

Forum:[Hack Forums](#)

Thread: [Looking for RAT Developer to Add Driver Installation Feature for Persistence \[Paid Jo](#)

david28 - April 18, 2025, 11:59 pm

Hello HackForums community,

I'm seeking an experienced RAT developer to enhance my existing Remote Access Tool with a new feature. Here are my requirements:

Feature Description: I want to add a functionality where, after a victim is infected with my RAT (Trojan), I can manually install a driver on their machine. Once the driver is installed, it should ensure long-term persistence, keeping the machine connected and preventing it from going offline.

The driver should ensure the RAT maintains a stable connection even after reboots or network changes.

The driver should operate at the kernel level, bypassing standard security measures (e.g., UAC), and remain stealthy.

The RAT and driver should remain FUD (Fully Undetectable) against major AV/EDR solutions, such as Windows Defender, Kaspersky, etc.

Compatibility: This feature must work on Windows 10 and Windows 11 (x64).

Stability: The solution should be stable, minimizing crashes, and ensuring the driver doesn't cause system instability.

Additional Info:

I already have a functional RAT, but it lacks this driver-based persistence feature.

Budget: I'm willing to pay a fair price for high-quality work (please provide your quote).

Payment: I can pay via cryptocurrency (BTC, Monero, or USDT).

Contact: Please PM me or reply to this thread with your experience, estimated timeline, and quote. I'm also available on Skype/Telegram for further discussion (PM me for my ID).

Looking forward to working with a skilled developer! <https://t.me/tm816>

Shrdw - April 19, 2025, 12:21 am

What you are wanting is Kernel Mode Driver and a rootkit, and you are going to wanting to sign the driver because even with everything included long term FUD will be hard with out updating it. Multiple bypass methods could possibly need to be added and then tested thoroughly and you will end up with many issues until this is done.

Then you have the rat and the actual payload that connects back for monitoring any changes.

I have no interest in helping with this, but this is what you are asking i doubt many here have the skills to do this anymore.

That being said you will need pretty deep pockets though i assume you already knew this so this should be an issue.

Either way i look forward to seeing how this plays out, I love interesting software a hobby of mine is recreating malware by known Advanced Persistent Threat groups and source code infecting only my own systems is still okay for testing. I have a decent amount overall but i no longer do anything that can get be locked up again this is why i will not help. :p

david28 - April 19, 2025, 12:26 am

(Apr 19, 2025 12:21 AM)Shrdw Wrote: [\[CITE\]](#) What you are wanting is Kernel Mode Driver and a rootkit, and you are going to wanting to sign the driver because even with everything included long term FUD will be hard with out updating it. Multiple bypass methods could possibly need to be added and then tested thoroughly and you will end up with many issues until this is done.

Then you have the rat and the actual payload that connects back for monitoring any changes.

I have no interest in helping with this, but this is what you are asking i doubt many here have the skills to do this anymore.

That being said you will need pretty deep pockets though i assume you already knew this so this should be an issue.

Does it have to be updated after a while

aerohacker - April 19, 2025, 12:30 am

(Apr 18, 2025 11:59 PM)david28 Wrote: [\[CITE\]](#) Hello HackForums community, I'm seeking an experienced RAT developer to enhance my existing Remote Access Tool with a new feature. Here are my requirements:

Feature Description: I want to add a functionality where, after a victim is infected with my RAT (Trojan), I can manually install a driver on their machine. Once the driver is installed, it should ensure long-term persistence, keeping the machine connected and preventing it from going offline. The driver should ensure the RAT maintains a stable connection even after reboots or network changes.

The driver should operate at the kernel level, bypassing standard security measures (e.g., UAC), and remain stealthy.

The RAT and driver should remain FUD (Fully Undetectable) against major AV/EDR solutions, such as Windows Defender, Kaspersky, etc.

Compatibility: This feature must work on Windows 10 and Windows 11 (x64).

Stability: The solution should be stable, minimizing crashes, and ensuring the driver doesn't cause system instability.

Additional Info:

I already have a functional RAT, but it lacks this driver-based persistence feature.

Budget: I'm willing to pay a fair price for high-quality work (please provide your quote).

Payment: I can pay via cryptocurrency (BTC, Monero, or USDT).

Contact: Please PM me or reply to this thread with your experience, estimated timeline, and quote. I'm also available on Skype/Telegram for further discussion (PM me for my ID).

Looking forward to working with a skilled developer! <https://t.me/tm816>

You need a Rootkit Ring 0 that operates in Kernel mode/level like AntiVirus or a MBR Bootkit to load before the Windows.

Does your RAT has HVNC or HRDP features?! You can use this features to install the driver hidden and manually with administration privileges.

Shrdw - April 19, 2025, 12:33 am

(Apr 19, 2025 12:26 AM)david28 Wrote: [\[CITE\]](#) Does it have to be updated after a while Even when signing using a proper certificate from a trusted authority eventually something will get flagged depending on what the target is due to the kind of software this is.

This is my understanding at least though others may have better methods

david28 - April 19, 2025, 12:39 am

(Apr 19, 2025 12:33 AM)Shrdw Wrote: [\[CITE\]](#) Even when signing using a proper certificate from a trusted authority eventually something will get flagged depending on what the target is due to the kind of software this is.

This is my understanding at least though others may have better methods

Can you leave your TG, or you look for me at TG, and I will take a screenshot to show you the problem I want to solve? Is it convenient for you?

(Apr 19, 2025 12:30 AM)aerohacker Wrote: [\[CITE\]](#) You need a Rootkit Ring 0 that operates in Kernel mode/level like AntiVirus or a MBR Bootkit to load before the Windows.

Does your RAT has HVNC or HRDP features?! You can use this features to install the driver hidden and manually with administration privileges.

I can take screenshots of these questions on TG to show you for better communication

Shrdw - April 19, 2025, 12:56 am

(Apr 19, 2025 12:39 AM)david28 Wrote: [\[CITE\]](#) Can you leave your TG, or you look for me at TG, and I will take a screenshot to show you the problem I want to solve? Is it convenient for you?

I can take screenshots of these questions on TG to show you for better communication

I do not develop malware for the sole purpose of spreading it anymore as i mentioned above the post you quoted i just figured i would explain what you where asking a little better when someone who does this outside of a hobby came along. Because the wording was a bit confusing initially though this other guy may have a point though doing this would still take a great deal of skill either way to ensure long term persistence.

So i won't be sharing my telegram sorry. Ill keep it as a hobby doing 10 years in a federal prison was a learning experience i don't care to repeat.

Either way be careful many eyes roam the internet anymore and practice proper Operational Security.

DramaKing - April 19, 2025, 5:54 am

Why don't you just say that you want a kernel rootkit? Ring 0 rootkits are scarcer than hens' teeth today. If you're willing to spend \$5k, you can get an EV certificate, which will allow the rootkit to run temporarily until it is discovered, analyzed, and the certificate is added to the revocation list. Rinse and repeat.

david28 - April 19, 2025, 7:05 am

(Apr 19, 2025 05:54 AM)DramaKing Wrote: [\[CITE\]](#) Why don't you just say that you want a kernel rootkit? Ring 0 rootkits are scarcer than hens' teeth. If you're willing to spend \$5k, you can get an EV certificate, which will allow the rootkit to run temporarily until it is discovered, analyzed, and the certificate is added to the revocation list. Rinse and repeat.

Brother, you are so humorous

DramaKing - April 19, 2025, 7:51 am

(Apr 19, 2025 07:05 AM)david28 Wrote: [\[CITE\]](#) Brother, you are so humorous
Oh, you think that I'm joking?

DramaKing - May 19, 2025, 4:06 pm

Found anyone to build your rootkit and provide a certificate yet?

david28 - May 22, 2025, 12:02 am

(May 19, 2025 04:06 PM)DramaKing Wrote: [\[CITE\]](#) Found anyone to build your rootkit and provide a certificate yet?

Yes, at the moment, we use drivers instead of persistence