

Forum:[Hack Forums](#)

Thread: [Encryption and cryptography is so fucking interesting.](#)

Curs3d - February 26, 2026, 2:09 pm

There is something different in this field of "hacking" it feels almost like magic to take an old public virus such as Async Rat and get it to dance by billion dollar companies. Once you achieve a FUD file, it almost feels "god like" its addicting almost. The constant cat and mouse game as I sit behind my computer writing code in my spare time. Meanwhile there are teams of people who are paid higher than me, trying to stop someone like us. Yes you can buy malware here on the Marketplace, however almost none are built to be undetectable, its almost lazy. They just make loud noisy malware and leave it all up to the "crypter."

5chn4pp - February 26, 2026, 2:37 pm

(Feb 26, 2026 03:09 PM)Curs3d Wrote: [\[CITE\]](#) Meanwhile there are teams of people who are paid higher than me, trying to stop someone like us.

And we are pretty good at it. Your encrypted file still leaves traces that SOC Analysts have an easy time spotting. Only the companies who skimp out on security have this problem.

methcelik12 - February 27, 2026, 12:53 am

(Feb 26, 2026 03:09 PM)Curs3d Wrote: [\[CITE\]](#) There is something different in this field of "hacking" it feels almost like magic to take an old public virus such as Async Rat and get it to dance by billion dollar companies. Once you achieve a FUD file, it almost feels "god like" its addicting almost. The constant cat and mouse game as I sit behind my computer writing code in my spare time. Meanwhile there are teams of people who are paid higher than me, trying to stop someone like us. Yes you can buy malware here on the Marketplace, however almost none are built to be undetectable, its almost lazy. They just make loud noisy malware and leave it all up to the "crypter." You're absolutely right.

Curs3d - February 27, 2026, 12:36 pm

(Feb 26, 2026 03:37 PM)5chn4pp Wrote: [\[CITE\]](#) And we are pretty good at it. Your encrypted file still leaves traces that SOC Analysts have an easy time spotting. Only the companies who skimp out on security have this problem.

Im sure some company will eventually have AI built into their scan engine and will have the ability to watch behavioral analysis IRT. Until then, it will be able to keep being bypassed.

5chn4pp - February 27, 2026, 12:52 pm

(Feb 27, 2026 01:36 PM)Curs3d Wrote: [\[CITE\]](#) Im sure some company will eventually have AI built into their scan engine and will have the ability to watch behavioral analysis IRT. Until then, it will be able to keep being bypassed.

They already do. Windows Defender for Business, CrowdStrike, SentinelOne, and others already use ML + behavioral analysis. It's misconfiguration and economics that are the problem.

Curs3d - February 27, 2026, 1:02 pm

(Feb 27, 2026 01:52 PM)5chn4pp Wrote: [\[CITE\]](#) They already do. Windows Defender for Business, CrowdStrike, SentinelOne, and others already use ML + behavioral analysis. It's misconfiguration and economics that are the problem.

All listed are beaten with sleep obfuscation and byte junk. ML and AI i feel are two different things.

5chn4pp - February 27, 2026, 1:15 pm

(Feb 27, 2026 02:02 PM)Curs3d Wrote: [\[CITE\]](#) All listed are beaten with sleep obfuscation and byte junk. ML and AI i feel are two different things.

AI is a broad umbrella term that includes machine learning. You could say that ML is a subset of AI.

I feel like you're mixing up standard antivirus with modern EDR solutions which have SOC Analysts behind them.

Curs3d - February 27, 2026, 1:33 pm

(Feb 27, 2026 02:15 PM)5chn4pp Wrote: [\[CITE\]](#) AI is a broad umbrella term that includes machine learning. You could say that ML is a subset of AI.

I feel like you're mixing up standard antivirus with modern EDR solutions which have SOC Analysts behind them.

EDR solutions, only pass to SOC analysts when there is a detection. I think you are a SOC analyst since you referenced this multiple times.

5chn4pp - February 27, 2026, 1:42 pm

(Feb 27, 2026 02:33 PM)Curs3d Wrote: [\[CITE\]](#) EDR solutions, only pass to SOC analysts when there is a detection. I think you are a SOC analyst since you referenced this multiple times.

EDR continuously records telemetry and alerts are only one output. SOCs also hunt proactively and investigate suspicious activity that stays quiet. And those billion dollar companies you mentioned typically have a SOC or an MSSP. EDR with nobody responding is just expensive logging.

Curs3d - February 27, 2026, 1:46 pm

(Feb 27, 2026 02:42 PM)5chn4pp Wrote: [\[CITE\]](#) EDR continuously records telemetry and alerts are only one output. SOCs also hunt proactively and investigate suspicious activity that stays quiet. And those billion dollar companies you mentioned typically have a SOC or an MSSP. EDR with nobody responding is just expensive logging.

I get what you're saying, but I think you're assuming every org runs a mature SOC.

Plenty of companies buy CrowdStrike/SentinelOne/Carbon Black because "compliance says so," then nobody actually hunts or reviews telemetry.

In those environments, the EDR really does end up functioning as expensive logging with a few alerts sprinkled in.

So the gap isn't in the tech. It's in the operational follow-through.

Plumbing companies dont review telemetry.

5chn4pp - February 27, 2026, 1:53 pm

(Feb 27, 2026 02:46 PM)Curs3d Wrote: [\[CITE\]](#) I get what you're saying, but I think you're assuming every org runs a mature SOC.

Plenty of companies buy CrowdStrike/SentinelOne/Carbon Black because "compliance says so," then nobody actually hunts or reviews telemetry.

In those environments, the EDR really does end up functioning as expensive logging with a few alerts sprinkled in.

So the gap isn't in the tech. It's in the operational follow-through.

Sounds like we agree on the core point :)

As I said earlier: "Only the companies who skimp out on security have this problem."

If a company buys EDR just because compliance says so, they're skimping on the people and process needed to run it (monitoring, hunting, response). Even large companies sometimes don't

prioritize that due to economics or misunderstanding what operating EDR actually takes.

Curs3d - February 27, 2026, 1:55 pm

(Feb 27, 2026 02:53 PM)5chn4pp Wrote: [\[CITE\]](#) Sounds like we agree on the core point :)

As I said earlier: "Only the companies who skimp out on security have this problem."

If a company buys EDR just because compliance says so, they're skimping on the people and process needed to run it (monitoring, hunting, response). Even large companies sometimes don't prioritize that due to economics or misunderstanding what operating EDR actually takes.

Hopefully malware doesn't nuke services. :)

[Video: <https://www.youtube.com/watch?v=5v6JUzxWoGw&list=RDRo7vzNz0NmY&index=27>]