RSA®

The Security Division of EMC

White paper

Fighting the Enemy: Making Sense of the Growing Crimeware Threat

The most popular method used to commit financial fraud in the online channel is by identity takeover. This occurs when a fraudster takes over an existing identity or account in order to steal funds from the account. Committing fraud through traditional identity theft tactics, such as creating a new identity and defaulting on a loan, still exist but are not as prevalent as the online channel offers several advantages for fraudsters. There are several reasons that fraud has continued to increase in the online channel, including:

- Universal accessibility: The Internet allows fraudsters to operate on a global scale, with relatively little bearing on geography, language or nationality
- Scalability : Alternatives to identity takeover are costly in terms of resources and sophistication
- Ease of operation: Taking over an existing identity and impersonating a genuine user is easy
- Anonymity: The Internet offers complete anonymity and makes it difficult to track the true identity of a fraudster

Identity takeover in the online world has traditionally been performed through "social engineering" tactics, usually a scam that unwittingly dupes consumers into revealing their personal credentials (such as username or password). Phishing, the act of posing as a legitimate organization or entity, usually via email, and directing consumers to a fraudulent website with the intent of acquiring their personal information, is the best example of this approach and most commonly used by fraudsters.

Hacking, the act of "breaking in" or using vulnerabilities on an Internet site in order to gain unauthorized access, has been romanticized in popular culture but has rarely been used as a technique to commit financial fraud. Hacking is used more often as a tool to set up infrastructure for other types of scams (such as hosting for phishing attacks or as a method for malicious software to be spread) or to penetrate relatively small and unprotected websites in an attempt to re-use the credentials in their databases on larger financial sites.

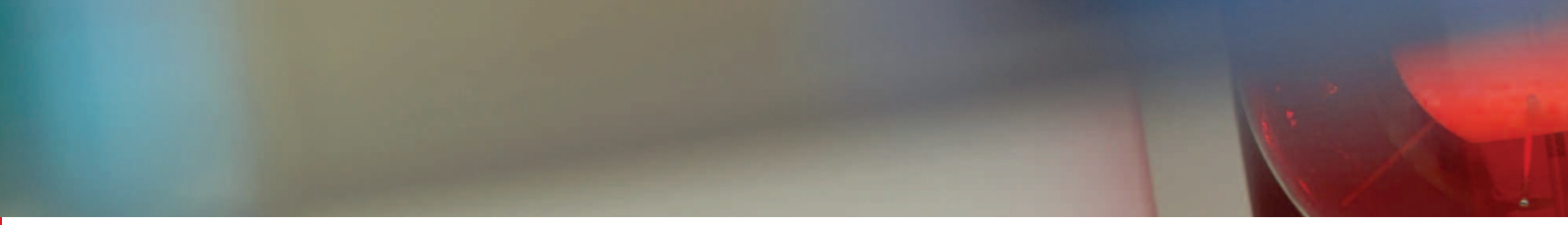
As organizations have learned to effectively manage the known risks and fraudsters seek to increase their yield, a new method of identity and account takeover has emerged—crimeware or financial Trojans.

Crimeware: The Next Generation Threat

Crimeware is a malicious program that is downloaded unknowingly onto a user's PC either by deceiving the victim into running it or by exploiting a vulnerability in the user's operating system, browser or other software installed on the PC. While there are many different types of malicious software in the online world, crimeware, for the purpose of this paper, can be defined as any malicious piece of software that satisfies at least one of the following criteria:

1. Stealing online credentials, personal data, or any other piece of information necessary for identity takeover, with the intent of using the stolen identity to steal funds

2. Performing unauthorized online transactions in order to steal funds; this includes Trojans that "hijack" online banking or other secure sessions of infected users and carry out fraudulent transactions after the user has logged out



Crimeware may perform secondary actions, as well. Most commonly, crimeware may disable protective systems on a user's PC, such as anti-virus software or personal firewalls, or even use the infected machine as a platform to commit fraudulent activities. For example, some crimeware exploits a user's infected PC to send out spam emails or as a hosting site for phishing attacks (as part of a botnet).

Crimeware can be broken out into two categories. The first category of Trojans includes keyloggers, screen-scrapers, and pharming Trojans such as Torpig, Briz, Haxdoor, and Gozi/Banksniff. The second category is more rare and less publicized than the others; it includes the e-gold Trojan and some variants of the Metaphisher Trojan.

The Rise and Spread of Crimeware

In order to understand the prevalence of crimeware and its impact, one needs to consider the reason for its emergence from the perspective of a fraudster. Online fraud tends to occur where the functionality is conducive to fraudulent behavior. The preferred targets for online fraud include those sites that allow:

- The ability to transfer funds that are as close to instantaneous as possible (transactions that take a long time may be detected as fraudulent, cancelled, or used in order to set up a "sting" operation)
- The ability to commit money laundering
- The ability to emulate a real user's behavior

The evolution of crimeware transpired to address the two main challenges facing the fraudster community with regards to this functionality:

- Scalability – or getting "more bang for the buck"
- Adaptation – overcoming new security measures that institutions or governments have implemented to combat online fraud

In terms of scalability, there are certain markets and geographies where the functionality that is beneficial to fraud has matured and the traditional methods of perpetrating financial fraud do not fully utilize the potential of the market for fraud. Thus, crimeware was developed as a means to effectively compromise more credentials (versus traditional methods of attack), albeit at a higher investment in infrastructure and operational costs. As such, crimeware is likely to continue existing side-by-side with more traditional methods of online fraud such as phishing, credential "replay" and dictionary attacks.

In terms of adaptation, because of the implementation of measures such as strong authentication and increased consumer awareness, traditional online attack methods that rely on the user to willingly surrender their personal credentials have become less effective or even useless. Instead, fraudsters are left to rely on crimeware to replace traditional forms of fraud.

Spotlight on Trojans: Torpig

Torpig – also know as "Anserin" or "Sinowal"—is one of the more nefarious families of Trojans – a set of malicious code that embeds itself on a user's computer, targeting a variety of personal information, though primarily online banking credentials. Once a user logs in to a site, Torpig overwrites the genuine page – while still maintaining the valid SSL and address bar – with the same look-and-feel of the genuine site. Most users are often unaware that a Torpig is even on their computer as it is very difficult to detect.

Torpig also retrieves all usernames and passwords saved on Internet Explorer, Outlook, Eudora, etc. The value in having credentials, such as email address and password, is that some financial institutions send confirmation emails of particular transactions having been completed. By having the email address and password of the genuine user, fraudsters can sign-in to the email account and delete the email, thus the genuine user is not immediately aware of the fraudulent transaction that has taken place.

Torpig is extremely dangerous and constantly evolving. Torpig also can't be deleted in a running system since it's always running on an infected user's system. In addition, it updates itself several times a day via the "mother ship", a command-and-control server operating from an unknown location using a cryptographic communication channel, further adding to the difficulty in mitigating this type of crimeware.

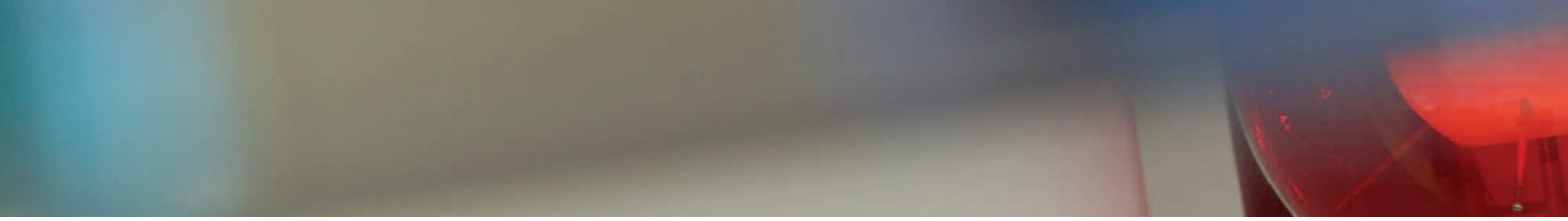
Quantifying the Crimeware Threat

The prevalence of financial crimeware and Trojans are increasing at an alarming pace:

- In 2006, SOPHOS saw more than 41,000 new malware threats
  - 41% contained spyware characteristics
  - 42% were downloaders, designed to turn off security before downloading crimeware
- Recent RSA analysis of a single Gozi/BankSniff variant showed 30,000 infected users in a single month.
- Prices of crimeware in the fraudster underground are also falling, indicating a maturing of the market for malicious code.

In understanding how this analysis translates to actual impact, we must consider several criteria.

Geography. There are certain geographical regions that are already almost exclusively hit by financial Trojans. For example, in Germany, over 90% of online banking fraud is the direct result of Trojans. The same can be said for Benelux, Switzerland and other geographies. In these geographies, regulations or laws have mandated strong authentication at login for online banking services which makes simple fraud attacks like phishing, replaying credentials from stolen databases, or brute force guessing less effective. In countries where one-time password tokens are common, more sophisticated types of crimeware are at play, such as session-hijacking Trojans and their associated variants. In the U.S, with the FFIEC Guidance requiring financial institutions to employ strong authentication at login, Trojans are likely to succeed phishing as the major type of online banking fraud in the future.



Impact of a single attack. To understand the impact of Trojans, we must compare a phishing attack to a Trojan. A phishing attack usually lives between 5 hours or fewer (if you are a customer of the RSA®FraudAction℠ anti-phishing service) to an industry average of 105 hours[1]. RSA recently analyzed the logs of a Trojan called Gozi/Banksniff that was active for five months before being shut down. The Trojan went undetected by most major anti-virus vendors during that time and it compromised 30,000 new computers a month on average (compared to several dozen credentials that a typical phishing attack might yield).

Consequences. For financial institutions, it is much more difficult to manage the risk associated with Trojans because:

- They have no control over their users' PCs and cannot mandate patches or anti-virus protection.
- Unlike a phishing attack that cannot be hidden (it will eventually be reported) or a brute force attack (someone will eventually go over the logs and see it), Trojans can remain undetected for months, causing financial institutions unimaginable fraud losses and general loss of consumer confidence in the online channel.
- Financial institutions are affected by crimeware despite not being directly attacked, yet they are often financially liable for the losses associated with an attack.

Another way of determining the potential havoc created by crimeware is to examine the susceptibility of consumers to fall prey to this type of attack.

Every online user is susceptible to downloading a piece of crimeware onto their computer. While crimeware has traditionally been spread by links in emails or attachments, there is a more frightening trend emerging - the spread of Trojans through legitimate online sites. This occurs when a fraudster hacks into a legitimate site and infects users with a Trojan by prompting them to download a program or exploiting a vulnerability in Microsoft Windows or Internet Explorer, which then silently infects the user's computer. A good example of this was the use of the Miami Dolphins official website to spread a keylogger (a piece of crimeware that steals information typed through the browser) during the Super Bowl. And the ever-growing phenomenon of Web 2.0 further exacerbates the potential for millions of users to be silently infected by crimeware as content is shared and distributed freely across the web (such as via YouTube and MySpace). In a recent consumer research study conducted by RSA, nearly half of online users worldwide are already increasingly concerned about Trojans and crimeware – and this figure is expected to rise sharply over the next several months.

Behind-the-Scenes: Evolution of Crimeware Technology

- Most Trojans today are rootkit-based and progressively moving towards all being rootkit-based in nature.
- Major Trojan "vendors" closely monitor major anti-virus companies to see if their software is being detected. If their crimeware is detected, they issue an update "within hours" for a small fee.
- Most Trojans are designed to circumvent special "visual key" grabbing technology, such as virtual keyboards, JavaScript keyboards, and FLASH-based keyboards.
- Select Trojans can delete cookies, cache and auto-complete passwords from Internet Explorer, Firefox and Opera in order to force the user to retype his personal credentials.
- Some Trojans have the ability to do local pharming by using the system API, rather than by modifying the hosts file.

1 Source: Anti-Phishing Working Group (APWG)

Spotlight on Trojans: Gozi/Banksniff

The Gozi/BankSniff Trojan was first witnessed in 2005 and has been infecting and targeting customers of financial institutions and other web sites in order to steal user credentials ever since. Gozi/BankSniff collects usernames and passwords of targeted web sites, including those of banks, online merchants and email providers such as Google and Yahoo!. The crimeware waits until the user of the infected computer accesses a targeted site, and then performs key-logging, thereby collecting the user's details and sending them to a "drop" server(s).

Although Gozi/BankSniff is not a new threat, many anti-virus products cannot detect it as it constantly changes through a fast mutation process. In addition, the crimeware's communication with the drop server and its control channels can be encrypted. The Trojan's remote control access is password-protected, and the Trojan's controller uses a different password for every infected computer.

In January 2007, RSA was able to identify the Trojan's main drop server and obtain logs of information stolen by the Trojan which was collected during a one month period. The size of the log file indicated that a huge amount of information had been collected compared to other crimeware that RSA had detected in the past. Other interesting findings from RSA's analysis include:

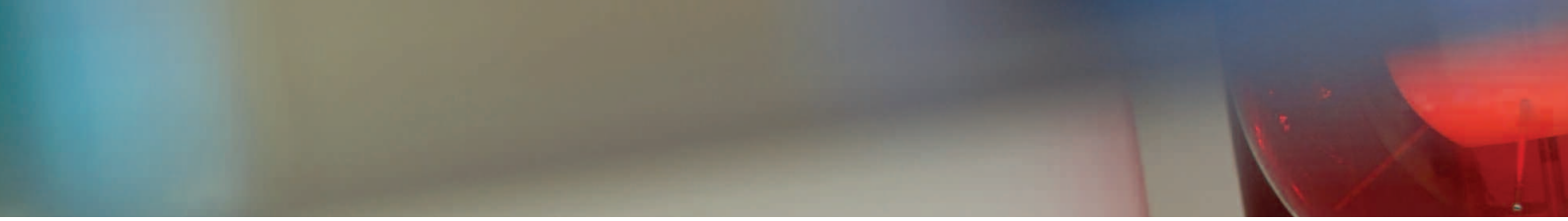
- The logs indicate that the Trojan collected the usernames, passwords, IP addresses and browser information of 50,000 – 70,000 infected computers in the one month period. The total number of account details that were stolen during this period was 9,993.
- IP-geo location data of the victims indicate that the Trojan's infection base is widespread. During the month, the Trojan collected information from users' computers in 160 countries, primarily in Turkey, India, U.S., Brazil, U.K. and Germany.
- Analysis of the logs indicates that the Trojan's owners arrange the data that they collect in a well-structured SQL database. Information can be retrieved from this database based on the IP address, targeted site and other characteristics of the data.

Current mitigation strategies

The standard means of combating malicious software focus on software running on the potential victim's machines or within an organization's perimeter. This strategy is usually inadequate in fighting financial crimeware for the following reasons:

1. Non-direct protection. Despite the fact that financial institutions can fall victim to financial Trojan attacks, they cannot directly protect themselves against these attacks by installing software, as the malicious software resides on their customers' computers and not within their own infrastructure. Financial institutions usually cannot control or enforce their customers' use of appropriate anti-virus software or ensure that signatures and patches are up-to-date. While many financial institutions develop programs and campaigns in an attempt to educate their customers on how to avoid becoming infected by crimeware, in many cases, this approach has not proven to be very successful.

2. Awareness of the attacks. While a phishing attack is visible and thus more easily detected, it is often difficult for a financial institution to know that it is being targeted by crimeware. Most Trojans are passive and do not show any interaction with the end user, lessening the chance that a customer will report unusual activity. In addition, a financial institution cannot usually detect the attack from information in its own servers and anti-virus vendors rarely publicize which institutions are attacked by a given piece of malware (they typically provide information on how to remove the malware and how it operates). The result: Trojans are often the 'mysterious' or 'silent' cause of unattributed fraud losses.



3. Ineffective solutions. Most anti-virus solutions are rarely effective at protecting consumers from these types of Trojans – even when they do have anti-virus software installed. Why?

- Low coverage. Financial Trojans are less widespread than botnets, spyware or other types of malicious software, making them harder to detect. Therefore, Trojans typically receive a lower priority from anti-virus vendors.
- Insufficient impact. Anti-virus vendors usually prefer to release updates for malware that has a noticeable impact on the consumer's machine. Since these types of Trojans are passive, they are likely to receive a low update priority.
- Time-sensitive. Unlike botnets or spyware, these types of Trojans are time-sensitive. Much damage can be done in the time it takes an anti-virus company to release an update.

Mitigating the Threat of Crimeware

There is no pinpointed solution to mitigate the threat posed by malicious crimeware. Financial institutions must employ a layered approach, combining a variety of solutions that are each designed to fight the threat of crimeware at different levels.

1. The first point of possible defense lies within the functionality of an institution's own applications. For example, dividing payment transfers into two categories—the first category would allow an immediate transfer to existing payees and the second category would require a 24-hour delay in transferring funds to new payees. By implementing such measures, real-time "session hijacking" or Man-in-the-middle attacks would be nearly impossible as it is highly unlikely that the fraudulent destination of a money transfer is one that the legitimate user has transferred funds to in the past.

2. Financial institutions should employ a Trojan and phishing intelligence and shutdown service, such as RSA® FraudAction℠, which provides information and analysis of the new variants of crimeware that exist and the ability to take action against malicious software if it is affecting an institution's customer base.

3. Implementing a solution that provides strong authentication at login, such as RSA® Adaptive Authentication for Web, could make most information gathering crimeware irrelevant or ineffective.

4. By utilizing a real-time, back-end fraud monitoring solution, such as RSA® Transaction Monitoring, financial institutions could track and locate fraudulent transactions that are the result of account takeover and greatly reduce the ability of "session-hijacking" or Man-in-the-middle Trojans to operate.

Additional Information

RSA's Anti-Fraud Command Center (AFCC) operates on a 24x7 basis to shut down phishing, pharming and Trojan attacks. To date, the AFCC has shut down more than 40,000 attacks in over 130 countries. For more information, please visit www.rsa.com.

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 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. ©2006-2007 RSA Security Inc. All rights reserved.

CRIME WP 0607

RSA
The Security Division of EMC

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