

Forum:[Hack Forums](#)

Thread: [SMB WORM SOURCE CODE \[CODED BY ME\] \[CUSTOM PSEXEC\]](#)

Freak OG - August 11, 2020, 3:50 am

Just one of the many features in DarkIRC botnet which u can buy [HERE](#), the full version of this botnet includes 2 other self replication mechanisms, (RDP and MSSQL)

The main way this is done, is by creating a service on the remote machine, using winapi calls to wininet.dll. wininet.dll is a fucking hacking machine and is capable of pwning everything ? with the right credentials that is.

Using OpenSCManagerA and using the handle u get with correct credentials u can successfully run CreateServiceA to run a command as a windows service (NT AUTHORITY/SYSTEM) on your target machine. ??

without further ado, I give you, "SMB Retard".

Includes my custom password list for servers, 226 usernames, 1600+ passwords.

Enjoy! Dont go to crazy, cause i might have to botkill u fuckers for using my passlist ???

MavenGradle - August 11, 2020, 4:01 am

Code try {

```
...
}
catch() {
// nothing here
}
finally {
// nothing here
}
```

Absolutely no error handling. Empty code blocks, catching them all like the pokémon you think they are instead of the ones that are relevant to your use case and doing something useful with those exceptions.

Code while (true)

Extremely bad practice. Your application is now forced to be SIGKIL'd in order to quit and cannot gracefully quit. You have no idea how network scanning really works or how to even present the results of a network scan, at all. What happens if i don't have an internal network set up in IPv4? What if all my devices are IPv6 only hosts? Right, you're completely skipping that part.

Code if (count > bruteSubThreads)

```
{
    for (int i = 0; i < bruteSubThreads; i++)
    {
        threads[i].Join();
    }
}
```

```
count = 0;
GC.Collect();
```

```
}
```

Let's block threads and while we're at it, let's add another bad practice of calling the garbage collector manually. Not only are you reducing the performance of your application significantly, you are completely missing the fundamentals of the concept behind garbage collection and task parallelism:

<https://docs.microsoft.com/en-us/dotnet/standard/garbage-collection/fundamentals>

<https://docs.microsoft.com/en-us/dotnet/standard/parallel-programming/task-parallel-library-tpl?redirectedfrom=MSDN>

GC.Collect(), nice joke though. Thanks for the laughs, perhaps you're doing this because you're not properly disposing of your connected Socket instances ??

```
Code public static void SMBHaxx
```

How is this a proper method name? In addition, why is this static, or public for that matter? Are you missing the concepts of Object Oriented Programming and access modifiers?

```
Code public static void TestPW(string ip, string user, string passwd)
```

```
{
    ip = "\\" + ip;
```

```
....
}
```

Since this is a public method with an awful name that doesn't follow any convention, what if the IP is not an IP address or network location at all? What if it already contains 20 backslashes and what if.. So many what if's that you're not validating or handling properly. Bad practice all around.

In the TestPW method, at the very end, you have this:

```
Code if (serviceHandle.Invalid)
```

```
{
    return;
}
```

What, exactly, is the point of this useless code? It would have returned either way, even without the if statement, so what are you doing here, exactly? Useless code.

And there's lots of code duplication in your file.

Need I say more. Would not pay \$75 for this, at all. Would not pay a single thing. Nice way to advertise your broken software though.

```
Code public static int bruteSubThreads = 64;
```

You think 64 threads on a 2/4 core CPU will make it go any faster? Ever heard of TPL?

<https://docs.microsoft.com/en-us/dotnet/standard/parallel-programming/task-parallel-library-tpl?redirectedfrom=MSDN>

Freak_OG - August 11, 2020, 4:10 am

(Aug 11, 2020 04:01 AM)MavenGradle Wrote: [\[CITE\]](#) Code [code]

```
public static int bruteSubThreads = 64;
```

You think 64 threads in a 2/4 core CPU will make it go any faster? Ever heard of TPL?

<https://docs.microsoft.com/en-us/dotnet/standard/parallel-programming/task-parallel-library-tpl?redirectedfrom=MSDN>

[ctedfrom=MSDN](#)

the actual function of TestPW only takes about 1 second to complete, and the multithreading is very stable.

Some of the code for mimikatz I had to remove (obviously cause I cant just give it out) which is why some of the code looks like it has nothing in it, nice try to roast my code tho.

(Aug 11, 2020 04:01 AM)MavenGradle Wrote: [\[CITE\]](#) [code]

Need I say more. Would not pay \$75 for this, at all. Would not pay a single thing. Nice way to advertise your broken software though.

Also, this is kind of stupid, bro, the code I am selling has RDP and MSSQL self rep in it too, which is worth 1-4k lmao 75\$ may as well be free

Also the mimikatz code dumps lsass.exe credentials and replays through internal network.

Say u infect 1 pc in a office, administrator access. in network with 50+ pcs, using domain logon, u can infect the entire internal network XD

MavenGradle - August 11, 2020, 4:13 am

(Aug 11, 2020 04:10 AM)Freak_OG Wrote: [\[CITE\]](#) the actual function of TestPW only takes about 1 second to complete, and the multithreading is very stable.

Some of the code for mimikatz I had to remove (obviously cause I cant just give it out) which is why some of the code looks like it has nothing in it, nice try to roast my code tho.

Bad try at justifying broken logic. This is an advertisement, plain and simple, for software which by the looks of it, would be worth less than cat shit. In fact, cat shit is worth more because sometimes people make coffee out of it.

Freak_OG - August 11, 2020, 4:15 am

(Aug 11, 2020 04:13 AM)MavenGradle Wrote: [\[CITE\]](#) Bad try at justifying broken logic. This is an advertisement, plain and simple, for software which by the looks of it, would be worth less than cat shit. In fact, cat shit is worth more because sometimes people make coffee out of it.

bruh lets see your fucking worm code and lets compare XD I bet mine is still better than urs....

MavenGradle - August 11, 2020, 4:18 am

(Aug 11, 2020 04:15 AM)Freak_OG Wrote: [\[CITE\]](#) bruh lets see your fugging worm code and lets compare XD I bet mine is still better than urs....

I've seen beginners write cleaner, less error prone and functionally sound code. I don't code worms, because I have better things to do. In addition, I don't have anything to prove to you at all. I'm just here in the hopes that people do not settle for garbage code.

Freak_OG - August 11, 2020, 4:20 am

(Aug 11, 2020 04:18 AM)MavenGradle Wrote: [\[CITE\]](#) I've seen beginners write cleaner, lesserror prone and functionally sound code. I don't code worms, because I have better things to do. In addition, I don't have anything to prove to you at all. I'm just here in the hopes that people do not settle for garbage code.

Explain to me whats garbage in it? This is probably the first proper SMB worm library coded in C# that has been publicized that actually works. The least you could do is say thank you and not be a dick about it man.

Atleast give productive criticism.

MavenGradle - August 11, 2020, 4:58 am

(Aug 11, 2020 04:20 AM)Freak_OG Wrote: [\[CITE\]](#) Explain to me whats garbage in it? This is probably the first proper SMB worm library coded in C# that has been publicized that actually works. The least you could do is say thank you and not be a dick about it man.

Atleast give productive criticism.

You call this proper? You haven't got the slightest clue what the word proper means or entitles in the world of programming. Why should I thank you for this? I'd print this code out and use it as toilet paper or to have a good laugh in the morning when I wake up. I guess that does deserve a thank you.

Anyway, the post above has been modified to explicitly tell you what's wrong with it because apparently for a \$75 "proper" program, you haven't got a clue in regards to what's wrong with it. We're a bit full of ourselves, aren't we.

You're not even posting a fraction of your code base so really, if this is just the start, how in the seven seas will the rest be any better? This is the part you're obviously the most proud of, even though you're posting it half complete and fully non-functional.

Freak_OG - August 11, 2020, 5:04 am

(Aug 11, 2020 04:58 AM)MavenGradle Wrote: [\[CITE\]](#) This is the part you're obviously the most proud of, even though you're posting it half complete and fully non-functional.

It's actually the part I'm least proud of, the rdp selfrep is my favourite. I decided to share this with the community, so people could have a little bit of fun with it, was hoping people would like it..... Alot of people want this kind of code, and usually willing to pay for it, releasing this code for free only does everyone a favour.

The code is functional, it does work. Its not pseudocode lol.

EDIT: if this is some kind of ruse to get me to post my rdp selfrep code im not doing it XD

Also, why you gotta hate on everyones code so much, I see you do it on everyones threads, and yet u never post your own code why is that. is it too perfect to post?

gigajew - August 11, 2020, 4:37 pm

You can take my Steam Chat Spreader code from github and put in your app too if you want to, I don't care. It's not licensed. I would combine it with a idle detector though to make sure nobodys watching the screen type by itself. <https://github.com/gigajew/Steam-Spreader>

Suspect. - August 15, 2020, 1:07 pm

(Aug 11, 2020 05:04 AM)Freak_OG Wrote: [\[CITE\]](#) It's actually the part I'm least proud of, the rdp selfrep is my favourite. I decided to share this with the community, so people could have a little bit of fun with it, was hoping people would like it..... Alot of people want this kind of code, and usually willing to pay for it, releasing this code for free only does everyone a favour.

The code is functional, it does work. Its not pseudocode lol.

EDIT: if this is some kind of ruse to get me to post my rdp selfrep code im not doing it XD

Also, why you gotta hate on everyones code so much, I see you do it on everyones threads, and yet u never post your own code why is that. is it too perfect to post?

He is correct about the Exception handling for one, an Empty catch is completely useless apart from just ignoring potential exceptions so your program doesn't close.

Rather Handle the exceptions correctly than just ignoring them, there is plenty of opensource Loggers around for you to log your exception and its details and whether or not its expected. Perhaps Maven is a harsh critic although I don't feel he is incorrect.

Pawnhub - August 16, 2020, 12:57 am

One of the first times I ever seen Maven go full on sicko mode.

I'm subbing this thread, lmao.

Accord - August 16, 2020, 11:49 pm

(Aug 11, 2020 04:15 AM)Freak_OG Wrote: [\[CITE\]](#) bruh lets see your fugging worm code and lets compare XD I bet mine is still better than urs....

Accept that your code needs improvement, has flaws, and has wrong approach. thats how you improve. you keep arguing with fallacy, you dont even refute all those pointed errors

Freak_OG - August 17, 2020, 12:00 am

(Aug 16, 2020 11:49 PM)Accord Wrote: [\[CITE\]](#) Accept that your code needs improvement, has flaws, and has wrong approach. thats how you improve. you keep arguing with fallacy, you dont even refute all those pointed errors

None of them are errors really, just bad coding practices that have no real effect to the program at all, what hes saying is really pointless

Suspect. - August 17, 2020, 6:02 am

(Aug 17, 2020 12:00 AM)Freak_OG Wrote: [\[CITE\]](#) None of them are errors really, just bad coding practices that have no real effect to the program at all, what hes saying is really pointless

Handling Exceptions is not pointless at all, It's likely the most important part of programming. What are you going to do if infuture you encounter issues? How are you going to determine what the issue is? Are you going to remove the Empty try catch(s) then debug? whats the point in that when you can just handle the exceptions and log them to a file.

MavenGradle - August 17, 2020, 7:28 am

(Aug 16, 2020 12:57 AM)UnknownPawn Wrote: [\[CITE\]](#) One of the first times I ever seen Maven go full on sicko mode.

I'm subbing this thread, lmao.

Would you like to know why? The man sells \$75 malware ([which he claims is worth \\$75k by the way](#)), posts snippets of his code here which are incomplete and absolutely pointless, filled with several design flaws and he responds like this:

(Aug 17, 2020 12:00 AM)Freak_OG Wrote: [\[CITE\]](#) None of them are errors really, just bad coding practices that have no real effect to the program at all, what hes saying is really pointless

As a general rule, I try not to review malware code because it's mostly stolen from somewhere or someone else and no one will benefit from malware code reviews anyway (because it's malware and won't do society any good). But I like making exceptions for the tools people claim are worth \$75k (while in reality it's closer to \$0.99).

What you fail to understand is that you are offering a service here, and you're advertising it in this section. You should have expected this to happen. Your code is not up to par. Period. The fact that you cannot understand why or even attempt to fix it is all the more reason not to purchase your software but I guess bad advertisements are advertisements all the same?

You haven't even disposed of your connected sockets properly, you have zero input validation, an infinite loop and no error handling and you are essentially slowing your application down as has been pointed out in previous replies. If you cannot see that, well then we have nothing more to discuss.