RSA White Paper

Making Sense of Man-in-the-browser Attacks:

Threat Analysis and Mitigation for Financial Institutions

Background

Fraudsters are using newer and more advanced methods to target online users. One of the latest tactics being developed and deployed is the use of Trojans to launch man-in-the-browser (MITB) attacks. In the last year, RSA has witnessed an exponential increase in the number of these attacks against financial institutions including the European consumer banking and US corporate banking markets.

RSA®
The Security Division of EMC

Contents

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 itself in a user's browser and can be programmed to activate when a user accesses specific online sites, such as an online banking sites. 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, Adrenaline, Sinowal, and Silent Banker. 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 pin number in addition to their username and password).
- Real-time integration of Trojans with mule account databases to aid in the automated transfer of money.
- The ability to circumvent various two-factor authentication systems including CAP/EMV, transaction signing, iTANs, and one-time password authentication[1]

MITB Trojans commonly perform what is known as "session hijacking" – abusing a legitimate user's session with the site being accessed while the user is logged into their account. By hijacking a session in this way, all actions performed by the Trojan actually become part of the user's legitimate session such as conducting a malicious activity (i.e., a fraudulent money transfer, changing a postal address) or even injecting JavaScript code that can then perform this automatically.

The basic flow of a MITB attack is as follows[2]:

1. A consumer gets infected with a Trojan capable of launching an MITB attack.
2. Upon the initiation of a legitimate online transaction, the Trojan is triggered into action and launches its. MITB functionalities
3. The user passes all authentication stages, including any two-factor authentication when needed. The Trojan waits silently for successful login and/or transaction authorization.
4. The Trojan manipulates the transaction details – payee, and sometimes the amount. In most cases the legitimate payee account is replaced with a mule account that the fraudster can use.
5. By using social engineering techniques the user is unaware that they are being impacted. The Trojan displays fake pages to the user, which may show the transaction details as originally entered by the user. If additional authentication is necessary to complete the transaction, the Trojan will interact with the user and ask the user to enter their authentication credentials in real-time to approve the transaction.

What makes MITB attacks difficult to detect is that any activity performed seems as if it is originating from the legitimate user's browser. Characteristics such as the HTTP headers 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.

A Global Threat

MITB attacks are not contained to one region or geography; They are a global threat, affecting all regions of the world. However, they are especially prevalent in areas where two-factor authentication is densely deployed. Today, MITB attacks are increasing in their deployment and scale:

- In the UK, banks are suffering an increasing number of MITB attacks. One financial institution alone reported a loss of £600,000 as a result of a single attack by the PSP2-BBB Trojan.[3] European countries such as Germany, the Netherlands, Spain, France, and Poland have deployed two-factor authentication in the last few years, which have attracted a rise in the numbers of MITB attacks in these regions. Germany has been particularly hard hit by an abundance of MITB attacks as it is one of the few successful paths to commit online banking fraud in the country.

1 Notably, time based one-time passwords are less vulnerable to man-in-the-middle and man-in-the-browser attacks compared to event-based one-time passwords as the window of opportunity for time-based solutions is typically less than a minute.

2 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.

3 RSA Anti-Fraud Command Center

– Banking innovations such as the Single Euro Payments Area (SEPA) and pressure to deliver faster payments have also increased exposure to transaction fraud. The increased ease and speed of moving money is advantageous for legitimate transactions, but reduces the flexibility to investigate and prevent suspicious transactions.

– U.S. financial institutions are attacked by MITB; however, the threat has been mainly confined to commercial banking or high net worth customers. Because one-time password authentication is not very common amongst consumers in the U.S., MITB attacks against the general consumer public are less common compared to the volume experienced by consumers in Europe. However, as security defenses increase and the ability to infect more machines with MITB Trojans increases the expected number of attacks on US retail banking institutions is also expected to rise.

– Financial institutions in Australia, Asia and Latin America are increasingly deploying two-factor authentication for their online banking users, and as a result, have experienced an increasing number of MITB attacks.

Evolution of Man-in-the-Browser Attacks

MITB Trojans are part of the natural evolution of online fraud. Before the introduction of strong authentication, online criminals could gather information to commit fraud through phishing attacks or standard Trojans that did not intervene with a user's online activity or transactions. Due to increased consumer awareness and stronger online security mechanisms, fraudsters had to update their methods and tools to overcome two-factor authentication.

The idea of MITB attacks was conceived primarily for the purpose of circumventing strong authentication. In a web forum post uncovered by RSA, fraudsters discussed the various options available to them to bypass one-time password authentication (see Figure 1). "Auto Transfers," the term used by fraudsters to refer to MITB attacks, was one of the methods they discussed. One fraudster criticized other suggested methods, claiming MITB is the only solution against one-time passwords.

Exponential Infection Rate

RSA has witnessed Trojan infections increase tenfold in recent months – findings that are supported by other industry observations and reports.[4] This growth is driven in part by the number of 'drive by download'[5] infections where vulnerabilities on legitimate websites are exploited by fraudsters, allowing them to use infection kits to embed an iFrame within the breached website. The iFrame silently directs a genuine user's browser to botnets that host infection points that attempt to download a Trojan on the user's computer.

A good example this type of attack is the breach of Paul McCartney's fan page (see Figure 2). In April 2009, the site was hacked for two days and all visitors were silently infected with a variant of a MITB Trojan.

Another highly effective infection method is the use of popular events or issues to drive traffic to infected sites.

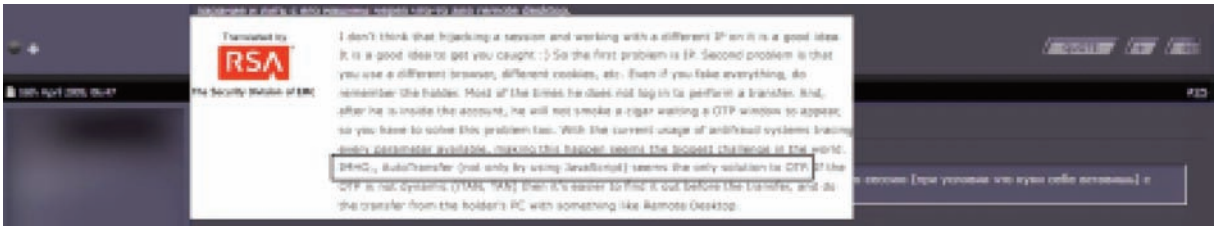

Figure 1: Fraudsters discuss options to bypass two-factor authentication

4 Panda Labs reported an eight-fold increase in the growth of MITB infection rates between H1 and H2 2008.)

5 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)

Figure 2: Legitimate sites, such as Paul McCartney's official website, are hacked by fraudsters and used to deliver malware to visitors

RSA uncovered and shut down such a scam which was designed to coax users, via an email spam attack, to a fake news website that looked like CNN.com. The 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 getting infected with a Trojan.

Finally, the huge popularity of social networking sites and the number of users that engage in social networking activities has also contributed to the growth of MITB attacks. 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] Social networking sites are not only efficient for distributing Trojans due to their large reach, but they also provide a channel to interact with an end users where they will be less suspicious of social engineering attacks.

The end result is an exponential growth in the number of Trojan infected machines. The most prevalent Trojan is Zeus, which means Zeus' MITB capabilities potentially reside on millions of consumers' machines – and continues to proliferate every day.

A Trojan in Action – MITB Attack with the Zeus Trojan

Zeus is one of the most advanced and most popular Trojan kits used today. RSA analysed the configuration file for a Zeus Trojan detected in the wild and discovered that it was automated to conduct real-time transfers to a designated mule account (see Figure 3). The exact "auto transfer" features of Zeus were also described in a fraudster tutorial RSA uncovered in April 2009. The fraudster that developed the Trojan explains: " The process of an automatic transfer is 'on-the-fly' modification of any kind of information (mostly having to do with payment) from a client PC to a server of any kind of corporation (most cases banks or payment systems) without the user being notified about it. The Zeus Trojan offers these possibilities for online banking systems and payment systems operated by web protocols. It can be either passive, only modifying the info during transfers initiated by users, or active, capable of executing all the operation (load the transfer form, filling the fields, sending the info) without any action taken by the user (they only perform a login)."

6 Breach Security Labs, " Web Hacking Incidents Database (WHID) 2009 Bi-Annual Report")

Figure 3: Trojan code: Retrieval of Criminal's Mule Account

Mitigation Strategies

As a result of extensive investigation into the Trojan threat, and specifically man-in-the-browser, several conclusions can be drawn:

- Login protection is not enough to stop MITB attacks. Even if the genuine user logs into the account, the Trojan can take over the account after the user logs in.
- MITB attacks are hard to detect without transaction monitoring and protection. A MITB Trojan can hijack a user' s device so any malicious transactions that are conducted will still appear as though they are originating from the legitimate user. Beyond device or IP tracking, strong behavioral profiling capabilities are critical to detecting fraud.
- Due to the fact that some Trojans use HTML injection to request credentials for additional authentication, out-of-band authentication is more resilient to MITB as it circumvents the online channel.
- Manual investigations are not enough. Trojans can be fully automated to perform the entire process – from infection to cash out – in real-time. The faster the window to allow funds to be transferred the less time there is to manual investigate cases. In these instances step-up authentication (preferably true out-of-band authentication) should be leveraged.
- Intelligence is an important part of mitigation. Mule accounts, for example, play a huge role in the cash out process. Having access to information such as this is crucial to developing a complete solution.

A layered security approach that combines risk-based transaction monitoring, Trojan detection, shutdown, and intelligence services, and out-of-band capabilities provides a solid defense against the threat of man-in-the-browser attacks. The following RSA solutions help organizations ease the challenge posed by man-in-the-browser attacks:

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 is attempted, such as transferring money out of the account. 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 gives the ability to conduct full case and investigation management with focus on only the highest risk transaction. 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.

Transaction Monitoring is able to detect Trojans by conducting advance 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 into their bank account to take action.

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, the fraud data, transaction profile, mule account info and device fingerprints are moved to a shared data repository. The eFraudNetwork directly contributes feeds on fraud data to RSA Transaction Monitoring 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 that occur in the online channel. 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 thousands of crimeware 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. Since January 2009, the number of Trojan communication resources, including infection points, update points, and drop sites, that RSA has addressed has increased over 300%.

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 online criminals. 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.

To demonstrate, the RSA FraudAction Research Lab has determined that MITB attacks are able to thrive because of the network of mule accounts that fraudsters have established to receive stolen funds. By gaining access to the details on mule accounts, organizations can block any future transactions attempted to a mule account.

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 "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

Online criminals are continually evolving their tools and tactics to work around the defenses established by even the most security-conscious organizations. Man-in-the-browser attacks are one of the most advanced threats affecting organizations around the world today and login protection is not enough to stop them. Organizations must combine the use of risk-based transaction monitoring, Trojan detection, shutdown and intelligence, and out-of-band capabilities to create a truly solid defense against the threat of man-in-the-browser attacks.

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; governance & risk 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.

Confidentiality

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

The Security Division of EMC

MITB WP 0510