The Invisible Threat – MitB (Man in the Browser)
About Me

- Uri Fleyder
- Security Researcher
- FraudAction Research Lab @ RSA
• Plan for the following 28 minutes:

  – Get familiar with the MitB threat
  – Live demonstration
  – Discuss possible solutions
• Video demonstration

..\Video\MitB.mxf
• Do you **trust** your endpoint device?

- Desktop PC
- Laptop
- Notebook
- Mobile phone
• What is trust?

• Definition for trust @ thefreedictionary.com:

"The condition and resulting obligation of having confidence placed in one"
• Your endpoint device can be compromised in numerous ways by various techniques, with or without the user’s active intervention
• Malicious links via spam emails and messages in social networks

• Malicious executable files via file sharing services and free download websites

• Drive-by exploits

• Built-in backdoors in legitimate software

• Malicious worms - spreading inside and outside your LAN
• Most of the users trust their endpoint device

• They will follow almost any instructions displayed by the web-browser

• The instructions should be written, displayed or shown in a reliable enough manner (correct context, spelling, grammar).
Let us assume that you are using your own PC in order to log in to your online banking account and displayed with one of the following:
Validate Security Information

Your security is important to us, so please answer your security question before logging in.

Enter your User ID and Password below:

User ID: 
Password: 

LOG IN

Have you forgotten your User ID or Password?
Lutte anti-fraude Vérification

Mise à jour de vos informations

Date de naissance:

N° de téléphone:

N° de permis de conduire (facultatif):

État éventuel de la permis de conduire (facultatif):

Confirmez les informations

Pour accéder à votre compte, vous devez entrer vos informations de identification dans les champs ci-dessous. Cette information est utilisée à des fins de vérification seulement.

Note: Votre carte de crédit ne sera pas débitée.
• How would you react?

• Most of the users would not suspect that something is "phishy" here, many of them will follow the instructions and provide the requested information
Welcome to banking

Please enter your banking user ID below, and click continue

User ID
Passphrase:
One Time Code (OTC):

Continue

User Information

- Your banking user ID can be obtained from your local administrator
- Please click here for further information about our terms & conditions

IMPORTANT: UNAUTHORISED ACCESS PROHIBITED. SESSIONS MAY BE MONITORED
You are required to have appropriate authorisation to access this service and you must comply with all the terms and conditions governing its use. Banking in your use of this service, evidence of unauthorised use and criminal activity on this system will be reported to the appropriate authorities

Important links:
- Fraud Prevention
- Security
- Legal Notices
- Privacy Policy
- Information
Welcome to Banking

Please enter your Banking User ID below, and click Continue

Authorization Required

Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don't reload the page while performing required steps.

Please wait 5 minutes. We are checking your security settings.

Remaining time: 274.3 sec.

Continue
Welcome to Banking

Authorization Required

Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don't reload the page while performing required steps.

Step 1. Please generate a new access code using your token device:

Token code #1: ____________________

Important Links:
- Fraud Prevention
- Security
- Legal Notices
- Privacy Policy
- Information
Authorization Required

Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don't reload the page while performing required steps.

Step 2. Please generate a new access code using your token device:

Token code #2: 

Continue
Authorization Required

Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don't reload the page while performing required steps.

Step 3. Please generate a new access code using your token device:

Token code #3: 

Important Links:
- Fraud Prevention
- Security
- Legal Notices
- Privacy Policy
- Information
Authorization Required

Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don’t reload the page while performing required steps.

Thank you for verification. Online banking is currently under scheduled maintenance. Please check back in 24 hours.

You are required to have appropriate authorization to access this service and you must comply with all the terms and conditions governing Banking in your use of this service. Evidence of unauthorised use and criminal activity on this system will be reported to the appropriate authorities.

Important Links:
Fraud Prevention  Security  Legal Notices  Privacy Policy  Information
Online banking is currently under scheduled maintenance. Please check back in 12-24 hours.
• People tend to trust their endpoint devices more than they trust 3-party service providers

• Typical user:
"this annoying bank is probably upgrading their website, oh well..."
• The endpoint devices in all of the above cases were compromised by a financial Trojan with MitB capabilities

• MitB capable Trojans are using code hooks in order to inject predefined malicious content into the relevant process
  
  – iexplore.exe
  – firefox.exe
  – chrome.exe
  – opera.exe
  – explorer.exe
• MitB?

  – No man (and no woman) inside

  – It is all about customized, tailor made (per target) client side code snippet (JavaScript), injected into the active process responsible for web browsing
• Simple HTML injections
  – The web browser displays false information in order to steal additional personal and financial information

• ATS (Automatic Transfer System)
  – Malicious client side injections are capable to automatically transfer money from your banking account

• Manual MitB
  – Malicious client side injections are capable to send the login credentials to the fraudster in real time while blocking the user
During the last 3 years our research lab studied and analyzed more than 11,000 unique variants of financial Trojans.

All of the analyzed variants used client side injections.
• Demonstration

  – Install of financial Trojan kit
  – Install of Exploit kit
  – Configuration of client side injections
• Solutions?

  – Web injections are triggered by visiting specific URL/domain - Changing the URL/domain is not feasible

  – Injected code usually relies on the DOM's objects, randomization and obfuscation of the DOM’s namespace will disable most of the current MitB injections
• Questions?
• Please rate my talk 😊

https://www.surveymonkey.com/s/Research12_UriFleyder