

MAKING SENSE OF MAN-IN-THE-BROWSER ATTACKS

Threat Analysis and Mitigation for Financial Institutions

Background

Cybercriminals are using newer and more advanced methods to target online users. One of the fastest growing threats in the wild today is man-in-the-browser (MITB) Trojan attacks. Man-in-the-browser attacks are part of the natural evolution of cybercrime, a result of stronger online security and increased consumer awareness. Propagation of man-in-the-browser attacks is being helped by spear phishing attacks, the popularity of social networking sites, and the increase in drive-by downloads. In the last year, there has been an exponential increase in the number of these attacks against financial institutions including the European consumer banking and U.S. corporate banking markets.

An Introduction to Man-In-The-Browser Attacks

A man-in-the-browser attack is designed to intercept data as it passes over a secure communication between a user and an online application. A Trojan embeds in a user's browser application and can be programmed to trigger when a user accesses specific online sites, such as an online banking site. Once activated, a man-in-the-browser Trojan can intercept and manipulate any information a user submits online in real-time. A number of Trojan families are used to conduct MITB attacks including Zeus/SpyEye, URLzone, Silent Banker, Sinowal, and Gozi. Some MITB Trojans are so advanced that they have streamlined the process for committing fraud, programmed with functionality to fully automate the process from infection to cash out. Additional capabilities offered by MITB Trojan developers include:

- HTML injection to display socially engineered pages (i.e. injecting a field into a page asking for the user's ATM card and PIN number in addition to their username and password).
- HTML or JavaScript pop-ups to communicate with the victim in real-time (i.e., requests that the victim enters a valid one-time password or divulge answers to their secret questions).
- Real-time interaction of Trojans with mule account databases to aid in the transfer of funds.

For criminals, the process of cashing out through mules has become automated. Some versions of the Zeus/SpyEye Trojan, for example, are built with scripts that interact with mule management tools. Each time an MITB transaction is attempted through an infected machine, the Trojan reaches out to the mule management tool and pulls the next record of a mule account that is available to accept the stolen funds.

The basic flow of a MITB attack is as follows¹:

1. A user gets infected with an MITB Trojan
2. Upon initiating an online banking session, the Trojan is triggered into action and launches its MITB functionalities
3. The user passes all authentication stages, including two-factor authentication when needed. The Trojan waits silently for successful login and/or for the user to initiate a money transfer.
4. The Trojan manipulates the transaction details such as the payee and the amount of the transfer. The legitimate payee is replaced with a mule account.
5. The Trojan maintains an apparently legitimate face of the transaction by using social engineering techniques. It displays bogus HTML pages to the user, which show the details of the legitimate transaction². If additional authentication is necessary to complete the transaction, the user proceeds to approve the transaction using whatever authentication method is required by the financial institution.

What makes MITB attacks difficult to detect from the bank's server side is that any activity performed seems as though it is originating from the legitimate user's web browser. Characteristics such as the Windows language and the IP address will appear the same as the user's real data. This creates a challenge in distinguishing between genuine and malicious transactions.

Exponential Infection Rate

Today, the dramatic growth in the number of man-in-the-browser attacks (and the spread of malware in general) is being helped by a number of vectors including spear phishing, the growth of social networking sites, and drive-by downloads³.

Spear phishing is a major contributor to the spread of man-in-the-browser attacks. Using well-crafted social engineering schemes, criminals are launching sophisticated spear phishing campaigns to target corporate banking clients and high net worth individuals. The availability of data about individuals on the Internet, including sites such as Facebook and LinkedIn, allow criminals to gather enough credible information about their targets to send emails that are highly believable and will likely elicit a response. Spear phishing does not only target consumers, but also goes after employees within the enterprise. Forty-five percent of employees indicate they have received a phishing email at work⁴.

The huge popularity of social networking sites and the number of users that engage in social networking activity has also contributed to the spread of Trojans and malware. The heavy traffic and global reach of these sites have made them a prime target for exploitation by criminals. Today, 40% of users on social networking sites have encountered some form of malware attack⁵.

1 This is a general description of MITB attacks. There may be other use cases and scenarios, but these steps are common to most MITB attacks witnessed by RSA. For the purpose of this paper, we focus on Trojans which are completely automatic, manipulating the data of a transaction generated by a legitimate user.

2 Some Trojans are programmed to replace the balance field on the user's account statement, showing the account balance as it should have appeared following the legitimate transaction.

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

4 RSA 2011 Workplace Security Report

5 Sophos Security Threat Report 2011

RSA has conducted extensive research into examining the MITB threat and the mule network that supports it. Some insights that we gathered from having studied mule management operations include:

- Average age of a mule: 31
- Average lifespan of a mule account: 3 days (this reflects the average between first use and last use, not from when the mule was actually recruited)
- Average number of fraud attempts made per mule account: 18
- Average amount transferred through a mule: \$3,980 for retail banking

Finally, drive-by downloads also have played a major role in the growth of MITB attacks. A drive-by download is initiated when a user is redirected to a site that was custom-built by criminals to infect users – most often after clicking on a link in an email. In other cases, criminals are able to take advantage of vulnerabilities on legitimate sites to serve up malicious code by redirecting traffic to infection points without the user having any knowledge that they are even being infected with such content. Today, about 2 out of every 1,000 pages displayed to users from search engine results contain a drive-by download⁶.

The end result is an exponential growth in the number of users infected with some form of malware. The most prevalent banking Trojan is Zeus/SpyEye which accounted for over 80% of all Trojan attacks targeting financial institutions in the first quarter of 2011⁷. This family of malware is not only the most widely spread, it is also known to have the most sophisticated MITB features and functionality available for sale in the criminal underground.

MITB Features and Functionality

Man-in-the-browser capabilities have topped the wish list of most criminals today. After Zeus' successful implementation of MITB capabilities, other Trojans followed suit: Bugat, Clod, Gozi (v2, 2010), Lamp, Mimicker, Patcher, Silent Banker, Silon, SpyEye, Syscron, and URLZone. All of these Trojans have some form of MITB functionality to automate fraudulent transactions using custom-built scripts. The following list outlines an example of some of the MITB functionality common in a number of active Trojan families today:

Zeus/SpyEye

Zeus/SpyEye has the ability to identify and intercept different types of internet traffic in real-time and is mainly exploited to conduct *automated* attacks, such as using an array of the victim's personal and device identifiers. Zeus/SpyEye can also facilitate manual hijacking of a victim's active online session. In order to be successful in this case, the criminal needs the victim to be present and ready to provide a valid OTP upon request.

In order to enter a session in progress, the criminal must impersonate the victim to near perfection. For example, the criminal will need access to the victim's cookies. HTTP cookies have a digital signature appended to them to keep them in the unique use of the intended person. A cookie cannot be forged; hence criminals have to *steal* them and then present the cookie to the bank's server in order to gain access to a legitimate online banking session.

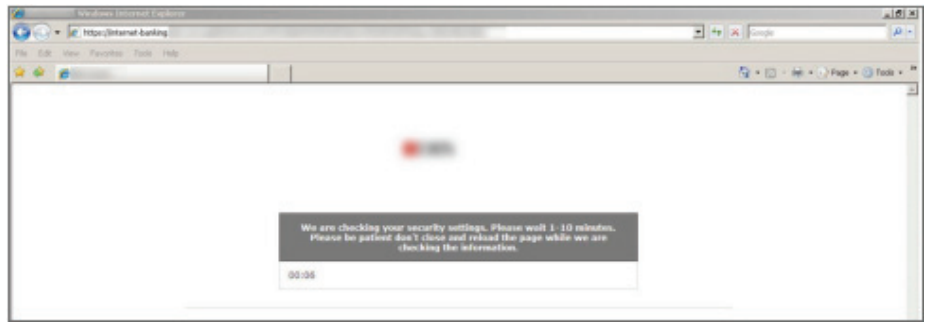
Intercepting an ongoing banking session is not always something that can be done covertly; in order to divert the user's attention, Zeus/SpyEye offers HTML injection code to present fake pop-up messages such as maintenance messages advising the user that a session has been temporarily suspended.

Using a SpyEye variant, a criminal was able to override a user's log-off request and continue the transaction in the background. As soon as the user submitted his credentials, the Trojan pulled up a fake notice page, falsely advising the user that his security settings were being checked. Figure 1 depicts the fake message displayed to the user requesting him to not close or reload the page since the criminal is actually still logged on to that same session and performing a fraudulent money transfer.

6 Microsoft Intelligence Report, Volume 9: 100

7 RSA FraudAction Quarterly Trojan Report, April 2011

Figure 1: An example of a fake page that infected users might be presented with during a man-in-the-browser attack



SilentBanker

The SilentBanker Trojan offers several advanced MITB features including:

- MITB scripts that intercept data sent from the victim to the bank
- An OTP grabber which can intercept and steal SMS codes, TAN numbers and other one-time password (OTP) codes used by banks to authenticate a user's money transfer
- Local HTML Injections to mimic the design of the targeted financial institutions' websites; SilentBanker uses seamless HTML injections mostly to obtain one-time passwords.

SilentBanker typically waits until a victim successfully logs in to the bank's genuine website, at which point it 'injects' entirely new HTML content into the page. The newly injected fields prompt victims to divulge sensitive data that is seldom requested by their service provider such as their debit card and PIN number.

URLzone

URLzone has the ability to inject code into a webpage that is loaded into a user's browser to launch MITB attacks. URLzone uses traditional session hijacking to steal customers' OTP codes in order to complete unauthorized transactions. URLzone relies on a variety of social engineering schemes to conduct a successful MITB attack. Most often, this is performed through another code injection that creates a page with a fake error message – after the user has already provided a valid OTP (i.e., “We are not able to complete your transaction at this time. Please try again later”).

Gozi

A recent variant of Gozi is programmed to steal a number of different data types; Gozi has injections that have already managed to steal SMS token codes and TANs as well as scripts that scrape⁸ additional information such as daily transfer limits and balances on checking, savings and credit card accounts.

Gozi Trojan logs containing automated transaction procedures clearly show that Gozi is pre-programmed to determine what percentage of the account balance can be transferred at a time. In order to determine the amount to transfer, Gozi first retrieves the current account balance. Figure 2 displays a record created by Gozi when performing automated money transfers. The Trojan log shows that Gozi picks up the account balance and daily transfer limit and then uses the TAN to complete the transfer.

⁸ Data Scraping is used by Trojans to access the page's source code, locate pertinent data on it and send it to the criminal.

- **Trojan Detection, Shutdown and Intelligence:** The RSA® FraudAction™ Anti-Trojan Service works to mitigate the impact of Trojans through the identification and shutdown of known infection points and blocking the resources that Trojans use to communicate (i.e., drop servers, Command & Control servers). In addition, the service attempts to extract stolen credentials and information on mule accounts that are set up to receive fraudulent money transfers.
- **RSA eFraudNetwork:** RSA® Adaptive Authentication and RSA Transaction Monitoring leverage information on fraud patterns that is contained within the RSA® eFraudNetwork™ data repository. The eFraudNetwork receives feeds of fraud data supplied by a vast network of customers, end users, ISPs, and other third parties. Frequent contributions on cybercrime intelligence are also provided by analysts at RSA's Anti-Fraud Command Center on a regular basis.
- **Out-of-band Authentication:** RSA offers out-of-band phone authentication that allows users to enter a one-time password into the keypad on their telephone. Out-of-band authentication offers a powerful defense against man-in-the-browser attacks because it separates the authentication process from the Web channel making it more difficult to compromise.

Transaction monitoring

While protecting login is critical, fraudsters have developed technology capable of manipulating transactions after login has occurred. Transaction protection refers to an organization's ability to monitor and identify suspicious post-login activities – a capability most often provided by a risk-based fraud monitoring solution.

Transactions typically require more scrutiny and pose more risk than just the act of logging in to an account. For example, an unauthorized user might secure login access to an account, but the most risk is posed once a transaction, such as transferring money out of the account, is attempted. A transaction protection solution will alert fraud investigation teams or challenge the users appropriately in these instances.

RSA Transaction Monitoring is powered by the self-learning RSA Risk Engine that conducts a risk assessment of all users behind the scenes. It can work with any existing authentication solution and can be completely invisible to the end user. When a user attempts a transaction, a unique risk score is assigned to each activity. When the risk score exceed a certain acceptable threshold (set by the deploying organization) or an organizational policy is violated, a case will be opened in the RSA Case Manager tool. The Case Manager allows for full case and investigation management with focus on only the highest risk transactions. In cases of extreme risk or when there is not sufficient time to manually review a case, the user can be challenged in real-time with an out-of-band phone call before the transaction can proceed.

RSA Transaction Monitoring is also able to detect potential Trojan activity by conducting advanced behavioral analysis. The normal patterns of a behavior for each individual user are observed, and when any behavior that deviates from that pattern occurs, it will likely raise the risk score for that user. Analysis of user behavior, especially behavior such as payment activities initiated by an end user, is critical at the transaction level. This is especially true for a man-in-the-browser Trojan as it waits until the genuine user logs in before it is triggered.

During the session itself, some patterns might indicate unusual behavior such as an activity of adding a new payee followed by an immediate payment transaction to this payee - an activity that cannot be detected at login. Additionally, RSA Transaction Monitoring offers more advanced Trojan detection capabilities such as manual session hijacking detection, Trojan behavior pattern analysis, mule account detection and HTML injection detection.

Transaction Monitoring is also supported by the RSA eFraudNetwork, a cross-organization repository of fraud patterns gleaned from RSA's extensive network of customers, ISPs, and third party contributors across the globe. When an activity is identified as being high-risk, transaction profile, IP address and device fingerprints are moved to a shared data repository.

The eFraudNetwork directly contributes feeds on fraud data to the RSA Transaction Monitoring system and is one of the many sources used in assigning a risk score. This includes data on mule accounts offered through the RSA FraudAction Anti-Trojan service.

Trojan detection, shutdown and intelligence

The RSA FraudAction Anti-Trojan Service, a core part of RSA FraudAction, is focused on minimizing the impact of Trojan attacks. Man-in-the-browser is one of the attacks that RSA has been focused on analyzing and has incorporated this intelligence into the RSA FraudAction Anti-Trojan service.

Early detection, blocking, and shutdown are the key to minimizing the impact a Trojan can have and reducing the amount of damage it can cause. However, shutting down or blocking access to Trojan infection points, update points, drop sites and drop emails is more complicated than it seems. In addition, Trojans are a more complex threat to address due to the unprecedented number of malware variants that exist.

By working with top financial institutions worldwide and monitoring multiple attacks, RSA has created ongoing relationships with some of the world's largest ISPs and registrars. The RSA Anti-Fraud Command Center leverages these relationships to initiate the cease-and-desist process on a 24x7 basis.

RSA strengths and services are enhanced by the RSA FraudAction Research Lab, a team of top researchers who are dedicated to ongoing research into the latest technology, tools and tactics being utilized by cybercriminals. This team is assigned to tackle new threats, such as man-in-the-browser, and to build the tools and processes that enable the fastest shutdown possible.

Out-of-band capabilities

Out-of-band (OOB) communication methods are a powerful weapon against advanced threats because they circumvent the communication channel most often used by fraudsters – the online channel. This is especially true in the case of man-in-the-browser when a Trojan is installed directly into a user's browser. Out-of-band communication methods can include regular postal mail, the telephone, or text message (also referred to as Short Message Service or SMS).

The RSA Adaptive Authentication Out-of-band Phone module provides users with a one-time passcode that appears in the Web browser. The system will then ask the user to select one of the phone numbers previously recorded during enrollment at which to receive a phone call and an automated phone call is generated. The call reviews the transaction details and prompts the user to enter the one-time passcode that is displayed on the Web browser into the keypad on their phone. Once the number is entered into the phone and confirmed to be correct number, the transaction will continue without disruption.

This is dubbed "true" out-of-band authentication because the passcode is actually entered into the phone, as opposed to entering the passcode back into the user's infected machine (as is usually the case when receiving a passcode via email or SMS).

Conclusion

Cybercriminals are continually evolving their tools and tactics to work around the defenses established by even the most security-conscious financial institutions. Man-in-the-browser attacks are one of the most advanced threats targeting users and affecting financial institutions across all geographies today. Login protection is simply not enough to stop them. Financial institutions must combine the use of risk-based transaction monitoring, Trojan detection, shutdown and intelligence, and out of-band capabilities for true layered security to mitigate the impact of man-in-the-browser attacks.

About RSA

RSA is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.

RSA, the RSA logo, EMC², EMC and where information lives are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners. ©2011 EMC Corporation. All rights reserved. Published in the USA.

MITB WP 0611

www.rsa.com

