



The Security Division of EMC

White paper

# Mitigating Man-in-the-middle and Trojan Attacks

Best Practices for Combating Emerging  
Threats with Layered Security



# “How can you defend yourself from something you can’t see?”

As financial institutions across the globe continue to deploy strong, multi-factor authentication, fraudsters are simultaneously developing more sophisticated ways to launch attacks and to circumvent established security measures such as one-time password (OTP) authentication. Man-in-the-middle, Trojans and other malicious software (“malware”) attacks are the emerging means that fraudsters are using to target financial institutions and their customers.

Man-in-the-middle and malware attacks are happening today and are emerging as the latest practical and “in the wild” threats. The number of attacks has been increasing steadily as the level of difficulty and cost of execution for fraudsters has been lowered. Statistics released by a number of sources are alarming and support the reality that the threat is not going away. According to a security report released by Sophos, a web page is infected with malware every five seconds. In addition, Microsoft® reported that malware was removed from more than 450 million unique computers worldwide in the second half of 2007.

---

## Contents

---

The Evolution of the Fraud Landscape	page 1
A New Wave of Online Threats	page 1
Best Practices for Mitigating Advanced Threats	page 2
Understand the threats that are targeting your institution	page 2
Use multi-factor authentication to protect login	page 3
Monitor transactions and activities that occur post-login	page 3
Making the Most of Security Investments	page 4
Educating Your Customers	page 5
Summary	page 5
Appendix	page 6

In this white paper, we will examine:

- How the fraud landscape has evolved
- The types of advanced threats facing financial institutions and how to protect against them
- Best practices for implementing a layered approach to security
- How financial institutions can make the most of their security investments by applying the principles of vulnerability, materiality and probability of risk
- The effect of customer education on minimizing the risk of future attacks

---

## The Evolution of the Fraud Landscape

---

The widespread implementation of strong authentication has made it extremely difficult for fraudsters to get into bank accounts to steal money. In addition, the increase in consumer education about phishing and identity theft has made it harder to dupe customers using traditional attack vectors. This has forced fraudsters to evolve by increasing their level of sophistication in many areas, but mostly in the technology and tactics they use to gain access to online accounts.

A recent example is the use of malware by the Rock Phish gang, reported by RSA in April 2008. “Rock Phish” refers to a series of ongoing phishing attacks that have been targeting financial institutions worldwide since as early as 2004. The Rock Phish group is believed by many experts to be responsible for more than half of all phishing attacks worldwide. Traditionally, they have used a network of compromised computers (often called a “botnet”) to send spam and phishing e-mails. The concept behind the attacks and the architecture used by the group make it extremely difficult to shut them down.

However, the Rock Phish group elevated their level of sophistication in recent attacks by using their phishing sites as malware infection points. More specifically, if an online user clicks on a link and is redirected to one of these phishing sites, in addition to having their personal data stolen, they are also infected with the Zeus Trojan to steal additional information in the future. The Zeus Trojan is designed to perform advanced key logging when infected users access specific web pages, including pages which are protected by SSL protocols.

# The implementation of strong authentication has made it extremely difficult for fraudsters to get into bank accounts to steal money.

Another recent example is the use of social engineering techniques to dupe online users into downloading malware onto their computers. Fraudsters are sending e-mails posing as legitimate businesses to online users, providing a tracking number for an undeliverable package or details of recently purchased airline tickets. A zip file is attached within the e-mail that claims to have information on the package shipment or particulars of a flight itinerary, but it actually contains harmful malware that is downloaded with the intent of gathering personal details, passwords and other information from the user’s computer.

---

## A New Wave of Online Threats

---

The increase in man-in-the-middle and Trojan attacks is further evidenced by the increased demand for malware on the black market. It is such a hot commodity that malware developers even offer upgrade packages that include service level agreements and technical support to buyers in the fraudster underground and guarantee that if malware strains become detectable by anti-virus providers, they will deliver a new “undetectable” variant at minimal cost.

To demonstrate this threat in the real-world, one only needs to turn to a recent blog by Brian Krebs on [washingtonpost.com](http://washingtonpost.com). In June 2008, it was reported that malware-laden e-mails had been sent to individuals at small- and mid-sized businesses. When opened, malware proceeded to be downloaded onto their computers. When someone with an infected computer attempted to login to their banking site with two-factor authentication (in this case, one-time passwords), the fraudsters were able to display a page on the victim’s screen that looked like the legitimate bank site with an alert that read, “Please allow 15 to 30 minutes for your request to be synchronized with our server.” In that time, the fraudsters were able to intercept the user’s regular password and one-time password, and unbeknownst to the user, drain the bank account in the background.

### Emerging Threat Alert: Man-in-the-browser Attacks

A man-in-the-browser attack occurs when a fraudster installs a Trojan on a user's computer that is capable of intercepting and/or interacting with the user's online transactions in real-time. Unlike a phishing attack, where the user is directed to a fraudulent website, most often by clicking on a link in an e-mail, a man-in-the-browser attack occurs simply when the user enters a URL into their browser – or clicks on a stored bookmark – independent of being triggered by a prompt such as an e-mail or other notification.

It operates in similar fashion to session-hijacking / funds-transfer malware in which the wiring out of funds occurs in real-time, and isn't otherwise focused on simply stealing credentials (such as an online banking username/password or credit card number) for use at a later time. A man-in-the-browser attack is a type of man-in-the-middle attack, but is done in the browser and closer to the user rather than on the traffic stream. A man-in-the-browser attack is more difficult to detect and prevent, however, because the action is actually occurring on the user's machine. Internet Explorer® and Firefox® have both been circumvented.

Many analysts and industry observers have recommended that companies implement a transaction protection solution as a way to mitigate the risk of being targeted by a man-in-the-browser attack.

This is a clear-cut case of the man-in-the-middle attack “theory” coming to life. It demonstrates the lengths to which fraudsters are willing to go (and even more menacing, are capable of going) to circumvent one of the most advanced security defenses on the market – one-time password (OTP) technology. (For an in-depth look at the threats targeting financial institutions today, see the Appendix )

Is there a silver bullet for stopping fraud? And what approach can financial institutions take to minimize the effect on their customers, their brand and assets, and the integrity of their online channel?

---

## Best Practices for Mitigating Advanced Threats

---

There are several individual solutions available on the market today to help financial institutions combat the threat of new innovative attack methods and the spread of malware. However, security experts agree that a layered security approach that combines external threat protection, login authentication and risk-based transaction monitoring is the ideal solution for providing the most comprehensive protection to online users. Applying the following best practices can help financial institutions mitigate the risk posed by advanced threats.

### Understand the threats that are targeting your institution

The first step is to understand the nature of the threats that are targeting your business. By proactively identifying the threats that exist, financial institutions can mitigate the damage that is caused by an attack or even prevent it from occurring at all. By gathering and sharing intelligence and developing a broad knowledge of potential threats, financial institutions can better evaluate their own vulnerabilities and implement security solutions to address them.

Gathering and sharing intelligence is key to helping financial institutions understand the threats posed by the fraud community and the potential impact on their business. Intelligence can be gathered through a number of sources including active monitoring of the fraudster underground and cross-organizational information sharing.

A good example of an intelligence source is the RSA eFraudNetwork™ service, a cross-organization online fraud network dedicated to sharing and disseminating information on fraudulent activity. Information is contributed by over 50 of the world's leading financial institutions, credit and debit card issuers, thousands of regional banks and credit unions, and major ISPs.

The eFraudNetwork service is engineered to identify and track fraudster profiles, patterns and behavior across more than 60 countries. When an active fraud pattern is identified, the fraud data, transaction profile and device fingerprints are moved to a confirmed, centralized database. The fraud data is then disseminated to all network members, providing financial institutions and their customers insight into new and debilitating threats.

Another proactive measure financial institutions should consider would be to use a third party service that offers protection against threats such as Trojans and malware. By employing an anti-Trojan service, financial institutions fight back against the threat of Trojans and malware by detecting and stopping them at the source. An anti-Trojan service allows financial institutions to stay ahead of fraudsters and provides insight into the malware that is targeting their customers and how it operates. By identifying the threat and taking action to curb it before a targeted attack is launched, financial institutions proactively protect their customers and their business.

#### Use multi-factor authentication to protect login

Username and password is not enough to protect sensitive data with the advanced nature of today's threat landscape. Moreover, many countries have imposed regulations requiring financial institutions to protect their customers with a second form of strong authentication. There are a number of ways that financial institutions can provide authentication at login to their online users including:

- **Time-synchronous, one-time password authenticators.** A time-synchronous, one-time password authenticator offers a unique symmetric key (or "seed record") that is combined with a proven algorithm to generate a new one-time password (OTP) every 60 seconds. The OTP authenticator is synchronized with a security server that confirms the legitimacy of the entered password for that 60-second window<sup>1</sup>. From a usability perspective, traditional hardware authenticators are small enough to fit on a keychain and meet the needs of users who prefer a tangible solution, access the Internet from a number of different locations, or perform high-value and high-risk transactions.
- **Software toolbars.** A software toolbar is a one-time password authenticator embedded within a standard Internet browser such as Internet Explorer or Mozilla Firefox. Like a standard hardware authenticator, software toolbars generate a new one-time password (OTP) every 60 seconds.

## A risk-based transaction monitoring solution can help financial institutions identify and challenge high-risk activities.

- **Device identification and profiling.** Device identification and profiling uses sophisticated technology to transparently authenticate a user by analyzing the device profile (the device where the user accesses from) and the behavioral profile (what activities the user typically performs) and matching the current activity against these profiles.
- **Site-to-user Authentication.** Site-to-user authentication provides a visible security reminder to users at each login so they are assured that they are transacting with a legitimate website. The security "reminder" includes a personal security image and caption that has been pre-selected by the user at login (both are selected during a previous enrollment session). Users are instructed to only enter their password after the website they are accessing has proven its authenticity by displaying their personal security image and caption.

#### Monitor transactions and activities that occur post-login

While putting a lock on the front door is suitable in most cases, fraudsters have developed technology to bypass login authentication – whether launching a phishing attack in an attempt to secure answers to challenge questions or developing advanced man-in-the-middle Trojans to bypass one-time password systems. So in addition to authentication solutions that challenge users to prove their identity at login, financial institutions should consider implementing a transaction protection solution that monitors and challenges high-risk transactions after login has occurred.

---

<sup>1</sup>This time window could be narrowed down even further, adding more complexity for a fraudster attempting an attack.

Transaction protection refers to a financial institution's ability to monitor and identify suspicious post-login activities – a capability most often provided by a risk-based authentication solution. Transactions typically require more scrutiny and pose more risk to financial institutions and their customers than just the act of logging in to an account. For example, a fraudster or unauthorized user might secure login access to an account, but the most risk is posed once he attempts to perform a transaction - transferring money out of the account, engaging in pump-and-dump stock-trading schemes, or ordering debit cards or credit cards to a recently changed address.

By either actively authenticating or passively monitoring post-login activities or events, financial institutions can provide comprehensive protection for their customers' identities and assets. While the nuances of actively verifying versus passively investigating suspicious transactions and activities are relevant, the overall concept remains much the same - by implementing a risk-based transaction monitoring solution, financial institutions will directly benefit from identifying and challenging high-risk activities and protecting the most vulnerable areas of their online channel.

#### Solution Requirements

- An integrated security approach that employs external threats protection and strong authentication at both the login and transactional level
- Strong relationships with a broad partner network, such as anti-virus firms, ISPs, and browser developers, to enhance identification, blocking and shutdown capabilities
- Ability to identify and address emerging threats before an attack occurs
- Strong intelligence and understanding of the fraudster underground

## Making the Most of Security Investments

While a layered approach to security is the best defense in the face of a constantly evolving fraud environment, budgets are not unlimited and applying every possible defense is simply impractical. When it comes to maximizing security investments practitioners must take a risk-based approach balancing three key variables: vulnerability, probability and materiality.

- **Vulnerability.** What threats and vulnerabilities is my institution exposed to?
- **Probability.** How probable is it that those vulnerabilities will be exploited?
- **Materiality.** How material are the consequences of exposure?

So how do these principles work in practice and why is a layered approach to security so important? Consider the example of the man-in-the-middle exploit reported in The Washington Post, as mentioned earlier. While the vulnerability may be low to the financial institution through the use of strong, one-time password authentication by its commercial users, the probability of risk and the materiality are high. Therefore, fraudsters are willing to devote the resources to circumvent OTP security in order to target high-value accounts.

By implementing a layered approach to security, financial institutions can thwart the efforts of fraudsters. In this instance, the financial institution could employ one-time password authentication, combined with transaction-level, risk-based authentication (RBA) to provide a solid defense against man-in-the-middle attacks. If the one-time-password entered by the user is intercepted, once the fraudster attempts to complete a transaction, the RBA system will recognize a number of unusual patterns (i.e., the sum of money being transferred, the transfer destination, or the device characteristics of the fraudster). By the time the fraudster attempts another login, the one-time password on the user's authenticator will have expired. The unpredictable nature of the one-time password and the unpredictable user flow due to risk-based authentication make it nearly impossible for a fraudster to bypass.

Even more so, if the financial institution employed some form of third party intelligence service or belonged to an information sharing network, they may have been alerted to the threat beforehand.

---

## Educating Your Customers

---

There is an ongoing debate about the impact of customer education and how much it really does to mitigate the threat of online fraud. RSA offers a number of resources to help financial institutions communicate the importance of online security to their customers including guides on phishing and malware.

There are a number of public sources available, as well. For example Carnegie Mellon University developed a new tool called Anti-Phishing Phil. It can be accessed at: [http://cups.cs.cmu.edu/antiphishing\\_phil/](http://cups.cs.cmu.edu/antiphishing_phil/). The game teaches users how to identify phishing URLs, where to look for cues in web browsers, and how to use search engines to find legitimate sites. Interactive tools such as this are great ways to engage consumers and raise online safety and security awareness.

RSA offers a number of resources to help financial institutions communicate the importance of online security to their customers including guides on phishing and malware.

---

## Summary

---

Layered security for financial institutions to combat online fraudsters can be compared to a real-world burglar attempting to break into your house. You watch the prowler as he walks around your house and comes up on the porch. Similarly, financial institutions need to keep a vigilant eye on fraudsters – how they operate and the means they use to attack. Next, the prowler attempts to enter your home so you turn the deadbolt. For financial institutions, the addition of strong two-factor authentication makes it more difficult for fraudsters to gain access to an account. Finally, the prowler uses a window to gain access to your home so you call the police to prevent him from stealing your possessions. Likewise for financial institutions, developing effective institutional policies and implementing a risk-based transaction protection solution will set off the alarm to prevent fraudsters from stealing your customer's valuable assets.

Man-in-the-middle attacks, Trojans and malware, once just considered theoretical musings of information security experts, have come to fruition. The threat is here – and it is real. When financial institutions erect a roadblock, fraudsters are always innovating ways to drive around it. This is apparent from the advanced technology and tactics being used to target financial institutions and the low cost and ease of execution for fraudsters to attack. Yet, these are only a few examples of the types of threats that exist.

It is critical for financial institutions to establish defenses at every corner and to never assume they are not vulnerable to these threats. As long as there is fraud, financial institutions will always be working to discover that delicate balance between security and risk.

---

## Appendix

---

The following glossary of terms provides a comprehensive look at the advanced threats that are targeting financial institutions and their customers.

### Trojans

The term Trojan refers to a family of malicious software (“malware”) which resides on a user’s computer and has the capability to perform certain actions transparently, all without the end user’s knowledge. For simplicity, Trojans can be divided into several families:

**Phishing/Pharming Trojans** – Performs a redirect to a fraudulent website without the user’s knowledge. Financial institutions that are targeted face risks similar to those of a phishing attack.

**Page-in-the-middle** – Waits until the user logs in to a specific site, performs a redirect to a page for data collection without the user’s knowledge, and then redirects the user back to the financial institution’s genuine site. These Trojans are more reliable than traditional phishing attacks, but serve the same purpose for a fraudster.

**Active Trojans (man-in-the-middle Trojan)** – Installs a type of proxy on the user’s computer that interacts with the financial institution’s genuine site on the user’s behalf. As the Trojan is interacting with the financial institution’s site through the user’s computer, it allows the fraudster to imitate the user’s profile. Some Trojans of this type wait until the user logs in to the genuine site and performs a concurrent web session automatically. Thus, the Trojan will appear to be transacting from the same IP and device as the user.

**Keyloggers/Screen-scrapers** – Captures the user’s keystrokes or tiny images of on-screen selection (for targeting financial institutions that use virtual keyboards at login). Details are then sent to a “drop zone” (an e-mail account or a remote server).

**Active Keylogger+Proxy (Botnet) Trojan**– Steals a user’s credentials using a keylogger or screen-scrapers and then sends the information to the fraudster. The fraudster will access the financial institution’s site from his computer, using the user’s PC as a proxy (botnet). While the fraudster is imitating the user’s IP, the device credentials of the fraudster’s and end user’s PC are not the same.

**Man-in-the-middle Attacks** – A man-in-the-middle (MITM) server attack involves an end user interacting with a website that appears to be the financial institution’s genuine site, but is actually a spoofed site. At the same time and unnoticed in the background, a fraudster, serving as “a man in the middle,” is feeding the data entered by the user in real-time to the actual financial institution’s site, validating the user and performing a malicious transaction. If the user is challenged to provide additional authentication, the MITM server will pass the request to the user and validate himself. These types of attacks may appear genuine, even to the most sophisticated end user.

**Botnet** – A series of Internet computers that have been compromised with malicious software and are used to send transmissions (of mostly spam or malware) to other computers on the Internet. Users are often unaware that their computer has been infected. Online users can become part of a botnet in several ways. First, if their computer is left unprotected, fraudsters can install malicious software through “open doors.” Second, software can also be sent through attachments, links or images embedded within e-mails and when a user clicks on them, they will install malicious software in the background. Finally, a user can be infected with this software just by visiting a website or downloading files (often called a “drive-by download”).

### About RSA

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world’s leading organizations succeed by solving their most complex and sensitive security challenges. RSA’s information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, 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](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

RSA, eFraudNetwork, the RSA logo 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. ©2008 RSA Security Inc. All rights reserved.