

Forum:[Hack Forums](#)

Thread: [RAT loaders that re-download the payload after AV removal](#)

NoAccess123 - September 8, 2026, 2:31 pm

Hey everyone.

I remember, back in old days the clients used to suddenly disappear just because AV was able to find the stub and clean it completely.

So is there any kind of dropper/loader existing in RAT or cytper that stays separately on the system and periodically checks a URL for a fresh payload?

Basically, I'm thinking of a setup where the actual RAT gets detected and removed by AV, but the loader survives. Then later it fetches a newly crypted/FUD version of the RAT from a configurable URL and installs/runs it again silently.

CyberXero - September 8, 2026, 2:32 pm

(Sep 8, 2026 02:31 PM)NoAccess123 Wrote: [\[CITE\]](#) Hey everyone.

I remember, back in old days the clients used to suddenly disappear just because AV was able to find the stub and clean it completely.

So is there any kind of dropper/loader existing in RAT or cytper that stays separately on the system and periodically checks a URL for a fresh payload?

Basically, I'm thinking of a setup where the actual RAT gets detected and removed by AV, but the loader survives. Then later it fetches a newly crypted/FUD version of the RAT from a configurable URL and installs/runs it again silently.

following thread as i am also looking for something similar.

DeathPenalty666 - September 8, 2026, 2:38 pm

I can make you a FUD tool to reload your rat easily. Otherwise i have a loader i can sell with low detection rate that redownload the rat. But the first alternative is much better its 100% fud and can redownload your payload every X min, drop 2 and more

DramaKing - September 8, 2026, 3:25 pm

I like your idea, but I sell a downloader that drops an unencrypted file to disk, waits for it to be quarantined, then automatically restores the file and executes. Microsoft relies too much on "security boundaries." I won't tell you exactly how it works, of course, but you may be able to figure it out yourself. It didn't take me much research.

NoAccess123 - September 8, 2026, 3:37 pm

(Sep 8, 2026 02:38 PM)DeathPenalty666 Wrote: [\[CITE\]](#) I can make you a FUD tool to reload your rat easily. Otherwise i have a loader i can sell with low detection rate that redownload the rat. But the first alternative is much better its 100% fud and can redownload your payload every X min, drop 2 and more

I am not inclining towards a FUD tool because if for some reason my stub is perished due to some

scan. (Which usually used to happen in Darkcomet days), and I kept wondering if PC has not been switched on yet.

I may also not start my RAT for weeks, not knowing if my bot is still working.

I want a FUD loader, which will redownload the RAT. Since, I may experiment with lot of crypters, if the crypter I am using suddenly stopped becoming FUD, I should be able to put my updated FUD stub somewhere that loader would download automatically.

(Sep 8, 2026 03:25 PM)DramaKing Wrote: [\[CITE\]](#) I like your idea, but I sell a downloader that drops an unencrypted file to disk, waits for it to be quarantined, then automatically restores the file and executes. Microsoft relies too much on "security boundaries." I won't tell you exactly how it works, of course, but you may be able to figure it out yourself. It didn't take me much research.

I will not be able to figure it out.

Can you please share link to where your selling the downloader?

DramaKing - September 8, 2026, 4:00 pm

(Sep 8, 2026 03:37 PM)NoAccess123 Wrote: [\[CITE\]](#) I am not inclining towards a FUD tool because if for some reason my stub is perished due to some scan. (Which usually used to happen in Darkcomet days), and I kept wondering if PC has not been switched on yet.

I may also not start my RAT for weeks, not knowing if my bot is still working.

I want a FUD loader, which will redownload the RAT. Since, I may experiment with lot of crypters, if the crypter I am using suddenly stopped becoming FUD, I should be able to put my updated FUD stub somewhere that loader would download automatically.

I will not be able to figure it out.

Can you please share link to where your selling the downloader?

You use a simple while loop in PowerShell and Test-Path to conditionally redownload a file if it is missing, then use saps or the call operator to execute said file. You would just have to periodically update the hosted file.

<https://hackforums.net/showthread.php?tid=6312021>