

Forum: [Hack Forums](#)

Thread: [Aeternum C2 Botnet Stores Encrypted Commands on Polygon Blockchain to Evade Takedown](#)

Stanley - March 7, 2026, 4:05 pm

Aeternum C2 Botnet Stores Encrypted Commands on Polygon Blockchain to Evade Takedown

Cybersecurity researchers have disclosed details of a new botnet loader called Aeternum C2 that uses a blockchain-based command-and-control (C2) infrastructure to make it resilient to takedown efforts.

"Instead of relying on traditional servers or domains for command-and-control, Aeternum stores its instructions on the public Polygon blockchain," Qrator Labs said in a report shared with The

<https://thehackernews.com/2026/02/aeternum-c2-botnet-stores-encrypted.html>

W1NK1LL3RX - March 8, 2026, 7:53 am

This botnet uses the Polygon blockchain to store its hidden commands. That makes it harder to shut down than a normal server-based attack. It's a smart trick by attackers, but bad news for defenders.

Basically, criminals are using blockchain to make malware more persistent.

Immortal - March 8, 2026, 8:11 am

(Mar 8, 2026 07:53 AM)W1NK1LL3RX Wrote: [\[CITE\]](#) This botnet uses the Polygon blockchain to store its hidden commands. That makes it harder to shut down than a normal server-based attack.

Harder to shut down, sure, but it's not invincible. We've seen similar logic with Namecoin and Bitcoin's OP_RETURN in the past. The real advantage here isn't just "blockchain magic" it is the fact that Polygon's RPC nodes act as a massive, legitimate proxy layer.

Defenders can't exactly null route the entire Polygon network without breaking dozens of legitimate enterprise apps. Aeternum is basically hiding in plain sight. As long as the wallet address isn't hardcoded and can be rotated, the persistence is nearly 100% until the infection is nuked at the endpoint level.

(Mar 8, 2026 07:53 AM)W1NK1LL3RX Wrote: [\[CITE\]](#) Basically, criminals are using blockchain to make malware more persistent.

It was only a matter of time before someone moved away from the more expensive chains to something like Polygon for C2. Traditional takedowns rely on registrars and hosting providers playing ball. You can't send a DMCA or a "cease and desist" to a smart contract.

It's a cat & mouse game. Defenders will eventually just start flagging any outbound traffic to common RPC endpoints (Infura, Alchemy, etc.) from unauthorized processes, but by then, the dev will have already swapped to a different sidechain.

(Mar 8, 2026 07:53 AM)W1NK1LL3RX Wrote: [\[CITE\]](#) It's a smart trick by attackers, but bad news for defenders.

It's the ultimate "dead drop." Using a public ledger for C2 instructions means the botnet doesn't even need to "phone home" in the traditional sense. It just needs to read the latest transaction data from a specific contract or wallet.

The real "bad news" for defenders is that this architecture essentially eliminates the single point of failure. You can sinkhole a domain, but you can't sinkhole the Polygon mainnet. Expect to see more of this as gas fees on Layer 2s continue to drop.