecessor. As the development and propagation of such software toolkits continue to increase over the next year, RSA predicts to see the number of unique Trojan variants soar and challenge the rate of detection by anti-virus providers.

Fraud-as-a-Service – new services popping up in the criminal economy

Fraud-as-a-Service, or “FaaS”, is not a new concept. FaaS was coined by RSA in November 2008 to refer to the advanced supply chain that offers goods and services for sale to online criminals to aid them in committing fraud. In 2008, RSA observed an increase in the amount of services offered for hire in the underground – everything from hosting services, to Trojan infection kits, to cashout services.

RSA expects these services to evolve even further over the next 12 months in order to support the development of the fraud economy. Online criminals turn to “one-stop” service providers who offer centralized fraud services. These services are provided for a flat fee or on a subscription basis, depending on the nature of the service, and help facilitate some tasks which the common criminal may find to be too complicated to accomplish. RSA anticipates the following underground services will grow:

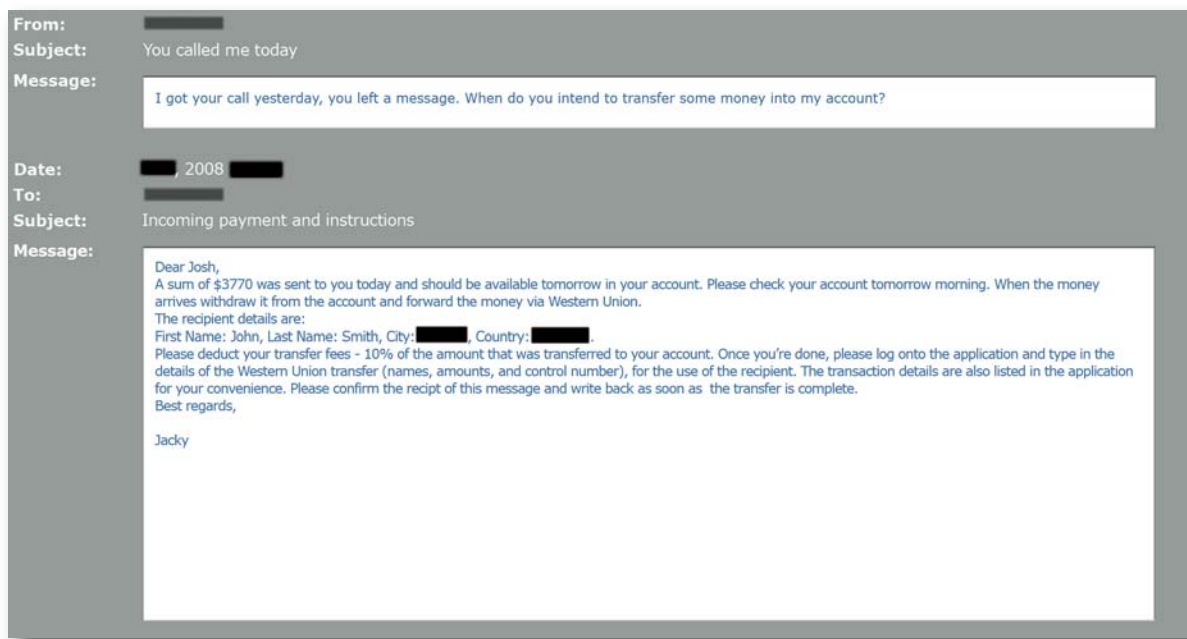
- **Centralized Trojan infection.** This service will allow various criminal groups to infect users’ computers worldwide through a centralized infection service and is already being used by criminals who pay a per-infection fee to a service provider.
- **“All-in-one” Trojan packages.** Trojan servers with C&C panels are available for sale in the underground, along with corresponding botnets of infected computers. Criminals that purchase these services receive control over a Trojan, with all of its corresponding C&C features, and over hundreds or thousands of computers already infected with the Trojan.

- **Ready-made HTML injection kits.** These kits will be crafted by service providers and sold within the underground. HTML injections are very common as part of almost any Trojan attack. These bogus pages are already developed by subject matter experts and sold within centralized repositories, very much like phishing kits.
- **Professional call center services.** Online criminals will use these services in order to commit phone channel fraud and also facilitate fraud in other channels. Such services already exist and provide online criminals with the capability to conduct phone channel fraud to any destination and in any language.

Money muling

Money mule recruitment networks and “mule herders” – managers who control the network of mules – are a specialized cashout service offered for sale within the fraud underground. In 2008, RSA observed numerous mule recruitment scams that directed online users to websites that offered allegedly legitimate jobs to perform money transfers. These websites lured people to 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. As a result of the weakened global economy, RSA expects that money mules will be easier to recruit over the next year or two until the economy improves, and more money muling operations will develop over the next year. The continuing economic slump means more people will be looking for jobs and will be less selective in the jobs to which they apply. This will enable online criminals to recruit more people as money mules.

A real sample of correspondence between an online criminal and a potential mule.



Fraudster adaptations to two-factor authentication deployments

With the advent and rapid increase of online banking in certain parts of the world, online criminals have new markets and victims to potentially exploit. As a result, various types of two-factor authentication technologies continue to be deployed around the globe. RSA expects online criminals to respond to the increased deployment of two-factor authentication in a number of ways:

- The number of Trojan attacks attempting to bypass two-factor authentication measures will increase. Even though RSA still expects to see more phishing than Trojan attacks, the proportions of these two leading attack vectors are likely to change in order to circumvent the new security mechanisms.
- Two-factor authentication will directly affect the level of sophistication we see in Trojans in terms of both technical features and the social engineering techniques surrounding the attack. RSA expects online criminals to improve these techniques, luring Internet users into divulging personal and financial details that will assist them in attempting to bypass two-factor authentication measures.
- Fully automated man-in-the-browser (MITB) and “human-in-the-middle” (HITM) attacks. The intimidating concept of fully automated MITB Trojan attacks is now spreading into new territories where two-factor authentication is deployed, but is still not as widespread as other tactics. RSA expects that such attacks will continue to increase, but will be specific to certain geographies that have a greater density of two-factor authentication deployments.

RSA also anticipates an increase in the number of HITM attacks which require the presence of a person who operates in real-time (or near real-time) and in parallel to the legitimate online user. These attacks involve social engineering techniques that are intended to bypass two-factor authentication. The victim’s personal details and authentication credentials are sent, in real-time, to a criminal who manually logs into an online banking account to conduct fraudulent transactions. These attacks are not completely automated and require human involvement.

- Transaction signing will be targeted. Some financial institutions employ two-factor authentication solutions in order to “sign” and authenticate a specific transaction. This is especially common within business and

commercial banking units. RSA expects to see an increased effort to bypass transaction signing methods, most likely through the combination of social engineering and Trojans.

The consolidation of “traditional” phishing and malware attacks

In April 2008, RSA discovered a new technique that merged classic phishing and malware content and tactics. The Rock Phish group was the first to pioneer this double vector attack as they used both phishing sites and the Zeus Trojan to attack and infect online users. Upon receiving the fraudulent correspondence, victims of these attacks were directed to phony websites that solicited personal information. Concurrently, the Zeus Trojan infected their computers. Therefore, even if the online user did not fall for the phishing scam and divulge personal details on the website, the Trojan would later steal information that was transmitted while the victim interacted with other websites.

As online users have become more educated about cybercrime and the risks they face by providing their personal information on many websites, criminals have had to develop alternative ways to dupe them. By leveraging spammed emails designed to initiate a phishing attack and direct unsuspecting users to a malware infection site, criminals achieve greater results. In this way, a computer infected by a Trojan via this attack method helps to ensure that fraudsters can gain access to personal information without requiring online users to submit their information themselves.

The volume of phishing attacks detected by RSA during 2008 grew 66% over those detected throughout 2007. Despite heightened awareness among online users, phishing remains a popular platform for fraudsters as it has a very low execution cost, can reach broad sets of users, and requires limited technical expertise to set up. For these reasons, RSA expects that the rate of phishing attacks will continue to increase throughout 2009 and beyond. And while silent “drive-by download” infections (in many cases, planted within legitimate web pages) is a leading Trojan infection method, RSA anticipates an increase in combined phishing and Trojan attacks. Socially engineered online attacks using spammed email that contain information on popular societal issues² will also serve as an additional way to direct unsuspecting users to malware infection sites.

Enterprise fraud will increase

Enterprise fraud is still in its infancy and online criminals are just starting to realize the potential benefits of it. RSA has witnessed many incidents of enterprise credentials being compromised by Trojans. For example, RSA's fraud analysts have uncovered VPN and webmail account credentials within drop zones during the credential recovery process. RSA has also witnessed transactions occurring among fraudsters such as the solicitation of e-mail addresses for top executives at U.S. corporations going for as much as \$50 each. This is indicative of the likelihood there will be an increase in the number of spear phishing³ incidents in the coming year.

RSA expects to see an increase in enterprise fraud in the next 12 – 18 months. This is an especially nefarious threat as online criminals stand the chance of gaining access to sensitive corporate data such as intellectual property and business plans.

Layered security is the best protection

Staying a step ahead of online criminals and being prepared to address new threats as they come knocking at the door is critical to fending off fraud. Organizations must consider instituting a layered approach to security which is key to lowering the overall risk that online crime poses. A layered security approach has three core elements:

- Understand the threat landscape
- Use multi-factor authentication to protect login
- Monitor user activities and transactions

Understand the threat landscape

Organizations must understand the threats that are targeting their business and the relative risks they pose. By doing so, organizations can mitigate the risk of online fraud or even prevent it from occurring at all. By gathering and sharing intelligence and developing a broad knowledge of potential threats, organizations can better evaluate their own vulnerabilities and implement security solutions to address them.

Use multi-factor authentication to protect login

Username and password authentication is not enough to protect access to sensitive data with the advanced nature of today's threat landscape. Moreover, many countries have imposed regulations requiring organizations to protect access to user accounts and personal information with a second form of strong authentication. Multi-factor authentication is essential to preventing unauthorized access to a user's sensitive and personal data.

Monitor transactions and activities that occur post-login

Beyond authentication solutions that challenge users to assure their identity at login, organizations should consider implementing a transaction monitoring solution that analyzes and challenges high-risk transactions after login has occurred. Transactions typically require more scrutiny and pose more risk to organizations and their customers than just the act of logging in to an account. Transaction monitoring can help identify suspicious post-login activities and mark them for further review.

³ For more information on similar scams, read RSA's blog, *Online Fraudsters Prey Upon the Media and Public Interest in Current Events to Launch "Cease-Fire Trojan Attack."* http://www.rsa.com/blog/blog_entry.aspx?id=1416

³ A fraud attempt that targets organizations, most often executives at the company, in an attempt to gain access to sensitive corporate data.

Staying a step ahead of online crime

RSA is on the forefront of fraud detection. Our team of fraud analysts are dedicated to staying abreast of all the latest threats and fraud trends and sharing that expertise with our customers and the public. Following are highlights of some of the major discoveries we have reported on:

February 2009: RSA discovered the source code of a desktop application that functions as a payment card checker to test the viability of illegally obtained payment cards before they are used. The card checker application can be employed on a mass scale and automatically sends authorization requests through a legitimate online merchant's web site. During the check, any error message that is received is interpreted by the online criminal as an invalid account.

January 2009: RSA identified a fraud website coined the "Web Injection Shop" that sells HTML injections designed to steal information from online users. The injections are tailored to 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 runs locally on the user's PC and seeks out a bank account's balance field, copies the amount and sends it to the criminal's drop server.

January 2009: RSA uncovered and shut down 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 webpage 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, but were actually launching a Trojan designed to capture financial and personal information of the infected user.

October 2008: RSA announced the discovery of a backend server containing more than 500,000 compromised credentials that were collected by a Trojan known as Sinowal, or Mebroot. The Trojan is believed to have been collecting information from infected PCs since 2006, including online banking credentials and credit card data. In total, Sinowal infected more than 300,000 PCs.

July 2008: RSA reported that information had been discovered that indicated the creators of Neosploit were closing down. Neosploit is the one of the most advanced infection kits used by online criminals to exploit numerous system vulnerabilities and infects PCs worldwide with malware. RSA was wary of the claim, reporting whether Neosploit "will actually cease its business, and whether or not it will return, is a question that only time can answer." In August 2008, Neosploit reemerged in the fraudster underground.

April 2008: RSA discovered a new technique used by the Rock Phish group that spread the Zeus Trojan, a form of financial crimeware, using traditional phishing tactics. Victims of these attacks were subject to having their personal data stolen and getting infected with the Zeus Trojan.

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 and access control, encryption and key management, compliance and 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.



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

The Security Division of EMC

RSA and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2009 RSA Security Inc. All rights reserved.

RSATRENDS WP 0409