pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialis
Article by Piotr Bania
All rights reserved
pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialised.info pb.specialis

Notes of **Protty** **(v.01a)**

The Shellcode Execution Prevention Library

By Piotr Bania <bania.piotr@gmail.com>
http://pb.specialised.info

I. Introduction and description of the mechanism

Protty is a ring 3 library developed to protect against shellcode execution on Windows NT based systems. The full description of the mechanism was published within the Phrack magazine volume #63, available here: http://www.phrack.org/phrack/63/p63-0x0f_NT_Shellcode_Prevention_Demystified.txt (sources of the initial release are also available) . Currently Protty stops most known Windows shellcodes. Moreover it can block some types of viruses which use similiar methods as shellcodes do.

II. Current features

Main Protty v.01a (test phase) features are:

- Process Environment Block protection (currently 2 modules protection used)
- Structured Exception Handling protection
- Import section killing (currently main application only)
- Export section protection (currently 2 modules protection used)
- RtlEnterCrticialSection protecting (currently disabled)

III. What you should know (what Protty will not protect you from)

Of course using Protty (like almost every mechanism) don't give you 100% guarantee that your computer will be unexploitable – you should remember this fact.

Currently Protty will not protect you from:

- windows syscall shellcodes (for example the one I have developed for SecurityFocus article, available here: http://www.securityfocus.com/infocus/1844)
- hardcoded libraries addresses (go and do some imagebase randomizations)
- using unprotected modules for gaining informations (upcoming release should protect all running modules)

Problems:

There are libraries which may not use the standard way of “dll loading” etc. etc. that may cause problems with Protty usage, since it tries to blocks such types of hacks. Generally it should be a stable release at least it was here on my Microsoft XP SP1.

The code is published under Piotr Bania license called “If you don’t like it, don’t use it”.

IV. Configuration

Open and edit “C:\Protty\config.dat” file, and add modules which you want to protect (like shown in the “config.dat” file).

Logs are stored in “protty-log.txt” file stored in the same dir.

V. Sponsors and support

If you want to sponsor or support Protty library with your own ideas. don’t hesitate to contact me, you can do this by using this email: bania.piotr@gmail.com.