Binder and Malware (Part 1)

The malware issue is not new and we cannot chase them away immediately. In fact, we have spent a lot of money dealing with criminals using Trojans, viruses and bots. Not just users

Don Parker

The malware issue is not new and we cannot chase them away immediately. In fact, we have spent a lot of money dealing with criminals using Trojans, viruses and bots. Not only ordinary users are attacked by malware but users in companies are also their target of attack. That is the purpose for us to introduce this series. Having an antivirus program running on a user's computer is a great thing, just as there is a content checking program running on your Exchange server. The best way to prevent these attacks is to guide the user. Because there are always many types of malware that can overcome your preventive measures, they can be a new trojan or a new client vulnerability in the web browser. By providing users with knowledge about the problem, they will be able to mitigate the threat of malware in the corporate network environment.

This article will support system administrators (sys admin) who work in corporate networks. The number of programs used on the network, anti-virus software or systems to prevent Intrusion Prevention Systems (IPS) will not be the main problem in this series, but the main purpose is to provide a method This method can help you protect your network, we focus on the weakest links and users. That does not mean only for sellers, accountants or office workers. We offer all the different skills and in this case it is an understanding of computer security. It is a knowledge of security in many different forms and can allow users in the corporate network to perform their work in a safe and positive way.

What needs to be done now is to show users how malware gets into mainstream programs. To do this we will use a number of different tools, both orthodox and unorthodox. The script will use a binder program called YAB, a trojan called Optix Pro, and a game called Pong.exe. With these three individual programs, we will build a disguised trojan as a game called Pong.exe. We will take a step-by-step approach to look at how this malware is at the byte level to recognize them. By watching malware in Hex format can show us a lot of benefits about what's inside.

Begin

Please note that we do not provide links to the malware binder named YAB, or trojan Optix Pro. However, you only need to spend a little time or perform a search by Google all the related programs above. Now start!

First we configure Optix Pro trojan. You can assume that this is a trojan written earlier. If you want to read more about it, you can refer here. We will not stop on the detailed configuration of the trojan but only do some things necessary for the given purpose. You can look at the picture below on what the Optix Pro folder looks like when you download and extract them.

Figure 1

Double-click the ' *Builder* ' icon to call the server so we can make some simple configuration changes. You should observe Figure 2 below.

Figure 2

In this image, we will click 'Main Settings'. Only change what we do with the trojan server here because we don't take a lot of time and show our users thoroughly about the dangers of malware. You can use the default port TCP 3410 if you like or change it to another option. The default language setting for Optix Pro is English. If you want to make other changes to the trojan server, this is the time to do so. If you click on the ' *Build / Create Server* '

icon in the upper left corner of the trojan GUI, it will prompt you for the name as shown in Figure 3 below.

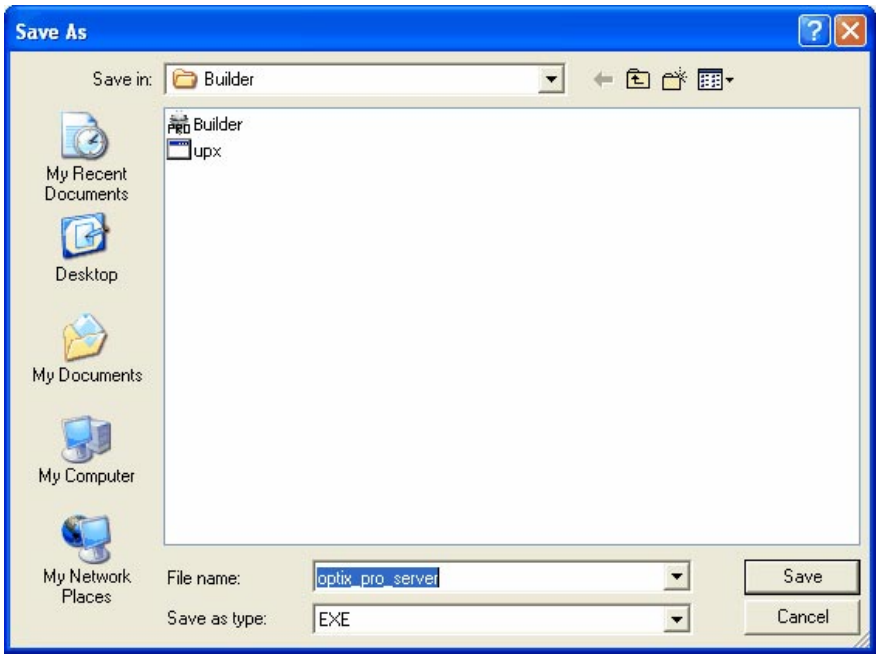


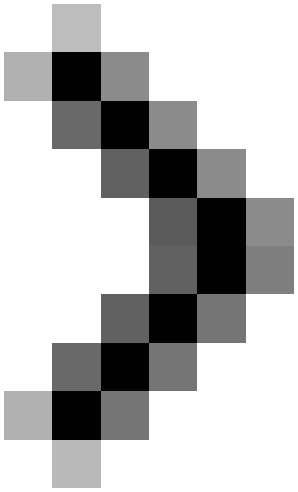
Figure 3

Choose any name you like and the path to save it. You can also save it in the Optix folder to simplify and put everything in one place. When you're done naming it, you'll see a message like the one below.

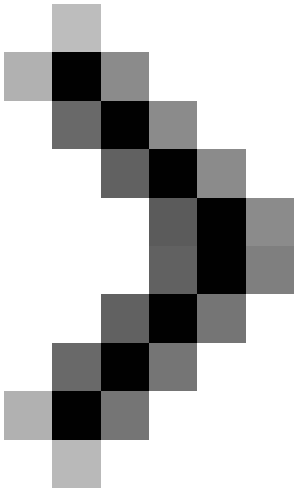
Figure 4

Here you can proceed to build the server or you can choose to compress it via the UPX program. What they will do is compress the trojan server to get a smaller size. This is also often done with large programs or files that can make someone suspicious, especially if they have some knowledge of computer security. They will realize that a certain program or file will not be as large as it was announced. What needs to be done is to have a server to compress with UPX. Let's look at the UPX compressed trojan server later in this article. Once you've done the settings, just press' *OK all done!* .

In Part 2 of this series, we will continue to look at the malware binder called YAB and an official game program Pong.exe. That will be the last two components to 'cook' to know the 'taste' of malware. In fact, this series not only applies to users in corporate networks but also for us. You can't say that you know everything even as a security expert. We must really say that we didn't know exactly how someone built such a malware until we decided to publish an article to learn about them. Hopefully, with the things you encounter in this situation, I will help you have more knowledge in practice. Only way to do something is to really understand the problem.



Binder and Malware (Part 2)



Binder and Malware (Part 3)

You finished reading the article "**Binder and Malware (Part 1)**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.