Cyber crimes increase everyday

Did you take precautions?

New generation of malware

designed to target online banking

designed to remain undetected by AV solutions

steals billions of dollars each year

Stop attackers. Trace infection attempts. Eliminate losses.

We Keep You Safe!
ZEMANA® LABS

Attack Vector Series

Man In The Browser Attacks

The Greatest Threat to Online Banking

First described in 2005, Man-in-the-Browser (MitB) attacks work by utilizing common facilities provided to enhance browser capabilities such as browser helper objects, browser extensions and user scripts. This type of attack has been used by sophisticated malware targeted at draining bank accounts, stealing login credentials, credit card numbers and other sensitive information. It is specifically developed to intercept information transmitted over Secure Sockets Layer (SSL) encrypted internet connections.

Capabilities

MitB attacks are used to intercept and manipulate calls between the the browser and its security mechanisms or libraries on-the-fly. The most common objective of this attack is to cause financial fraud by manipulating transactions of Internet Banking systems, even when other authentication factors are in use. Some of the most common capabilities include:

➡ Obtain full credit card details during any online transaction

➡ Add fields during the internet banking login to steal customer PIN, full credit card number, and other sensitive information

➡ Change the amount and the destination account during online banking transactions

➡ Change any amount users see, such as remaining balance, past transactions, etc.

Spread and Impact

MitB attacks are typically used as part of narrowly focused financial malware. In recent years there is a trend towards increased number of financial malware, which replaced the trend of continuous development of a single strain. Most analysts attribute this to the leaked source code of ZeuS, which allowed further development of the already extremely complex and efficient malicious code. Some of the more prominent pieces of financial malware that use MitB are:

ZeuS
First seen: July 2007
Impact: over 13 million PCs worldwide
Damage: over USD 500 million
Most infected: USA, Egypt, Mexico, Saudi Arabia, Turkey

SpyEye
First seen: 2012
Widely regarded as the successor of ZeuS, after ZeuS's source code was leaked.
No data exists to date about distribution and damage

Carberp
First seen: 2010
Price on the black market: US$ 40.000 per kit
Damage: over US$ 250 million
Capabilities: completely disable anti-virus products, detects and removes competing infections, such as ZeuS, takes full control over infected machines.
Seen as the most advanced form of financial malware today.

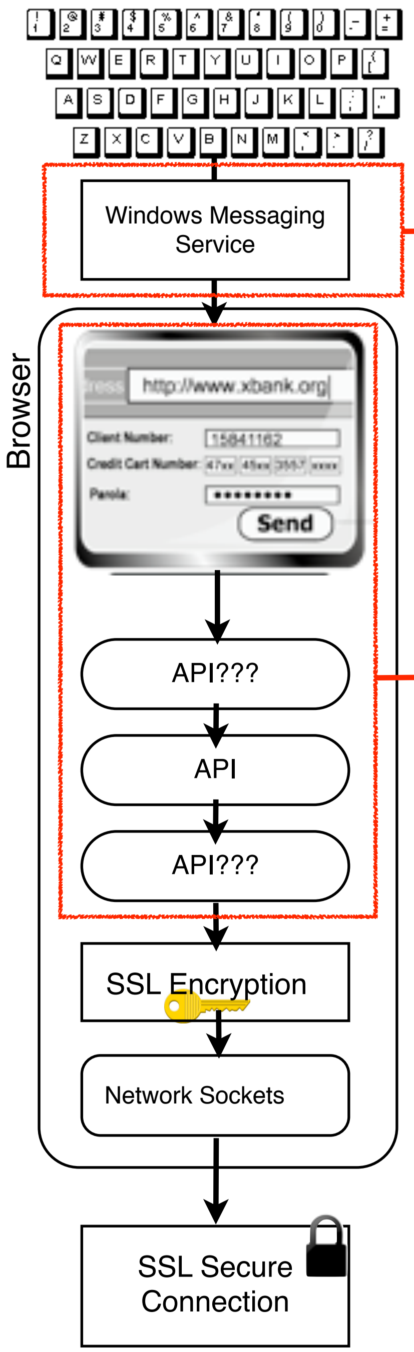
Detection

Numerous independent organizations test security solutions capabilities to detect and stop financial malware attacks. Average detection rate of traditional anti-virus solutions for ZeuS stands at only 20%. Traditional solutions are virtually useless against new strains. A test by MRG Effitas showed that out of 28 A-brand security solutions only 3 were able to detect a zero-day MitB attacker. All of them dedicated safe browsing and encryption solutions that do not rely on traditional signature fingerprint approach.

The reason is quite simple: traditional security solutions are looking for known malicious files. Financial malware is designed to change its fingerprint every couple of hours, effectively avoiding detection.

Zemana's software solutions detect attack vectors, regardless whether the attacking file is known or unknown. Our solutions work on the assumptions that the system is infected, allowing only known safe files to be executed. Next to making our software lightweight and small, this approach makes our solutions efficient against zero-day threats, custom hacking attempts and what the industry refers to "Advanced Persistent Threats."

Attack Details



http://www.xbank.org

Client Number: 15841162

Credit Cart Number: 47xx 45xx 3557 xxxx

Parola: ••••••••••

Key Logger Vulnerability
Key loggers can intercept keystrokes. Reliable protection methods are keystroke encryption or behavior-based anti-hooking methods. Zemana AntiLogger © and Zemana KeyCrypt © are light, efficient and tested technologies that provide redundancy in closing this vulnerability.

Man-in-the-Browser Vulnerability
Infected browser can be fully controlled by the banker Trojan. This vulnerability is becoming the preferred method by modern financial malware. Latest malware does not feature key-logging functionality, it is being replaced by MitB attack.

This bring a number of advantages for the malware creators:

- Only targeted and valuable SSL traffic is transmitted
- Virtually impossible to detect by traditional anti-virus solutions
- Full control over infected browsers, instead of simply access to passwords, account and credit card numbers

Zemana's SSL security technology ensures the integrity of the SSL Container and SSL Data Path before encryption takes place.

Cloud-based reporting service allows you to identify infected machines.

Contact us today
For free of charge evaluation of your current security software

sales@zemana.com
US Toll Free +1.866.293.2016

Be ready for tomorrow’s treats

About Zemana

We are a technology-driven security software solutions provider. We proclaim a layered approach to endpoint security as the only strategy that will ensure an adequate response to the breadth and depth of online threats today. Our solutions are used by a rapidly growing number of individuals and organizations that realise traditional security products are not powerful enough to protect them against some of the most dangerous threats out there: identity theft, industrial espionage, financial malware, spyware.

Our technology protect over 10 million endpoints worldwide. Our partners and clients include large telecoms, banks, companies operating in the nuclear and military fields.