Proof of concept; a worm botnet.

Abigail ECCLESTON, B00140442

Jérémy PRIMARD, B00168148

Tytus KOPERA, B00140074

School of Informatics and Cybersecurity, Faculty of Computing, Digital & Data,

Technological University Dublin

Submitted to Technological University Dublin in partial fulfillment of the requirements for the degree of

Bachelor of Science in Computing in Digital Forensics & Cyber Security

Supervisor:

Mark Lane

May 2024

Declaration

I herby certify that this material, which I now submit for assessment on the programme of study leading to the award of Degree of **Bachelor of Science in Computing in Digital Forensics & Cyber Security** in Technological University Dublin, is entirely my own work except where otherwise stated, and has not been submitted for assessment for an academic purpose at this or any other academic institution other than in partial fulfilment of the requirements of that stated above.

Dated: 04/15/2023

Abigail ECCLESTON

Jérémy PRIMARD

Tytus KOPERA

Abstract

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

Keywords: Botnet, malware, virus, rust, TODO.

Contents

I. Introduction

I.1. Definitions

In a world where more and more things rely on computing, it is necessarry to know how virus works, especially some of the worse ones. Worms, a type of virus that can self replicate in order infect more and more. It is usually use to lauch some ransomewares and other denial of service attacks. Because of it's self replicated nature, once launched, it doesn't need a head to continue spreading if it's codded to do that. It have also the good ability, depending what is it's purpose, to conceal the pirate. Botnets, another type of virus that takes control of multiples machines in order to do evil things, like Distributed Denial of Services (DDOS) attacks, or win more power in order to either mine cryptomoney, or crack password are another.

I.2. Origins of the project

This is where the idea of the project started. Because one of the huge flaw of botnet is that they need a head to works, we think of this idea. What if we can allied the ability to conceal the perpretrator of the attack from the worm, and the ability to control bots of a botnet? More precisally, our idea is to make a botnet that spreading like a worm, so that only a verry little quantity of machine actually knows the address of the head of the botnet. We remind here that our project is simply a proof of concept, and so, it's only meant to be shown in the final demo of the project. Several parts of it, if not all of them, would need real improvments, in order to overcome some of it's limits. Again, we remind that this project isen't meant to show the virus of the future, but only to show, and give a proof of concept, of a type of botnet there isen't enough research on it. Indeed, the closest thing we could find to our idea, was Peer to peer botnet, that's similar to what we want to do, but it's wasn't enough. (https://ieeexplore.ieee.org/abstract/ document/ 5684002/) (https://citeseerx.ist.psu.edu/ document?repid=rep1& type=pdf& doi=5de6987574e48076fa5f024f347d44c77a6fa080) We can also added to it that we were interested by the field

I.3. Preliminary research over an existing botnet and an existing worm that appears in the last 25 years.

Before begining to talk about the implementation of our botnet, let's find three examples of pretty well known worm and botnet, to get an idea of what already exist.

The first worm that we find was wanacry. (https://en.wikipedia.org/wiki/WannaCry_ransomware _attack) It's a bot which appeared on 2017 and targeted only Microsoft windows softwares. It was spread using a critical vulnerability of the SMB server that is on every windows machines. The way it's works is the same way as most worm, that means that if a machine is vulnerable, the worm will drop and exec a file, wich goal is to first self-replicate the worm, install a ransomware, and target other machines. (https://www.csoonline.com/article/563017/ wannacry-explained-a-perfect-ransomware-storm.html)

The other example we choosed, is the opensource, mirai botnet. (https://en.wikipedia.org/wiki/

Mirai_(malware)) It's a botnet spreading over ports 23 and 2323, in order to make new bots. It's way of working is simple. It tries to bruteforce some linux iot devices, using the default built-in credential, assuming that nobody changed it. After that, the bot awaits it's orders. Usually, it was to DOS a DNS server or a big cloud company.

Another botnet example, is the so called Hajime botnet (https://en.wikipedia.org/wiki/ Hajime_(malware)) which goal was simply to protect device against the mirai botnet, by closing telnets ports. This is a really well know botnet, using peer to peer capabilities, to hide it's owner address, and thanks to that, makes it a lot more difficult to be blocked by ISP to takes down the botnet. (https://thehackernews.com/2017/04/ vigilante-hacker-iot-botnet_26.html)

II. Our implementation and design

II.1. Thigs necessary for the project we had to either find or makes.

Our project had different parts.

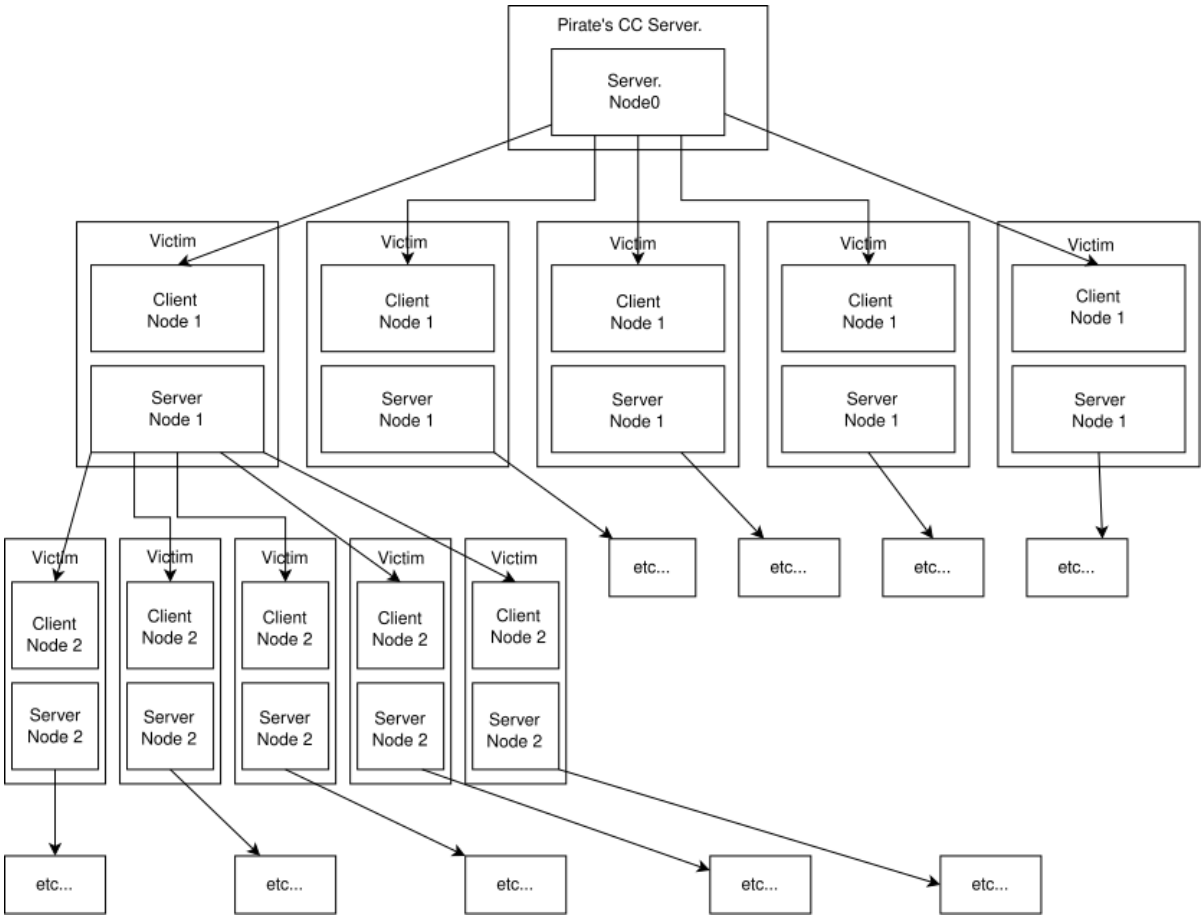
- Make a sandboxing environment, to test it, while been sure that it can't escape. We used qemu and unshare to make an environnment that couldn't reach the external network. In the end, it wasn't really usefull to make it, because we decided that for the demo, the victims ip should be knowed at launched time, so that we won't see unexpected things in the final demo.

- Find an exploit to use. It had to be a remote code execution, easy to setup, and easy to exploit, because it's not in the purpose of the project to find a new vulnerability, make a exploit or another crazy thing like that. We spend hours looking for the perfect exploit, and in the end, we find somebody else project on github, that was doing exactly what we were looking for. (https://github.com/opsxcq/ exploit-CVE-2014-6271) Thanks to opsxcq works, we had an easy vulnerability to exploit. We choosed shellshock, CVE-2014-6271. We find in opsxcq repository, a vulnerable docker image to shellshock CVE-2014-6271, and an easy command to exploit it. The other two interested vulnerability that we found in his repos, but that in the end we choosed to not use, was CVE-2016-10033 and CVE-2017-7494. There were both unadapted to our needs because of how difficults they would makes us write the exploit. We also find Log4J, but in the end decided that we would better to abandon it, and try an easier vulnerability to exploit.

- Demonstrate the botnet. Like all botnet run things, we had to find a way to prove that the botnet has really taken control of several machine. For that, we made one more Vm, that we called vulnerableDOS. We simply run wireshark into, and once the botnet has taken control of the bots, it will make them ping our machine. At first, we wanted to make our botnet run an actual DDOS attack on the vulnerableDOS machine, but because it's not in the purpose of the project to make it run a complex attack, our goal is just to prove that we have indeed taken control of the vulnerables machines, we choosed to do only ping.

Obviously, we also had to make the actual botnet.

II.2. design explanations about the botnet.



III. Part 2

III.1. Something part

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

III.2. Something part

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

III.3. Something part

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

IV. Part 3

IV.1. Something part

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

IV.2. Something part

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

IV.3. Something part

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

Conclusion

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis. Suspendisse interdum ac tellus nec ultricies. Nullam eu bibendum ipsum. Pellentesque in ipsum vel orci ullamcorper malesuada in at turpis. Nulla facilisi. Quisque ullamcorper at sem eget porttitor. Ut sed mi fermentum, fermentum purus in, molestie sem.

Glossary

- **Botnet:** A type of malware which takes control of numerous machines to lauch somes attacks. Althought it's usually used to lauch denial of services attacks, it can also be used to crack password or even mine cryptocurrency.
- **Other example:** Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque viverra pulvinar dui ut venenatis.

Refenrences

[1] This website is the first example that came to my mind as an example.. https://example.com

[2] This is another example to show peoples what is en entry in the references chapter.
https://secondexample.com