

Forum:[Hack Forums](#)

Thread: [What should be first? Loader / Stager / Dropper](#)

DustyDog123 - March 30, 2024, 12:23 pm

Hey,

I've been reading loads of posts on this forum and cannot figure out the type of malware I should be spreading in the first instance.

What is everyone else's choice and opinion on this?

Raven™ - March 30, 2024, 2:20 pm

(Mar 30, 2024 12:23 PM)DustyDog123 Wrote: [\[CITE\]](#) Hey,

I've been reading loads of posts on this forum and cannot figure out the type of malware I should be spreading in the first instance.

What is everyone else's choice and opinion on this?

Start with NJRat variants. The best i recommend to any new comers.

DustyDog123 - March 30, 2024, 2:22 pm

(Mar 30, 2024 02:20 PM)Raven™ Wrote: [\[CITE\]](#) Start with NJRat variants. The best i recommend to any new comers.

I think you've misinterpreted what I asked.

Raven™ - March 30, 2024, 2:25 pm

(Mar 30, 2024 02:22 PM)DustyDog123 Wrote: [\[CITE\]](#) I think you've misinterpreted what I asked. Good catch! Ok, so start with Loader.

DustyDog123 - March 30, 2024, 2:26 pm

(Mar 30, 2024 02:25 PM)Raven™ Wrote: [\[CITE\]](#) Good catch! Ok, so start with Loader. Thanks, that is what I thought.

But what is the point of a stager?

Raven™ - March 30, 2024, 2:29 pm

(Mar 30, 2024 02:26 PM)DustyDog123 Wrote: [\[CITE\]](#) Thanks, that is what I thought.

But what is the point of a stager?

A fileless malware used in multistage cyberattacks. This requires more complex form of planning.

Hollows - March 31, 2024, 4:24 am

You can start off with just an un-signed loader (built as WinPE .exe format) that loads your mutated modules into memory safely and go from there, this is the setup that I see most following when starting off. Any loader should be responsible for verifying the integrity of the system, maintain a secure channel of communication with your C&C and load modules (ideally into memory) if needed.

Don't complicate things in the start with a multi-stage payload, good luck.

