

# Forum:[Hack Forums](#)

Thread: [Binders and Malware - How malware are binded with legit files](#)

--([S7N])-- - March 25, 2010, 9:31 pm

## Binders and Malware

How malware authors bind the malware to legitimate files

Hi,

I was searching over at WindowSecurity, where I came across this great article that explains how malware authors bind the malware to legitimate files and how malware binders work.

Although this may seem like basic information to some, I suggest reading it.[Part 1](#)

[Part 2](#)

[Part 3](#)

## Introduction

The problem of malware is neither a new one, nor is it one that is going to go away any time soon. There is far, far too much money involved for the criminals who use Trojans, viruses, and bot armies to simply give up using them. It is not only home users who are targeted with these malware attacks, but it is also the corporate end-user. That brings us to the point of this article series. It is only through education that this problem can be eradicated. Having an anti-virus program running on a user's computer is great, just as it is to have a content checking program run on your Exchange server. Your best line of defense is an educated user. There will always be a new breed of malware that is able to slip past your defenses, be it a new trojan, or a new client side exploit in a web browser. By virtue of making your users aware of the problem you will have gone a long way towards mitigating the threat of malware in your corporate network environment.

This article is aimed squarely at the system administrator (sys admin) who works in any corporate network setting. The number of programs you have running on your network, be they anti-virus or Intrusion Prevention Systems (IPS) won't factor in for this article series. We will take the approach that, to help secure our networks, we need to address the weakest link; the end-user. That is not meant as an insult to the salesman, accountant, or office staff. We all have differing skillsets, and in our case it is computer security savvy. It is through our knowledge of computer security, in its many forms, that will enable us to help the corporate network users do their work in as secure a fashion as possible.

What we shall now go about doing is to show our end-users just how malware gets grafted onto a legitimate looking program. Only by recreating exactly how this is done will our goal of educating them to the online threats aimed at them be realized. To do this we will be using a variety of tools, both legitimate, and illegitimate. For our scenario I shall use the binder program called YAB, the trojan called Optix Pro, and the game called Pong.exe. With these three programs alone, we will construct a trojan disguised as a game called Pong.exe. We shall go one step further in that we will also look at this malware at the byte level to recognize what it looks like. By viewing malware in a hex editor we are able to see certain indicators which tell us that something is amiss in a specific

executable program. Viewing malware in a hex editor also has the added benefit of allowing you to see inside of it in a safe fashion, as you are not actually executing the program, but rather only looking at its contents.

Rest of the guide in the link provided above.

Thanks,  
S7N

**Paradoxum** - March 25, 2010, 10:54 pm

People will learn binding with this. ?

--([S7N])-- - March 25, 2010, 10:59 pm

(Mar 25, 2010 10:54 PM)Paradoxum Wrote: [\[CITE\]](#) People will learn binding with this. ?  
Lol, then move this to the Beginner Forums? Lol.

**Paradoxum** - March 25, 2010, 11:33 pm

Nah, it will serve two purposes. It is mainly White Hat, after all.

--([S7N])-- - March 25, 2010, 11:53 pm

(Mar 25, 2010 11:33 PM)Paradoxum Wrote: [\[CITE\]](#) Nah, it will serve two purposes. It is mainly White Hat, after all.  
Yeah. ?

**shaddy@123** - March 25, 2010, 11:55 pm

It was made for White hat reasons, but it's right, they may learn how to bind too instead.