

---

# AI-Enhanced Ransomware Attacks: **Slopoly**

---

# A Start to AI-Enhanced Ransomware Attacks: Slopoly

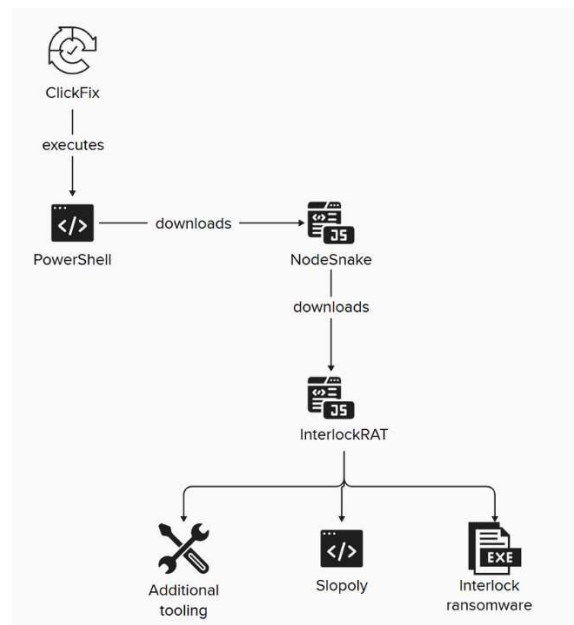
A new malware strain named Slopoly has emerged as a key component in Interlock ransomware operations, and researchers believe it was likely generated by a large language model. Deployed after a ClickFix social engineering ruse, the Slopoly backdoor allowed threat actors to maintain access to a compromised server for over a week, exfiltrating data before encryption.

## From ClickFix to Ransomware

The breach began with a ClickFix social engineering flow, a technique that tricks users into running malicious commands under the guise of fixing an issue. From there, the attackers deployed multiple malware components:

- Slopoly: A PowerShell-based C2 client acting as a persistence and command framework.
- NodeSnake: Additional backdoor functionality.
- InterlockRAT: Remote access tool for deeper control.
- JunkFiction Loader: Delivered the final Interlock ransomware payload.

The attackers remained on the server for more than a week, exfiltrating data before encryption, a hallmark of modern extortion operations.



# Slopoly: AI-Generated C2 Framework

Researchers analyzed the Slopoly PowerShell script and found strong indicators of LLM-assisted development:

- Extensive inline commentary.
- Structured logging and error handling.
- Clearly named variables and functions.
- Code organization atypical of human-developed malware.

The script was generated by an AI model, then likely customized by a builder that inserted configuration values like beacon intervals, C2 addresses, mutex names, and session IDs.

## Unsophisticated Malware

Despite being described in its own comments as a "Polymorphic C2 Persistence Client," Slopoly lacks true polymorphism, it cannot modify its own code during execution. However, the builder can generate new clients with randomized configurations and function names, a standard practice among malware builders.

## Slopoly Capabilities

Deployed to C:\ProgramData\Microsoft\Windows\Runtime\, Slopoly performs:

- System information collection.
- Heartbeat beacons to C2 every 30 seconds (/api/commands).
- Command polling every 50 seconds.
- Execution of received commands via cmd.exe.
- Output exfiltration back to C2.
- Rotating persistence log maintenance.
- Persistence via scheduled task named "Runtime Broker".

Supported commands include:

- Download and execute EXE, DLL, or JavaScript payloads.
- Run shell commands and return results.
- Change beaconing intervals.
- Update itself.
- Exit its own process.

## Hive0163

The operators behind this campaign are tracked as Hive0163, a group focused on extortion through large-scale data exfiltration and ransomware. For initial access, Hive0163 is known to leverage

ClickFix and malvertising and reportedly also relies on initial access brokers (IAB) such as TA569 (SocGholish malware) and TAG-124 (Landupdate808, KongTuke) TDS.

They have previously claimed attacks against Texas Tech University System, DaVita, Kettering Health, City of Saint Paul, Minnesota. Researchers note possible associations with developers behind Broomstick, SocksShell, PortStarter, SystemBC, and Rhysida ransomware operators.

## Interlock Ransomware Payload

The final ransomware payload is the Windows version of the Interlock ransomware, it is a 64-bit portable executable (PE) file delivered via the JunkFiction loader.

- Executes as a scheduled task running as SYSTEM.
- Uses Windows Restart Manager API to release locked files.
- Prior to encryption, appends the file extension `!.NT3RLOCK` or `.int3R1Ock` extensions to encrypted files.

Interlock ransomware first emerged in 2024 and was an early adopter of ClickFix social engineering, later also using a FileFix variant.

## Recommendations and Indicators of Compromise (IoC)

- Scams will be trained offline against the exact models millions rely on.
- They will be optimized until they work flawlessly on first contact.
- The AI browser that protects you today may be the vector that delivers you tomorrow.

When your AI explains why it stopped, it's teaching attackers how to get past it. The transparency built for trust is now fuel for compromise.

Indicator	Indicator type	Context
0884e5590bdf3763f8529453fbd24ee46a3a460 bba4c2da5b0141f5ec6a35675	SHA256	Redacted Slopoly script (uploaded to VirusTotal by X-Force)
plurfestivalgalaxy[.]com	Domain	Slopoly C2 server domain (no longer active)
94[.]156[.]181[.]89	IPv4	Slopoly C2 server IP address
77[.]42[.]75[.]119	IPv4	C2 server associated with Hive0163
23[.]227[.]203[.]123	IPv4	C2 server associated with Hive0163
172[.]86[.]68[.]64	IPv4	C2 server associated with Hive0163
bridal-custody-private-bodies[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
corner-teacher-guam-characterization[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
yen-hansen-cartoon-aims[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
cigarette-assumed-biotechnology-checklist[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
meet-noted-tax-qualification[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
liverpool-patterns-lanes-specified[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
jane-practitioner-lightning-preservation[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
misc-elliott-mouth-leading[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
playback-attributes-interviews-processing[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
postal-ssl-converted-quantity[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
forget-canal-chancellor-mas[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
chronic-dividend-amendments-das[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
planners-mixing-edmonton-endless[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
baseline-include-priority-bar[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
specials-storm-height-warriors[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
safe-accepted-salem-early[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163

bits-promotions-turned-editions[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
logan-practitioners-percent-cartridges[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
eugene-examinations-contained-timber[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
moore-cgi-pen-drove[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
screenshots-executive-joins-hammer[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
coffee-lloyd-families-excluded[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
communist-flying-provision-calendar[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
lamp-voters-biodiversity-phillips[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
rpm-chicken-during-staying[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
module-source-tree-diverse[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
offers-listing-screenshot-alpha[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
electrical-protect-molecular-underground[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
silk-lift-porter-correctly[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
wives-bufing-humans-prot[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
describe-absent-operational-seventh[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
edinburgh-packaging-sense-idol[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163
gzip-picked-istanbul-maple[.]trycloudflare[.]com	Domain	C2 server associated with Hive0163

**Ready to see how AICenturion can secure you against AI risks?**

Request a demo today: [hello@cytex.io](mailto:hello@cytex.io)

Connect with our social media channels

