**Find The Owner - Pwnium CTF 2014 Writeup**

**Introduction:** Simple Check was an easy 100 point reverse engineering challenge that was part of the 2015 School Ctf Winter organized by Tunisian Pwnium team. This writeup was made possible using resources from the [CTF Wiki](https://github.com/ctfs/write-ups-2014/tree/master/confidence-ds-ctf-teaser/stegano50).

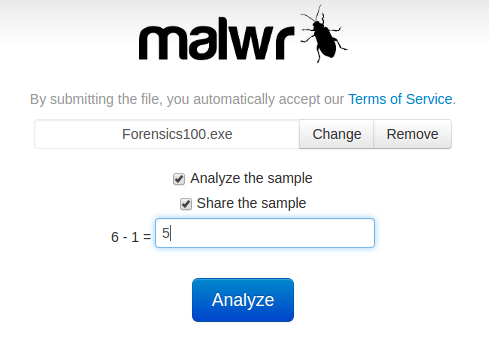
**Task:** Using the provided .zip file, find the flag. The flag format is Pwnium{md5[ip:port]}. **The provided file is malware, use caution.**

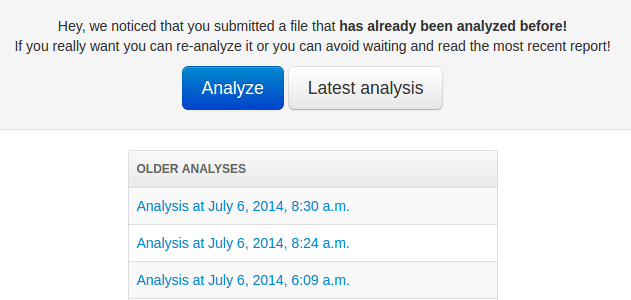
**Solving:** Excellent, we’re provided with a .zip file that contains a malware executable. To solve this challenge we need to find the IP and port this executable communicates with and create an Md5 hash. The real question is how do we find the IP and port this executable communicates on?

There are several ways we could approach this problem at first. Since I know from the get go that this provided file is malware, and I don’t want to harm my PC. I’m going to start off by analyzing the binary using an online sandbox. There are several free sandboxes hosted online, some better than others. I’ll be using [Malwr.com](http://malwr.com) today because it’s free, fast, and has a lot of really neat features.

Sandboxes like the one hosted at Malwr.com are amazingly handy tools to have when analyzing a suspicious file. They’ll provide quick access to information ranging from a quick overview of the binary, behavioral analysis, and network analysis. All of this information is provided to us without having to use our own special tools, VM, or Deep Freeze. Running binaries in a sandbox environment should often be one of your first stops when an analyzing a suspicious binary.

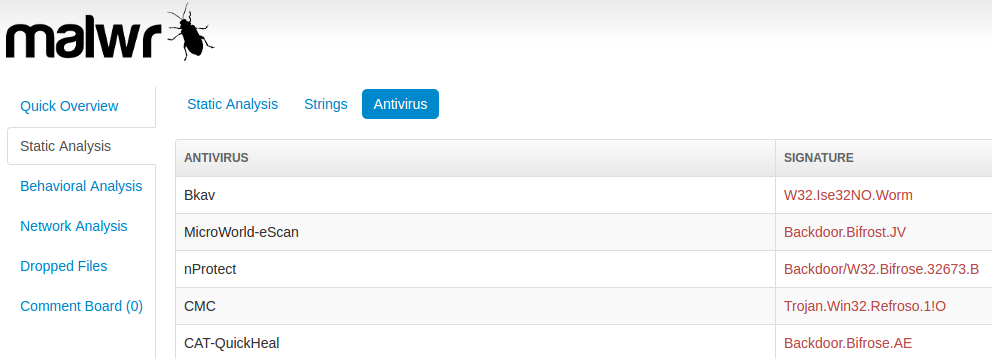
Let’s begin by uploading the binary to Malwr.com





Hey! Would you look at that, it seems our mysterious binary has been analyzed in the past. Another plus to the sandbox environment is when a binary’s been analyzed previously you don’t have to wait for the analysis again.

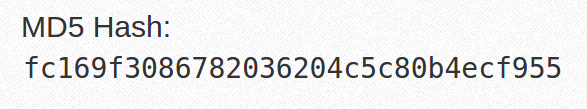
Since we’re interested in finding the IP and port this binary uses I’m going to jump straight to the Network Analysis tab. Where we notice that the IP 193.95.68.245 is used. Unfortunately, there’s no destination port here, we’ll have to look elsewhere. Since we were told beforehand that the binary is malicious, let's go have a look at the Static Analysis section for clues.



It seems this binary matches a known piece of malware known as Bitfrose, or Bitfrost. Searching on google for information about Bitfrose lead us to a wiki page about [Bitfrost](https://en.wikipedia.org/wiki/Bifrost_(Trojan_horse)). After some light reading we learn that Bitfrost is a piece of malware that targets Windows 95 through Windows 7 to allow a remote attacker to execute arbitrary code on the compromised machine.

Further down the page we see the most important information of all. When running Bitfrost connects to a predefined IP address on TCP port 81.

We seemingly have all of the information we need for the challenge. Lets try creating an MD5 Hash of the IP:Port that we found; 193.95.68.245:81. For simplicities sake I’ll use an [online hash calculator](http://www.miraclesalad.com/webtools/md5.php)



Viola, our flag is Pwnium{fc169f3086782036204c5c80b4ecf955}