

Forum:[Hack Forums](#)

Thread: [xmrig and process hollowing ram execution?](#)

0x0SH3 - December 18, 2023, 3:05 am

I developed my first crypter that has process hollowing as execution method, I use it for xmrig execution but I don't know if it's enough to evade av. I use a modded version of xmrig without dev fees so it has 3-4 less detections than the official xmrig (around 25 av detect it) but it's not blocked by windows defender.

- Do you know if I'll have runtime problems with antivirus solutions (the crypter runpe is near fud, I'm not sure about xmrig when it's running in memory)?
- xmrig.exe will be executed in RAM as child process of svchost.exe but maybe some antivirus are able to stop it by process name or I don't know how?

osn64698 - December 18, 2023, 3:09 am

Process hollowing in it's natural form is a method from 2006. Without adapting it properly you will be instantly detected.

Tentco - December 18, 2023, 3:38 am

(Dec 18, 2023 04:05 AM)0x0SH3 Wrote: [\[CITE\]](#) I developed my first crypter that has process hollowing as execution method, I use it for xmrig execution but I don't know if it's enough to evade av. I use a modded version of xmrig without dev fees so it has 3-4 less detections than the official xmrig (around 25 av detect it) but it's not blocked by windows defender.

- Do you know if I'll have runtime problems with antivirus solutions (the crypter runpe is near fud, I'm not sure about xmrig when it's running in memory)?
- xmrig.exe will be executed in RAM as child process of svchost.exe but maybe some antivirus are able to stop it by process name or I don't know how?

Buddy, you're using RunPE, stop it.

0x0SH3 - December 18, 2023, 3:39 am

(Dec 18, 2023 04:09 AM)osn64698 Wrote: [\[CITE\]](#) Process hollowing in it's natural form is a method from 2006. Without adapting it properly you will be instantly detected.

It's scantime 100% fud, I'm not sure how to check runtime with multiple antivirus without configuring too much vm. Do you know a service with don't distribute for runtime checking?

Tentco - December 18, 2023, 3:40 am

(Dec 18, 2023 04:39 AM)0x0SH3 Wrote: [\[CITE\]](#) It's scantime 100% fud, I'm not sure how to check runtime with multiple antivirus without configuring too much vm. Do you know a service with "don't distribute" for runtime checking?
scanner.to kid

0x0SH3 - December 18, 2023, 3:41 am

(Dec 18, 2023 04:38 AM)Tentco Wrote: [\[CITE\]](#) Buddy, you're using RunPE, stop it.
what methods should I use?

Tentco - December 18, 2023, 3:46 am

(Dec 18, 2023 04:41 AM)0x0SH3 Wrote: [\[CITE\]](#) what methods should I use?

You're dumb, the fact that you're saving non-encrypted raw bytes for your payload is just plain stupid, consider learning red teaming first.

Any method you will employ will need heavy modification.

0x0SH3 - December 18, 2023, 4:55 am

(Dec 18, 2023 04:46 AM)Tentco Wrote: [\[CITE\]](#) You're dumb, the fact that you're saving non-encrypted raw bytes for your payload is just plain stupid, consider learning red teaming first.

Any method you will employ will need heavy modification.

what? my crypter works fully in memory, it doesn't drop anything in the disk and the payload is decrypted in memory before execution, I don't know why you assume bytes are non-encrypted just by reading "hollowing" or "runpe" that are only execution methods, they have nothing to do with what was done at payload before execution..

Tentco - December 18, 2023, 5:57 am

(Dec 18, 2023 05:55 AM)0x0SH3 Wrote: [\[CITE\]](#) what? my crypter works fully in memory, it doesn't drop anything in the disk and the payload is decrypted in memory before execution, I don't know why you assume bytes are non-encrypted just by reading "hollowing" or "runpe" that are only execution methods, they have nothing to do with what was done at payload before execution..

When did I said it drops anything to disk? you don't know anything stop wasting my time.

0x0SH3 - December 18, 2023, 7:03 am

(Dec 18, 2023 06:57 AM)Tentco Wrote: [\[CITE\]](#) When did I said it drops anything to disk? you don't know anything stop wasting my time.

yeah the disk, ok thanks for your useful and not toxic comments, good luck

- Jon Snow

osn64698 - December 18, 2023, 7:52 am

(Dec 18, 2023 04:41 AM)0x0SH3 Wrote: [\[CITE\]](#) what methods should I use?

You seem to think there is a "magic" method that works for every AV. It doesn't work this way. Don't buy this "priceless" BS.

Here is an actual suggestion: Go study reverse engineering, open a debugger, figure out why your shit gets caught, what triggers an AV detection runtime? What are you executing? Are you creating a new thread? Are you suspending one? are you writing your pages within MEM_IMAGE?

You are trying to achieve something without understanding how it works, do you know what NtMapViewOfSection does? Behind the scenes? what about NtUnmapViewOfSection? If not, you have no reason to use RUNPE, go back to basics.

Study the windows PE loader, then ask yourself how you can add your own customization. There is no NEED to call any WINAPI in order to load a basic PE file.

The only reason people still use "RunPE" is because they can copy & paste it. Takes 0 brain cells. It is 2023, you can use your brain to not use a 2006 method.

Tentco - December 18, 2023, 9:30 am

(Dec 18, 2023 08:52 AM)osn64698 Wrote: [\[CITE\]](#) You seem to think there is a "magic" method that works for every AV. It doesn't work this way. Don't buy this "priceless" BS.

Here is an actual suggestion: Go study reverse engineering, open a debugger, figure out why your shit gets caught, what triggers an AV detection runtime? What are you executing? Are you creating a new thread? Are you suspending one? are you writing your pages within MEM_IMAGE?

You are trying to achieve something without understanding how it works, do you know what NtMapViewOfSection does? Behind the scenes? what about NtUnmapViewOfSection? If not, you have no reason to use RUNPE, go back to basics.

Study the windows PE loader, then ask yourself how you can add your own customization. There is no NEED to call any WINAPI in order to load a basic PE file.

The only reason people still use "RunPE" is because they can copy & paste it. Takes 0 brain cells. It is 2023, you can use your brain to not use a 2006 method.

Thanks for these descriptive posts man, even though this shit is asked infinite no. of time, your post quality remains great always, love you.

YAK_CODER - December 18, 2023, 10:11 am

(Dec 18, 2023 08:52 AM)osn64698 Wrote: [\[CITE\]](#) You are trying to achieve something without understanding how it works, do you know what NtMapViewOfSection does? Behind the scenes? what about NtUnmapViewOfSection? If not, you have no reason to use RUNPE, go back to basics. Very correct

(Dec 18, 2023 04:05 AM)0x0SH3 Wrote: [\[CITE\]](#) blocked by windows defender.add amsi bypass bro <https://github.com/search?q=amsi%20bypass&type=repositories>

0x0SH3 - December 18, 2023, 12:53 pm

(Dec 18, 2023 08:52 AM)osn64698 Wrote: [\[CITE\]](#) You seem to think there is a "magic" method that works for every AV. It doesn't work this way. Don't buy this "priceless" BS.

Here is an actual suggestion: Go study reverse engineering, open a debugger, figure out why your shit gets caught, what triggers an AV detection runtime? What are you executing? Are you creating a new thread? Are you suspending one? are you writing your pages within MEM_IMAGE?

You are trying to achieve something without understanding how it works, do you know what NtMapViewOfSection does? Behind the scenes? what about NtUnmapViewOfSection? If not, you have no reason to use RUNPE, go back to basics.

Study the windows PE loader, then ask yourself how you can add your own customization. There is no NEED to call any WINAPI in order to load a basic PE file.

The only reason people still use "RunPE" is because they can copy & paste it. Takes 0 brain cells. It is 2023, you can use your brain to not use a 2006 method.
thank you