

Forum:[Hack Forums](#)

Thread: [Crypter with Hidden Startup and Hidden Process features?!](#)

aerohacker - November 22, 2024, 12:01 pm

Which Crypter here has both features?! The most has Hidden Startup but not Hidden Process, I need both features to make the server invisible from Windows and thirdy-party tools.

DramaKing - November 22, 2024, 1:24 pm

(Nov 22, 2024 01:01 PM)aerohacker Wrote: [\[CITE\]](#) Which Crypter here has both features?! The most has Hidden Startup but not Hidden Process, I need both features to make the server invisible from Windows and thirdy-party tools.

I have no ide what Hidden Startup is, but process hiding requires a ring 3 kernel rootkit. You will need privilege escalation for this.

aerohacker - November 22, 2024, 7:00 pm

(Nov 22, 2024 02:24 PM)DramaKing Wrote: [\[CITE\]](#) I have no ide what Hidden Startup is, but process hiding requires a ring 3 kernel rootkit. You will need privilege escalation for this.

Hidden Startup will run the server invisible from startup options in msconfig and task manager.

DramaKing - November 22, 2024, 7:46 pm

(Nov 22, 2024 08:00 PM)aerohacker Wrote: [\[CITE\]](#) Hidden Startup will run the server invisible from startup options in msconfig and task manager.

And hidden from the Startup menu? It's probably using a Run registry key, not startup.

aerohacker - November 22, 2024, 7:56 pm

(Nov 22, 2024 08:46 PM)DramaKing Wrote: [\[CITE\]](#) And hidden from the Startup menu? It's probably using a Run registry key, not startup.

Or Task Scheduler.

(Nov 22, 2024 08:46 PM)DramaKing Wrote: [\[CITE\]](#) And hidden from the Startup menu? It's probably using a Run registry key, not startup.

I can add the server to task scheduler manually or make this automatically, using a Crypter with Hidden Startup feature to hide the server from startup folder, msconfig and task manager options.

And to hide the process, which Ring3 or Ring0 Rootkit do you recoomend?!

I know the in Github has a lot of cool projects, but I want something compiled, run the Rootkit and hide the process from task manager or another process managers tools.

The r77 Rootkit works like that, but after install it and rename the server using the prefix \$77 it's hide all related with the server (Which is very cool, it's my intention), but after that the server don't run too.

DramaKing - November 23, 2024, 4:03 am

(Nov 22, 2024 08:56 PM)aerohacker Wrote: [\[CITE\]](#) Or Task Scheduler.

I can add the server to task scheduler manually or make this automatically, using a Crypter with Hidden Startup feature to hide the server from startup folder, msconfig and task manager options.

And to hide the process, which Ring3 or Ring0 Rootkit do you recoomend?!

I know the in Github has a lot of cool projects, but I want something compiled, run the Rootkit and hide the process from task manager or another process managers tools.

The \$77Rootkit works like that, but after install it and rename the server using the prefix \$77 it's hide all related with the server (Which is very cool, it's my intention), but after that the server don't run too.

You mean r77 rootkit. It's a common Ring 3 rootkit. Ring 0 rootkits have been practically unheard of since at least Windows Vista. Drivers need to be signed by EV certificates to run in kernel mode. These certificates can be revoked at any time by Microsoft.

<https://www.bleepingcomputer.com/news/security/new-windows-driver-signature-bypass-allows-kernel-rootkit-installs/>

aerohacker - November 23, 2024, 1:25 pm

(Nov 23, 2024 05:03 AM)DramaKing Wrote: [\[CITE\]](#) You mean r77 rootkit. It's a common Ring 3 rootkit. Ring 0 rootkits have been practically unheard of since at least Windows Vista. Drivers need to be signed by EV certificates to run in kernel mode. These certificates can be revoked at any time by Microsoft.

<https://www.bleepingcomputer.com/news/security/new-windows-driver-signature-bypass-allows-kernel-rootkit-installs/>

Yeah, the r77 rootkit is what I found, compiled with the injector and etc, simple and works well, but the "problem" is, after install the r77 rootkit and rename the server using to \$77server (example), everything related with the file disappear (Which is the function of the rootkit, but the same don't run too just be invisible).

There's a way to use r77 rootkit buy only to hide the process server?!

(Nov 23, 2024 12:16 PM)m0hx Wrote: [\[CITE\]](#) If I remember hidden process was possible in windows 7 and below. Not sure if there's any now :/ mayb private ones but I haven't seen any recently.

It's possible to hide process in new Windows versions too.

DramaKing - November 23, 2024, 3:45 pm

(Nov 23, 2024 02:25 PM)aerohacker Wrote: [\[CITE\]](#) Yeah, the r77 rootkit is what I found, compiled with the injector and etc, simple and works well, but the "problem" is, after install the r77 rootkit and rename the server using to \$77server (example), everything related with the file disappear (Which is the function of the rootkit, but the same don't run too just be invisible).

There's a way to use r77 rootkit buy only to hide the process server?!

It's possible to hide process in new Windows versions too.

Aren't you trying to hide the client? Why hide the C2 server?

Open a GitHub issue. I don't know the code to be able to answer.

aerohacker - November 23, 2024, 5:13 pm

(Nov 23, 2024 04:45 PM)DramaKing Wrote: [\[CITE\]](#) Aren't you trying to hide the client? Why hide the C2 server?

Open a GitHub issue. I don't know the code to be able to answer.

Not the RAT client, but I want to hide the RAT server process.

Example:

I use a lot of RATs both: Native and .NET, and after install the server on Windows, I like to do the server as hidden possible from user and even computer tech, so I always make:

- Hidden Installation - Install the server on Roaming/AppData and use attrib +h +s
- Hidden Startup - Install the server on Task Scheduler and make invisible from Startup Folder and Startup tab/programs on MSConfig and Task Manager
- Hidden Process - Hide the process server from Task Manager, Process Explorer, Process Hacker

Using r77 Rootkit the program hide everything what is very cool, but for some reason the server does becomes functional after being invisible, so that a way to use r77 rootkit but only for hide the process and not then server itself or another compiled Rootkit to do that?!

Or a free or paid Crypiter with custom install, hidden startup and hidden process features to make all this things automatically?!

DramaKing - November 23, 2024, 7:14 pm

(Nov 23, 2024 06:13 PM)aerohacker Wrote: [\[CITE\]](#) Not the RAT client, but I want to hide the RAT server process.

Example:

I use a lot of RATs both: Native and .NET, and after install the server on Windows, I like to do the server as hidden possible from user and even computer tech, so I always make:

- Hidden Installation - Install the server on Roaming/AppData and use attrib +h +s
- Hidden Startup - Install the server on Task Scheduler and make invisible from Startup Folder and Startup tab/programs on MSConfig and Task Manager
- Hidden Process - Hide the process server from Task Manager, Process Explorer, Process Hacker

Using r77 Rootkit the program hide everything what is very cool, but for some reason the server does becomes functional after being invisible, so that a way to use r77 rootkit but only for hide the process and not then server itself or another compiled Rootkit to do that?!

Or a free or paid Crypiter with custom install, hidden startup and hidden process features to make all this things automatically?!

Install the server on the victim PC? I'm too confused at this point, except to suggest a fileless crypter, nothing to hide then.

n1k7 - November 23, 2024, 11:17 pm

Its' better to use file less techniques along with abusing LOLBINS (<https://lolbas-project.github.io/>), other than that, you will have to escalate your privileges, move on to kernel and stay as a rootkit to hide network traffic along with your own process.

Takes a great feat to do so, due to the modern EDR blocking lots of user land and kernel activities if they seem to be suspicious. Numerous events are generated which are collected automatically and the target victim is notified of such activities, of course in an secure corporate environment.

aerohacker - November 24, 2024, 11:13 am

(Nov 23, 2024 08:14 PM)DramaKing Wrote: [\[CITE\]](#) Install the server on the victim PC? I'm too confused at this point, except to suggest a fileless crypter, nothing to hide then.

What I says is when I install a server on PC user physically or remotelly, I like to make the servers most hidden as possible from user.

DramaKing - November 24, 2024, 12:45 pm

(Nov 24, 2024 12:13 PM)aerohacker Wrote: [\[CITE\]](#) What I says is when I install a server on PC user physically or remotelly, I like to make the servers most hidden as possible from user.

So what do you run the client or payload on? Your PC?

aerohacker - November 24, 2024, 4:20 pm

(Nov 24, 2024 01:45 PM)DramaKing Wrote: [\[CITE\]](#) So what do you run the client or payload on? Your PC?

The RAT client I run on my PC on a VM and the server on the user PC.

The point is that once the server is installed on the user's machine, I like to do the server as hidden as possible on the OS, hiding files, process and etc...

The question with the r77 rootkit is I installed the rootkit, renamed the server with prefix \$77 and everything related to it disappeared (Which was expected), but at the same time while the file is invisible, it stops working too, and because of that I just want to use it to hide only the process.