

Forum:[Hack Forums](#)

Thread: [µProtect - Kernel injection \[Ring0 Rootkit\]](#)

Novelty - February 20, 2012, 8:08 am

Hey all, I'm working on secret project calld µProtect.

It injects into the kernel and do a man-in-the-middle attack of the PC.

This is really dangerous though so i just wanted to hear your guys suggestions and like what price you would pay for it

van1lle - February 20, 2012, 8:09 am

Seems like your project is not that secret.

What does it do exactly?

Novelty - February 20, 2012, 8:14 am

It binds your program or virus to itself and run in kernel-mode, ring0, infects drivers, so forth, basically this is what is used to create huge botnets.

i don't knwo if its allwoed to be sold here though since its blackhat, and people can use it with a spreader that spreads ring0 as well, GG internet

deadaccount01 - February 20, 2012, 8:18 am

One of these things infected my old laptop, thing is god damn deadly. I hate russians. Its pretty much impossible to remove it without wiping the drive.

+Xenon - February 20, 2012, 8:20 am

Based on your thread and your most recent reply, I would venture to say you haven't the slightest clue what you are doing. First of all, "huge botnets" are a 2 part deal: the bot and the owner. You can't rely 100% on your bot doing all the work for you, you have to put in a little effort too. Also, I am definitely not a bot coder (in any language really), but as far as I know, all these features have shown up in nearly every worthwhile bot on HF...

van1lle - February 20, 2012, 8:28 am

(Feb 20, 2012 09:14 AM)Novelty Wrote: [\[CITE\]](#) It binds your program or virus to itself and run in kernel-mode, ring0, infects drivers, so forth, basically this is what is used to create huge botnets.

How would you run your virus in ring0, since are only able to use the native api? And who creates a bot using only the native api? :3

(Feb 20, 2012 09:18 AM)Query Wrote: [\[CITE\]](#) One of these things infected my old laptop, thing is god damn deadly. I hate russians. Its pretty much impossible to remove it without wiping the drive.

Why don't you boot a linux live cd/usb and remove dat shit?

Novelty - February 20, 2012, 8:33 am

@van1lle it basically runs in ring0 mode.

Nothing else to it!

FuckYouAllCuntz - February 20, 2012, 8:43 am

> "It injects into the Kernel and does a man in the middle attack"..

Seriously gtfo now. Where does a MITM attack come into this process? Do you even know what an MITM attack is?

Pineapple - February 20, 2012, 8:55 am

No way do you even have any chance of coding Ring0 rootkit or even close. You'll need 0day exploits for it, and any REAL hardcore rootkits like that aren't going to be sold on HF, and will also cost thousands.

Just give up. ???

Skep - February 20, 2012, 12:15 pm

There's already public Ring0 Rootkits that allow kernel hooking.

eXero - February 20, 2012, 12:18 pm

I guess it's not a secret anymore. But honestly I have never heard of this, anyone care to link me to the wikipedia link about it?

Skep - February 20, 2012, 12:29 pm

<http://en.wikipedia.org/wiki/Rootkit>

Spoiler ([Click to View](#))

Code // Example of a little rootkit

// from opensc.ws

```
#include <windows.h>
```

```
#include <iostream>
```

```
// DECLARACIONES:
```

```
BYTE *BufferFF; // Buffer to use original FindFirstFileW
```

```
BYTE *BufferFN; // Buffer to use original FindNextFileW
```

```
char Prefijo[] = "miniRoot_"; // prefix for hide files
```

```
// FUNCIONES:
```

```
void Hookear(); // FunciÃ³n que hookearÃ¡ el api
```

```
// FunciÃ³n que serÃ¡ llamada en vez de FindFirstFileW
```

```
HANDLE __stdcall miFindFirstFileW(LPCTSTR lpFileName, LPWIN32_FIND_DATAW  
lpFindFileData);
```

```
// Puntero a funciÃ³n con el cual llamaremos al api FindFirstFileW original
```

```
HANDLE (__stdcall *pBuffFF) (LPCTSTR lpFileName, LPWIN32_FIND_DATAW lpFindFileData);
```

```
// FunciÃ³n que serÃ¡ llamada en vez de FindNextFileW
```

```
HANDLE __stdcall miFindNextFileW(HANDLE hFindFile, LPWIN32_FIND_DATAW  
lpFindFileData);
```

```
// Puntero a funciÃ³n con el cual llamaremos al api FindNextFileW original
```

```
HANDLE (__stdcall *pBuffFN) (HANDLE hFindFile, LPWIN32_FIND_DATAW lpFindFileData);
```

```
// FUNCIÓN MAIN
```

```
bool WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
```

```
{  
    // Si cargan la DLL hookeamos  
    if (fdwReason == DLL_PROCESS_ATTACH)  
    {  
        MessageBox (0, "CARGADA!!", "", 0);  
        Hookear();  
    }  
}
```

B00b5_ - February 20, 2012, 1:48 pm

everyone on hf is fucking stupid

the op has no idea what's he's talking about. a man in the middle attack is across a fucking network, not intercepting api calls from the fucking kernel.