

Forum:[Hack Forums](#)

Thread: [YouTube Ghost Network, Wild How Deep This Malware Thing Goes](#)

JoseMar - October 26, 2025, 7:31 pm

YouTube Ghost Network

Wild How Deep This Malware Thing Goes

Okay, yeah, title is dramatic but also accurate? Maybe. I'm still half awake and mad at a Monday, so this is me thinking out loud. Saw a report (Check Point? maybe) about this "YouTube Ghost" gig, thousands of malicious vids pretending to be cracked software / game mods, and I keep wanting to slam my head on the desk because the whole thing is so stupid and so clever at the same time.

Short version who don't want to read all?:

A coordinated network weaponized YouTube as a distribution/credibility layer. Videos upload, comment farms simulate legit users, pinned comments point to file-hosting links, posts give archive passwords, and boom, people download what they think is a crack or a trainer and instead get an infostealer. They've been doing this since... well... long time... and apparently ramped the production in 2025. That's the cliffnotes. No screenshots, no step-by-step, not because I'm shy, because I'm not in the business of repeating things that help criminals.

Why this pissed me off (and you should care)

Two reasons:

It's dumb people getting hacked for cheap thrills, people chase "free Photoshop" or a "cracked FL Studio" and end up with their passwords, cookies, whatever, stolen. You think you're saving €20? You might be handing over your login to everything.

The tech behind it is annoyingly effective: legit platforms (MediaFire, Google Drive, etc.) are used as the delivery mechanism. The files are big, passworded archives, so automatic scanners have a hard time. URL shorteners hide the real destination. Fake comments make the whole thing look legit. It's social engineering 101 married to just enough technical sauce to bypass lazy heuristics.

Also: this thing scales. Thousands of videos. Thousands. One video allegedly had hundreds of thousands of views. So it's not a single script-kiddie; it's an ecosystem.

Technical bits (kinda), don't copy paste this into your brain if you're tempted to experiment

Alright, I'll be clear: I'm summarizing what I read, not sharing anything you could use to replicate it. The core payloads were described as infostealers, malware that quietly collects credentials, browser cookies, stuff like that. Researchers noted a pivot over time: one strain was disrupted and the actors moved to another. They rotated command-and-control infrastructure frequently. There were also mentions of installer formats that evade many AV engines (MSI files with low detection rates, etc.).

Some specifics in the report were redacted in my head and should stay redacted, IPs, exact gateway URLs, and archive passwords are not something to fling around in public forums. If you're the kind of person who downloads pirated software and then posts in a thread how to bypass security to run it , stop. That's literally the target here.

How people fall for it , (and how dumb I feel for being judgmental until I remember I've done sketchy stuff too)

We like quick wins. We also like the illusion of community validation. So a video has 50k views and a comment pinned saying "use password 1337" and a dozen replies like "works perfect, ty" , suddenly it's believable. Combine that with updated posts that refresh the "download link" and you've got an ongoing operation.

Also, to be fair ,not everyone has a security mindset. If you aren't used to thinking about supply-chain hygiene for random .zip files, you click, you extract, you run. That's on the user, yeah, but the attackers designed everything to look normal. That's their job. Their job is to be convincing. Ours should be to not be dumb.

So what can people actually do? (no panicking, just practical-ish thoughts)

I hate the "use common sense" advice because it reads smug. But also: it's not wrong. Don't download cracked software. Don't run random installers. Use a VM if you're testing sketchy stuff (yes I said the dirty word), and keep separate accounts for dumb experiments. Keep MFA on your important services. Use browsers that compartmentalize sessions, and maybe, I dunno, pay for the software you use if it matters.

Also: platform moderation needs to do better. YouTube can't be blameless here , millions of users, I get that, but fake engagement and malicious files shouldn't be able to parade around for years. This speaks to detection gaps on large platforms.

My messy ending

I'm ranting and also part-conflicted. On one hand, it's satisfying to watch defenders win and researchers unmask these farms. On the other hand, actors adapt , they'll change tactics, host files elsewhere, buy fresh accounts, whatever. It's an arms race. And, realistically, most victims aren't bots or companies; they're people clicking fast because they want a cracked plugin to finish a beat or a game cheat to feel good for five minutes.

So yeah, don't be the victim in the next "I lost all my passwords" thread. Learn the basics. Be suspicious of anything that leans on "password: X" in a pinned comment. And if you're someone who actually benefits from pirated software, take a breath, weigh the cost, and maybe don't be that person this time.

Anyway, that's my messy brain dump. Anyone else following these reports? Seen weird YouTube uploads lately that screamed "too legit"? Share screenshots (obviously redact any real IPs/passwords), argue with me, tell me I'm old ,go.?

Bastille - October 27, 2025, 2:02 am

I've seen many of these videos recently, I can't blame people falling into this because I used to look

for cracked software when I was younger. The difference between 20 years ago and now is that most malware back in the days were just annoying, like random windows popping, or computer crashing with weird GFX and music, it was mostly troolling. Nowadays it targets personal data and can be more harmful.

As the new generation is less comfortable with computer, I'm wondering if they'll be more exposed to such risks. A lot of young people now only have a smartphone, and they're not really familiar with computers.

Thanks for this thread, as great as everytime JoseMar :)