# Malware reconciliation design (part 1)

For many people today, reverse engineering is a rather strange mechanism. They don't even know what it is and how to use it. Why can reverse use of architecture of an executable? The skills needed to perform

For many people today, reverse engineering is a rather strange mechanism. They don't even know what it is and how to use it. In this series, we will introduce you to the basics of how to apply reverse engineering in the field of security, which is rapidly developing and transforming.

**Reverse Engineering and you**

I heard of this term for the first time a few years ago. But I didn't really notice at the time, and it didn't have anything special to immediately get into my head. After moving to research some areas of computer security such as network protocols, intrusion detection, Web application security, I started to pay much attention to reverse engineering. Why can reverse use of architecture of an executable? What skills are needed to perform this task? When doing something, the desire to do is half the problem. The other half needs an understanding of how to accomplish that job.


Before discussing the skills and knowledge required to practice reverse engineering, perhaps we should understand why it is so important for people who do administrative or security practices. As you know, computer networks are always the target of attacks. There are hundreds, even thousands of hackers with many different skill levels, many types of penetration, attack, and sweeping, always lurking around, making your network always in danger. The problem is not "whether or not" but "when" a certain attack will visit you. Should we create a lucky opportunity for the attacker or always actively control the game every day?

Assume that an attacker has broken through your defenses. Quickly detect the attack, stop immediately, minimize the damage caused by it is the biggest skill you have. The reason is because IDS has done the warning in the shortest time. But is enforcement used to sabotage your network completely blocked? You can find it by verifying the IDS log, then you can put the computer offline. There is no information in the log file to reveal anything more. What can you do?

**The first step in many steps**

The first step in encountering an attack is to intercept it, then clean up all the compromised machines, then determine which vulnerabilities have been exploited. Is it zero-day, or is it simply because you are lax in using patches on a PC. If it is true that you have not fully updated the updates and patches, rebuild the computer and apply it fully. If in other cases, you should block the copying of the vulnerability and see if it is a source code or recompiled. I have heard many people say "that is almost impossible". The same is true, but you can find a flaw with some kind of creative search. There are now many compact mailware search methods available. We will learn about them in the limited content of this series. It was created and uploaded by the highly intelligent HDM tool of Metasploit.

With the information provided in your hand, now is the time to download and find out what the actual malware program is. Of course, "to enter the tiger" is impossible without certain dangers. But as our family members have said, 'If we enter tiger cave, we can catch tiger', if we do not understand "rival", how can we prevent and protect our network effectively. You should work within VMware image limits or use a dedicated computer separately from your network. So there is no need to fear or worry that I can destroy my own network when installing malware.

**Use some malware**

Pay attention to the security warnings given above. You can then download and use some of the malware samples available on some websites such as FrSirt (which can now be greatly restricted) or Securiteam. Depending on the skill level you should choose a moderate malware. You may not know how to compile the source code into a PE implementation. There are some moderately advanced instructions for you.

This is the first contextual information about reverse engineering. This is because there are several important reasons: reverse engineering is not an easy subject to grasp; Readers have many different skill levels. To best suit, before really embarking on reverse engineering, you should equip yourself with the most basic knowledge and skills such as reading the code, compiling the source code, .

**Download malware**

To implement reverse engineering, you need the following skills at different levels:

**1.** First and foremost is programming skills, or at least read the source code. This becomes extremely important when you use a disassembler language like Ollydbg or IDA Pro. In this article we will use those languages ??as an example. It is very valuable and quite practical.

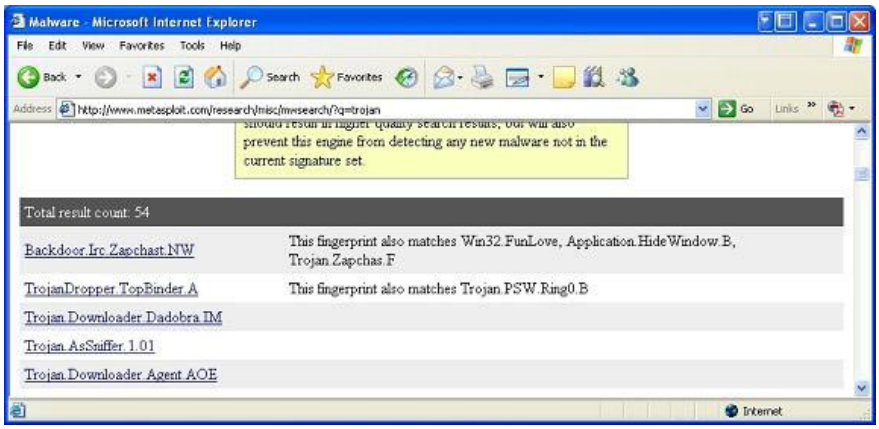
**2.** Understand the methodology, ie all theories on how and principles of reverse engineering. It includes both static and dynamic parts.

**3.** Know which tools to use in each dynamic, static part.

The above three steps may sound daunting, but in fact, you just need to gather enough information, appropriate testing tools and computers, read and try a little, everything becomes easy and clear. . The most important skill is knowledge of programming. You don't need to be an enterprise-level developer to understand and practice Reverse Engineering. You don't even need to be a programmer, simply reading the source code with some programming functions is already able to perform the simplest steps.

Finally download a sample malware and practice. You can find malware on the Metasploit website as mentioned above. But again, the computer security principles must be followed. When you click on the link, you will see the screen image as below:


This is the home page, type malware into the search box and press enter. A series of sample mailware is available for download.



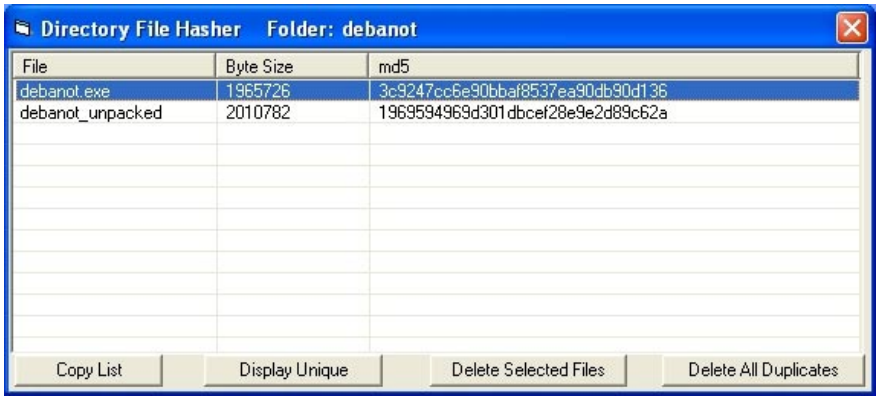

Using the mouse or the scroll key up and down, select the malware you want to use for testing. But remember that you have to make sure you're testing malware in a secure environment: don't do this on a working computer or contain important data.

**What is next?**

Now you have the sample malware downloaded safely on a VMware image or a standalone computer. We will begin to review it. Before you start, you should prepare yourself carefully for organized ways of working with appropriate steps. You may encounter many identical malware pieces. You will have to show the difference between them. In addition to hash table conflicts, you can use MD5 hash. Malware often has many different

variants. Pointing out the differences between them is not easy if your reverse engineer is not very good. Therefore, using MD5 hash is a very useful solution for you.

You can download some utilities that perform the above functions in Windows such as MAP or Malcode Analyst Pack. These utilities were developed from iDefense. The program is very compact but does a lot of work for you. It has the ability to run MD5 checksum procedures to check files and folders, placed in MSI packages. The installation part is quite normal, nothing special. If you right-click on the file or folder under test, more options will appear. 'Hash Files' (ie file hashing algorithm) is one of them. Simply select an option and let the program do its job. See the illustration below for a sample of the output file.




You will see that the content of the 'debanot' folder has an MD5 hash with a value very similar to the value shown. In addition to some other important information like file name, size in bytes, you can rely on MD5 hash running at some part of the malware to analyze, find out the difference between them. You should also consider MAP more carefully. It has many components that help us analyze malware very well. It is also the purpose of writing the program.

**Ready?**

Now that you have the malware in hand, use MD5 hash, and proceed to actually crack its crack. You will need an editor like Heaventools. There are many free editors, but specifically here we will make an example with a commercial version.

The Malware you download may be different from malware for example. Does it use the Trojan keyword in Metasploit's search engine with a specific icon? Can the icon of winzip or winrar be used often, or is the icon of executing Microsoft Windows aka aka PE format?

As mentioned above, there are many steps taken when analyzing malware. Do not always believe in what you see. Everything in the world of malware is not always the same as what they represent outside. Because their main purpose is to deceive users. Learning about reverse engineering, your security knowledge has been greatly improved. Part one please pause here. We will continue to meet again in part two with some other interesting jobs.

**Malware counterpart design (part 2)**

tips and guides. Thank you for reading and for following us regularly.