Free Censorship-Resistant Infrastructure:

When Malware Uses the BSC Testnet Better Than Web3 Startups

Thomas LOWAGIE

Pass the SALT — RUMP Session

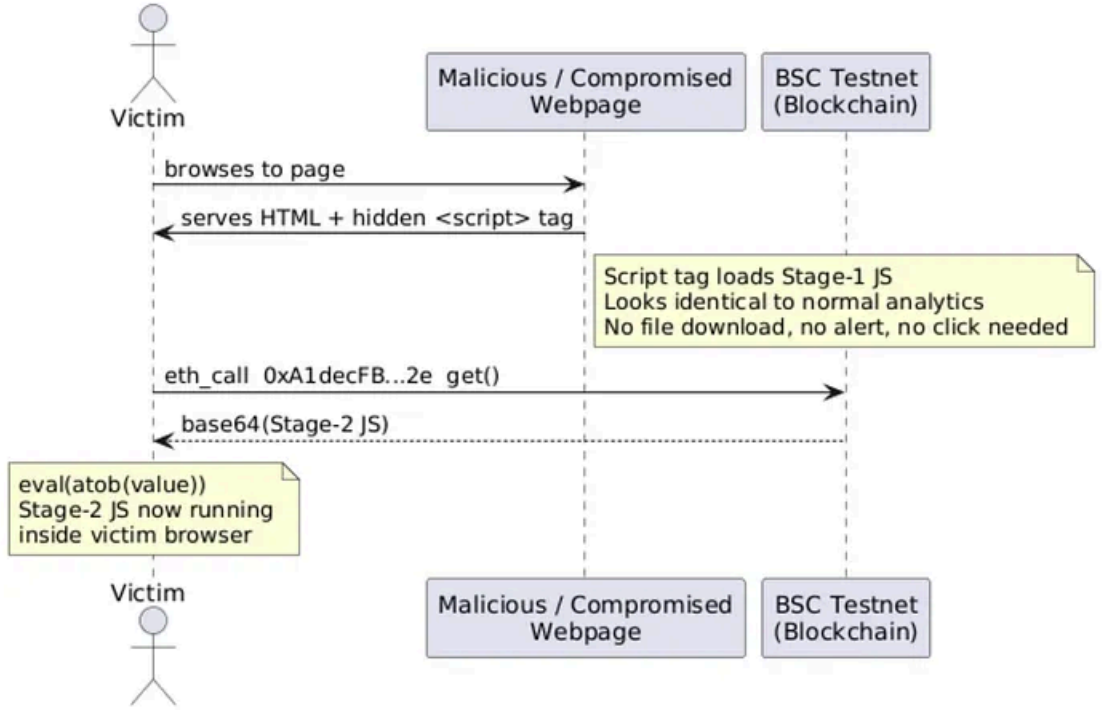
EtherHiding Overview

Using blockchain as attacker infrastructure

Two main usages

- C2 resolution (dead drop)
- Payload / code storage

Example:
eth_call → decode → extract C2 or payload



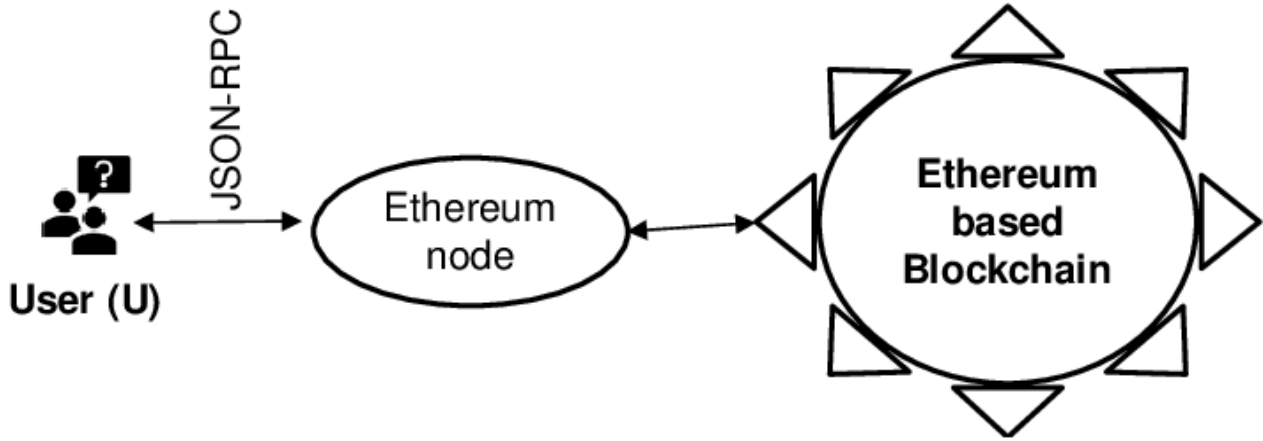
Why Attackers Love It

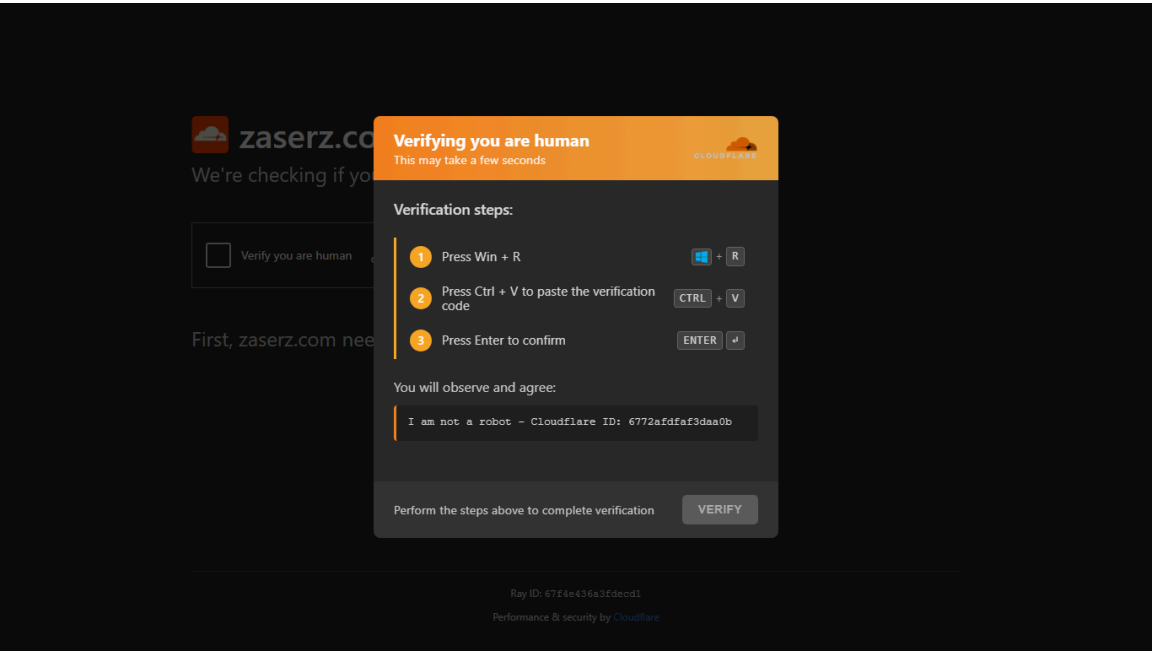
Key advantages

- No central server
- Hard to take down
- Public but trusted infrastructure
- Easy to update remotely

Resilient & flexible C2

Already documented by Mandiant, Sekoia, Guardio…





ClickFix + EtherHiding

Social engineering infection chain:

1. Malicious webpage
2. Fake CAPTCHA
3. User executes command

New observation

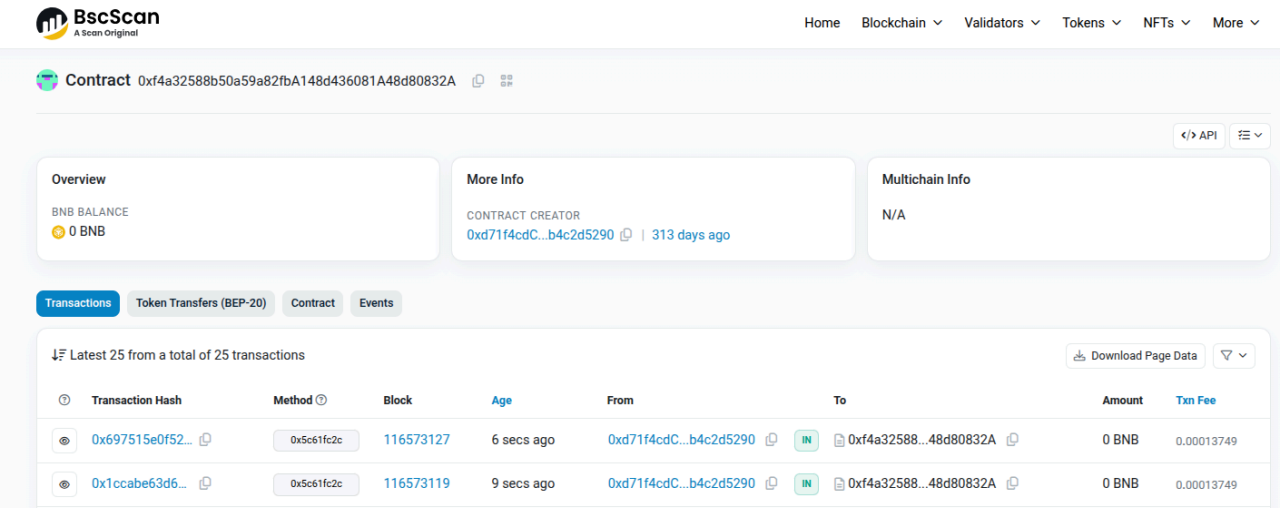
- Smart contract interaction
- Uses victim identifier (usr_id)
- Reads AND writes on-chain

Blockchain used to track victims

Threat Intelligence Opportunity

Blockchain properties

- Public
- Immutable
- Timestamped



Reality

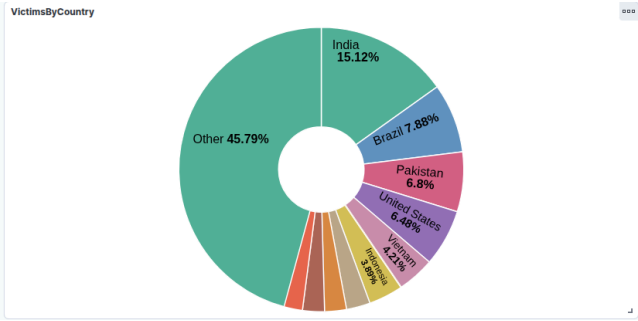
- Not indexed by default
- BUT accessible via:
  - explorers
  - RPC APIs

Tracking a Campaign

What we can follow

- Victims → transaction logs → Kibana
- C2 → contract / Polygon
- Payloads → (sometimes on-chain)

Continuous campaign visibility

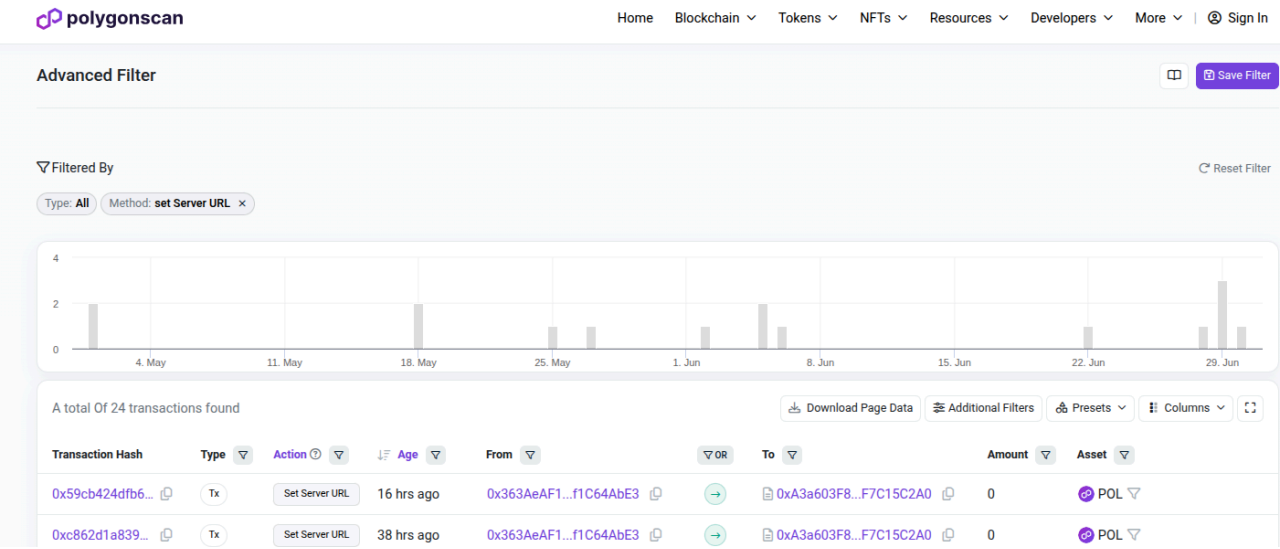


What’s Next?

New opportunities

- Detect similar contracts
  - find-similar-contracts
  - advanced-filter
- Track campaigns without samples
- Correlate attacker activity
- Monitor evolution over time

Blockchain = intel source



Conclusion

- They wanted immutability.
  - They got a permanent, timestamped confession.
- EtherHiding is evolving — victim tracking, not just C2
  - If it's on-chain, it's observable
  - If it's observable, it's huntable

Full writeup + IOCs