

Forum:[Hack Forums](#)

Thread: [Oppresor's RunPE without weird names or api delegates](#)

gigajew - February 24, 2018, 12:07 pm

I was looking around for Oppresor's RunPE to study it, and I found it with delegates to windows api functions and odd names, so I "re-created" or cleaned it and also changed the api signatures a bit. It helped me understand the process a little bit better, and see what I did wrong and where. Hopefully with some commenting more people can understand how it works. Don't expect it to be FUD or anything.

HFDone - February 24, 2018, 1:28 pm

so old and not even his runpe <https://hackforums.net/showthread.php?tid=2759604>
you better check aeon runpe (clean code) if you want to understand how its work.

Menalix - February 24, 2018, 2:59 pm

(Feb 24, 2018 02:28 PM)HFDone Wrote: [\[CITE\]](#) so old and not even his runpe <https://hackforums.net/showthread.php?tid=2759604>
you better check aeon runpe (clean code) if you want to understand how its work.
No reason to look at aeonhacks runpe which is just an altered version with a for loop for stability, this is just as simple to follow.

0xDEAD10CC - February 24, 2018, 5:03 pm

(Feb 24, 2018 03:59 PM)Menalix Wrote: [\[CITE\]](#) No reason to look at aeonhacks runpe which is just an altered version with a for loop for stability, this is just as simple to follow.
Except they all appear to be non-portable being that they rely on BitConverter which isn't always going to be little endian among other things. After so many revisions, still nothing incredibly amazing to see. Part of the above code isn't even used. I don't understand why we need a million versions of the same thing. They all derive from Aeon's version from what I follow or the original one of this... (including yours). It just looks like people have taken the one-function version and split it up, used different structs, changed the looping semantics around, and split it up into functions.

At the end of the day it's all still the same old semi-decent code.

Menalix - February 25, 2018, 3:02 am

(Feb 24, 2018 06:03 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Except they all appear to be non-portable being that they rely on BitConverter which isn't always going to be little endian among other things. After so many revisions, still nothing incredibly amazing to see. Part of the above code isn't even used. I don't understand why we need a million versions of the same thing. They all derive from Aeon's version from what I follow or the original one of this... (including yours). It just looks like people have taken the one-function version and split it up, used different structs, changed the looping semantics around, and split it up into functions.

At the end of the day it's all still the same old semi-decent code.

Well maybe that's because a RunPE isn't amazing, it's a plain simple technic.

Derive from Aeonhack? Aeonhack was properly the last one to release a RunPE. He just made yet another revision with a for loop, and all the crypter tards bought the for loop for 250 euro, cause they didn't have the brains to do a for loop themselves.

HFDone - February 25, 2018, 3:46 am

(Feb 25, 2018 04:02 AM)Menalix Wrote: [\[CITE\]](#) Well maybe that's because a RunPE isn't amazing, it's a plain simple technic.

Derive from Aeonhack? Aeonhack was properly the last one to release a RunPE. He just made yet another revision with a for loop, and all the crypter tards bought the for loop for 250 euro, cause they didn't have the brains to do a for loop themselves.

? including you. first i thought to link him to your rp but it same as aeon.

Menalix - February 25, 2018, 11:57 am

(Feb 25, 2018 04:46 AM)HFDone Wrote: [\[CITE\]](#) ? including you. first i thought to link him to your rp but it same as aeon.It's not, mine was just a proof of concept to show you can patch .net payloads to inject a target with any architecture type, since a guy here on HF called it impossible.

He said I faked my video, so I released the code.

My personal RunPE is not based on CreateProcess, AV's detects it too easyli. It's better to use a job object to catch processes started by the end-user and then suspend those and do the injection.

gigajew - February 25, 2018, 2:47 pm

(Feb 25, 2018 12:57 PM)Menalix Wrote: [\[CITE\]](#) It's not, mine was just a proof of concept to show you can patch .net payloads to inject a target with any architecture type, since a guy here on HF called it impossible.

He said I faked my video, so I released the code.

My personal RunPE is not based on CreateProcess, AV's detects it too easyli. It's better to use a job object to catch processes started by the end-user and then suspend those and do the injection.

I tried the RunPE code you released, and it didn't seem very stable at all.

Menalix - February 25, 2018, 6:16 pm

(Feb 25, 2018 03:47 PM)gigajew Wrote: [\[CITE\]](#) I tried the RunPE code you released, and it didn't seem very stable at all.

ye it isn't.

0xDEAD10CC - February 25, 2018, 9:45 pm

A lot of people don't read about the PECOFF file format anyways here which is publicly available to understand how a PE is laid out on disk.

Electron - February 26, 2018, 5:01 am

(Feb 25, 2018 07:16 PM)Menalix Wrote: [\[CITE\]](#) ye it isn't.

About the code I've seen, there were many things to be fixed. Not sure if you left it so just because of leakers.

HFDone - February 26, 2018, 6:04 am

(Feb 26, 2018 06:01 AM)Noxious™ Wrote: [\[CITE\]](#) About the code I've seen, there were many things to be fixed. Not sure if you left it so just because of leakers.

probably some of and just managed files.

Menalix - February 26, 2018, 12:28 pm

(Feb 26, 2018 06:01 AM)Noxious™ Wrote: [\[CITE\]](#) About the code I've seen, there were many things to be fixed. Not sure if you left it so just because of leakers.

It was released in a rush due to a discussion here on hf, whether you could patch the .net payload to inject into a target of any architecture. So I just made a proof of concept code as an argument for a post.