

Forum:[Hack Forums](#)

Thread: [scantime and runtime are skid terms](#)

JOHNsfds - July 30, 2016, 3:29 pm

Anti virus scanners determine the behavior of a process during runtime, what most of you morons fail to understand is the architecture of the virtual machine.

There's a huge discrepancy between x86 and x64 in terms of kernel security and detection measures.

Ever wonder why you scan a file and it's detected by a certain anti virus, but during execution on your PC it's undetected? Well that's because on x64 there is a security mechanism referred to as KPP / Patch Guard which doesn't allow kernel memory to be patched, unless you were to disable PG, load before PG, or any other means of manipulating the PG timer. Anti viruses therefore detect less viruses on x64, and because of this they result to usermode hooks and documented methods, such as filtering process handles, and intercepting process creation. Anti virus scanners don't just scan for signatures, this isn't 1990

Please stop saying "Scantime" vs "runtime" You're all a bunch of clueless fucking retards.

Go scan a 64 bit application, it'll be FUD.

[nodistribute.com/result/vp7CrMAYIWFQHaq8NmP6TO](#) (The VM's don't support 64 bit)

[virustotal.com/en/file/e609fddf513561c74906463733041d969ac6ed9f852c755c3da8d1204e9a11e5/analysis/1469917859/](#)

The process scanned above writes to the registry, and hooks all processes.

Determining if the process is detected on my system from these scan results is absurd, these scan results provide no evidence, the scan results are inconclusive.

tldr; Anti viruses operate differently on different architectures and operating systems, deeming a "crypter" scantime only is retarded.

You will rarely see truly FUD malware today.

ImASKidCX - July 30, 2016, 7:43 pm

(Jul 30, 2016 03:29 PM)JOHNsfds Wrote: [\[CITE\]](#) Anti virus scanners determine the behavior of a process during runtime, what most of you morons fail to understand is the architecture of the virtual machine.

There's a huge discrepancy between x86 and x64 in terms of kernel security and detection measures.

Ever wonder why you scan a file and it's detected by a certain anti virus, but during execution on your PC it's undetected? Well that's because on x64 there is a security mechanism referred to as KPP / Patch Guard which doesn't allow kernel memory to be patched, unless you were to disable PG, load before PG, or any other means of manipulating the PG timer. Anti viruses therefore detect less viruses on x64, and because of this they result to usermode hooks and documented methods,

such as filtering process handles, and intercepting process creation. Anti virus scanners don't just scan for signatures, this isn't 1990

Please stop saying "Scantime" vs "runtime" You're all a bunch of clueless fucking retards.

Go scan a 64 bit application, it'll be FUD.

nodistribute.com/result/vp7CrMAYIWFQHaq8NmP6TO (The VM's don't support 64 bit)

virustotal.com/en/file/e609fddf513561c74906463733041d969ac6ed9f852c755c3da8d1204e9a11e5/analysis/1469917859/

The process scanned above writes to the registry, and hooks all processes.

Determining if the process is detected on my system from these scan results is absurd, these scan results provide no evidence, the scan results are inconclusive.

tldr; Anti viruses operate differently on different architectures and operating systems, deeming a "crypter" scantime only is retarded.

You will rarely see truly FUD malware today.

Is this in anyway helpful to the Good Lord himself? ?

Good job for trying, but maybe you're in the wrong section...you should totally reroute your little dinky ass into the "Cryptography, Encryption, and Decryption" section ? and post your narcissistic comments in there! ?

JOHNSfds - July 30, 2016, 9:13 pm

(Jul 30, 2016 07:43 PM)ImASkidCX Wrote: [\[CITE\]](#) Is this in anyway helpful to the Good Lord himself? ?

Good job for trying, but maybe you're in the wrong section...you should totally reroute your little dinky ass into the "Cryptography, Encryption, and Decryption" section ? and post your narcissistic comments in there! ?

narcissistic? im the dumbest kid on this forum kid

Backopy - July 30, 2016, 9:30 pm

(Jul 30, 2016 03:29 PM)JOHNSfds Wrote: [\[CITE\]](#) You will rarely see truly FUD malware today. Right.

You should familiarize yourself with what a [rootkit](#) is.

A lot of the commercial malware crypters like on HF are very poorly coded in the first place.

JOHNSfds - July 30, 2016, 9:33 pm

(Jul 30, 2016 09:30 PM)Dasace Wrote: [\[CITE\]](#) Right.

You should familiarize yourself with what a

A lot of the commercial malware crypters like on HF are very poorly coded in the first place.

What do Rootkits have to do with FUD Malware? Are you aware of what a rootkit is used for? I suggest you READ that Wikipedia page on what a rootkit is used for, then in your own words explain it, because it seems to me you're clueless.

Suggesting a rootkit for FUD malware. You're a fucking retard.

Backopy - July 30, 2016, 9:39 pm

(Jul 30, 2016 09:33 PM)JOHNSfds Wrote: [\[CITE\]](#) What do Rootkits have to do with FUD Malware? Are you aware of what a rootkit is used for?

You're talking to the wrong crowd here buddy. You make it sound as if every malware coder just uses a crypter and assumes that's their final payload.

Any large malware operation is going to implement soundly coded rootkits into their bots, data encryption with the bin is just a part of the process.

JOHNSfds - July 30, 2016, 9:40 pm

(Jul 30, 2016 09:39 PM)Dasace Wrote: [\[CITE\]](#) You're talking to the wrong crowd here buddy. You make it sound as if every malware coder just uses a crypter and assumes that's their final payload.

Any large malware operation is going to implement soundly coded rootkits into their bots, data encryption with the bin is just a part of the process.

And again, What does a rootkit have to do with FUD malware? No one on HF is capable of writing a rootkit.

"Any large malware operation"

Are you aware of Dridex, Locky, Petya?

You won't find a good rootkit without some type of initial startup persistence such as an MBR Bootkit, this is because installation first is key to who wins... You're not going to be able to install a rootkit under an anti viruses supervision simply because the AV good av will revert any changes done to the kernel.

Rootkits have nothing to do with crypters. But yeah be my guest and market your shitty crypter with a shitty rootkit feature that doesn't even work outside of wow64.

Gigabot - July 30, 2016, 10:26 pm

(Jul 30, 2016 09:40 PM)JOHNSfds Wrote: [\[CITE\]](#) And again, What does a rootkit have to do with FUD malware? No one on HF is capable of writing a rootkit.

"Any large malware operation"

Are you aware of Dridex, Locky, Petya?

You won't find a good rootkit without some type of initial startup persistence such as an MBR Bootkit, this is because installation first is key to who wins... You're not going to be able to install a rootkit under an anti viruses supervision simply because the AV good av will revert any changes done to the kernel.

Rootkits have nothing to do with crypters. But yeah be my guest and market your shitty crypter with a shitty rootkit feature that doesn't even work outside of wow64.

Dude, we get it, you're a Hacker..

ThePacketBaron - July 31, 2016, 8:07 am

(Jul 30, 2016 09:39 PM)Dasace Wrote: [\[CITE\]](#) Any large malware operation is going to implement soundly coded rootkits into their bots

Not always, sometimes rootkits are pretty unnecessary and if anything can alert security products (or someone looking for it) even more. Hooking and injecting into processes can just cause more noise and raise more red flags when it comes to your process. Furthermore if your rootkit "hides traffic" (such as FU rootkit), imagine how suspicious it looks if you packet sniff on the infected computer and nothing comes up while another computer on the network can pick up that same

computer sending malicious traffic.

Saying "any" large campaign is just inaccurate because it depends on what the campaign is trying to do. If it is just trying to ransom your pc or steal banking credentials, it only needs to be done once, hence no rootkit needed.