Firesheep goes Man-in-the-middle

Version 101107

Antago GmbH | Robert Bosch Stra e 7 | D 64293 Darmstadt
Tel.: +49 . 6151 . 428568 . 0 | Fax: +49 . 6151 . 428568 . 1
E-Mail: sicherheit@antago.info | Web: http://www.antago.info
HRB 89141 | Gesch ftsf hrer: Mark Semmler , Silke Thielmann

Sitz der Gesellschaft: Darmstadt | Registergericht: Darmstadt
Steuer-Nr.: 007 228 03 203 | Ust-IDNr.: DE 27 237 9849
Konto-Nr.: 0133 106 971 | BLZ: 508 526 51 | Sparkasse Dieburg
IBAN: DE07 5085 2651 0133 1069 71 | BIC: HELADEF1DIE

Introduction

Firesheep (http://codebutler.github.com/firesheep/) is "a Firefox extension that demonstrates HTTP session hijacking attacks". The attacking technique used by Firesheep isn't spectacular but Firesheep is very easy to use. This makes Firesheep real dangerous.

But there is a limitation: Firesheep just works in shared mediums (f.e. wireless LAN hotspots).

During the last weeks more and more users of Firesheep were looking for the possibility to use it in a switched environment. So the next step to support the target of Firesheep (showing how dangerous the usage of plain HTTP really is) was to find a easy solution to perform HTTP session hijacking in a switched network environment by combining Firesheep with ARP spoofing.

This paper describes how to archive this goal with a user friendly interface. We focus in this paper on Windows – just because we decided to do so (if you are able to port the solution described here to MacOS, please write us a mail).

What we have done is nothing spectacular but it was fun to do it and the result is useful to demonstrate the insecurity of the most web based applications today: They - maybe - perform a HTTPS login but fail to protect their users properly afterwards, making HTTP session hijacking an easy task to perform.

Dependencies

We assume, that you work on a Windows box with Firesheep (http://codebutler.github.com/firesheep/) and WinPcap (http://www.winpcap.org/) already installed.

Install External Application Buttons mod for Firefox 3.0+

Go to https://addons.mozilla.org/de/firefox/addon/12892/ and klick „Add to Firefox".
Follow the instructions. Be aware: This extension has not been reviewed by Mozilla.

Download and extract Arpspoof

Go to http://arpspoof.sourceforge.net/, download the rar file and extract it to your local harddrive. We assume, that you extract it to `c:\arpspoof\` (which is not the way you should work, but wit spares some keystrokes, right?).

Be aware: Arpspoof will be recognized by many antivirus software as a hacker tool. You have to turn off your antivirus or circumvent the scanning of Arpspoof if you want to continue.

Download and extract Antago Arpspoof Extension

Go to our webpage https://www.antago.info/ and download the zip file "`antago-arpspoof-extension-v0.1.zip`" from the section "PAPERS". Extract it to your local drive.

Check if you got the right file by comparing the checksums:
The md5 checksum of `antago-arpspoof-extension-v0.1.exe` is dddd8156464f182cf04303bd145243ac.
The sha1 checksum of `antago-arpspoof-extension-v0.1.exe` is a39139e2a2763febf20b862be4f9d63bc031da13.

We assume, that you extract it again to `c:\arpspoof\` (which is again not the way you should work, but it spares again some keystrokes, right?).

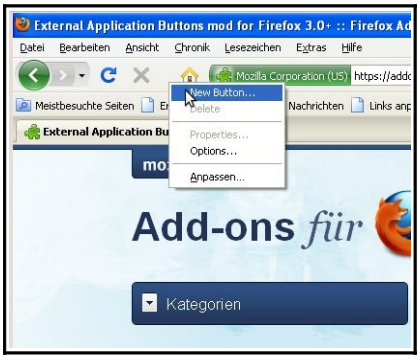
Be aware: According to Virustotal (http://www.virustotal.com/) antago-arpspoof-extension-v0.1.exe will be recognized by the antivirus software Jiangmin (http://global.jiangmin.com/) as "TrojanDropper.BAT.Dmenu.aj". This is a false positive (trust me!). But in future maybe other antivirus software will rate Antago Arpspoof Extension as a hacker tool.

Set up

Add a button for the Antago Arpspoof Extension to your browser

Start Firefox. Open the menu View → Toolbars → Customize. Drag and drop the item "External Application Buttons mod" from the menu to your toolbar. Please note: There is no icon for this item – after closing the menu you will notice the item inside your toolbar only by a small empty space – so remember where you dropped it.

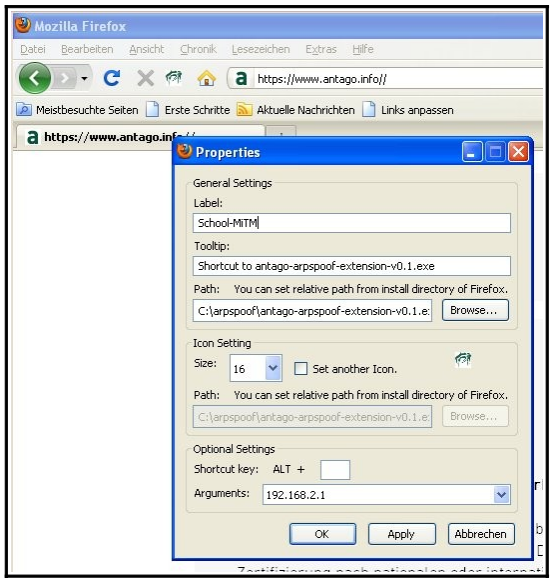
After you have closed the menu, perform a right click on the "External Application Buttons mod" item inside your toolbar (the empty space - you remember?) and choose „New Button" in the appearing context menu:



In the next window locate and choose „`antago-arpspoof-extension-v0.1.exe`". If you followed the instructions above, you'll find it inside `c:\arpspoof\`. After clicking okay, you can see a little fiddler crab (our company mascot) as the icon of the new button (marked with a red frame in the following picture).

Configure the Antago Arpspoof Extension

Before you can use the new button you have to set up some parameters. Therefore right click on the fiddler crab and choose „Properties“:

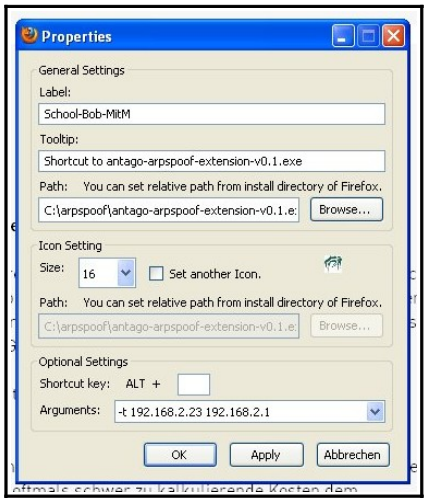


Here you can choose a label, a tooltip and a icon for the button and specify arguments which will hand over to the called application (in our case `antago-arpspoof-extension-v0.1.exe`). This enables you to set up different MiTM profiles for different environments, each one linked with its own button inside your toolbar.

The central configuration is inside the „Arguments“ field. In this field you have to place the parameters for Arpspoof. The syntax of Arpspoof can be found inside the manpage (f.e. http://www.irongeek.com/i.php?page=backtrack-3-man/arpspoof).

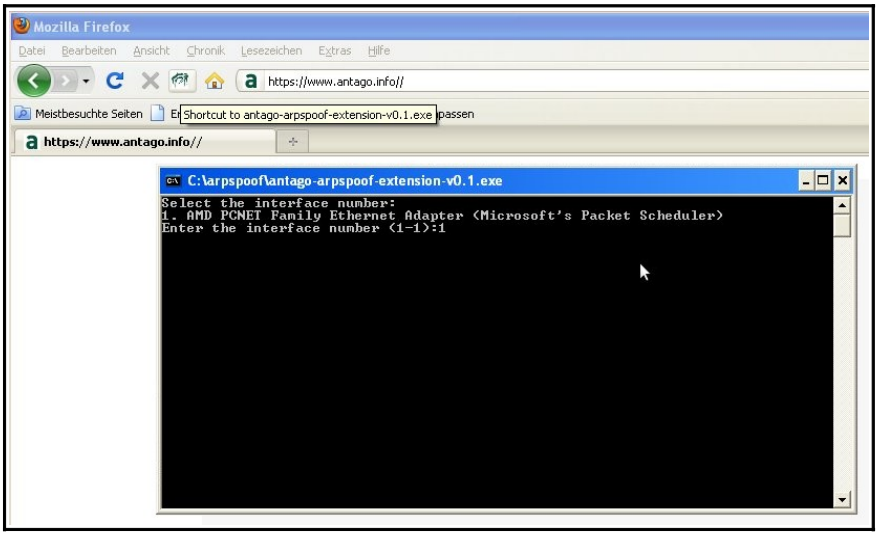
If you want to sniff the whole network traffic between your network neighbors and the internet, in most environments you have just to enter the IP of your default gateway (to get the IP of the gateway just „`ipconfig /all`“ inside a shell).

If you want to sniff network traffic beetween two computers just type a „`–t`” (for target) followed by the IP of the two computers:

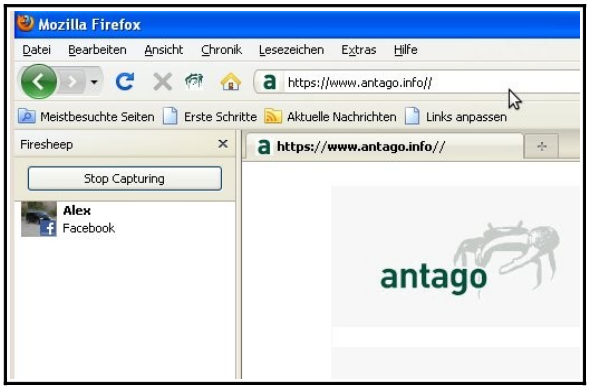


Using Antago Arpspoof Extension

In order to start the configured MiTM attack, just click on the fiddler crab. A shell appears, asking you for the network device which should be used. Choose the right one and hit Enter:



After that you can start Firesheep by clicking View → Sidebar → Firesheep. Press „Start Capturing" and be surprised, you're sniffing inside a switched network.



Responsibility

It is our intention to force Facebook, Wer-kennt-wen, StudiVZ, webmailers and all the other poorly secured web based applications to make the next step and protect their users in a appropriate way.

Firesheep is a powerful tool to demonstrate the lack of security and build up some pressure to achieve this goal. With the MiTM extension it has become even more powerful.

As a user of Firesheep (with or without the Antago Arpspoof Extension), you should be kind to your neighbors and co-workers and check twice, what you are doing.

We deeply apologize for...

...the lack of any testing

This step-by-step tutorial has been made in order to show how easy it is to integrate MiTM capabilities quick-n-dirty to Firesheep by using Firefox Add-ons. But this is a quick-n-dirty solution, version 0.1. No quality checks or any kind of deeper testing has been performed.

There aren't any experiences for attacking from wireless to wireless or running the attack out of a complex virtual boxes.

...the lack of warranty

We can not give any warranty for any software mentioned in this paper. This includes the Antago Arpspoof Extension.

The Antago Arpspoof Extension is provided “as is”, without warranty of any kind, express or implied, including but not limited to the warranties of merchantability. In no event shall the Antago GmbH be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the software or the use or other dealings in the software.

...our bad English

This paper has been written without any support of professional translators. I think you already guessed this.

Feedback

We would like to hear from you. The mail address for feedback is firesheep-mitm [at] antago [dot] info.

Please notice:

We will not provide

- **any kind of 1st-level-support for Firesheep**
- **any kind of 1st-level-support for Firefox**
- **any kind of 1st-level-support for Arpspoof**
- **any kind of 1st-level-support for unexperienced users or**
- explanations about MITM or ARP spoofing.