

# Forum:[Hack Forums](#)

Thread: [Malware Compatibility](#)

**nucleo\_type09** - February 14, 2024, 8:45 am

hi there, i was wondering, what's the biggest concern/issue regarding malware development in the field? is it architecture/platform compatibility? OS? Users? AV?

**HALx86** - February 14, 2024, 11:05 am

I've been mostly focused with Linux malware. I think it's a lot easier as all of the code is open source so you can see all of the internal code.

Kernel 5.7+ made malware a little harder as the `sys_call_table` used to intercept systems calls was no longer exported. Luckily a lot of smart people found out that you can still pull the table by using a `kprobe`.

I'm sure I'll find more other interesting issues the more experience I gain but that was the first one that came to mind.

**nucleo\_type09** - February 14, 2024, 11:40 am

why is linux easier if there are literally no malware developed for linux at all? why are there so few of them? im just asking, windows has more malware developement then linux, is that because of its architectural structure or the OS itself?

**HALx86** - February 14, 2024, 12:07 pm

(Feb 14, 2024 12:40 PM)nucleo\_type09 Wrote: [\[CITE\]](#) why is linux easier if there are literally no malware developed for linux at all? why are there so few of them? im just asking, windows has more malware developement then linux, is that because of its architectural structure or the OS itself?

That's a good question that I also wonder. I guess maybe there isn't much money to be made since most organizations use Windows workstations and Active Directory.

Linux actually makes it super easy. You're able to plug in kernel modules, recompile system binaries, access running memory, and use `strace` to figure out the steps a process takes. Takes some knowledge in C though. I think now people are using Rust but I'm not good at that language.

**nucleo\_type09** - February 14, 2024, 12:29 pm

(Feb 14, 2024 01:07 PM)HALx86 Wrote: [\[CITE\]](#) That's a good question that I also wonder. I guess maybe there isn't much money to be made since most organizations use Windows workstations and Active Directory.

Linux actually makes it super easy. You're able to plug in kernel modules, recompile system binaries, access running memory, and use `strace` to figure out the steps a process takes. Takes some knowledge in C though. I think now people are using Rust but I'm not good at that language.

are we even sure there are NO linux walware yet? haha maybe there are, and we don't know yet!

**Hackers** - February 14, 2024, 12:46 pm

(Feb 14, 2024 09:45 AM)nucleo\_type09 Wrote: [\[CITE\]](#) hi there, i was wondering, what's the biggest concern/issue regarding malware development in the field? is it architecture/platform compatibility? OS? Users? AV?Biggest concern should be legality... but for hackers it's probably whether or not they have a spread method available for that OS or not, and whether that OS is a specific distro / version / etc. It feels like default AV/scanners are shit compared to a private AV so I'm guessing it's that... I'm new to this myself.

(Feb 14, 2024 01:07 PM)HALx86 Wrote: [\[CITE\]](#) That's a good question that I also wonder. I guess maybe there isn't much money to be made since most organizations use Windows workstations and Active Directory.

Linux actually makes it super easy. You're able to plug in kernel modules, recompile system binaries, access running memory, and use strace to figure out the steps a process takes. Takes some knowledge in C though. I think now people are using Rust but I'm not good at that language. Do you think this is still super easy for someone to infect another system if there are no sudo'd users available, no root perms, etc? I know that you can access all of that, but are people actually stealing sudo/root access on their own, or just taking advantage of a system that isn't protected? The reason this is important is because you can do anything with a rooted Linux user the same way you can pretty much do anything with a Windows admin. Obviously a bit different, but I feel like Linux is actually easier to secure than Windows in a lot of cases.

I don't know enough about Linux malware though, so please correct me if this is a horrible take.

(Feb 14, 2024 01:29 PM)nucleo\_type09 Wrote: [\[CITE\]](#) are we even sure there are NO linux malware yet? haha maybe there are, and we don't know yet! There's tons of malware on Linux servers, it just usually targets another system first. For example there are WordPress hacks that would use WP to execute PHP with escalated permissions by injecting malicious code into admin files, or if possible just creating a new backdoor shell somewhere else. You can see the same thing with cPanel hacks. The reason that this is often not classified as "Linux malware" is because it really is more likely to be a software (WP, cP, etc) exploit more than it is a traditional "malware". The reason that these get injected into PHP files is because those are already set up to execute and may have escalated permissions for system changes (ex: an admin-only file).

It's harder to spread on Linux because unless the server is not setup properly, it's most likely using restricted users for processes so it's harder to escalate or use directory traversal to break out of a cage.

Also Linux sys admins that do custom setups usually know what they're doing and the rest of them are usually secure images auto-deployed by a hosting provider.

**nucleo\_type09** - February 14, 2024, 1:01 pm

what if AVs have backdoors in them and people don't know? did anyone ever check that out for every AV out there?

**HALx86** - February 14, 2024, 7:26 pm

(Feb 14, 2024 01:46 PM)nodes Wrote: [\[CITE\]](#) Do you think this is still super easy for someone to infect another system if there are no sudo'd users available, no root perms, etc? I know that you can access all of that, but are people actually stealing sudo/root access on their own, or just taking advantage of a system that isn't protected? The reason this is important is because you can do anything with a rooted Linux user the same way you can pretty much do anything with a Windows admin. Obviously a bit different, but I feel like Linux is actually easier to secure than Windows in a lot of cases.

I mean, I think you have a pretty good take on it! Hopefully sudo should be pretty hard to obtain if the system is patched (blocking things like loony tunables, polkit), the admin is capable (protect against GTFOBins) and you're not a target of a Nation State. If it's the last one, I don't think it matters how good someone is.

(Feb 14, 2024 02:01 PM)nucleo\_type09 Wrote: [\[CITE\]](#) what if AVs have backdoors in them and people don't know? did anyone ever check that out for every AV out there?

I think this could be always be a threat. I certainly wouldn't be able to tell if my AV is opening reverse shells or using me for lateral movement.

**M?tt** - February 14, 2024, 7:30 pm

Just because the target audience for Linux is much smaller than other operating systems doesn't mean it doesn't exist. I assure you all that malware and exploits exist for just about every operating system (or at least kernel) available. Just because it's unknown to us doesn't mean there isn't a way to manipulate or exploit a machine or device.

**nucleo\_type09** - February 14, 2024, 9:53 pm

(Feb 14, 2024 01:07 PM)HALx86 Wrote: [\[CITE\]](#) That's a good question that I also wonder. I guess maybe there isn't much money to be made since most organizations use Windows workstations and Active Directory.

Linux actually makes it super easy. You're able to plug in kernel modules, recompile system binaries, access running memory, and use strace to figure out the steps a process takes. Takes some knowledge in C though. I think now people are using Rust but I'm not good at that language. i would never use rust for malware dev, i hate rust personally, it is just weird as a language, why would someone even invest time learning those concepts found NOWHERE else other than rust? i think if you want low level access, go for C/C++, if you want high level access, go for Python, GO, LUA...

**Hackers** - February 15, 2024, 6:52 am

(Feb 14, 2024 08:26 PM)HALx86 Wrote: [\[CITE\]](#) I mean, I think you have a pretty good take on it! Hopefully sudo should be pretty hard to obtain if the system is patched (blocking things like loony tunables, polkit), the admin is capable (protect against GTFOBins) and you're not a target of a Nation State. If it's the last one, I don't think it matters how good someone is.

I think this could be always be a threat. I certainly wouldn't be able to tell if my AV is opening reverse shells or using me for lateral movement.

Related to this - Windows added sudo abilities so devs can escalate privs on projects and have set users. Going to be pretty cool but will definitely change how people approach this subject.

**HALx86** - February 15, 2024, 11:28 am

(Feb 15, 2024 07:52 AM)nodes Wrote: [\[CITE\]](#) Related to this - Windows added sudo abilities so devs can escalate privs on projects and have set users. Going to be pretty cool but will definitely change how people approach this subject.

For sure! I'm guessing the majority of Windows home users use the same account for regular use as the account that has permission to run as administrator. If sudo can also be run like that, that's going to be a large number of machines.