

Forum:[Hack Forums](#)

Thread: [Can you disable antivirus before you drop RAT?/Masking reverse TCP to avoid detection](#)

midichlorianchip - December 15, 2023, 8:05 pm

Hey guys, been lurking for a while, trying to soak up as much knowledge as I can. I have a question.

Let's say you're using an open source RAT, crypted. And the target has AVAST installed. AVAST, of course, whether or not your RAT is crypted, will detect the reverse tcp connection, and immediately kill your RAT. Additionally, because open source RATS are quite popular, the AV might end up detecting it after some time, crypted or not. This, of course is not good.

I've been researching Loaders. What I am getting, is that a Loader is like "Malware Light" that doesn't create a reverse tcp connection, but can change system settings, then download additional payloads, like an open source RAT?

So, my question is, can a Loader, in theory, disable AVAST, WD, and so on, and then download the RAT? Am I understanding what a loader does? I don't know what I don't know. So clarifications are welcomed.

If not, what tool gives threat actors the ability to alter system settings (let's say run a PowerShell script to disable WD). Or, do they just drop the RAT, and use other techniques to mask reverse tcp traffic?

Tentco - December 15, 2023, 8:45 pm

(Dec 15, 2023 09:05 PM)midichlorianchip Wrote: [\[CITE\]](#) Hey guys, been lurking for a while, trying to soak up as much knowledge as I can. I have a question.

Let's say you're using an open source RAT, crypted. And the target has AVAST installed. AVAST, of course, whether or not your RAT is crypted, will detect the reverse tcp connection, and immediately kill your RAT. Additionally, because open source RATS are quite popular, the AV might end up detecting it after some time, crypted or not. This, of course is not good.

I've been researching Loaders. What I am getting, is that a Loader is like "Malware Light" that doesn't create a reverse tcp connection, but can change system settings, then download additional payloads, like an open source RAT?

So, my question is, can a Loader, in theory, disable AVAST, WD, and so on, and then download the RAT? Am I understanding what a loader does? I don't know what I don't know. So clarifications are welcomed.

If not, what tool gives threat actors the ability to alter system settings (let's say run a PowerShell script to disable WD). Or, do they just drop the RAT, and use other techniques to mask reverse tcp traffic?

This is why, SSL Pinning, Domain Fronting exists, you should encrypt your connections first, use TLS/SSL.

Yes a Loader can disable Avast, WD services using BYOVD or LPE.

A loader typically works as a dropper/stager for your final payload.

midichlorianchip - December 16, 2023, 9:55 am

(Dec 15, 2023 09:45 PM)Tentco Wrote: [\[CITE\]](#) This is why, SSL Pinning, Domain Fronting exists, you should encrypt your connections first, use TLS/SSL.

Yes a Loader can disable Avast, WD services using BYOVD or LPE.

A loader typically works as a dropper/stager for your final payload.

Understood. Thanks.