Firefox tunnel to bypass any firewall

Antonio Costa aka CoolerVoid - e-mail:coolerlair@gmail.com or acosta@conviso.com.br

Figure 1: *Fox on tunnel by pixabay*

Abstract

A crucial element for the Red Teams task is having stealth to perform the attack, success in the ability to expose an aggressive mindset and a true crackers point of view. If the red team win, they can help building a better defense for the Blue Team in the future. This content is meant for good purposes, don't worry.

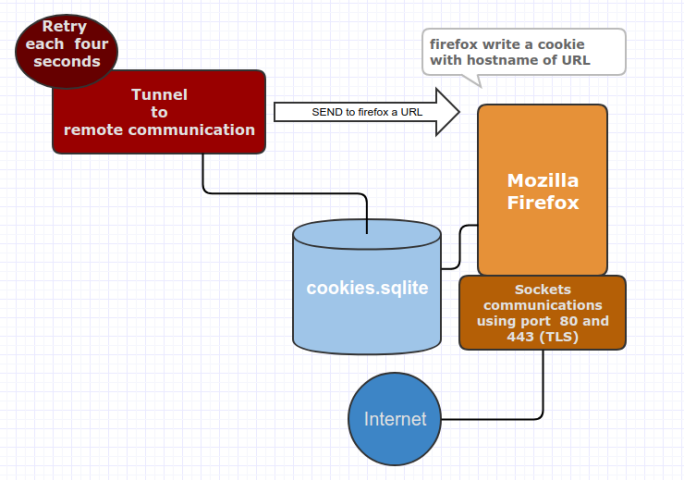
At this paper, the content is about a different attack approach to get remote control of the machine and bypass the firewall. We have a lot of weapons to work in that perspective, something like veil framework, msfvenom... but sometimes following different path, will generally bring good result

Keywords: red team, hacking, security, evasion,bypass firewall

1 The Basics of the attack

The objective of the attack is to use Firefox to make all the communications between the client and the server by using hookings. This is not impossible, yet DLL injection sometimes can be boring to implement and even harder to make it portable. Did you know that x32 and x64 architecture need different approaches for development? (later I discovered that easyhook api can solve that). I was studying the firefox internals, reading something about the use of SQLite to work with cookies, that give to me a different focus.

Look that following:

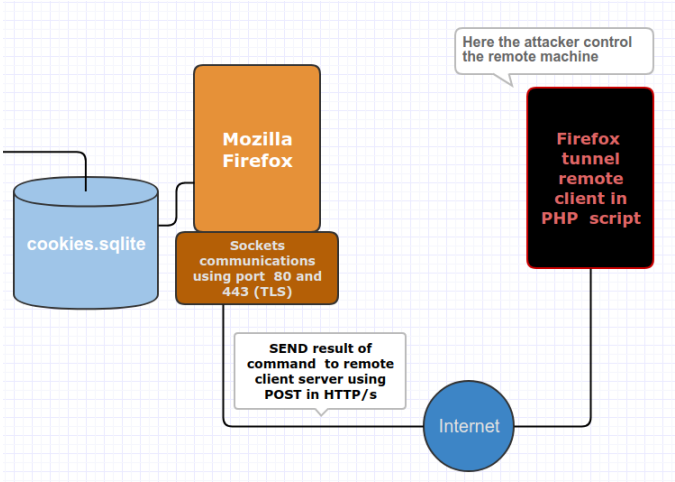


2 Create the attack

To create a program like firefox tunnel. These are the steps to get started:

- The program calls Firefox Browser in hidden mode, sends a URL that contains an evil server and finally that evil server sends a cookie with a command.
- Tunnel gets the cookie of evil server (cookie.sqlite) and uses that to call a command shell.
- The result of command shell is used to write an HTML with javascript to make auto submit with the content result.
- The Programm opens HTML in hidden mode to send the result of CMD to the evil server.

Look that following:



3 The proof of concept

In order to see this in action I have created a repository with everything you need and even a PoC. Please check the following link: `https://github.com/convisoappsec/firefox_tunnel`

4 Future insights

- Insert persistence, using function RegOpenKeyEx() to open path Software/Microsoft/Windows/CurrentVersion/Run and write with function RegSetValueEx() to launches a program automatically at system startup.
- Use images in I/O using steganography.
- Running process in hidden mode.
- Turn tunnel unkillable process.
- Create DLL to inject in system process.
- Function to search different firefox binary path to execute.
- Make portable to others browsers like chrome and IE.

5 Possible mitigations

- Global hooking, to get OpenFile(), CreateFIle() functions and filter argv cookie.sqlite and block when programm route is different of firefox.exe.
- File watch api to monitor the database of cookies.
- Programm to open database of cookies by periodicity and search evil domain or hosts using query SELECT, that can use black list and uses DELETE query to remove the evil cookie.
- Put firefox directory in different path.
- Change firefox name of binary file.
- Programm to hooking SQLite and block non common querys.
- Consult us for more ideas.

6 Contact Information

If you have questions or suggestions regarding this document, please contact Antonio Costa at “coolerlair@gmail.com” or “acosta@conviso.com.br”.

Acknowledgements

Nash Leon for introducing me about headless trick.

Daniel Bermudez, Wagner Elias, Luan Souza aka p4ck4g3 for revision

References

AUTHORS: ALLEN, GRANT, O. M. The definitive guide to sqlite. `https://www.apress.com/br/book/9781430232254`.

AUTHORS: ELIAS BACHAALANY, J. K. The antivirus hacker’s handbook. `http://shop.oreilly.com/product/9781119028758.do`.

AUTHORS: RASMUS LERDORF, KEVIN TATROE, P. M. Programming php. `http://shop.oreilly.com/product/0636920012443.do`.

FLANAGAN, D. Javascript: The definitive guide. `http://shop.oreilly.com/product/9780596805531.do`.

JR., H. S. W. Hackers delight. `http://www.hackersdelight.org/`.

LOVE, R. Linux system programming. `https://www.safaribooksonline.com/library/view/linux-system-programming/9781449341527`.

MCFARLANE, N. Firefox hacks. `https://www.safaribooksonline.com/library/view/firefox-hacks/0596009283`.

STROUSTRUP, B. Programming – principles and practice using c++. `http://www.stroustrup.com/programming.html`.