Man-in-the-browser

By Contributors to Wikimedia projects

Published: 2008-07-30 · Archived: 2026-04-02 10:37:14 UTC

From Wikipedia, the free encyclopedia

Man-in-the-browser (**MITB**, **MitB**, **MIB**, **MiB**), a form of Internet threat related to man-in-the-middle (MITM), is a proxy Trojan horse[1] that infects a web browser by taking advantage of vulnerabilities in browser security to modify web pages, modify transaction content or insert additional transactions, all in a covert fashion invisible to both the user and host web application. A MitB attack will be successful irrespective of whether security mechanisms such as SSL/PKI and/or two- or three-factor authentication solutions are in place. A MitB attack may be countered by using out-of-band transaction verification, although SMS verification can be defeated by **man-in-the-mobile** (**MitMo**) malware infection on the mobile phone. Trojans may be detected and removed by antivirus software,[2] but a 2011 report concluded that additional measures on top of antivirus software were needed.[3] [*needs update*]

A related, simpler attack is the **boy-in-the-browser** (**BitB**, **BITB**).

The majority of financial service professionals in a 2014 survey considered MitB to be the greatest threat to online banking.[4]

The MitB threat was demonstrated by Augusto Paes de Barros in his 2005 presentation about backdoor trends "The future of backdoors - worst of all worlds."[5] The name "man-in-the-browser" was coined by Philipp Gühring on 27 January 2007.[6]

A MitB Trojan works by using common facilities provided to enhance browser capabilities such as Browser Helper Objects (a feature limited to Internet Explorer), browser extensions and user scripts (for example in JavaScript).[6] Antivirus software can detect some of these methods.[2]

In a nutshell example exchange between user and host, such as an Internet banking funds transfer, the customer will always be shown, via confirmation screens, the exact payment information as keyed into the browser. The bank, however, will receive a transaction with materially altered instructions, i.e. a different destination account number and possibly amount. The use of strong authentication tools simply creates an increased level of misplaced confidence on the part of both customer and bank that the transaction is secure. Authentication, by definition, is concerned with the validation of identity credentials. This should not be confused with transaction verification.

Examples of MitB threats on different operating systems and web browsers:

Man-in-the-Browser examples

Name	Details	Operating system	Browser
Agent.DBJP[7]		Windows	IE, Firefox
Bugat[8]		Windows	IE, Firefox
Carberp	targets Facebook users redeeming e-cash vouchers[9]	Windows	IE, Firefox
ChromeInject*[10]	Greasemonkey impersonator[11]	Windows	Firefox
Clampi[12]		Windows	IE
Gozi[1]		Windows	IE, Firefox
Nuklus[2][11]		Windows	IE
OddJob[13]	keeps bank session open	Windows	IE, Firefox
Silentbanker[14]		Windows	IE, Firefox
Silon[15]		Windows	IE
SpyEye[16]	successor of Zeus, widespread, low detection	Windows	IE, Firefox
Sunspot[17]	widespread, low detection	Windows	IE, Firefox
Tatanga[18]		Windows	IE, Firefox, Chrome, Opera, Safari, Maxthon, Netscape, Konqueror
Tiny Banker Trojan[19]	Smallest banking Trojan detected in wild at 20KB	Windows	IE, Firefox
Torpig**[15]		Windows	IE, Firefox
URLZone**** [1]		Windows	IE, Firefox, Opera
Weyland-Yutani BOT[20]	crimeware kit similar to Zeus, not widespread[20][21]	Mac OS X	Firefox
Yaludle[15]		Windows	IE
Zeus***[12]	widespread, low detection	Windows	IE, Firefox

Key	Windows: IE	Windows: IE & Firefox or Firefox	Windows: other	Mac OS X: any
*ChromeInject a.k.a. ChromeInject.A, ChromeInject.B, Banker.IVX, Inject.NBT, Bancos-BEX, Drop.Small.abw[10]				
**Torpig a.k.a. Sinowal, Anserin[1]				
***Zeus a.k.a. ZeuS, Zbot,[22] Wsnpoem,[23][24] NTOS,[25] PRG,[25] Kneber,[26] Gorhax[26]				
****URLZone a.k.a. Bebloh!IK, Runner.82176, Monder, ANBR, Sipay.IU, Runner.fq, PWS.y!cy, Zbot.gen20, Runner.J, BredoPk-B, Runner.EQ				

Known Trojans may be detected, blocked, and removed by antivirus software.[2] In a 2009 study, the effectiveness of antivirus against Zeus was 23%,[25] and again low success rates were reported in a separate test in 2011.[3] The 2011 report concluded that additional measures on top of antivirus were needed.[3]

- Browser security software: MitB attacks may be blocked by in-browser security software such as Cymatic.io, Trusteer Rapport for Microsoft Windows and Mac OS X, which blocks the APIs from browser extensions and controls communication.[11][12][15]
- Alternative software: Reducing or eliminating the risk of malware infection by using portable applications or using alternatives to Microsoft Windows like Mac OS X, Linux, or mobile OSes Android, iOS, ChromeOS, Windows Mobile, Symbian, etc., and/or browsers Chrome or Opera.[27] Further protection can be achieved by running this alternative OS, like Linux, from a non-installed live CD, or Live USB.[28]
- Secure Web Browser: Several vendors can now provide a two-factor security solution where a Secure Web Browser is part of the solution.[29] In this case, MitB attacks are avoided, as the user executes a hardened browser from their two-factor security device rather than executing the "infected" browser from their own machine.

Out-of-band transaction verification

[edit]

A theoretically effective method of combating any MitB attack is through an out-of-band (OOB) transaction verification process. This overcomes the MitB trojan by verifying the transaction details, as received by the host (bank), to the user (customer) over a channel other than the browser; for example, an automated telephone call, SMS, or a dedicated mobile app with graphical cryptogram. OOB transaction verification is ideal for mass market use since it leverages devices already in the public domain (e.g. landline, mobile phone, etc.) and requires no additional hardware devices, yet enables three-factor authentication (using voice biometrics), transaction signing (to non-repudiation level), and transaction verification. The downside is that the OOB transaction verification adds to the level of the end-user's frustration with more and slower steps.

Mobile phone mobile Trojan spyware **man-in-the-mobile** (**MitMo**)[31] can defeat OOB SMS transaction verification.[32]

- ZitMo (Zeus-In-The-Mobile) is not a MitB Trojan itself (although it performs a similar proxy function on the incoming SMSes), but is mobile malware suggested for installation on a mobile phone by a Zeus-infected computer. By intercepting all incoming SMSes, it defeats SMS-based banking OOB two-factor authentication on Windows Mobile, Android, Symbian, and BlackBerry.[32] ZitMo may be detected by Antivirus running on the mobile device.
- SpitMo (SpyEye-In-The-Mobile, SPITMO) is similar to ZitMo.[33]

Web fraud detection

[edit]

Web fraud detection can be implemented at the bank to automatically check for anomalous behaviour patterns in transactions.[34]

Keyloggers are the most primitive form of **proxy trojans**, followed by browser-session recorders that capture more data, and lastly MitBs are the most sophisticated type.[1]

SSL/PKI etc. may offer protection in a man-in-the-middle attack, but offers no protection in a man-in-the-browser attack.

A related attack that is simpler and quicker for malware authors to set up is termed **boy-in-the-browser** (**BitB** or **BITB**). Malware is used to change the client's computer network routing to perform a classic man-in-the-middle attack. Once the routing has been changed, the malware may completely remove itself, making detection more difficult.[35]

Clickjacking tricks a web browser user into clicking on something different from what the user perceives, by means of malicious code in the webpage.

- Form grabbing
- IT risk
- Threat (computer)
- Timeline of computer viruses and worms
- Security token
- Transaction authentication number
- DNS hijacking

1. ^ Jump up to: *a b c d e* *Bar-Yosef, Noa (2010-12-30). "The Evolution of Proxy Trojans". Retrieved 2012-02-03.*
2. ^ Jump up to: *a b c d* *F-Secure (2007-02-11). "Threat Description: Trojan-Spy:W32/Nuklus.A". Retrieved 2012-02-03.*
3. ^ Jump up to: *a b c* *Quarri Technologies, Inc (2011). "Web Browsers: Your Weak Link in Achieving PCI Compliance" (PDF). Retrieved 2012-02-05.*
4. ^ *Fernandes, Diogo A. B.; Soares, Liliana F. B.; Gomes, João V.; Freire, Mário M.; Inácio, Pedro R. M. (2014-04-01). "Security issues in cloud environments: a survey". International Journal of Information*

Security. ***13*** *(2): 113–170. doi:10.1007/s10207-013-0208-7. ISSN 1615-5270. S2CID 3330144.*

5. ^ *Paes de Barros, Augusto (15 September 2005). "O futuro dos backdoors - o pior dos mundos" (PDF) (in Portuguese). Sao Paulo, Brazil: Congresso Nacional de Auditoria de Sistemas, Segurança da Informação e Governança - CNASI. Archived from the original (PDF) on July 6, 2011. Retrieved 2009-06-12.*
6. ^ Jump up to: **a** **b** *Gühring, Philipp (27 January 2007). "Concepts against Man-in-the-Browser Attacks" (PDF). Archived from the original (PDF) on 2018-12-21. Retrieved 2008-07-30.*
7. ^ *Dunn, John E (2010-07-03). "Trojan Writers Target UK Banks With Botnets". Archived from the original on 2010-11-25. Retrieved 2012-02-08.*
8. ^ *Dunn, John E (2010-10-12). "Zeus not the only bank Trojan threat, users warned". Retrieved 2012-02-03.*
9. ^ *Curtis, Sophie (2012-01-18). "Facebook users targeted in Carberp man-in-the-browser attack". Archived from the original on 2012-01-23. Retrieved 2012-02-03.*
10. ^ Jump up to: **a** **b** *Marusceac Claudiu Florin (2008-11-28). "Trojan.PWS.ChromeInject.B Removal Tool". Archived from the original on 2012-04-01. Retrieved 2012-02-05.*
11. ^ Jump up to: **a** **b** **c** *Nattakant Utakrit, School of Computer and Security Science, Edith Cowan University (2011-02-25). "Review of Browser Extensions, a Man-in-theBrowser Phishing Techniques Targeting Bank Customers". Retrieved 2012-02-03.* `{{cite web}}` : CS1 maint: multiple names: authors list (link)
12. ^ Jump up to: **a** **b** **c** *Symantec Marc Fossi (2010-12-08). "ZeuS-style banking Trojans seen as greatest threat to online banking: Survey". Archived from the original on 2011-08-08. Retrieved 2012-02-03.*
13. ^ *Ted Samson (2011-02-22). "Crafty OddJob malware leaves online bank accounts open to plunder". Retrieved 2012-02-06.*
14. ^ *Symantec Marc Fossi (2008-01-23). "Banking with Confidence". Retrieved 2008-07-30.*
15. ^ Jump up to: **a** **b** **c** **d** *Trusteer. "Trusteer Rapport". Retrieved 2012-02-03.*
16. ^ *CEO of Trusteer Mickey Boodaei (2011-03-31). "Man-in-the-Browser attacks target the enterprise". Archived from the original on 2011-12-08. Retrieved 2012-02-03.*
17. ^ *www.net-security.org (2011-05-11). "Explosive financial malware targets Windows". Retrieved 2012-02-06.*
18. ^ *Jozsef Gegeny; Jose Miguel Esparza (2011-02-25). "Tatanga: a new banking trojan with MitB functions". Archived from the original on 2012-06-27. Retrieved 2012-02-03.*
19. ^ *"Tiny 'Tinba' Banking Trojan Is Big Trouble". msnbc.com. 31 May 2012. Retrieved 2016-02-28.*
20. ^ Jump up to: **a** **b** *Borean, Wayne (2011-05-24). "The Mac OS X Virus That Wasn't". Retrieved 2012-02-08.*
21. ^ *Fisher, Dennis (2011-05-02). "Crimeware Kit Emerges for Mac OS X". Archived from the original on September 5, 2011. Retrieved 2012-02-03.*
22. ^ *F-secure. "Threat DescriptionTrojan-Spy:W32/Zbot". Retrieved 2012-02-05.*
23. ^ *Hyun Choi; Sean Kiernan (2008-07-24). "Trojan.Wsnpoem Technical Details". Symantec. Archived from the original on February 23, 2010. Retrieved 2012-02-05.*
24. ^ *Microsoft (2010-04-30). "Encyclopedia entry: Win32/Zbot - Learn more about malware - Microsoft Malware Protection Center". Symantec. Retrieved 2012-02-05.*
25. ^ Jump up to: **a** **b** **c** *Trusteer (2009-09-14). "Measuring the in-the-wild effectiveness of Antivirus against Zeus" (PDF). Archived from the original (PDF) on November 6, 2011. Retrieved 2012-02-05.*

26. ^ Jump up to: ***a*** ***b*** *Richard S. Westmoreland (2010-10-20). "Antisource - ZeuS". Archived from the original on 2012-01-20. Retrieved 2012-02-05.*
27. ^ *Horowitz, Michael (2012-02-06). "Online banking: what the BBC missed and a safety suggestion". Retrieved 2012-02-08.*
28. ^ *Purdy, Kevin (2009-10-14). "Use a Linux Live CD/USB for Online Banking". Retrieved 2012-02-04.*
29. ^ *Konoth, Radhesh Krishnan; van der Veen, Victor; Bos, Herbert (2017). "How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication". In Grossklags, Jens; Preneel, Bart (eds.). Financial Cryptography and Data Security. Lecture Notes in Computer Science. Vol. 9603. Berlin, Heidelberg: Springer. pp. 405–421. doi:10.1007/978-3-662-54970-4_24. ISBN 978-3-662-54970-4.*
30. ^ *Chickowski, Ericka (2010-10-05). "'Man In The Mobile' Attacks Highlight Weaknesses In Out-Of-Band Authentication". Archived from the original on 2012-03-01. Retrieved 2012-02-09.*
31. ^ Jump up to: ***a*** ***b*** *Schwartz, Mathew J. (2011-07-13). "Zeus Banking Trojan Hits Android Phones". Archived from the original on 2012-07-06. Retrieved 2012-02-04.*
32. ^ *Balan, Mahesh (2009-10-14). "Internet Banking & Mobile Banking users beware – ZITMO & SPITMO is here !!". Retrieved 2012-02-05.*
33. ^ *Sartain, Julie (2012-02-07). "How to protect online transactions with multi-factor authentication". Retrieved 2012-02-08.*
34. ^ *Imperva (2010-02-14). "Threat Advisory Boy in the Browser". Retrieved 2015-03-12.*

- Virus attack on HSBC Transactions with OTP Device Archived 2016-04-02 at the Wayback Machine
- Virus attack on ICICI Bank Transactions Archived 2016-04-04 at the Wayback Machine
- Virus attack on Citibank Transactions Archived 2016-04-03 at the Wayback Machine
- Hackers outwit online banking identity security systems BBC Click
- Antisource - ZeuS A summary of ZeuS as a Trojan and Botnet, plus vector of attacks
- Man-In-The-Browser Video on YouTube Entrust President and CEO Bill Conner
- Zeus: King of crimeware toolkits Video on YouTube The Zeus toolkit, Symantec Security Response
- How safe is online banking? Audio BBC Click
- Boy-in-the-Browser Cyber Attack Video on YouTube Imperva
