

Forum:[Hack Forums](#)

Thread: [Cryper for MacOS](#)

bhoppa - August 5, 2013, 3:27 pm

Hey,

Would it be possible to make a crypter for MacOS? Not for malware undetection, but just to protect applications.

I imagine you need to make some sort of RunPE without WinAPI.
And also getting the information from the (embedded)resources without WinAPI.

Anyone tried this?

Regards,
Bhoppa

Kroflica - August 5, 2013, 4:12 pm

(Aug 5, 2013 03:27 PM)bhoppa Wrote: [\[CITE\]](#) Hey,

Would it be possible to make a crypter for MacOS? Not for malware undetection, but just to protect applications.

I imagine you need to make some sort of RunPE without WinAPI.
And also getting the information from the (embedded)resources without WinAPI.

Anyone tried this?

Regards,
Bhoppa

If RunPE can be implemented on unix-like OS, wine already did it (does anyone know how to do WriteProcessMemory on linux??) so you can use winapi and then simply -lwine the program. If not, see ptrace(2) but I bet it won't work cause of privileges break stuff like that...

Shihanus - August 5, 2013, 4:49 pm

(Aug 5, 2013 04:12 PM)Kroflica Wrote: [\[CITE\]](#) If RunPE can be implemented on unix-like OS, wine already did it (does anyone know how to do WriteProcessMemory on linux??) so you can use winapi and then simply -lwine the program. If not, see ptrace(2) but I bet it won't work cause of privileges break stuff like that...

They do have pr_write, if that's what he's wondering.

wacked3 - August 7, 2013, 5:31 pm

(Aug 5, 2013 04:12 PM)Kroflica Wrote: [\[CITE\]](#) wine already did it (does anyone know how to do WriteProcessMemory on linux??)Take a look at wine to find out?

You have to understand that RunPE only works on windows for various windows specific reasons. It could very well load all dlls, do relocations and similar - just don't do TLS callbacks and don't call the entrypoint. (That code is executed in the DLLs is more of a semantic issue)
Only because Windows chooses not to do this RunPE works.

(Resources are also a windows concept. Mach-O does not have that so probably the proper way would be to put it into a new section)

So what should you do? Learn how to do a packer and not some skiddie runpe bullshit.

Shihanus - August 7, 2013, 5:43 pm

(Aug 7, 2013 05:31 PM)wacked3 Wrote: [\[CITE\]](#) Take a look at wine to find out?

You have to understand that RunPE only works on windows for various windows specific reasons. It could very well load all dlls, do relocations and similar - just don't do TLS callbacks and don't call the entrypoint. (That code is executed in the DLLs is more of a semantic issue)
Only because Windows chooses not to do this RunPE works.

(Resources are also a windows concept. Mach-O does not have that so probably the proper way would be to put it into a new section)

So what should you do? Learn how to do a packer and not some skiddie runpe bullshit.
Overwrite the entry point with a jump to the decrypt routine. It decrypts the whole .text section.

Stryker™ - August 8, 2013, 9:30 am

well the problem is that a crypter or runpe on mac os would not protect your application, anyone with a little computer knowledge would just hook the memory writing function and dump the payload, that way they would receive the original application that was crypted :P