

Forum:[Hack Forums](#)

Thread: [question about crypter functionality](#)

mixer - July 29, 2024, 1:07 pm

i have some questions about Crypters:

1. where are the best places/sections of the stub to keep a payload?
2. what are the most effective injection techniques?

globalroot - July 30, 2024, 2:37 am

1. A server.

2. Read this by mistermistake which I totally agree:

"Process hollowing is one of shittiest evasion techniques imo. Removing sections, adding new sections, setting thread context are very obvious operations. Especially when the thread is suspended, itz not hard to see that the process is hollowed out. svchost.exe is a very suspicious and widely used process. Can even compare it with copy on disk."

mixer - July 30, 2024, 3:38 am

(Jul 30, 2024 02:37 AM)globalroot Wrote: [\[CITE\]](#) 1. A server.

2. Read this by mistermistake which I totally agree:

"Process hollowing is one of shittiest evasion techniques imo. Removing sections, adding new sections, setting thread context are very obvious operations. Especially when the thread is suspended, itz not hard to see that the process is hollowed out. svchost.exe is a very suspicious and widely used process. Can even compare it with copy on disk."

don't all these crypters (even the ones being sold on this forum) use these injection techniques?

globalroot - July 30, 2024, 3:41 am

(Jul 30, 2024 03:38 AM)mixer Wrote: [\[CITE\]](#) don't all these crypters (even the ones being sold on this forum) use these injection techniques?

Even if they do, they shouldn't.

mixer - July 30, 2024, 3:47 am

(Jul 30, 2024 03:41 AM)globalroot Wrote: [\[CITE\]](#) Even if they do, they shouldn't.

then what are the better ways to do it?

globalroot - July 30, 2024, 8:10 am

(Jul 30, 2024 03:47 AM)mixer Wrote: [\[CITE\]](#) then what are the better ways to do it?

Other evasion techniques, like dll unhooking.

Tentco - July 30, 2024, 8:13 am

(Jul 29, 2024 01:07 PM)mixer Wrote: [\[CITE\]](#) i have some questions about Crypters:

1. where are the best places/sections of the stub to keep a payload?
2. what are the most effective injection techniques?

1. Keep it as shellcode and xor it and saved it as chunks along the section, some loader does it.

2. There are many injection techniques most crypter uses same old techniques but with advancement for eg LoadPE with their own windows loader or shc injector with indirect/veh calls etc...

happygonutty - August 1, 2024, 3:43 am

(Jul 29, 2024 01:07 PM)mixer Wrote: [\[CITE\]](#) i have some questions about Crypters:

1. where are the best places/sections of the stub to keep a payload?
2. what are the most effective injection techniques?

1. The best way you can do is improvise techniques that aren't well known, you can check out lots of sources by reading malware write-ups and checking their mistakes why they got detected.

2. There are some and globalroot has already indicated a good one which is DLL unhooking which is not very obvious and doesn't get easily detected as long as you have a "personal" or "private" technique on how to unload it. And of course, since this is something out of the ordinary question, 100% that nobody would answer this question since these types of questions are normally answered in exchange for money. Most answers you will get are from people who just searched google and advise you with existing methods that can already be detected.

(Jul 30, 2024 03:38 AM)mixer Wrote: [\[CITE\]](#) don't all these crypters (even the ones being sold on this forum) use these injection techniques?

True, but there are some here who make improvisations so it cannot be detected easily but most of the time it would get detected but the crypter author would definitely patch the crypter and notify their users via thread or pm I think.

(Jul 30, 2024 08:10 AM)globalroot Wrote: [\[CITE\]](#) Other evasion techniques, like dll unhooking. I vouch this and this is one of the unusual methods that up to this date, doesn't get detected easily especially if the writer has a way of unhooking DLLs in an unusual way and not yet known.