Trojan Based Man-in-the-Browser (MITB) Attacks

Manush Pandya

Institute of Computer Technology

Ganpat University

Abstract

Extraction of sensitive and confidential data by performing a Man in the Browser (MITB) attack is a problem that has been studied by the cyber security community for a long time. Although the tools and methods for this have varied, the basic idea behind the attack has always been the same. Along with that the MITB attack being one of the most common occurring malware-based attacks used to steal data is a compelling reason for this survey. In this paper, we review detection and prevention techniques used to protect ourselves against these attacks, breaking down the attack performed using Carberp Malware and comparing the various research done by other people in the community to provide the most optimal techniques.

Introduction

The rise in usage of online resources has been accompanied by a sharp increase in cyberattacks – specifically MITB attacks.

The attack being easier to perform and cover tracks is a favorite for criminals at the moment. A MITB attack works when an attacker injects malware in the system of the victim this malware then gives the attacker the ability to read and change data going in and out of the browser. MITB has been mostly used for phishing attacks but it can be used for other forms of cyber threats as well. A MITB is similar to Man-in-the-Middle Attack as far as basic concept is concerned but at the same time is different in terms of execution. In Man-in-the-Middle, the attacker is based between the server and the browser and has to deal with encrypted data mostly. But in Man-in-the-browser attack, the attacker is based inside the victim's browser and hence they can read and modify data before it is encrypted by the browser.

Literature Review

Introduction

Man-in-the-Browser plays a key role in modern society. As we see there is loads of increase within the Crime rates for the Browser Attacks. The major antivirus corporations have analyzed the Browser attacks. In 2015, there were 1,966,324 registered notifications regarding tried malware infections that aimed to steal cash via online access to bank accounts around thirty 4.2% of user computers were subjected to a minimum of one internet attack over the year and to hold out their attacks, cybercriminals used 6,563,145 distinctive hosts in keeping with the Kaspersky (2015).

Literature Related to the problem

A comprehensive survey of solutions against client-side attacks can be found in the RSA White Paper (2015). The countermeasures against attacks on internet banking are categorized into two types. One type is known as two-channel authentication scheme, which uses two different channels between user and server. The other type is known as two-factor authentication scheme, which typically uses a password and a token. As a former example, mTAN (mobile transaction authentication number), Bhargavan, Delignat-Lavaud, Fournet, Pironti, and Strub (2014) has already been introduced in some European countries. When a bank server receives a transaction request from a user, it generates a one-time password and sends an SMS message which includes the one-time password with the details of the transaction. The user can verify the transaction details and approve it by 14 entering the password onto the website. If the user finds any forgery in the transaction details, he or she can cancel the transaction by not entering the password onto the website. This countermeasure assumes that it is impossible to forge the source address of SMS and that it is also impossible to eavesdrop and tamper with the transaction details. Moreover, it assumes that the mobile phone is free from malware.

Literature Related to the methodology

Day-by-day Trojan Viruses are increasing exponentially, so there has been extensive research on attacks to HTTPS/SSL connections and the browser cache, as well as corresponding defenses. Clicking through of SSL warnings. When an SSL warning is shown for a web page, the user is supposed to close the page to protect him/her from MITM attacks. However, 33.0% and 70.2% of users choose to click through SSL warnings on various websites in Mozilla Firefox (beta channel) and Google Chrome stable channel) respectively, according to the investigation by Akhawe and Felt (2013). Various other Man-in-the-Middle Attacks are explained in Saltzman and Sharabani (2009), Yaoqi et al. (2014), and these are related to Man-inthe-Middle. But now even hackers are updated with the new Man-in-the-Browser Attack which they started attacking from the Same internet Protocol addresses. Dhamija, Tygar, and Hearst (2006) observe a 68% click through rate, and Sunshine, Engelman, Almuhimedi, Atri, and Cranor (2009) even record 90-95% clickthrough rates depending on the type of page. Herzberg (2009) studies the basic and advanced indicators and their usability problems.

What is 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.

MitB attacks are more famous due to their ease of use. In these attacks the victim is contacting the original sites only and hence the web application security measures are not used to prevent this. These attacks are also known to easily bypass browser security measures such as SSL certificates and steal and modify data without user's knowledge.

Attack Phases

Phase 1: Malware Insertion

The trojan horse gets inserted in the device's operating system when the user:

- downloads a corrupted software,
- visits any malicious site,
- opens or downloads malicious email attachments, or
- plugs corrupted external devices such as USB drives/CDs on their computers/tablets/mobile phones.

The trojan **automatically installs** a malicious extension in the web browser without the user's knowledge.

Whenever the user restarts the browser, the extension gets activated.

The malicious extension has a list of targeted websites which it can manipulate. Whenever the user opens a website from the list, the trojan does multiple tricks to modify the targeted webpages. For example, changing the fields of the forms or inserting JavaScript on the buttons like **Submit, Done, Send, Transfer, Complete**, etc.

Phase 2: Transaction Interruption

The unsuspecting user logs in with their credentials (their user ID, email address, password, one-time password [OTP], secret pins, etc). Then, they complete the regular transaction such as transferring funds, making payments, purchasing, or filling out sensitive details such as SSN, health info, etc.

When the user clicks Submit or any other authorization button, the malicious script modifies the transaction details. For example, changing the transaction amount, bank numbers, physical address, product, etc. and sends the modified information to the website's server. (Note: The information is modified before it enters the encrypted channel facilitated by the SSL/TLS certificates.)

The recipient website doesn't suspect anything about the modified transaction because it's coming directly from the user without bypassing any authentication step. Hence, the website completes the requested transaction.

Phase 3: Response Modification

The website sends the receipt to the user. The receipt contains the transaction details.

The corrupted browser modifies the receipts that match the details of the users' original transaction.

At this stage, even if the two-factor authentication (2FA) is activated, the user doesn't have anything to suspect in the confirmation receipt. Hence, they provide the unique secret code or OTP, which they generally receive on the mobile or email to complete the transaction.

Impact

How dangerous can MITB be? The word Dangerous is not enough to explain the Man-in-the-browser attacks. Listed below are the malicious activities that an attacker can perform using various Trojan based mitb attacks.

- Adding new columns/fields on the website or modifying the existing fields.
- Modifying the transaction information entered by the users. This data can be a transaction amount, bank account number, physical address, etc.
- Hijacking the entire transaction in real-time.
- Changing the appearance of the website.
- Modifying the servers' responses, such as confirmation messages and receipts.
- Intercepting the data entered by the user on the website.
- Removing the transaction details when the user revisits the website.

Below listed are some of the few malwares that perform mitb attacks.

- Carberp
- Zeus
- SpyEye
- Bugat
- Silon
- Tatanga

These attacks are generally used in websites where commercial transaction is taking place such as banks, insurance, shopping sites, payment portals, etc. they are also used to steal private information while using social media.

Prevention Techniques

In the below table are some of the basic prevention techniques that are used to prevent data theft, invalid transactions and protect the user. In the table they have been rated on their effectiveness against an mitb attack.

Method	Description	Effectiveness
Username/Password	Basic Username/Password Combination	Not Effective
Biometric	Fingerprint reader to unlock login, typing biometrics other methods	Not Effective
In Browser OTP	OTP and transaction details received in the browser or the device itself.	Not Effective
Manual Authentication	Pre-selected image or phrase set by user to ensure correct website is reached.	Not Effective
Out-Of-Band OTP	OTP and transaction details received on another device which cannot be modified.	Very Effective
Digital Certificates	Ssl certificates and encryption methods used by browser	Not Effective
Antivirus	Antivirus software that scans constantly for any malware injected into the computer as well as the browser.	Very Effective
Isolated Computer	A computer that is used only to do commercial transactions and nothing else	Effective but Inconvenient
Isolated Browser	A browser that is used only for transactions and nothing else	Effective but Inconvenient
Device Profiling	Transaction approved on certain devices that match using MAC address only.	Not Effective
Virtual Machines	Resettable virtual machines that can be reset every time a transaction is done so no malware in injected.	Effective but Inconvenient
Behavioural Fraud Detection	Capture and analysis of users web traffic to detect their	Very Effective

	activity in the session and create a behavioural pattern to detect fraud or malicious activities.	🟩

As we can see from the above table, Out-Of-Band OTP, Antiviruses, and behavioural fraud detection are our best bet at preventing man in the browser attacks. Other measures can still be used but they can be ineffective and inconvenient. A well designed mix of multiple preventive measures should be able to provide most protection against mitb attacks.

Apart from these measures, safe browsing of unknown websites, anti-phishing methods such as not installing or downloading unknown software and not clicking on unknown links are the basic methods that should be kept in mind for most protection.

Summary

There are many research papers on man in the middle attack and many people research on Trojans but day to day new Trojan are getting into the cyber world and each Trojan has its own characteristics and different from other Trojans. This is making things difficult for cyber security experts. This paper would collaborate the preventive methods against man in the browser attacks and their effectiveness.

References

1. Defeating Man-in-the-Browser Malware - Entust
2. Making Sense of Manin-the-browser Attacks: Threat Analysis and Mitigation for Financial Institutions – RSA White Paper
3. SECURE COLLABORATIVE PROCESSING ARCHITECTURE FOR MITB ATTACK DETECTION - Hani Qusa and Shadi Abudalfa
4. Man in the Browser Attacks - Krishna Sai Anudeep Ayyagari
5. Analyzing Man-in-the-Browser (MITB) Attacks – SANS Institute InfoSec Reading Room
6. https://doubleoctopus.com/blog/enterprise-security/the-ultimate-guide-to-man-in-the-middle-mitm-attacks-and-how-to-prevent-them/
7. https://codesealer.com/twelve-reasons-why-mitb-and-mitm-attacks-grows-with-the-pandemic/
8. https://sectigostore.com/blog/a-man-in-the-browser-attack-what-it-is-how-to-prevent-it/
9. https://owasp.org/www-community/attacks/Man-in-the-browser_attack