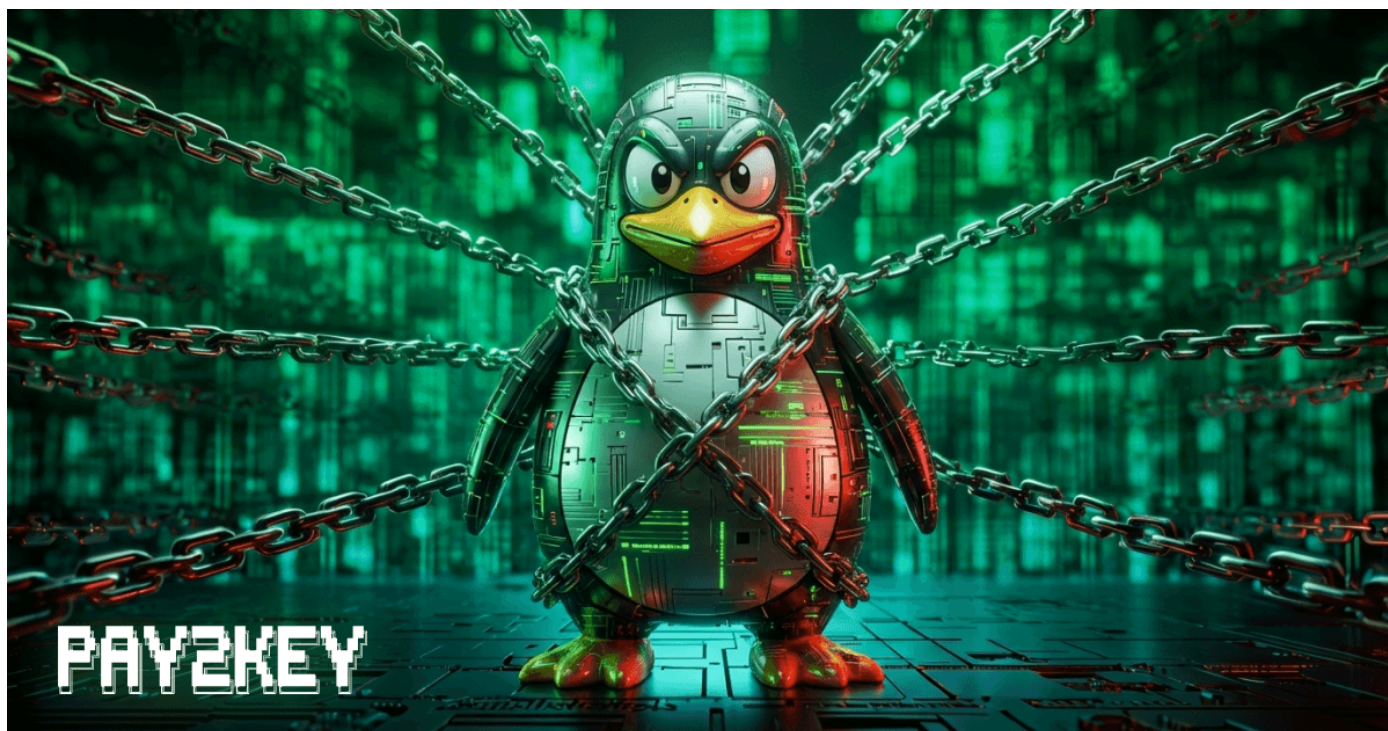


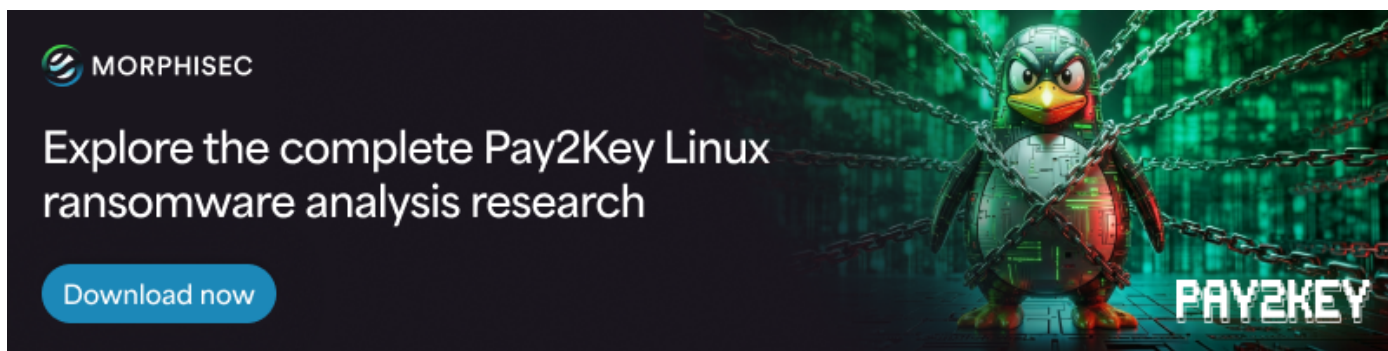
Inside Pay2Key: Technical Analysis of a Linux Ransomware Variant

 morphisec.com/blog/inside-pay2key-technical-analysis-of-a-linux-ransomware-variant

March 24, 2026



As the geopolitical landscape continues to evolve, Morphisec Threat Labs is bringing technical focus to threats that have gone under-analyzed. [Pay2Key](#), an Iranian-attributed ransomware group, has not been prominently active in recent campaigns, but their Linux variant offers a valuable lens into techniques that are shared across multiple active ransomware families today.



Introduction

Linux ransomware remains one of the least documented threat categories in public research, yet ransomware groups are increasingly adding Linux support to their arsenals, targeting the servers and infrastructure that organizations depend on most.

In this blog, we provide a deep technical dive into the Linux build of Pay2Key.I2 ransomware, [initially detected in the wild in late August 2025](#). The sample is configuration-driven, requires root-level privileges to execute, and is engineered to traverse broad filesystem scope, classify mounts, and encrypt data using ChaCha20 in full or partial modes. Understanding how it operates matters, not just for Pay2Key, but for the broader class of Linux ransomware it represents.

Morphisec prevents these attacks across both Linux and Windows environments.

Threat Analysis

Pay2Key's Linux variant is built for scale and stability. It first checks for root privileges, then reads a JSON configuration that controls what it targets and how it behaves. Before encryption, it weakens defences and removes friction by stopping services, killing processes, disabling SELinux and AppArmor, and installing a reboot-time cron entry. This lets the encryptor run faster and survive restarts.

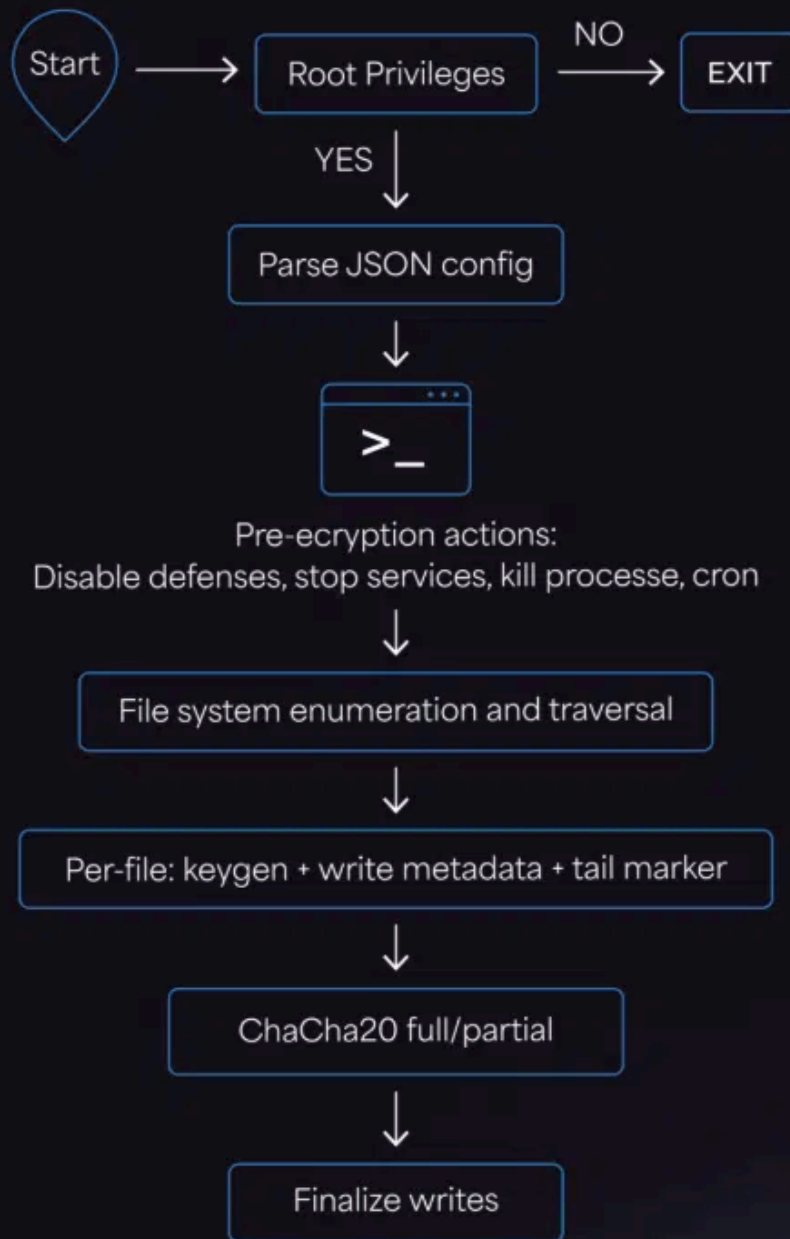
For filesystem coverage, the malware enumerates `/proc/mounts`, filters out pseudo-filesystems, and classifies mounts (read-only, removable, and other). It skips read-only mounts and routes work into different queues. During per-file processing it intentionally skips ELF/MZ binaries and zero-length files, which reduces the chance of crashing the host mid-run.

The encryptor uses ChaCha20 algorithm for file encryption with two modes: full-file encryption or sampled/partial encryption. The mode and boundaries are driven by configuration, giving operators flexibility for speed versus impact. Per-file keys are generated and stored in an obfuscated metadata block.

A hardcoded string, "DontDecompileMePlease", is serving two main purposes, one of which is the metadata key derivation, and a tail marker validation step confirms the metadata layout during processing, while the other purpose is implicitly hide the obvious logical flaw in the key storage mechanism.

The ransom note references a Clearnet portal and an I2P fallback, implying negotiation infrastructure. In the reviewed artifacts there is no evidence of a network C2 loop or data exfiltration routines; the observed "statistics" feature is local file/FIFO-based.

High level Attack Chain



How Morphisec Can Help

Pay2Key's Linux build is a reminder that [ransomware defense on Linux](#) must be purpose-built: once an encryptor with root-level access begins traversing the filesystem, response time collapses and the window to prevent irreversible damage closes fast.

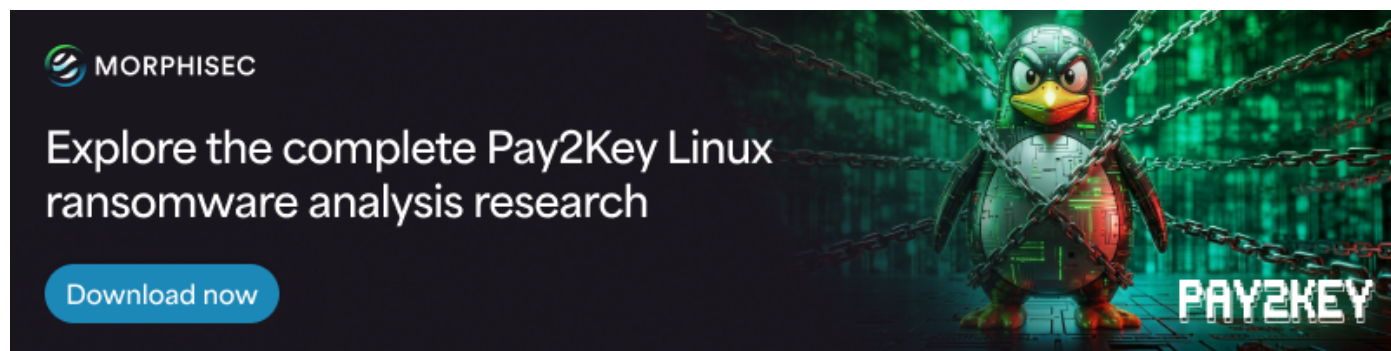
Morphisec's [Anti-Ransomware Assurance Suite](#) for Linux is purpose-built for exactly this threat profile. It is designed to stop ransomware execution paths before encryption can take hold; prevention-first controls keep encryption from ever reaching scale. This is achieved without relying on signatures or behavioral detection that kicks in too late.

[Automated Moving Target Defense \(AMTD\)](#) further reduces the attacker's ability to execute reliably across endpoints and workloads, adding a layer of unpredictability that disrupts the consistency that ransomware operators depend on.

Download the Full Technical Analysis

Morphisec Threat Labs conducted a deeper technical investigation into the Pay2Key Linux ransomware variant, including detailed reverse-engineering findings, encryption mechanics, and defensive implications for security teams.

Download the full Pay2Key Linux ransomware analysis (PDF) to explore the complete research:



About the author



Ilia Kulmin

Security Researcher @ Morphisec

Ilia Kulmin is an experience security researcher specializing in emerging and sophisticated threats. Ilia is bringing to this role a rich background in gathering and managing intelligence.

Unlock Your ROI Potential with Morphisec

[Calculate ROI](#)