

Forum:[Hack Forums](#)

Thread: [Overlord Detections](#)

I_H8_KDot - March 26, 2026, 11:55 am

Overlord has been out for about 3 months now. This is what the detections look like.

https://kleenscan.biz/runtime/scan_result/1272733dfe71716ebadb95fb81081e2f942a6e82655b10a86d24163fbc11f753

NO CRYPT.

https://kleenscan.biz/runtime/scan_result/fc98ce1155d9899b51f7859732dd6d337ee95562afb42bc2109b3eb41dd4a506

THIS IS NORMAL DONUT WITH NO AMSI PATCH.

MANY people come to my dms and complain about an open source project having detections but I can assure you that with a little shellcode magic or common crypting practices, you can refud Overlord within 15 minutes and have a version that won't get detected for weeks.

loadman - March 26, 2026, 12:03 pm

Since it's open source it's more likely to get flagged over time. A custom morpher would probably be more reliable and easy for you in the long run,, but yea i respect the effort that you are doing for everyone without taking anything in return ++++

possessed-client - March 26, 2026, 12:29 pm

Ah, you got a unique signature, at least from Nod32, congrats on the milestone!

Btw, what did you use to execute the Donut-produced shellcode file, if it's something custom then what chain of techniques and methods?

d3athgiver - March 26, 2026, 4:30 pm

(Mar 26, 2026 11:55 AM)I_H8_KDot Wrote: [\[CITE\]](#) Overlord has been out for about 3 months now. This is what the detections look like.

https://kleenscan.biz/runtime/scan_result/1272733dfe71716ebadb95fb81081e2f942a6e82655b10a86d24163fbc11f753

NO CRYPT.

https://kleenscan.biz/runtime/scan_result/fc98ce1155d9899b51f7859732dd6d337ee95562afb42bc2109b3eb41dd4a506

THIS IS NORMAL DONUT WITH NO AMSI PATCH.

MANY people come to my dms and complain about an open source project having detections but I can assure you that with a little shellcode magic or common crypting practices, you can refute Overlord within 15 minutes and have a version that won't get detected for weeks.

Some people forgot venom was around 3k and needed crypting and fully detected and lot of others paid rat can cost over 1k, are windows only and also require crypting... I know only 1 other rat multi os and it's not free lol. I am using that rat for a while without crypt and keep having new connection with very basic technique lol

CL1B - March 26, 2026, 5:03 pm

(Mar 26, 2026 12:29 PM)possessed-client Wrote: [\[CITE\]](#) Ah, you got a unique signature, at least from Nod32, congrats on the milestone!

Btw, what did you use to execute the Donut-produced shellcode file, if it's something custom then what chain of techniques and methods?

They've been flagging pretty much every decently built project deriving from HF since 2025, safe to say one of their researchers is rather active HF member.

DramaKing - March 26, 2026, 8:16 pm

It's still good to use crypting and anti-reverse-engineering. Yes, it's open-source but good practice.

benio2 - March 26, 2026, 8:55 pm

This won't bypass smartscreen or chrome browser. The only reason it's bypassing in the runtime scans is because it's dropping the file to desktop from it's own filesystem. Try your payload on defender in a vm, upload your shit in a zip file on mediafire or something similar. Use latest version of chrome to dl. Bet chrome catches it or smartscreen will catch it before it even runs. So this means the only way your payload truly bypasses is if you plug in a usb, which a lot of smart companies prohibit.

I_H8_KDot - March 26, 2026, 10:23 pm

(Mar 26, 2026 08:55 PM)benio2 Wrote: [\[CITE\]](#) This won't bypass smartscreen or chrome browser. The only reason it's bypassing in the runtime scans is because it's dropping the file to desktop from it's own filesystem. Try your payload on defender in a vm, upload your shit in a zip file on mediafire or something similar. Use latest version of chrome to dl. Bet chrome catches it or smartscreen will catch it before it even runs. So this means the only way your payload truly bypasses is if you plug in a usb, which a lot of smart companies prohibit.

Well that's because it doesn't matter how good your crypt is it will always still get caught on chrome (specifically when running after) due to MOTW. Just download tho? It's fine. But MOTW will fuck up when someone tries running it. The only way to get past this is to get a sig or end up on Microsoft's good boy list which is way harder than you'd imagine.

benio2 - March 26, 2026, 10:44 pm

(Mar 26, 2026 10:23 PM)I_H8_KDot Wrote: [\[CITE\]](#) Well that's because it doesn't matter how good your crypt is it will always still get caught on chrome (specifically when running after) due to MOTW. Just download tho? It's fine. But MOTW will fuck up when someone tries running it. The only way to get past this is to get a sig or end up on Microsoft's good boy list which is way harder than you'd imagine.

Stick a vulnerable exe with a hijacked dll inside an iso file, then zip the iso file. Download it from mediafire with chrome. Go test that in a vm. It will bypass mark of the web and smartscreen.? better than signing a fresh .exe, much harder to detect a .dll payload. Some av companies have caught on though and pretty much automatically block exe files loading a dll inside a container.

The best way is a browser/legitimate software exploit that drops a .dll into a vulnerable folder, it would use search order hijacking to find a path where a vulnerable .exe is looking for a .dll, it

wouldnt drop any exe (imagine onedrive launches it searches for random dll in %appdata%, your dll would be that file)

I_H8_KDot - March 27, 2026, 12:39 am

(Mar 26, 2026 10:44 PM)benio2 Wrote: [\[CITE\]](#) Stick a vulnerable exe with a hijacked dll inside an iso file, then zip the iso file. Download it from mediafire with chrome. Go test that in a vm. It will bypass mark of the web and smartscreen.? better than signing a fresh .exe, much harder to detect a .dll payload. Some av companies have caught on though and pretty much automatically block exe files loading a dll inside a container.

The best way is a browser/legitimate software exploit that drops a .dll into a vulnerable folder, it would use search order hijacking to find a path where a vulnerable .exe is looking for a .dll, it wouldnt drop any exe (imagine onedrive launches it searches for random dll in %appdata%, your dll would be that file)

Ok I don't think you understand half the things that you're saying.

When you say "vulnerable exe with a hijacked dll inside an iso file" you're just referring to sideloading. This works and is basically the ONLY way you can bypass MOTW without weird archive strats (hence the iso but this has been fixed by windows). Also no. It's not better than signing an exe. If you make a proper crypt that's binded and you sign it, it'll work much better. sideloading is also getting cracked down on by Defender with it's new AI updates. Obviously if you don't want to pay the 4k for a cert then your only choice is to use sideloading but I can assure you that a cert is the MUCH better option for anyone with money.

benio2 - March 27, 2026, 1:31 am

(Mar 27, 2026 12:39 AM)I_H8_KDot Wrote: [\[CITE\]](#) Ok I don't think you understand half the things that you're saying.

When you say "vulnerable exe with a hijacked dll inside an iso file" you're just referring to sideloading. This works and is basically the ONLY way you can bypass MOTW without weird archive strats (hence the iso but this has been fixed by windows). Also no. It's not better than signing an exe. If you make a proper crypt that's binded and you sign it, it'll work much better. sideloading is also getting cracked down on by Defender with it's new AI updates. Obviously if you don't want to pay the 4k for a cert then your only choice is to use sideloading but I can assure you that a cert is the MUCH better option for anyone with money.

No it's not. It bypasses defender just fine. If you find a unique hijack that isn't blacklisted it will even bypass much better av with out wasting your time and money on certs. Although signing an exe is a good way it's easier to detect after sandbox analysis. Drop a dll through an exploit so you can live off the land by abusing a phantom dll or search order. A java exploit that simply downloads a dll into the folder that you specify.

You should add undetectable in memory interactive mimikatz to pulsar 2.4.6 and release 2.4.7. This would be cool in legal red team engagements.

DramaKing - March 27, 2026, 5:08 am

(Mar 26, 2026 08:55 PM)benio2 Wrote: [\[CITE\]](#) This won't bypass smartscreen or chrome browser. The only reason it's bypassing in the runtime scans is because it's dropping the file to desktop from it's own filesystem. Try your payload on defender in a vm, upload your shit in a zip file on mediafire or something similar. Use latest version of chrome to dl. Bet chrome catches it or smartscreen will catch it before it even runs. So this means the only way your payload truly bypasses is if you plug in a usb, which a lot of smart companies prohibit.

Bypassing Chrome Safe Browsing with new malware is easy. I think that it works by checking URLs against a blacklist and running downloaded files against AMSI and the active AV engine. The focus

should always be AV evasion, not browser evasion.

SmartScreen triggers on any untrusted unsigned file with MotW. How many people go "Oh no, an unrecognized app! I'd better get rid of this now!" SmartScreen "catching" a downloaded file is understood.

It sounds like you're just trashing Overlord. Who in the target audience only spreads to companies, too?

benio2 - March 27, 2026, 9:39 am

(Mar 27, 2026 05:08 AM)DramaKing Wrote: [\[CITE\]](#) Bypassing Chrome Safe Browsing with new malware is easy. I think that it works by checking URLs against a blacklist and running downloaded files against AMSI and the active AV engine. The focus should always be AV evasion, not browser evasion.

SmartScreen triggers on any untrusted unsigned file with MotW. How many people go "Oh no, an unrecognized app! I'd better get rid of this now!" SmartScreen "catching" a downloaded file is understood.

It sounds like you're just trashing Overlord. Who in the target audience only spreads to companies, too?

It has nothing to do with overlord. I see people posting scans claiming their it bypasses when in reality it doesn't. Chrome browser scan is also checking for random ass freshly generated .exe files.

DramaKing - March 27, 2026, 12:07 pm

(Mar 27, 2026 09:39 AM)benio2 Wrote: [\[CITE\]](#) It has nothing to do with overlord. I see people posting scans claiming their it bypasses when in reality it doesn't.

KDot wouldn't post fake AV results for something that he gives away for free. Feel free to download the RAT and run your own scans.

(Mar 27, 2026 09:39 AM)benio2 Wrote: [\[CITE\]](#) Chrome browser scan is also checking for random ass freshly generated .exe files.

Plainly wrong. Never has Chrome ever popped up a message saying "Download blocked. File is too new."

benio2 - March 27, 2026, 2:39 pm

(Mar 27, 2026 12:07 PM)DramaKing Wrote: [\[CITE\]](#) KDot wouldn't post fake AV results for something that he gives away for free. Feel free to download the RAT and run your own scans.

Plainly wrong. Never has Chrome ever popped up a message saying "Download blocked. File is too new."

Yes because that's not the message it says. It blocks the file and says it's malicious.

DramaKing - March 27, 2026, 4:59 pm

(Mar 27, 2026 02:39 PM)benio2 Wrote: [\[CITE\]](#) Yes because that's not the message it says. It blocks the file and says it's malicious.

Yes, that's the point. You could download some previously unseen and unsigned program, and Chrome wouldn't give a peep. That's AMSI/AV. Defender results are not 100% consistent. You're probably just unlucky based on your region. Below is an example of Safe Browsing.

loadman - March 27, 2026, 6:19 pm

also before u look for ways to bypass chrome download detection, understand it how it works:

- > > step 1 -> Chrome Safe Browsing checks URL + file hash + reputation
- > > step 2 -> file gets saved with Zone.Identifier (MotW, ZoneId=3 = internet)
- > > step 3 -> MotW flags it as "from internet" to Windows/apps (not detection)
- > > step 4 -> when you run it, SmartScreen does reputation check
- > > step 5 -> Defender/AV may scan at runtime (memory/behavior)
- > > tldr -> download filter -> tag -> execution check

create a simple custom loader(or purchase one which is private or not burnt in public) for the payload along with a cloacker or u can use cf aswell for anti-crawler & autocrypti api to generate new build signature per download, this will maintain persistence from chrome/bin download alert and use legitimate name on file (any random name with spaces), this also bypasses chrome alert.

Sometime back I was able to bypass it by directly hosting it on azure file hosting, im not sure if it still works its probably been patched, there were other websites for hosting files that instantly gave reputation to the payload, allowing you to download it without detections, but I don't seem to remember them.

also another method is

using sigtheif and steal cert from another file and Combine with file packers to make the stolen cert look less out of place.

honestly there are many cheeeky ways to bypass chrome detection, just be creative thats all i can say

all these are things that ive used it for work in the past and not do any guessing game and things worked perfectly.

sideloading is also an option but make sure ur zip file dont get sigged coz then chrome will scream again

if u want to skip all this and take the easy way out just purchase the cert if u have too much money and no time to do all this

furthermore

LNK Stomping

Signed Binary Proxy Execution

Trusted Platform Abuse (Azure, Vercel, Subdomain Hosting *.web.app, *.netlify.app, *.github.io)
clickfix

If there are any repeated methods, I apologize it was 5 a.m. when I was writing this, and I was very tired. I might make a thread about this later.

[I_H8_KDot](#) [benio2](#) [DramaKing](#)

Lookdadon - April 24, 2026, 2:26 pm

i never spreaded a payload/file but worked with drainer/phishing which at some point throw the same problems. Very usefull technics was to:

- add a captcha before landing on page so it block google crawlers to access your page/cloudflare setup to block crawlers or even js code that block crawlers.

- write the malicious logic with rust as a wasm and let you have a code that dont need obfuscation other than minify and just use random name for func/variables and etc as the malicious part run in rust wasm who compile in binary which make it unreadable.

- pixel of webpage edited

- convert img and some codes in base64

i know isnt exact same thing when you host a payload but probably at somepoint some technics remain the same i guess... ex:if crawler are blocked by a captcha i guess maybe it could be blocked by a password protected archive or container? but one thing i think burn the shit is all visit come from a link and no organic.

the trusted reputation abuse LOADMAN mentionned was a total game changer for some time. it was totally easier and a good page could last a week or 2, now its rince and repeat very quickly. i found a smart technic somewhere: buy expired domain with big history and backlink etc

hope it give a hint or two

loadman - April 27, 2026, 1:39 pm

(Apr 24, 2026 02:26 PM)Lookdadon Wrote: [\[CITE\]](#) i never spreaded a payload/file but worked with drainer/phishing which at some point throw the same problems. Very usefull technics was to:

- add a captcha before landing on page so it block google crawlers to access your page/cloudflare setup to block crawlers or even js code that block crawlers.

- write the malicious logic with rust as a wasm and let you have a code that dont need obfuscation other than minify and just use random name for func/variables and etc as the malicious part run in rust wasm who compile in binary which make it unreadable.

- pixel of webpage edited

- convert img and some codes in base64

i know isnt exact same thing when you host a payload but probably at somepoint some technics remain the same i guess... ex:if crawler are blocked by a captcha i guess maybe it could be blocked by a password protected archive or container? but one thing i think burn the shit is all visit come from a link and no organic.

the trusted reputation abuse LOADMAN mentionned was a total game changer for some time. it was totally easier and a good page could last a week or 2, now its rince and repeat very quickly. i found a smart technic somewhere: buy expired domain with big history and backlink etc

hope it give a hint or two
angelferno?