

Forum:[Hack Forums](#)

Thread: [How much would you pay for a &\[b\]#34\[/b\];crypter&\[b\]#34\[/b\]; that doesn't use RunPE?](#)

Feminist - February 6, 2014, 11:40 pm

Developed in C++ and FASM

No dependencies

Resource cloner

FUD, runtime, scantime, bypass all av's including kaspersky, avast, and pretty much all other runtimes. (Unless the crypted file calls an API hooked with a ring0kit such as SetWindowsHookEx for keyboard hooks - nothing can bypass such paranoia)

It uses a unique method to protect the file, so no RunPE/WriteProcessMemory/etc API calls.

I will implement "add to startup" and "install" features. There is currently no support for EOF data. (This can be easily added)

How much would you pay for this per month?

N3oNight - February 7, 2014, 12:31 am

it dosent matter if uses runpe or not,

the thing matter is for how many days or how long will it be FUD.

OnlyBOTNET - February 7, 2014, 1:13 am

(Feb 7, 2014 01:31 AM)N3oNight Wrote: [\[CITE\]](#) it dosent matter if uses runpe or not, the thing matter is for how many days or how long will it be FUD.

And if it has dependencies.

#Thread

For FASM i would pay 50\$/week for C++ 20\$/week max.

?ain - February 7, 2014, 1:15 am

What difference would it not being RunPE make? I honestly don't know.

Feminist - February 7, 2014, 8:37 am

(Feb 7, 2014 04:45 AM)Conqueror Wrote: [\[CITE\]](#) Well.. every memory scan would detect it so.. its same of a runpe except that doesn't uses detected APIs by HIPS and Firewall.

Almost every single HIPS and Firewall detect RunPE nowadays. It's a dead horse, when there are so many better alternatives to use.

It is FUD for weeks at a time, and it has no dependencies outside of the windows operating system itself. It only needs kernel32.dll to run (and well, of course ntdll.dll) as well as any dll's that the crypted process needs (such as ws32_dll.dll, etc)

Raz?r - February 7, 2014, 8:41 am

(Feb 7, 2014 09:37 AM)Feminist Wrote: [\[CITE\]](#) Almost every single HIPS and Firewall detect RunPE nowadays. It's a dead horse, when there are so many better alternatives to use.

It is FUD for weeks at a time, and it has no dependencies outside of the windows operating system

itself. It only needs kernel32.dll to run (and well, of course ntdll.dll) as well as any dll's that the crypted process needs (such as ws32_dll.dll, etc)hips still have huge problems detecting dynamic forking and i don't see how a firewall should...

Also for the FUD-time, how can you tell? I tested a lot of techniques to increase it and only testing them on long-term was able to tell if they are effective.

Feminist - February 7, 2014, 8:49 am

(Feb 7, 2014 09:41 AM)Raz?r Wrote: [\[CITE\]](#) hips still have huge problems detecting dynamic forking and i don't see how a firewall should...

Also for the FUD-time, how can you tell? I tested a lot of techniques to increase it and only testing them on long-term was able to tell if they are effective.

All an antivirus needs to do is hook a few functions (such as CreateProcess, NtUnmapViewOfSection) and they will instantly know that you are using RunPE thus detect your payload.

Not every antivirus does this- but a lot do. Your RunPE crypter might be scantime FUD, but it won't work in runtime against many antiviruses these days.

Maybe in 2008/2009/2010 you could get away with RunPE; but these days its just something you can't get away with anymore.

In my opinion, there's no point calling a crypter FUD if it can't get past the AV's it should during runtime.

(Feb 7, 2014 09:41 AM)Raz?r Wrote: [\[CITE\]](#) hips still have huge problems detecting dynamic forking and i don't see how a firewall should...

Also for the FUD-time, how can you tell? I tested a lot of techniques to increase it and only testing them on long-term was able to tell if they are effective.

You can increase FUD time by giving users unique executables. Of course, there is always some "part" of your code they begin to detect- so even FUD time has its limits per reprogram.

AnonymousDDOxz - February 7, 2014, 9:52 am

(Feb 7, 2014 09:49 AM)Feminist Wrote: [\[CITE\]](#) All an antivirus needs to do is hook a few functions (such as CreateProcess, NtUnmapViewOfSection) and they will instantly know that you are using RunPE thus detect your payload.

Not every antivirus does this- but a lot do. Your RunPE crypter might be scantime FUD, but it won't work in runtime against many antiviruses these days.

Maybe in 2008/2009/2010 you could get away with RunPE; but these days its just something you can't get away with anymore.

In my opinion, there's no point calling a crypter FUD if it can't get past the AV's it should during runtime.

You can increase FUD time by giving users unique executables. Of course, there is always some "part" of your code they begin to detect- so even FUD time has its limits per reprogram. Give us some more information about that unique method that you didn't invent.

Feminist - February 7, 2014, 10:01 am

(Feb 7, 2014 10:52 AM)AnonymousDDOxz Wrote: [\[CITE\]](#) Give us some more information about that unique method that you didn't invent.

It's not publicly released. I never claimed to have invented it. It maps the executable into memory, fixes imports, relocs and passes control to it. It's also got a few layers of protection.

Bo Burnham - February 7, 2014, 10:02 am

I wouldn't care. As long as its FUD and as long as it works with a lot of software.

betamonkey - February 7, 2014, 10:03 am

People just want something that is undetected by both signature scans and behavior monitoring. The 'method' used is mostly irrelevant. On a side note:

Quote:but it won't work in runtime against many antiviruses these days.

Isn't true. All 'RunPE' is, is code injection to create a zombie process and there are plenty of ways to get around HIPS for that.

Feminist - February 7, 2014, 10:06 am

(Feb 7, 2014 11:03 AM)betamonkey Wrote: [\[CITE\]](#) People just want something that is undetected by both signature scans and behavior monitoring. The 'method' used is mostly irrelevant. On a side note:

Isn't true. All 'RunPE' is, is code injection to create a zombie process and there are plenty of ways to get around HIPS for that.

I'm sure that there are ways to get around HIPS for creating a zombie process. However, I'm sure most crypters on Hackforums are using the "standard" and "cookie-cutter" version of RunPE.

Additionally, some Antiviruses hook NtUnmapViewOfSection, WriteProcessMemory and will detect any file as malware if they call those functions.

Anyway. Nobody has really answered how much they would pay for this crypter per month.

betamonkey - February 7, 2014, 11:07 am

(Feb 7, 2014 11:06 AM)Feminist Wrote: [\[CITE\]](#) I'm sure that there are ways to get around HIPS for creating a zombie process. However, I'm sure most crypters on Hackforums are using the "standard" and "cookie-cutter" version of RunPE.

Additionally, some Antiviruses hook NtUnmapViewOfSection, WriteProcessMemory and will detect any file as malware if they call those functions.

Anyway. Nobody has really answered how much they would pay for this crypter per month. Just make it private and sell spots for something like \$200 per x week(s). Take on a few customers and you'll have way less stress with that rather than dealing with many dozens of whining kids expecting to pay \$20-something a month

Xenon - February 7, 2014, 11:27 am

If you want to make a crypter that will sell welll, give it a feature that the other popular crypters don't already have. Not a feature that's pointless, but something unique and useful. Get creative. Creativity is a key component to a successful product.

IRP_MJ_SCSI - February 7, 2014, 1:16 pm

(Feb 7, 2014 11:06 AM)Feminist Wrote: [\[CITE\]](#) Additionally, some Antiviruses hook NtUnmapViewOfSection, WriteProcessMemory and will detect any file as malware if they call those

functions.

That's absolute bullshit, tonnes of legitimate processes use both functions and aren't detected.

Feminist - February 7, 2014, 1:41 pm

(Feb 7, 2014 02:16 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) That's absolute bullshit, tonnes of legitimate processes use both functions and aren't detected.

So you are telling me not no antivirus in the world hooks any processes either in ring0 or ring3?

And that no antivirus in the world will detect a file as a virus for calling:

CreateProcessA

NtUnmapViewOfSection

WriteProcessMemory (for each section)

and then setting the context,

CreateRemoteThread

You are saying that no antivirus in the world does that?

Because I'm pretty sure your claim of "legitimate software" doing the above is false. Why not show me one "legit software" that does exactly as stated above?

Your assertions are laughable and can easily be disproved in a single screenshot.

IRP_MJ_SCSI - February 7, 2014, 1:57 pm

(Feb 7, 2014 02:41 PM)Feminist Wrote: [\[CITE\]](#) So you are telling me not no antivirus in the world hooks any processes either in ring0 or ring3?

And that no antivirus in the world will detect a file as a virus for calling:

CreateProcessA

NtUnmapViewOfSection

WriteProcessMemory (for each section)

and then setting the context,

CreateRemoteThread

You are saying that no antivirus in the world does that?

Because I'm pretty sure your claim of "legitimate software" doing the above is false. Why not show me one "legit software" that does exactly as stated above?

Your assertions are laughable and can easily be disproved in a single screenshot.

Do you have special needs or just no understanding of how security software works?

Proactive defense (or ring 3/ring 0 hooking as noobs call it) uses pattern matching and parameter checks to detect malicious use of certain native API functions, under no circumstance does it straight out detect a process just because it called a function.

Feminist - February 7, 2014, 3:08 pm

(Feb 7, 2014 02:57 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) Do you have special needs or just no understanding of how security software works?

Proactive defense (or ring 3/ring 0 hooking as noobs call it) uses pattern matching and parameter checks to detect malicious use of certain native API functions, under no circumstance does it straight out detect a process just because it called a function.

Come back to my thread when you have reverse engineered antiviruses, can program something

more than a hello world application, and know what you are talking about.

Avast antivirus increments an integer value for each time one of the above functions is called. Of course, it would have to check parameters to increment the specified integer for the specified process.

Once that integer reaches 3, it is detected as a virus.

So please, go away and come back when you have actually reverse engineered something and know what you are talking about.

Thanks.

IRP_MJ_SCSI - February 7, 2014, 3:17 pm

(Feb 7, 2014 04:08 PM)Feminist Wrote: [\[CITE\]](#) Come back to my thread when you have reverse engineered antiviruses, can program something more than a hello world application, and know what you are talking about.

Avast antivirus increments an integer value for each time one of the above functions is called. Of course, it would have to check parameters to increment the specified integer for the specified process.

Once that integer reaches 3, it is detected as a virus.

So please, go away and come back when you have actually reverse engineered something and know what you are talking about.

Thanks.

LMFAO, you're so stupid it's amazing. I just installed Avast and called WriteProcessMemory 4 times, no proactive detection: Please explain.

Big hackforums hacker who reverse engineers kernel mode antivirus components selling crypter on HF, hahahahah.

P.S Antiviruses can't even deploy SSDT hooks on x64.

Feminist - February 7, 2014, 3:22 pm

(Feb 7, 2014 04:17 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) LMFAO, you're so stupid it's amazing. I just installed Avast and called WriteProcessMemory 4 times, no proactive detection: Please explain.

Big hackforums hacker who reverse engineers kernel mode antivirus components selling crypter on HF, hahahahah.

P.S Antiviruses can't even deploy SSDT hooks on x64.

We're having communication issues because of your poor reading comprehension skills. Antiviruses can definitely still hook on x64. Oh no SSDT hooks patchguard skidding4lifeyolobean Copy paste a RunPE module and execute it. And you'll see what I mean. You clearly didn't read my post properly, and you're clearly only here to make trouble.

IRP_MJ_SCSI - February 7, 2014, 3:29 pm

(Feb 7, 2014 04:22 PM)Feminist Wrote: [\[CITE\]](#) We're having communication issues because of your poor reading comprehension skills. Antiviruses can definitely still hook on x64.

Copy paste a RunPE module and execute it. And you'll see what I mean. You clearly didn't read my post properly, and you're clearly only here to make trouble.

You're the one who cannot read, you specifically said "Additionally, some Antiviruses hook NtUnmapViewOfSection, WriteProcessMemory and will detect any file as malware if they call those functions."

What you said there was any file will be detected as malware if it calls NtUnmapViewOfSection and/or WriteProcessMemory, which isn't even close to true.

x64 they can't hook the SSDT which means they can't see if such functions are called without deploying usermode hooks which can be bypasses with like 3 instructions. Maybe you need to do some deeper reversing of your imaginary antivirus, because Proactive Defense uses complex heuristical patterns to detect malware based on in which order the functions are called, with which parameters and to which process, there's nothing as simple as "If NtUnmapViewOfSection is Called 3 times then detect as virus".

Need to study harder bro.

Feminist - February 7, 2014, 3:35 pm

(Feb 7, 2014 04:29 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) You're the one who cannot read, you specifically said "Additionally, some Antiviruses hook NtUnmapViewOfSection, WriteProcessMemory and will detect any file as malware if they call those functions."

What you said there was any file will be detected as malware if it calls NtUnmapViewOfSection and/or WriteProcessMemory, which isn't even close to true.

x64 they can't hook the SSDT which means they can't see if such functions are called without deploying usermode hooks which can be bypasses with like 3 instructions. Maybe you need to do some deeper reversing of your imaginary antivirus, because Proactive Defense uses complex heuristical patterns to detect malware based on in which order the functions are called, with which parameters and to which process, there's nothing as simple as "If NtUnmapViewOfSection is Called 3 times then detect as virus".

Need to study harder bro.

Now you're rambling about SSDT hooks being the only possible hook in kernel mode. Unbelievable.

Hilarious bro. I never said that if NtUnmapViewOfSection is called 3 times then it will detect it as a virus. I stated the threshold value is 3, and if certain commands with certain params are called it will trigger Avast. (different thresholds for different types)

I more then welcome you to download Avast and analyze its driver files in IDA Pro and analyze it yourself Mr Pro Reverse Code Engineer Who Is Denying Everything I Say.

IRP_MJ_SCSI - February 7, 2014, 3:46 pm

(Feb 7, 2014 04:35 PM)Feminist Wrote: [\[CITE\]](#) Now you're rambling about SSDT hooks being the only possible hook in kernel mode. Unbelievable.

I more then welcome you to download Avast and analyze its driver files in IDA Pro and analyze it yourself Mr Pro Reverse Code Engineer Who Is Denying Everything I Say.

Go on the, tell me how you will detect calls to NtWriteProcessMemory and NtUnmapViewOfSection from kernel mode without SSDT hooks?

I mean it's pretty clear that you're a scriptkiddie who thinks he's some amazing malware guru and antivirus expert, but I'll pretend to believe what you say. If you want I'll give you extra points for knowing what IDA is.

(Feb 7, 2014 04:35 PM)Feminist Wrote: [\[CITE\]](#) Hilarious bro. I never said that if NtUnmapViewOfSection is called 3 times then it will detect it as a virus. I stated the threshold value is 3, and if certain commands with certain params are called it will trigger Avast. (different thresholds for different types)

"Avast antivirus increments an integer value for each time one of the above functions is called. Of course, it would have to check parameters to increment the specified integer for the specified process.

Once that integer reaches 3, it is detected as a virus."

Your short term memory isn't great, might want to get that checked out.

Feminist - February 7, 2014, 4:03 pm

(Feb 7, 2014 04:46 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) Go on the, tell me how you will detect calls to NtWriteProcessMemory and NtUnmapViewOfSection from kernel mode without SSDT hooks?

I mean it's pretty clear that you're a scriptkiddie who thinks he's some amazing malware guru and antivirus expert, but I'll pretend to believe what you say. If you want I'll give you extra points for knowing what IDA is.

"Avast antivirus increments an integer value for each time one of the above functions is called. Of course, it would have to check parameters to increment the specified integer for the specified process.

Once that integer reaches 3, it is detected as a virus."

Your short term memory isn't great, might want to get that checked out.

You're 150% right bro. Absolutely. It's impossible to hook the kernel without using SSDT hooks. Absolutely 150% correct. Actually, you're 2000% correct.

You can only hook the kernel with SSDT hooks.

Spoiler [\(Click to View\)](#)

Hilarious. Just hilarious.

Now go troll someone else.

Thanks.

IRP_MJ_SCSI - February 7, 2014, 4:04 pm

(Feb 7, 2014 05:03 PM)Feminist Wrote: [\[CITE\]](#) You're 150% right bro. Absolutely. It's impossible to hook the kernel without using SSDT hooks. Absolutely 150% correct. Actually, you're 2000% correct.

You can only hook the kernel with SSDT hooks.

Spoiler [\(Click to View\)](#)

Hilarious. Just hilarious.

Now go troll someone else.

Thanks.

Are you trolling because you can't answer my question or because you legitimately think that somewhere in this thread I said "it is impossible to hook the kernel without using SSDT hooks".

Again more evidence of your reading disability.

Reporter - February 7, 2014, 5:22 pm

Same price as any crypter, how long its FUD that matter

~Tom~ - February 7, 2014, 6:49 pm

(Feb 7, 2014 01:31 AM)N3oNight Wrote: [\[CITE\]](#) it dosent matter if uses runpe or not, the thing matter is for how many days or how long will it be FUD.

??? As you can probably see from the replies in this thread hf isn't the place to be selling such crypter.

Raz?r - February 7, 2014, 7:00 pm

It is not even hard to make a runpe runtime FUD.

If you just C&P a public one it will be detected instantly, sure - but if you code one and modify it you can get it runtime FUD without any problem.

Good luck with your product, but 1. i think this is the wrong place to sell it and 2. you should actually stick to the truth when posting such "facts".

-Doesn't mean that i don't think runpes are overused, but if done right it is still effective.

Feminist - February 7, 2014, 7:07 pm

(Feb 7, 2014 08:00 PM)Raz?r Wrote: [\[CITE\]](#) It is not even hard to make a runpe runtime FUD.

If you just C&P a public one it will be detected instantly, sure - but if you code one and modify it you can get it runtime FUD without any problem.

Good luck with your product, but 1. i think this is the wrong place to sell it and 2. you should actually stick to the truth when posting such "facts".

-Doesn't mean that i don't think runpes are overused, but if done right it is still effective.

And by "code and modify" you mean changing variable names and adding junk code.

AutoIT.

Of course you are going to blatantly defend RunPE when you have a product to sell on this forum. The truth of the matter is that changing variable names and adding junk code isn't going to make your RunPE bypass AV's that actually look for things.

What facts? Care to elaborate which "facts" I am posting which are false?

Raz?r - February 7, 2014, 7:35 pm

(Feb 7, 2014 08:07 PM)Feminist Wrote: [\[CITE\]](#) And by "code and modify" you mean changing variable names and adding junk code.

AutoIT.

Of course you are going to blatantly defend RunPE when you have a product to sell on this forum. The truth of the matter is that changing variable names and adding junk code isn't going to make your RunPE bypass AV's that actually look for things.

What facts? Care to elaborate which "facts" I am posting which are false?I'm not going to argue

about AutoIT here, i already know that it gets called a "bad" language because of it's stub size and don't care about people with such ridiculous arguments.

In fact modifying variable names & adding junk code will not help against the most runtime detection (there are still shitty AVs that get confused by junk on runtime too - add 1M lines of junk to something runtime detected by bitdefender and watch what happens when you execute it - this is no solution that should be used to bypass runtime detection, but well just saying that it works on some AVs).

And sure i am "defending" runpes, as they still work - i know that they could get detected or even blocked very easily by AVs, but tell that the AV-companies as you can still bypass ALL AVs using a runpe without any problem. It is not my fault that AV-companies missed to fix this for years. The max you will ever get with a completely unknown runpe is a PUA detection and well if you ever needed to get around a PUA detection you know that it is no big deal.

Well you are implying that it is fact that runpes can't bypass AVs anymore - if you do some testing you will find out that it is not true very fast. Kaspersy, ESET, Norton - all the "big" AVs will fail detecting a runpe once it gets modified a bit and not using the common scheme.

? Razor

P.S.:

Also if you want to argue a bit about AutoIT, please do me a favor and take a look at the benefits of an interpreted language that works like AutoIT when it comes to this topic.

IRP_MJ_SCSI - February 7, 2014, 8:04 pm

@OP: I see you didn't answer my question because you don't know the answer. Just how i expected.

Edit: I came to hackforums expecting to see people arguing about how good AutoIT is for malware, wasn't disappointed. Only forum on the entire internet where AutoIT malware is acceptable. You're right about RunPe still being fuddable, but the only people who argue that AutoIT is good are people who cannot code anything better.

Feminist - February 7, 2014, 8:13 pm

(Feb 7, 2014 09:04 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) @OP: I see you didn't answer my question because you don't know the answer. Just how i expected.

Edit: I came to hackforums expecting to see people arguing about how good AutoIT is for malware, wasn't disappointed. Only forum on the entire internet where AutoIT malware is acceptable. You're right about RunPe still being fuddable, but the only people who argue that AutoIT is good are people who cannot code anything better.

That's because you never asked a question. You might be able to make RunPE FUD scantime, but the cookie cutter RunPE will not fool good AV's during runtime.

IRP_MJ_SCSI - February 7, 2014, 8:18 pm

(Feb 7, 2014 09:13 PM)Feminist Wrote: [\[CITE\]](#) That's because you never asked a question. You might be able to make RunPE FUD scantime, but the cookie cutter RunPE will not fool good AV's during runtime.

I will write a fud RunPe and show you it being undetected on runtime to every av when i have time.

Question was: how are you going to know if program calls NtUnmapViewOfSection or WriteProcessMemory using kernel mode hooks if you cant hook SSDT.

Feminist - February 7, 2014, 8:19 pm

(Feb 7, 2014 09:18 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) I will write a fud RunPe and show you it being undetected on runtime to every av when i have time.

Question was: how are you going to know if program calls NtUnmapViewOfSection or WriteProcessMemory using kernel mode hooks if you cant hook SSDT.

There are other ways to hook the kernel besides using SSDT hooks.

IRP_MJ_SCSI - February 7, 2014, 8:21 pm

(Feb 7, 2014 09:19 PM)Feminist Wrote: [\[CITE\]](#) There are other ways to hook the kernel besides using SSDT hooks.

I didn't ask if there are other ways I asked how are YOU going to do it, because I'm very sure you don't know the answer. If you really have reversed AVs and you're as smart as you think you are, you'd be able to explain about detecting such calls from kernel mode with patchguard enabled.

Feminist - February 7, 2014, 8:23 pm

(Feb 7, 2014 09:21 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) I didn't ask if there are other ways I asked how are YOU going to do it, because I'm very sure you don't know the answer.

Firstly, your whole argument on SSDT hooks is based on x64 operating systems. Many people still use x86 operating systems. With addition to that, I never stated that I programmed drivers. I stated that I reverse engineered avast antivirus to determine how its internals work.

With response to your updated post. I would be happy to tell you Avasts methodologies on x64 bit windows. However, I do not have a 64 bit computer. I have a 32 bit computer. If you provide me with Avast driver files for x64 bit and buy me the newest version of IDA Pro with support for 64 bit files; I will gladly analyze it and tell you anything you want to know.

I have only analyzed the 32 bit version of Avast.

The most common hooks I see in the kernel are either SSDT hooks, shadow SSDT hooks, or directly writing to the kernels memory and adding a jump.

IRP_MJ_SCSI - February 7, 2014, 8:27 pm

(Feb 7, 2014 09:23 PM)Feminist Wrote: [\[CITE\]](#) Firstly, your whole argument on SSDT hooks is based on x64 operating systems. Many people still use x86 operating systems. With addition to that, I never stated that I programmed drivers. I stated that I reverse engineered avast antivirus to determine how its internals work.

Well if you had reversed antiviruses, you'd know how the work on x64, but clearly they don't.

Yes my argument is based on x64 operating systems, because I've already stated that SSDT hooks use complex heuristics and can be bypassed by mixing things up. The whole x64 argument is just to further prove you have no idea what you're talking about.

:EDIT: lol at having a 32-bit computer, I thought a master researcher such as yourself would at least have a few VMs and more than 4gb of ram.

Feminist - February 7, 2014, 8:30 pm

(Feb 7, 2014 09:27 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) Well if you had reversed antiviruses, you'd know how the work on x64, but clearly they don't.

Yes my argument is based on x64 operating systems, because I've already stated that SSDT hooks use complex heuristics and can be bypassed by mixing things up. The whole x64 argument is just to further prove you have no idea what you're talking about.

You were asking me what Avast does on 64 bit operating systems. I cannot tell you how its drivers work on 64 bit operating systems. You are clearly trying to cause confusion to try and make it seem like you know what you are talking about.

You are the one who does not know what he is talking about. Clearly Avast will not use the same driver files for x86 and x64.

(Feb 7, 2014 09:27 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) Well if you had reversed antiviruses, you'd know how the work on x64, but clearly they don't.

Yes my argument is based on x64 operating systems, because I've already stated that SSDT hooks use complex heuristics and can be bypassed by mixing things up. The whole x64 argument is just to further prove you have no idea what you're talking about.

:EDIT: lol at having a 32-bit computer, I thought a master researcher such as yourself would at least have a few VMs and more than 4gb of ram.
You just get dumber by the minute.

I cannot have a 64 bit VM on my 32 bit computer for the following reasons:

1. I use VirtualBox
2. QEMU is too slow to work with (way too slow)
3. My processor doesn't have VT bit. My processor is 32 bit.

As of now, I've officially deemed you a troll and have decided to stop replying to your posts

IRP_MJ_SCSI - February 7, 2014, 8:39 pm

(Feb 7, 2014 09:30 PM)Feminist Wrote: [\[CITE\]](#) You were asking me what Avast does on 64 bit operating systems. I cannot tell you how its drivers work on 64 bit operating systems. You are clearly trying to cause confusion to try and make it seem like you know what you are talking about.

You are the one who does not know what he is talking about. Clearly Avast will not use the same driver files for x86 and x64.

Holy donkey balls christ. Now you're saying that I should have a 64 bit VM on a 32 bit windows host. You clearly have no idea what you're talking about and you are just a troll.

I'm actually not sure if you have special needs or just minor reading issues, You've misquoted or twisted my words at least 4 times in this post and 12+ times in this thread.

As a kernel driver developer and a long time malware researcher, it's fun to watch you fail. Anyone who was at all competent wouldn't be twisting my words and dancing around my questions. It's very clear you don't understand malware or antivirus internals other than what you learnt from some basic crypter development. RunPE is undesirable because the new process you create can be picked up by the emulator (so any anti-emulation you did in the previous process won't apply to the payload you just RunPE'd). RunPE is also frowned upon because of a misconception from HF skids (you) who are so used to seeing people using copy and paste RunPE that they have some idea that ALL RunPE code is runtime detected.

Please read my post at least 10 times to avoid misreading / misinterpreting my words again.

Feminist - February 7, 2014, 8:44 pm

(Feb 7, 2014 09:39 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) I'm actually not sure if you have special needs or just minor reading issues, You've misquoted or twisted my words at least 4 times in this post and 12+ times in this thread.

As a kernel driver developer and a long time malware researcher, it's fun to watch you fail. Anyone who was at all competent wouldn't be twisting my words and dancing around my questions. It's very clear you don't understand malware or antivirus internals other than what you learnt from some basic crypter development. RunPE is undesirable because the new process you create can be picked up by the emulator (so any anti-emulation you did in the previous process won't apply to the payload you just RunPE'd). RunPE is also frowned upon because of a misconception from HF skids (you) who are so used to seeing people using copy and paste RunPE that they have some idea that ALL RunPE code is runtime detected.

Please read my post at least 10 times to avoid misreading / misinterpreting my words again. You are the one who is twisting my words. You clearly suffer from some kind of retardation or you are a troll.

RunPE simply stands for run portable executable. Of course there are "many ways of doing this" but the cookie cutter HackForums code being copy pasted around here will be detected at runtime by every good antivirus.

In fact, my own version is technically RunPE, despite mapping the executable in its own memory using only VirtualAlloc. However, "RunPE" has a different meaning on HackForums than it does elsewhere and you have to understand that.

You are the one with reading issues, who continues to misquote me and take things out of context, as well as assume things.

I know I said I wouldn't further reply and feed the troll, but this is getting ridiculous now.

You are probably just mad because you are unable to code anything aside from something you copy pasted.

There is the door ---->

Have a good day

Raz?r - February 7, 2014, 9:03 pm

(Feb 7, 2014 09:44 PM)Feminist Wrote: [\[CITE\]](#) You are the one who is twisting my words. You clearly suffer from some kind of retardation or you are a troll.

RunPE simply stands for run portable executable. Of course there are "many ways of doing this" but the cookie cutter HackForums code being copy pasted around here will be detected at runtime by every good antivirus.

In fact, my own version is technically RunPE, despite mapping the executable in its own memory using only VirtualAlloc. However, "RunPE" has a different meaning on HackForums than it does elsewhere and you have to understand that.

You are the one with reading issues, who continues to misquote me and take things out of context, as well as assume things.

I know I said I wouldn't further reply and feed the troll, but this is getting ridiculous now.

You are probably just mad because you are unable to code anything aside from something you copy pasted.

There is the door ---->

Have a good day So you are using a runpe too, but are using a different method then most crypters here.

You can charge \$30 a month instead of \$20.

End of thread.

runNgun - February 7, 2014, 9:07 pm

Monthly should be about \$200 if coded properly. Get a small group of customers.

IRP_MJ_SCSI - February 7, 2014, 9:10 pm

(Feb 7, 2014 09:44 PM)Feminist Wrote: [\[CITE\]](#) You are the one who is twisting my words. You clearly suffer from some kind of retardation or you are a troll.

RunPE simply stands for run portable executable. Of course there are "many ways of doing this" but the cookie cutter HackForums code being copy pasted around here will be detected at runtime by every good antivirus.

In fact, my own version is technically RunPE, despite mapping the executable in its own memory using only VirtualAlloc. However, "RunPE" has a different meaning on HackForums than it does elsewhere and you have to understand that.

You are the one with reading issues, who continues to misquote me and take things out of context, as well as assume things.

I know I said I wouldn't further reply and feed the troll, but this is getting ridiculous now.

You are probably just mad because you are unable to code anything aside from something you copy pasted.

There is the door ---->

Have a good day facepalm Claims crypter doesn't use runpe -> admits it uses runpe.

Feminist - February 7, 2014, 9:13 pm

(Feb 7, 2014 10:10 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) *facepalm* Claims crypter doesn't use runpe -> admits it uses runpe.

There you are again, twisting my words. In the HackForums definition of RunPE it is not; it only uses VirtualAlloc. However, RunPE = Run Portable Executable. And what does it do? Just that.

Its pretty obvious who you are "TouchMe" a notorious skid and ban evader from Betamonkeys chatroom who thinks he is an experienced programmer because he can follow the book "rootkits subverting the windows kernel."

So please, before you troll my thread have a good look at your own self and start skidding away and Mexico.

salmonesus - February 7, 2014, 9:19 pm

well coding a crypter and maintaining it are two very different skill sets first of all...

and second - what you do for no relocation tables?

i had severe problems with this and andromeda bot...

i self relocated and then unmapped original exe to place imagebase of andro to it's rightful position (0x400000) but SOMETHING was allocating the memory at 0x400000 so i COULD NOT free it or find out who allocate it! it seemed to be allocated by the kernel or something, i mean anyone have encountered this before? is really weird, because it would work 50% of the time and then the other half it would fail with this mystery memory that could not be freed.

btw u can make runpe HIPS fud no problem...

Feminist - February 7, 2014, 9:22 pm

(Feb 7, 2014 10:19 PM)salmoneus Wrote: [\[CITE\]](#) well coding a crypter and maintaining it are two very different skill sets first of all...

and second - what you do for no relocation tables?

i had severe problems with this and andromeda bot...

i self relocated and then unmapped original exe to place imagebase of andro to it's rightful position (0x400000) but SOMETHING was allocating the memory at 0x400000 so i COULD NOT free it or find out who allocate it! it seemed to be allocated by the kernel or something, i mean anyone have encountered this before? is really weird, because it would work 50% of the time and then the other half it would fail with this mystery memory that could not be freed.

btw u can make runpe HIPS fud no problem...

If there is no relocation table, I set the imagebase to a lower value than the targets imagebase so there is enough space to be mapped in memory.

I have not encountered that problem before. You could try changing the imagebase of the executable. Unless there are any static coded values inside, it will work.

salmoneus - February 7, 2014, 9:24 pm

(Feb 7, 2014 10:22 PM)Feminist Wrote: [\[CITE\]](#) If there is no relocation table, I set the imagebase to a lower value than the targets imagebase so there is enough space to be mapped in memory.

I have not encountered that problem before. You could try changing the imagebase of the executable. Unless there are any static coded values inside, it will work.

image base of the mapper exe was 0xA400000

betamonkey - February 7, 2014, 9:24 pm

When Feminist said his was technically 'RunPE', he meant it differently then what people here believe it to be. He clarified himself as well but I dunno why no one here is acknowledging that. RunPE on this forum typically means spawn new process but in his instance, as he explained, he meant it as executing a PE file within the same process. Also whether anyone wants to take my word for it or not, Feminist is a smart guy (albeit a super annoying troll at times).

IRP_MJ_SCSI - February 7, 2014, 9:26 pm

(Feb 7, 2014 10:24 PM)betamonkey Wrote: [\[CITE\]](#) When Feminist said his was technically 'RunPE', he meant it differently then what people here believe it to be. He clarified himself as well but I dunno why no one here is acknowledging that. RunPE on this forum typically means spawn new process but in his instance, as he explained, he meant it as executing a PE file within the same process. Also whether anyone wants to take my word for it or not, Feminist is a smart guy (albeit a super annoying troll at times).

Within 5 minutes of mentioning your name you come and back people up. Allow me to try.

Betamonkey.

Also VirtualAlloc is a fucking shit what to allocate into your own process, you've lowered your standards if you're calling him smart.

Feminist - February 7, 2014, 9:26 pm

(Feb 7, 2014 10:24 PM)betamoney Wrote: [\[CITE\]](#) When Feminist said his was technically 'RunPE', he meant it differently then what people here believe it to be. He clarified himself as well but I dunno why no one here is acknowledging that. RunPE on this forum typically means spawn new process but in his instance, as he explained, he meant it as executing a PE file within the same process. Also whether anyone wants to take my word for it or not, Feminist is a smart guy (albeit a super annoying troll at times).

Appreciate the kind words.

(Feb 7, 2014 10:24 PM)salmoneus Wrote: [\[CITE\]](#) image base of the mapper exe was 0xA400000 I meant change the image base of the target you crypted, you could try that- it would fail sometimes if there are static coded values.

(Feb 7, 2014 10:26 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) Within 5 minutes of mentioning your name you come and back people up. Allow me to try.

Betamoney.

Also VirtualAlloc is a fucking shit what to allocate into your own process, you've lowered your standards if you're calling him smart.

I check return values and have alternatives on failure. There is nothing wrong with VA

IRP_MJ_SCSI - February 7, 2014, 9:28 pm

(Feb 7, 2014 10:26 PM)Feminist Wrote: [\[CITE\]](#) I meant change the image base of the target you crypted, you could try that- it would fail sometimes if there are static coded values.

Not sure if trolling or retarded....

Feminist - February 7, 2014, 9:31 pm

(Feb 7, 2014 10:28 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) Not sure if trolling or retarded....

Do tell why that would be a bad idea- except for the statement I made?

IRP_MJ_SCSI - February 7, 2014, 9:37 pm

(Feb 7, 2014 10:31 PM)Feminist Wrote: [\[CITE\]](#) Do tell why that would be a bad idea- except for the statement I made?

It would fail more than sometimes, more like 90% of the time. Images have imagebases for a reason, it's not position independent code.

On a side note, for someone who's calling me a skid, I'd at least expect you to be using NtMapViewOfSection, not VirtualAlloc.

Feminist - February 7, 2014, 9:39 pm

(Feb 7, 2014 10:37 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) It would fail more than sometimes, more like 90% of the time. Images have imagebases for a reason, it's not position independent code.

On a side note, for someone who's calling me a skid, I'd at least expect you to be using NtMapViewOfSection, not VirtualAlloc.

Doing that is not necessary. VirtualAlloc is just fine. Fail more than 90% of the time? That's a joke. Maybe for specific malware that uses direct addresses to access data (then it would fail all the time).

My crypter does not change the image base of the crypted target; only of the stub (if no .reloc

section is present) and only when necessary

IRP_MJ_SCSI - February 7, 2014, 9:47 pm

(Feb 7, 2014 10:39 PM)Feminist Wrote: [\[CITE\]](#) Doing that is not necessary. VirtualAlloc is just fine. Fail more than 90% of the time? That's a joke. Maybe for specific malware that uses direct addresses to access data (then it would fail all the time).

My crypter does not change the image base of the crypted target; only of the stub (if no .reloc section is present) and only when necessary

I thought you said change the image base of the crypted target, but never-mind.

Shad~ - February 7, 2014, 10:08 pm

(Feb 7, 2014 10:16 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) Wow, you're calling me a skid? Hahahha that's hilarious. If I'm a skid, I have some very bad news for you.

At least i can code a crypter that isn't some virtualalloc runpe shit.

While I like drama sometimes why the fuck do you have to consistently attempt to belittle others on every fucking board? You're more intelligent than most people in the scene today I get that. How about teaching others instead of bashing them?

~ OP As Beta and the other guy said please don't sell this to hundreds of idiots keep it small with a higher monthly price.

IRP_MJ_SCSI - February 7, 2014, 10:11 pm

(Feb 7, 2014 11:08 PM)Shad~ Wrote: [\[CITE\]](#) While I like drama sometimes why the fuck do you have to consistently attempt to belittle others on every fucking board? You're more intelligent than most people in the scene today I get that. How about teaching others instead of bashing them?

~ OP As Beta and the other guy said please don't sell this to hundreds of idiots keep it small with a higher monthly price.

It's not like i came in the thread and called him a retard right of the bat, I corrected him and then shit escalated into an argument :\

Feminist - February 7, 2014, 10:25 pm

Hilarious about him calling my crypter shit when he hasn't seen it and it is still in development. He doesn't even have a sample of it. And guess what, even if he did, and I did not use any kind of antidebug or file protectors; he would still not be able to RCE it because of his sheer skiddyness

In fact, I've never actually seen him code anything. All he does is "talk" about stuff he does.

TouchMe, you're hopelessly retarded and skiddy. I remember reading your blog post about you RCEing betamonkeys bot (and you actually didnt, you just posted generic information that i gave you over IRC and some bullshit news on the topic (not very RCE like))

I also remember you begging me for my IDA pro database that listed up all the imports on betabot and my analysis of it. Pretty funny for a self proclaimed "pro coder, pro driver development, and pro RCE" If you can't do such a simple task such as that, then you really aren't as smart as you think you are.

I know 12 year old kids who can RCE better than you can, and code better than you can.

I completely RCE'd betamonkeys bot, but never released it. I'm pretty sure he still remembers that (as well as his injection method)

/argument

IRP_MJ_SCSI - February 7, 2014, 10:41 pm

(Feb 7, 2014 11:25 PM)Feminist Wrote: [\[CITE\]](#) Hilarious about him calling my crypter shit when he hasn't seen it and it is still in development. He doesn't even have a sample of it. And guess what, even if he did, and I did not use any kind of antidebug or file protectors; he would still not be able to RCE it because of his sheer skiddyness

In fact, I've never actually seen him code anything. All he does is "talk" about stuff he does.

TouchMe, you're hopelessly retarded and skiddy. I remember reading your blog post about you RCEing betamonkeys bot (and you actually didnt, you just posted generic information that i gave you over IRC and some bullshit news on the topic (not very RCE like))

I also remember you begging me for my IDA pro database that listed up all the imports on betabot and my analysis of it. Pretty funny for a self proclaimed "pro coder, pro driver development, and pro RCE" If you can't do such a simple task such as that, then you really aren't as smart as you think you are.

I know 12 year old kids who can RCE better than you can, and code better than you can.

I completely RCE'd betamonkeys bot, but never released it. I'm pretty sure he still remembers that (as well as his injection method)

/argument

Link to my skiddie code, link to evidence of me being a skiddie at reversing, log of me begging you for betabot imports, link to my blog post claiming to reverse betabot and evidence of you giving me info about betabot, thanks.

Feminist - February 7, 2014, 10:43 pm

(Feb 7, 2014 11:41 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) Link to my skiddie code and link to evidence of me being a skiddie at reversing, thanks.

Or, like you expect others to do, how about you link some things you have reverse engineered and coded to prove that you are not a skid?

Crake - February 7, 2014, 10:44 pm

Nobody cares about your crypting method, only about the results it shows in terms of FUD time.

IRP_MJ_SCSI - February 7, 2014, 10:54 pm

(Feb 7, 2014 11:43 PM)Feminist Wrote: [\[CITE\]](#) Or, like you expect others to do, how about you link some things you have reverse engineered and coded to prove that you are not a skid?

No, you're the one saying my code is skiddie so you must have seen my code in order to label it as skiddie. Either that or you're full of shit (Now i remember why no one at voidptr liked you).

Anyway don't let me stop you making shit up, why don't you also tell everyone how i worshiped you and said you were the best coder I've ever seen then i asked to have have a go in you Lamborghini and on your \$200m yacht. Everything you said in that post was bullshit and we both know it, you never even finished reversing betabot.

Dam Son - February 8, 2014, 1:38 am

The only thing that really matter is the FUD time.

I don't think any customer really cares the method of delivery.

Cakeb\$\$\$ - February 8, 2014, 2:52 am

Holy shit I'm impressed. You have managed to keep your sandbox level of fight going for six pages. Good job.

Feminist - February 8, 2014, 6:43 am

(Feb 8, 2014 02:47 AM)Conqueror Wrote: [\[CITE\]](#) So what's the pro using loadPe instead of a runpe besides don't use detected APIS by just some hips ? Can you bypass memory scanner AVs based ? No, but I do have plans that I might implement to make it undetectable by AV's memory based. I will weigh the pro's and cons of implementing such a feature.

My method is lightweight and is not detected by antiviruses. cookie cutter RunPE may be scantime FUD, and it may get past a few av's on runtime but it won't get past any good AV's

(Feb 8, 2014 03:52 AM)yugurt Wrote: [\[CITE\]](#) Holy shit I'm impressed. You have managed to keep your sandbox level of fight going for six pages. Good job.

It wasn't even a fight. Just some skid called TouchMe trying to troll. Unfortunately, he picked a poor target to troll. Not only is he a copy pasting scriptkiddy who vastly exaggerates about his few accomplishments, but I don't give up.

IRP_MJ_SCSI - February 8, 2014, 8:01 am

(Feb 8, 2014 07:43 AM)Feminist Wrote: [\[CITE\]](#) No, but I do have plans that I might implement to make it undetectable by AV's memory based. I will weigh the pro's and cons of implementing such a feature.

My method is lightweight and is not detected by antiviruses. cookie cutter RunPE may be scantime FUD, and it may get past a few av's on runtime but it won't get past any good AV's

It wasn't even a fight. Just some skid called TouchMe trying to troll. Unfortunately, he picked a poor target to troll. Not only is he a copy pasting scriptkiddy who vastly exaggerates about his few accomplishments, but I don't give up.

If I'm so bad at trolling why are you so butthurt? "waaaahaaahaaa you're a skiddie who copy and pastes". You're sat here making basic crappy crypters and calling everyone you don't like a skid, congratulations! You've officially failed at life, you were even more successful when you were sat in IRC all day ranting about how much you hate women...

I've pastebined your posts accusing me of being a copy and paste skid so that others can laugh, maybe in a few years you'll read them and see what a typical hf kid you've turned into, accusing people of copy and pasting without seeing any of their code.

<http://pastebin.com/GzRMHXYF>

<http://pastebin.com/i3djX4JW>

Feminist - February 8, 2014, 8:12 am

(Feb 8, 2014 09:01 AM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) If I'm so bad at trolling why are you so butthurt? "waaaahaaahaaa you're a skiddie who copy and pastes". You're sat here making basic crappy crypters and calling everyone you don't like a skid, congratulations! You've officially failed at life, you were even more successful when you were sat in IRC all day ranting about how much you hate women...

You are the only person I've killed a skid on this thread, and you know its true. Why don't you go beg other people for some IDA databases or content for your crap blog?

I don't hate women. I am just against feminism. People like you (white knight manginas who suck women feet and worship them in futile attempts to get laid) are the reason why men have it so bad

in the legal system in America.

IRP_MJ_SCSI - February 8, 2014, 8:15 am

(Feb 8, 2014 09:12 AM)Feminist Wrote: [\[CITE\]](#) You are the only person I've killed a skid on this thread, and you know its true. Why don't you go beg other people for some IDA databases or content for your crap blog?

I don't hate women. I am just against feminism. People like you (white knight manginas who suck women feet and worship them in futile attempts to get laid) are the reason why men have it so bad in the legal system in America.

You're funny. You've turned into a typical HF idiot with your "skid" and "copy & paster" insults. Your parents must be so proud.

Tell me what sort of reverse engineering guru ends up on HF selling crypters, hint: not a very good one.

Feminist - February 8, 2014, 8:19 am

(Feb 8, 2014 09:15 AM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) You're funny. You've turned into a typical HF idiot with your "skid" and "copy & paster" insults. Your parents must be so proud.

Tell me what sort of reverse engineering guru ends up on HF selling crypters, hint: not a very good one.

Bro, I sell hacks for video games and I've completely emulated hackshield before. If I were a skid reverse engineer and you were a pro reverse engineer why were you begging me for my IDA database of betabot a while back?

Although I'm not one of the "best" reverse engineers, I am quite skilled at what I do and have reverse engineered many applications. I was one of the first 20 people to analyze VMProtect and one of the few people able to unpack Themida... I create MapleStory private server clients for servers and I bet I make more in one week than you do in a month.

Stop trolling son. Selling shit crypters on HackForums? You've never even seen my cryper, and added revenue is always good.

You're just mad because you have to wipe your ass with leaves down in Mexico.

EDIT: Heck, I bet I make more money for doing one job than you do per year.

IRP_MJ_SCSI - February 8, 2014, 8:22 am

(Feb 8, 2014 09:19 AM)Feminist Wrote: [\[CITE\]](#) Bro, I sell hacks for video games and I've completely emulated hackshield before. If I were a skid reverse engineer and you were a pro reverse engineer why were you begging me for my IDA database of betabot a while back?

Although I'm not one of the "best" reverse engineers, I am quite skilled at what I do and have reverse engineered many applications. I was one of the first 20 people to analyze VMProtect and one of the few people able to unpack Themida... I create MapleStory private server clients for servers and I bet I make more in one week than you do in a month.

Stop trolling son. Selling shit crypters on HackForums? You've never even seen my cryper, and added revenue is always good.

You're just mad because you have to wipe your ass with leaves down in Mexico.

hello hackforums I'm elite RCE guru first person to unpack vmprotect, how much my non-runpe

crypter that uses runpe sell for? Plz i need 2 buy food.

Feminist - February 8, 2014, 8:24 am

(Feb 8, 2014 09:22 AM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) hello hackforums I'm elite RCE guru first person to unpack vmprotect, how much my non-runpe crypter that uses runpe sell for? Plz i need 2 buy food.

I never said I was the first person, I said I was one of the first 20 to analyze and unpack it.

IRP_MJ_SCSI - February 8, 2014, 8:26 am

(Feb 8, 2014 09:24 AM)Feminist Wrote: [\[CITE\]](#) I never said I was the first person, I said I was one of the first 20 to analyze and unpack it.

hello hackforums I'm elite RCE guru first of 20 people to analyze vmprotect (i know this because every time someone opens vmprotect bin in debugger it alerts me), how much my non-runpe crypter that uses runpe sell for? Plz i need 2 buy food.

OnlyBOTNET - February 8, 2014, 8:41 am

(Feb 8, 2014 09:26 AM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) hello hackforums I'm elite RCE guru first of 20 people to analyze vmprotect (i know this because every time someone opens vmprotect bin in debugger it alerts me), how much my non-runpe crypter that uses runpe sell for? Plz i need 2 buy food.haha at first i was thinking you know a little bit,just a LITTLE bit.

But now i think you are a complete skid that all he knows is html,good luck hahaha

Feminist - February 8, 2014, 8:48 am

(Feb 8, 2014 09:26 AM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) hello hackforums I'm elite RCE guru first of 20 people to analyze vmprotect (i know this because every time someone opens vmprotect bin in debugger it alerts me), how much my non-runpe crypter that uses runpe sell for? Plz i need 2 buy food.

Wow, you are beyond skid. Do you release that when someone analyzes a file and releases it on the internet it shows to everyone?

By the way, thanks for keeping my thread on the first page at all times. I appreciate your skiddy trolling because it is actually beneficial to me.

OnlyBOTNET - February 8, 2014, 8:51 am

(Feb 8, 2014 09:48 AM)Feminist Wrote: [\[CITE\]](#) Wow, you are beyond skid. Do you release that when someone analyzes a file and releases it on the internet it shows to everyone?

By the way, thanks for keeping my thread on the first page at all times. I appreciate your skiddy trolling because it is actually beneficial to me.

Like they say..any publicity is good publicity.

Indaclub - February 8, 2014, 10:38 am

(Feb 7, 2014 04:08 PM)Feminist Wrote: [\[CITE\]](#) Come back to my thread when you have reverse engineered antiviruses, can program something more than a hello world application, and know what you are talking about.

Avast antivirus increments an integer value for each time one of the above functions is called. Of course, it would have to check parameters to increment the specified integer for the specified process.

Once that integer reaches 3, it is detected as a virus.

So please, go away and come back when you have actually reverse engineered something and

know what you are talking about.

Thanks. not a publicly released method? It's called manual mapping. It won't work with every executable.

Your method:

<http://www.ownedcore.com/forums/world-of-warcraft/world-of-warcraft-bots-programs/wow-memory-editing/309563-c-native-dll-mapper.html>

fixes imports, relocs

Alright say the remote process doesn't contain an imported library, what do you do? The entire behind the concept of manually mapping is to not call loadlibrary

(Feb 7, 2014 10:03 PM)Raz?r Wrote: [\[CITE\]](#) So you are using a runpe too, but are using a different method then most crypters here.

You can charge \$30 a month instead of \$20.

End of thread.

a runpe is the process of hollowing a process from its original base and replaced by the physical executable.

His method is mapping the entire process to an allocated block of memory to a running process.

(Feb 8, 2014 09:19 AM)Feminist Wrote: [\[CITE\]](#) Bro, I sell hacks for video games and I've completely emulated hackshield before. If I were a skid reverse engineer and you were a pro reverse engineer why were you begging me for my IDA database of betabot a while back?

Although I'm not one of the "best" reverse engineers, I am quite skilled at what I do and have reverse engineered many applications. I was one of the first 20 people to analyze VMProtect and one of the few people able to unpack Themida... I create MapleStory private server clients for servers and I bet I make more in one week than you do in a month.

Stop trolling son. Selling shit crypters on HackForums? You've never even seen my cryper, and added revenue is always good.

You're just mad because you have to wipe your ass with leaves down in Mexico.

EDIT: Heck, I bet I make more money for doing one job than you do per year.

lol. three calls to malicious functions activates the AV?

Feminist - February 8, 2014, 10:46 am

(Feb 8, 2014 11:38 AM)Indaclub Wrote: [\[CITE\]](#) not a publicly released method? It's called manual mapping. It won't work with every executable.

Your method:

<http://www.ownedcore.com/forums/world-of-warcraft/world-of-warcraft-bots-programs/wow-memory-editing/309563-c-native-dll-mapper.html>

fixes imports, relocs

Alright say the remote process doesn't contain an imported library, what do you do? The entire

behind the concept of manually mapping is to not call loadlibrary

a runpe is the process of hollowing a process from its original base and replaced by the physical executable.

His method is mapping the entire process to an allocated block of memory to a running process.

lol. three calls to malicious functions activates the AV?

Kindly stop trolling my thread, friend of TouchMe. It's clear beyond a doubt you both skids. Go back to writing 'hello worlds' in FASM and copy pasting drivers from your subverting the windows kernel ebook. Thanks.

You are mistaken.

I'm not mapping the executable to a remote process. I'm mapping it to the same process as the stub.

His code is in C#. Mine is written in FASM and it is much different from what you linked.

Don't believe me? Go RCE Avast yourself and see for yourself. I'm awaiting your reply.

"Not a publicly released method" as in it has no been released on the internet. I am using unique methods to fork the executable.

japen1 - February 8, 2014, 10:47 am

Hi,
can anybody help me to build botnets that can take all browser?
I can pay .
For more details please PM me please.
Thank

Indaclub - February 8, 2014, 10:47 am

(Feb 8, 2014 11:46 AM)Feminist Wrote: [\[CITE\]](#) You are mistaken.

I'm not mapping the executable to a remote process. I'm mapping it to the same process as the stub.

His code is in C#. Mine is written in FASM and it is much different from what you linked.

I'm not mapping the executable to a remote process. I'm mapping it to the same process as the stub.

You're still 'manually mapping' it.

It's in c# yes, you can easily convert it. I'm showing that your method is indeed public you fool. It's rather not hard. Especially when you only have to deal with x86 applications.

How is it infact any different? It maps the executable, fixes relocations, fixes imports, aligns sections...

You're lost

Feminist - February 8, 2014, 10:54 am

(Feb 8, 2014 11:47 AM)Indaclub Wrote: [\[CITE\]](#)

I'm not mapping the executable to a remote process. I'm mapping it to the same process as the stub.

You're still 'manually mapping' it.

It's in c# yes, you can easily convert it. I'm showing that your method is indeed public you fool. It's rather not hard. Especially when you only have to deal with x86 applications.

How is it infact any different? It maps the executable, fixes relocations, fixes imports, aligns sections...

You're lost

With that logic, crypters are the same as file protectors. Armadillo is the same as ASProtect. UPX is the same as VMProtect and Themida.

Your logic is indeed flawed and is a fallacy. I am doing much more than just "mapping the executable" and my crypter is still in development.

What is the difference between same process mapping and remote process mapping? Its an unbelievable question you indirectly ask me. The difference is several API calls... which in turn results in the difference from Avast detecting your malware or not detecting your malware.

PS: Its clear that you know how badly your logic is being defeated, since your little friend TouchMe reported my account and had my image and signature removed. Very low of you to use such attacks in a debate... unless you know you are losing and will resort to anything to try and get your opponent to submit.

Indaclub - February 8, 2014, 10:54 am

(Feb 8, 2014 11:54 AM)Feminist Wrote: [\[CITE\]](#) With that logic, crypters are the same as file protectors. Armadillo is the same as ASProtect. UPX is the same as VMProtect and Themida.

Your logic is indeed flawed and is a fallacy. I am doing much more than just "mapping the executable" and my crypter is still in development.

Yep, you have no idea as to what you're talking about.

Good luck with the project and all.

Feminist - February 8, 2014, 10:58 am

(Feb 8, 2014 11:54 AM)Indaclub Wrote: [\[CITE\]](#) Yep, you have no idea as to what you're talking about.

Good luck with the project and all.

You clearly don't know what you are talking about if you come to my thread and post such nonsense. Exactly what don't I know? Care to elaborate?

Thanks.

Dam Son - February 8, 2014, 11:56 am

(Feb 8, 2014 11:58 AM)Feminist Wrote: [\[CITE\]](#) You clearly don't know what you are talking about if you come to my thread and post such nonsense. Exactly what don't I know? Care to elaborate?

Thanks.

So you said you only had 32 bit copmuter.

Now, you've magically reverse engineered x64 Avast and know all its internals? lol

Feminist - February 8, 2014, 12:02 pm

(Feb 8, 2014 12:56 PM)vaXine Wrote: [\[CITE\]](#) So you said you only had 32 bit copmuter.

Now, you've magically reverse engineered x64 Avast and know all its internals? lol

More reading disordered kids coming to aid of their troll friends. He said I don't know what I'm talking about. I told him to tell me what I don't know what I'm talking about and he stopped replying; he knows he has been defeated because he's just a silly troll.

When did I say I RCE'd x64 Avast?

Show me, thanks.

Dam Son - February 8, 2014, 12:20 pm

(Feb 8, 2014 01:02 PM)Feminist Wrote: [\[CITE\]](#) When did I say I RCE'd x64 Avast?

Show me, thanks.Well, obviously you need to if want to start claiming how AVs work.

(Feb 7, 2014 02:41 PM)Feminist Wrote: [\[CITE\]](#) And that no antivirus in the world will detect a file as a virus for calling:

CreateProcessA

NtUnmapViewOfSection

WriteProcessMemory (for each section)

and then setting the context,

CreateRemoteThread

You are saying that no antivirus in the world does that?

Because I'm pretty sure your claim of "legitimate software" doing the above is false. Why not show me one "legit software" that does exactly as stated above?If you knew anything about reverse engineering, you'd know that most of those are standard WinAPI debugging functions, and every debugger uses (and needs to use) them.

Tons of other legitimate software also uses them, memory scanners, sandboxes, etc...

Feminist - February 8, 2014, 12:26 pm

(Feb 8, 2014 01:20 PM)vaXine Wrote: [\[CITE\]](#) Well, obviously you need to if want to start claiming how AVs work.

I stated I RCE Avast 32 bit. Stop taking things out of context. Since the first page I've been talking about why cookie cutter RunPE is garbage and it can't get past Avast.

I'm going to start reporting people if they keep trolling about the same thing like a broken tape recorder. Read prior pages and you'll see the argument is start to repeat itself.

Indaclub - February 8, 2014, 1:54 pm

(Feb 8, 2014 11:58 AM)Feminist Wrote: [\[CITE\]](#) You clearly don't know what you are talking about if you come to my thread and post such nonsense. Exactly what don't I know? Care to elaborate?

Thanks.

I don't even know how you would incorporate any of that logic you specified above to supporting your argument of 'inept logic'

Rather, you're just retarded.

Manually mapping is nothing special.

Feminist - February 8, 2014, 1:58 pm

(Feb 8, 2014 02:54 PM)Indaclub Wrote: [\[CITE\]](#) I don't even know how you would incorporate any of that logic you specified above to supporting your argument of 'inept logic'

Rather, you're just retarded.

Manually mapping is nothing special.

It's not just manually mapping my friend. I have a lot more features that I am working on adding such as protector techniques, a few polymorphic layers, and armadillo CopyMem-II integration (guard pages, except w/ hooks and not process debugging). I'm also considering to add basic virtualization and a few other features I am currently weighing.

Please cease the trolling and raging until you actually get a sample of my product.

Once you get a sample, I'll gladly let you RCE (if you can, which I doubt you would be able to since you are all bark and no bite) and then you can post whatever you want and back it up with evidence.

And since you are not bright enough to figure this out... I will be doing this in an attempt to defeat some memory scanners.

Indaclub - February 8, 2014, 1:59 pm

(Feb 8, 2014 02:58 PM)Feminist Wrote: [\[CITE\]](#) It's not just manually mapping my friend. I have a lot more features that I am working on adding such as protector techniques, a few polymorphic layers, and armadillo CopyMem-II integration (guard pages). I'm also considering to add basic virtualization and a few other features I am currently weighing.

Please cease the trolling and raging until you actually get a sample of my product.

Once you get a sample, I'll gladly let you RCE (if you can, which I doubt you would be able to since you are all bark and no bite) and then you can post whatever you want and back it up with evidence. You should re-read my initial argument, then read the fucking title of your own thread. I could care less if you're implementing more features.

Let me re-iterate, this will not work for every executable.

wacked3 - February 8, 2014, 3:52 pm

I also find RunPE stupid and encourage anyone to try something else.

(Feb 8, 2014 02:59 PM)Indaclub Wrote: [\[CITE\]](#) Let me re-iterate, this will not work for every executable. It will work if you just find a way to map it always at its expected base. For that you most probably need to find a way to unmap your crypter exe and then still have code running.

(Feb 7, 2014 12:40 AM)Feminist Wrote: [\[CITE\]](#) ... an API hooked with a ring0kit such as SetWindowsHookEx ...WHAT?

(Feb 7, 2014 12:40 AM)Feminist Wrote: [\[CITE\]](#) I will implement "add to startup" and "install" features. Why?

(Feb 7, 2014 12:40 AM)Feminist Wrote: [\[CITE\]](#) How much would you pay for this per month? If you can promise FUD files every damn time 500 per week is the normal Russian price for unlimited

crypts.

(Feb 7, 2014 08:35 PM)Raz?r Wrote: [\[CITE\]](#) I'm not going to argue about AutoIT here, i already know that it gets called a "bad" language because of it's stub size and don't care about people with such ridiculous arguments. Even though I agree that size isn't that much of a concern anymore (I have argued this multiple times before, if it interestes you go search for yourself) - RunPE looks basically the same in every language so why not just use a proper one? How about the fact that your AutoIT source can be easily recovered which might help to create generic detections?

(Feb 7, 2014 08:35 PM)Raz?r Wrote: [\[CITE\]](#) Also if you want to argue a bit about AutoIT, please do me a favor and take a look at the benefits of an interpreted language that works like AutoIT when it comes to this topic. Please enlighten us.

(Feb 7, 2014 09:23 PM)Feminist Wrote: [\[CITE\]](#) I stated that I reverse engineered avast antivirus to determine how its internals work. Avast's Sandbox is a joke so I don't think that the rest of this AV is any better.

In fact I know that on x64 systems the 'protection' is entirely in ring3

(Feb 7, 2014 09:23 PM)Feminist Wrote: [\[CITE\]](#) buy me the newest version of IDA Pro with support for 64 bit files; The leaked version has that..

(Feb 7, 2014 10:07 PM)runNgun Wrote: [\[CITE\]](#) Monthly should be about \$200 if coded properly. Get a small group of customers. 500 per week.

(Feb 7, 2014 10:19 PM)salmoneus Wrote: [\[CITE\]](#) well coding a crypter and maintaining it are two very different skill sets first of all... Damn right!

(Feb 7, 2014 10:19 PM)salmoneus Wrote: [\[CITE\]](#) unmapped original exe to place imagebase of andro to it's rightful position (0x400000) but SOMETHING was allocating the memory at 0x400000 so i COULD NOT free it or find out who allocate it! it seemed to be allocated by the kernel or something, i mean anyone have encountered this before? No! I always unmapped my binary at 0x400000 and could then use it without any problems.

(Feb 7, 2014 10:26 PM)Feminist Wrote: [\[CITE\]](#) I meant change the image base of the target you crypted, you could try that- it would fail sometimes if there are static coded values. It will almost always have static values.

(Feb 8, 2014 07:43 AM)Feminist Wrote: [\[CITE\]](#) No, but I do have plans that I might implement to make it undetectable by AV's memory based. I will weigh the pro's and cons of implementing such a feature. How would you do that?

(Feb 8, 2014 09:19 AM)Feminist Wrote: [\[CITE\]](#) I was one of the first 20 people to analyze VMProtect So you were already into reversing in 2003?

(Feb 8, 2014 09:19 AM)Feminist Wrote: [\[CITE\]](#) and one of the few people able to unpack Themida There are damn youtube videos on how to unpack Themida. Plus if you were such a great unpacker you would know that just saying "Themida" is worthless. You also need to talk about the protections enabled to make it possible to adequately evalaute your skillset.

(Feb 8, 2014 11:54 AM)Feminist Wrote: [\[CITE\]](#) I am doing much more than just "mapping the executable" You're also fixing the imports and calling TLS?

(Feb 8, 2014 02:58 PM)Feminist Wrote: [\[CITE\]](#) I'm also considering to add basic virtualization You

are aware that if you have that you can scratch any PE loading?

(Feb 8, 2014 02:58 PM)Feminist Wrote: [\[CITE\]](#) Once you get a sample, I'll gladly let you RCEI'd love one too.

Tyler777 - February 8, 2014, 4:31 pm

(Feb 7, 2014 09:49 AM)Feminist Wrote: [\[CITE\]](#) All an antivirus needs to do is hook a few functions (such as CreateProcess, NtUnmapViewOfSection) and they will instantly know that you are using RunPE thus detect your payload.

Not every antivirus does this- but a lot do. Your RunPE crypter might be scantime FUD, but it won't work in runtime against many antiviruses these days.

Maybe in 2008/2009/2010 you could get away with RunPE; but these days its just something you can't get away with anymore.

In my opinion, there's no point calling a crypter FUD if it can't get past the AV's it should during runtime.

You can increase FUD time by giving users unique executables. Of course, there is always some "part" of your code they begin to detect- so even FUD time has its limits per reprogram. Cant you solve this problem with polymorphic code in the main program so that each compile for each customer is almost always different? and then limit your customer base to say 20 users paying 20\$+ a month

Feminist - February 8, 2014, 4:35 pm

Also, in reference to youtube tutorials telling you to unpack themida on youtube- I'm sure these aren't the most recent versions of Themida.

I will implement "add to startup" and "install" features.

Why?

-Simply because the market demands it. Nothing more.

No, but I do have plans that I might implement to make it undetectable by AV's memory based. I will weigh the pro's and cons of implementing such a feature.

How would you do that?

-I haven't implemented it yet, but I would use encryption layers with guarded pages.

I was one of the first 20 people to analyze VMProtect

So you were already into reversing in 2003?

-No. I started reversing in 2007. I released my analysis 2011. I was one of the first people to release an analysis on VMProtect (as far as I know, that is, perhaps it was already done on some underground forum somewhere)

I am doing much more than just "mapping the executable"

You're also fixing the imports and calling TLS?

-I am fixing imports, .reloc and I plan on adding some more features (debating it) such as virtualization or CopyMem-II based off of armadillo (but w/ hooking)

I'm also considering to add basic virtualization

You are aware that if you have that you can scratch any PE loading?

-I only planned on making extremely basic virtualization. Only a few instructions.

Once you get a sample, I'll gladly let you RCE

I'd love one too.

-Okay.

(Feb 8, 2014 05:31 PM)Tyler777 Wrote: [\[CITE\]](#) Cant you solve this problem with polymorphic code in the main program so that each compile for each customer is almost always different? and then limit your customer base to say 20 users paying 20\$+ a month

No, I wouldn't do that for a few reasons:

1. the entry point would be detected as being malicious by a few crappy AVs
2. the file entropy would show it was a packed file, unless I added padding ; but this causes problems even with position independent code
3. id have to rewrite the loader each time, or morph the instructions. Even then, it wouldn't be completely FUD
4. i'd have to write time-lock puzzles and antiemulation code.
5. too many layers

Unless you are talking about a USG method? A lot of polymorphic engines get fucked over because of one tiny little piece of code that is always the same. Not to mention all the work. I'd probably stick with something simpler.

Along with the other things I wanted to do, this would end up making the project too much work to sell for \$20/month when I could go on other forums and get \$1k/month

I'd do a few trials with some beta testers to see customer satisfaction. If I'm doing a great job then I will eventually end up releasing it. I want my product to be good, I'm not only in this for the money

Tyler777 - February 8, 2014, 4:41 pm

(Feb 8, 2014 05:35 PM)Feminist Wrote: [\[CITE\]](#) I will implement "add to startup" and "install" features.

Why?

-Simply because the market demands it. Nothing more.

No, but I do have plans that I might implement to make it undetectable by AV's memory based. I will weigh the pro's and cons of implementing such a feature.

How would you do that?

-I haven't implemented it yet, but I would use encryption layers with guarded pages.

I was one of the first 20 people to analyze VMProtect

So you were already into reversing in 2003?

-No. I started reversing in 2007. I released my analysis 2011. I was one of the first people to release an analysis on VMProtect (as far as I know, that is, perhaps it was already done on some underground forum somewhere)

I am doing much more than just "mapping the executable"

You're also fixing the imports and calling TLS?

-I am fixing imports, .reloc and I plan on adding some more features (debating it) such as virtualization or CopyMem-II based off of armadillo (but w/ hooking)

I'm also considering to add basic virtualization

You are aware that if you have that you can scratch any PE loading?

-I only planned on making extremely basic virtualization. Only a few instructions.

Once you get a sample, I'll gladly let you RCE

I'd love one too.

-Okay.

No, I wouldn't do that for a few reasons:

1. the entry point would be detected as being malicious by a few crappy AVs
2. the file entropy would show it was a packed file, unless I added padding ; but this causes problems even with position independent code
3. id have to rewrite the loader each time, or morph the instructions. Even then, it wouldn't be completely FUD
4. i'd have to write time-lock puzzles and antiemulation code.
5. too many layers

Unless you are talking about a USG method? A lot of polymorphic engines get fucked over because of one tiny little piece of code that is always the same. Not to mention all the work. I'd probably stick with something simpler.

Along with the other things I wanted to do, this would end up making the project too much work to sell for \$20/month when I could go on other forums and get \$1k/month
Did not think about it in that sense.

Indaclub - February 8, 2014, 6:24 pm

(Feb 8, 2014 04:52 PM)wacked3 Wrote: [\[CITE\]](#) I also find RunPE stupid and encourage anyone to try something else.

It will work if you just find a way to map it always at it's expected base. For that you most probably need to find a way to unmap your crypter exe and then still have code running.

WHAT?

Why?

If you can promise FUD files every damn time 500 per week is the normal russian price for unlimited crypts.

Even though I agree that size isn't that much of a concern anymore (I have argued this multiple times before, if it interestes you go search for yourself) - RunPE looks basically the same in every language so why not just use a proper one? How about the fact that your AutoIT source can be easily recovered which might help to create generic detections?

Please enlighten us.

Avast's Sandbox is a joke so I don't think that the rest of this AV is any better.
In fact I know that on x64 systems the 'protection' is entirely in ring3

The leaked version has that..

500 per week.

Damn right!

No! I always unmapped my binary at 0x400000 and could then use it without any problems.

It will almost always have static values.

How would you do that?

So you were already into reversing in 2003?

There are damn youtube videos on how to unpack Themida. Plus if you were such a great unpacker you would know that just saying "Themida" is worthless. You also need to talk about the protections enabled to make it possible to adequately evalaute your skillset.

You're also fixing the imports and calling TLS?

You are aware that if you have that you can scratch any PE loading?

I'd love one too.It will work if you just find a way to map it always at it's expected base. For that you most probably need to find a way to unmap your crypter exe and then still have code running.
Expected base? this is why you fix relocs.

Feminist - February 8, 2014, 6:39 pm

(Feb 8, 2014 07:24 PM)Indaclub Wrote: [\[CITE\]](#) It will work if you just find a way to map it always at it's expected base. For that you most probably need to find a way to unmap your crypter exe and then still have code running.

Expected base? this is why you fix relocs.

He most likely meant when there is no .reloc section.

Indaclub - February 8, 2014, 7:37 pm

(Feb 8, 2014 07:39 PM)Feminist Wrote: [\[CITE\]](#) He most likely meant when there is no .reloc section.
And your solution would be to map to the 'expected' imagebase?

IRP_MJ_SCSI - February 8, 2014, 10:00 pm

Feminist, you're so full of shit it's amazing. Wannabe Reverse Engineering Guru who still refers to it

as "Reverse Code Engineering".

"You're a skid who copy and pastes and hasn't coded anything"

>Hasn't coded anything and only project he has even talked about his his hackforums crypter he's working on and how he incorrectly thinks he's the first of 20 people to analyze vmprotect.

Feminist - February 9, 2014, 7:48 am

(Feb 8, 2014 11:00 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) Feminist, you're so full of shit it's amazing. Wannabe Reverse Engineering Guru who still refers to it as "Reverse Code Engineering".

"You're a skid who copy and pastes and hasn't coded anything"

>Hasn't coded anything and only project he has even talked about his his hackforums crypter he's working on and how he incorrectly thinks he's the first of 20 people to analyze vmprotect.

Bro, you won't even find 20 articles on VMProtect right now. I guarantee that. Go ahead and find me more than 20 articles on VMProtect and we will see who's full of shit.

I haven't coded anything? Funny joke. More like you haven't coded anything

IRP_MJ_SCSI - February 9, 2014, 9:24 am

(Feb 9, 2014 08:48 AM)Feminist Wrote: [\[CITE\]](#) Bro, you won't even find 20 articles on VMProtect right now. I guarantee that. Go ahead and find me more than 20 articles on VMProtect and we will see who's full of shit.

I haven't coded anything? Funny joke. More like you haven't coded anything

20 Articles? lol. I probably couldn't find 20 articles about reversing a well known bit of malware. Not to mention pretty much nobody gives a fuck about vmprotect because it's so infrequently used. Surely you can come up with a better life achievement than opening vmprotect in IDA.

You're a fucking joke.

Feminist - February 9, 2014, 10:49 am

(Feb 9, 2014 10:24 AM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) 20 Articles? lol. I probably couldn't find 20 articles about reversing a well known bit of malware. Not to mention pretty much nobody gives a fuck about vmprotect because it's so infrequently used. Surely you can come up with a better life achievement than opening vmprotect in IDA.

You're a fucking joke.

Bro, you're just mad because you probably can't even unpack UPX.

IRP_MJ_SCSI - February 9, 2014, 11:05 am

(Feb 9, 2014 11:49 AM)Feminist Wrote: [\[CITE\]](#) Bro, you're just mad because you probably can't even unpack UPX.

You're yet to come up with an argument that doesn't involve packers or reverse engineering. OMG I ANALYZED VMPROTECT I AM BETTER THAN YOU ARE.

Feminist - February 9, 2014, 11:29 am

(Feb 9, 2014 12:05 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) You're yet to come up with an argument that doesn't involve packers or reverse engineering. OMG I ANALYZED VMPROTECT I AM BETTER THAN YOU ARE.

You come to my thread, trash my product (one you have not even before), personally attack me, report me, and get your friends to try and gang up on me when I've done nothing but answer your questions and concerns.

When did I ever say I was better than you? You're the one acting like a smug asshole trying to trash peoples threads.

IRP_MJ_SCSI - February 9, 2014, 11:34 am

(Feb 9, 2014 12:29 PM)Feminist Wrote: [\[CITE\]](#) You come to my thread, trash my product (one you have not even before), personally attack me, report me, and get your friends to try and gang up on me when I've done nothing but answer your questions and concerns.

I didn't get any friends to gang up on you, your dumb posts attracted trolls.

(Feb 9, 2014 12:29 PM)Feminist Wrote: [\[CITE\]](#) When did I ever say I was better than you? Oh idk, maybe the part when you called me a copy and pasting skiddie.

Indaclub - February 9, 2014, 12:56 pm

(Feb 9, 2014 12:34 PM)IRP_MJ_SCSI Wrote: [\[CITE\]](#) I didn't get any friends to gang up on you, your dumb posts attracted trolls.

Oh idk, maybe the part when you called me a copy and pasting skiddie. Don't bother arguing, the kids a goof.

Doesn't know what manual mapping is. Had to reiterate the argument several times for this kid to understand.

Dam Son - February 9, 2014, 10:56 pm

(Feb 8, 2014 05:35 PM)Feminist Wrote: [\[CITE\]](#) No, I wouldn't do that for a few reasons:

1. the entry point would be detected as being malicious by a few crappy AVs The entry point is extremely easy to change. Also, now AVs flag based on entrypoint location?

(Feb 8, 2014 05:35 PM)Feminist Wrote: [\[CITE\]](#) 2. the file entropy would show it was a packed file, unless I added padding ; but this causes problems even with position independent code ok

(Feb 8, 2014 05:35 PM)Feminist Wrote: [\[CITE\]](#) 3. id have to rewrite the loader each time, or morph the instructions.

Even then, it wouldn't be completely FUD That's the purpose of polymorphic code

(Feb 8, 2014 05:35 PM)Feminist Wrote: [\[CITE\]](#) 4. i'd have to write time-lock puzzles and antiemulation code. Umm, no you don't.

(Feb 8, 2014 05:35 PM)Feminist Wrote: [\[CITE\]](#) 5. too many layers wtf??

(Feb 8, 2014 05:35 PM)Feminist Wrote: [\[CITE\]](#) Unless you are talking about a USG method? A lot of polymorphic engines get fucked over because of one tiny little piece of code that is always the same. Not to mention all the work. I'd probably stick with something simpler. No.

Purpose is to not have any code be the same (Except of course common instructions). AVs don't flag your code due to a few bytes.

(Feb 8, 2014 05:35 PM)Feminist Wrote: [\[CITE\]](#) Along with the other things I wanted to do, this would end up making the project too much work to sell for \$20/month when I could go on other forums and get \$1k/month Too much work for someone who's reverse engineered Avast and VMProtect?

So you'd rather have a single stub for every crypt?

savvymatthew - February 10, 2014, 5:10 am

Im only on page 8.

But dam this is very fun to read.... you guys are great.

IRP_MJ_SCSI - February 10, 2014, 5:36 am

(Feb 10, 2014 06:10 AM)savvymatthew Wrote: [\[CITE\]](#) Im only on page 8.

But dam this is very fun to read.... you guys are great.
I'll be in the lobby signing autographs from 1pm.

Feminist - February 10, 2014, 7:44 am

(Feb 9, 2014 11:56 PM)vaXine Wrote: [\[CITE\]](#) The entry point is extremely easy to change. Also, now AVs flag based on entrypoint location?

ok

That's the purpose of polymorphic code

Umm, no you don't.

wtf??

No.

Purpose is to not have any code be the same(Except of course common instructions). AVs don't flag your code due to a few bytes.

Too much work for someone who's reverse engineered Avast and VMProtect?

So you'd rather have a single stub for every crypt?

In response to vaXine's assertions:

1. The entry point is located in the optional header. No matter what you change it to, it can still be found by the AV or any other programs. Some AV's scan the entry point to detect what your code was compiled with (C++ ..., C, VB6, etc) and some AV's flag specific instructions as being malicious (because nobody uses them anymore)

2. You didn't ask a question

3. Even the greatest polymorphic engines are defeated by one single mistake that the developer makes. It is too much work to maintain and nowadays antiviruses detect some polymorphic engines. (Key word some). You clearly do not understand the definition of "polymorphic" because what you are suggesting is a unique stub generator

4. Yes, I would have to write this unless I want the antivirus to detect my code in runtime. I'm not just going to let my code "run" upon entry and allow sandboxes such as Anubis to analyze my file.

5. Reference to the hypothetical polymorphic stub engine that was requested (though I sure wouldn't sell this on Hackforums for \$200/week or \$20/month if I made it)

6. Some antiviruses will flag your code just if you share a few bytes in common.

7. RCEing VMProtect was a cracking job. Yes, it would be too much work to sell on Hackforums for such a low price. It would also delay the development time significantly/

d4rkj4y - February 11, 2014, 10:08 pm

Feminist this thread sucks extremely bad.

How are you going to run a portable executable without using a "RunPE method" ?

kingroot - February 12, 2014, 8:42 pm

Seems like you have an idea as to what you're doing. Good luck.

Dam Son - February 12, 2014, 9:00 pm

(Feb 11, 2014 11:08 PM)d4rkJ4y Wrote: [\[CITE\]](#) Feminist this thread sucks extremely bad.

How are you going to run a portable executable without using a "RunPE method" ?

You think the generic runPE is the only way to run an executable?

kingroot - February 12, 2014, 9:03 pm

(Feb 12, 2014 10:00 PM)vaXine Wrote: [\[CITE\]](#) You think the generic runPE is the only way to run an executable? Clearly not, you can execute it from disk
?

Dam Son - February 12, 2014, 9:07 pm

(Feb 12, 2014 10:03 PM)kingroot Wrote: [\[CITE\]](#) Clearly not, you can execute it from disk
?

I think d4rkj4y meant executing a file without dropping to a disk, but nevertheless, there are lots of other ways.

kingroot - February 12, 2014, 9:08 pm

(Feb 12, 2014 10:07 PM)vaXine Wrote: [\[CITE\]](#) I think d4rkj4y meant executing a file without dropping to a disk, but nevertheless, there are lots of other ways.

Yeah, i know, was trying to be a smart ass.

Dam Son - February 12, 2014, 9:09 pm

(Feb 12, 2014 10:08 PM)kingroot Wrote: [\[CITE\]](#) Yeah, i know, was trying to be a smart ass.
[img]<http://cdn.memegenerator.net/instances/250x250/43117045.jpg>[/img]

d4rkj4y - February 12, 2014, 11:32 pm

(Feb 12, 2014 10:00 PM)vaXine Wrote: [\[CITE\]](#) You think the generic runPE is the only way to run an executable?

Did I mention, "generic" runPE?

I said, "RunPE"

RunPE, is, running a portable executable, in memory.

It can be done as a packer, meaning in the current process, or in a remote process, they are both RUNPE.

How the fuck else would you do it? "RunPE" isn't just suspending a process, and altering thread context which is definitely NOT suspicious at all, it's RUNNING a payload, A PE FILE, this cannot be emphasized enough.

kingroot - February 12, 2014, 11:46 pm

(Feb 13, 2014 12:32 AM)d4rkJ4y Wrote: [\[CITE\]](#) Did I mention, "generic" runPE?

I said, "RunPE"

RunPE, is, running a portable executable, in memory.

It can be done as a packer, meaning in the current process, or in a remote process, they are both RUNPE.

How the fuck else would you do it? "RunPE" isn't just suspending a process, and altering thread context which is definitely NOT suspicious at all, it's RUNNING a payload, A PE FILE, this cannot be emphasized enough.

well in the context of HF it's usually referred to as dynamic forking.

d4rkj4y - February 13, 2014, 12:54 am

(Feb 13, 2014 12:46 AM)kingroot Wrote: [\[CITE\]](#) well in the context of HF it's usually referred to as dynamic forking.

That's why hackforums is fucking retarded

xhflhkeuhwguu34 - February 13, 2014, 10:45 am

This thread is full of people that clearly don't know what they're doing, and those that do.

Spot the ones that do. Gogogo

kingroot - February 13, 2014, 11:04 am

(Feb 13, 2014 11:45 AM)Xen0n Wrote: [\[CITE\]](#) This thread is full of people that clearly don't know what they're doing, and those that do.

Spot the ones that do. Gogogo

What was the point of posting this?

Shinigami_ - March 25, 2015, 1:54 am

nice thread but no nice language in speaking