Payload Ransomware: In-depth technical analysis

By Editor

Published: 2026-05-05 · Archived: 2026-05-20 02:01:25 UTC

Payload is a cross-platform ransomware family with both Windows and Linux variants. In this blog, we will primarily focus on the Windows variant and its behavior in detail.

Payload provides extensive support for command-line arguments, suggesting it can be operated manually or remotely. It appears to work as an operator-driven ransomware executable rather than a simple one-click . This design allows operators to selectively enable or disable features based on the target environment or operational objectives .

Below is the list of arguments that can be supplied by the operators:

Flag	**Effect when present**	**Default behavior**
`–background`	Runs encryption in the background (no console window); does NOT re-spawn itself	N/A
`-m`	Skips mutex creation/check (allows multiple instances)	Mutex is created to enforce single instance
`-n`	Does NOT write the ransom note to disk	Ransom note is written
`-d`	Disables self-deletion	Self-deletion is executed after run
`-k`	Does NOT kill processes or stop services	Target processes/services are terminated
`-s`	Skips network share enumeration (only local drives targeted)	Network shares are also enumerated and encrypted
`-l`	Wipes all Windows Event Logs after encryption (anti-forensics)	Event logs are left unchanged
`-i`	Ignores filename filters (may re-encrypt its own files like notes or payload artifacts)	Filename filters are enforced to avoid its files and system files
`–bypass-etw`	Patches ETW functions in `ntdll` to disable logging	ETW remains functional
`–algo`	Forces a specific ChaCha20 implementation (AVX2 or SSE2 optimized)	Algorithm path is auto-detected based on CPU

Flag	Effect when present	Default behavior
`–threads N`	Sets number of worker threads for encryption	Defaults to number of CPU cores
`-p <path>`	Encrypts only the specified path	All drives are enumerated and encrypted
`–log <path>`	Overrides default log file location	Logs written to `C:\payload.log`

IOC Type	Value
Windows Variant Hash	1ca67af90400ee6cbbd42175293274a0f5dc05315096cb2e214e4bfe12ffb71f
Linux Variant Hash	bed8d1752a12e5681412efbb8283910857f7c5c431c2d73f9bbc5b379047a316
Mutex	MakeAmericaGreatAgain
Log File	C:\payload.log
Ransom Note	C:\RECOVER_payload.txt
Ransomware Infrastructure (Tor-based)	payloadynyvabjacbun4uwhmxc7yvdzorycslzmnleguxjn7glahsvqd[.]onion payloadrz5yw227brtbvdqpnlhq3rdcdekdnn3rgucbcdeawq2v6vuyd[.]onion

---

Source: https://www.egfincirt.org.eg/payload-ransomware