RedACTinsights

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

# RANSOMWARE AND AI
## ECONOMICS, PSYCHOLOGY, ACTORS, AND THE NEW TOOLING LOOP

**NOVEMBER 2025**

@SIGNORINA37

*real data. real threats.* ***ransomNews.***

# /about_insights

RedACT *insights* is the strategic analysis line of ransomNews.
Built as an extension of the monthly RedACT report, it delivers in-depth coverage of ransomware trends, threat actors, tactics, and sector-specific risks.

Each piece is **grounded in verified data**, manual intelligence workflows, and OSINT/SOCMINT methodologies - developed through extensive research and a deep passion for threat analysis.

Tailored for decision-makers, analysts, incident responders, and cybersecurity professionals, RedACT *insights* offers focused, actionable content drawn from real-world threat dynamics.

RedACTinsights

# /follow_us

ransomnews.online
bsky.app/profile/ransomnews.online
linkedin.com/company/ransomnews
github.com/ransomnews
x.com/ransomnews
desk@ransomnews.online

# /use_conditions

# **Ransomware and AI**
## Economics, psychology, actors, and the new tooling loop

**HIGHLIGHTS**

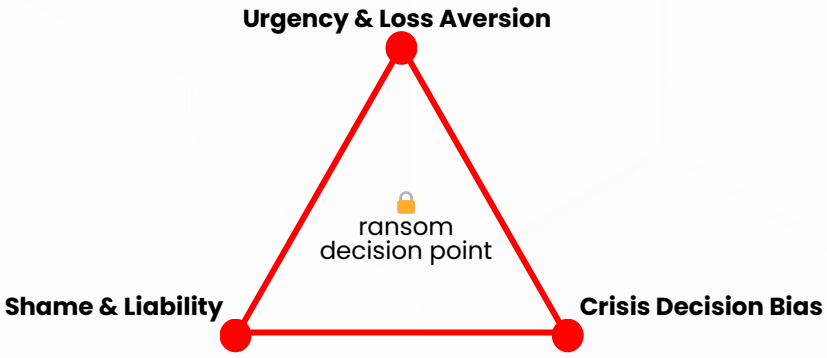
- **Ransomware has matured** from crude DOS "license renewals" into a global extortion economy with industrial-scale tooling, affiliate ecosystems, and aggressive multi-vector coercion. The current phase layers AI-assisted development and social engineering onto double/triple extortion playbooks, while law enforcement pressure and falling payment rates force gangs to consolidate and innovate.

- Current evolution reflects a **broader arms race** between automation and adaptation. As defensive frameworks integrate AI driven anomaly detection, attackers are mirroring that sophistication, using the same class of tools to fuzz detection thresholds, optimize payload delivery, and simulate legitimate user behavior. This kind of "co-evolution" has turned ransomware from a **static criminal product** into a **dynamic service ecosystem** powered by feedback loops: codebases mutate through stolen research, extortion scripts adjust to cultural and linguistic nuances, and AI aids in both the reconnaissance and persuasion layers of an attack.

## Why ransomware exists: psychological and economic levers

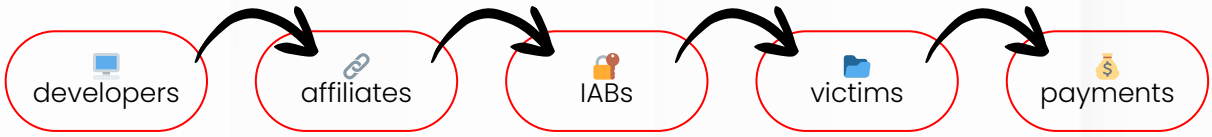
Ransomware works because it **converts time into leverage**.
Attackers amplify three human/economic pressure points:

- **urgency and loss aversion**: downtime costs escalate hourly
- **shame and liability**: data-leak exposure to customers/regulators
- **bounded rationality under crisis**: execs seek "fastest path to resume ops"




**Data theft** (as double extortion) and addon **DDoS/harassment** (as triple extortion) increase coercive power without any technical sophistication, raising willingness to pay even when backups exist.

**Ransomware-as-a-Service** (RaaS) reduces barriers, as core developers sell lockers and portals; affiliates run intrusion ops; initial-access brokers (IABs) sell footholds, and the whole structured ecosystem is satisfied.
Competition then shifts to "brand," support, builder quality, and payout splits.




Ransomware-as-a-Service economy: how crime scales like SaaS

2023 ransom flows hit a record of 1.1B$; by 2025 payment rates and medians are falling, forcing **more aggressive extortion** and faster "time-to-impact."

## Key actors (2024-2025)

**LockBit**: historically the highest-volume brand; disrupted by Operation Cronos (a jointed action by NCA/FBI/Europol), yet remnants and copycats persist. Takedown details and arrests significantly degraded infrastructure, but rebrands continue to appear.

One of the most prolific ransomware-as-a-service (RaaS) operations worldwide, active since 2019; US Domestic Cybersecurity & Infrastructure Security Agency (CISA) reports: "*In 2022, LockBit was the most active global ransomware group and RaaS provider in terms of victim count.*"
After disruption, LockBit resurfaced in Sept 2025 with version "LockBit 5.0 (ChuongDong)" targeting Windows, Linux, ESXi environments.


### Business model & evolution

- LockBit operates as a classic RaaS: core developers build/maintain the ransomware and infrastructure; affiliates carry out break-ins and deployment
- affiliates typically pay a cut or share of ransom proceeds; often reported LockBit claimed 20% with 80% going to affiliates in some versions
- they continuously evolve: from early versions in 2019 to LockBit 2.0, 3.0, Black/Green variants, incorporating new features (ESXi support) and expanding affiliate enrolment
- after the global law-enforcement disruption (Operation Cronos) they adapted by fragmenting infrastructure, using more proxies, and opening new variant channels

### Tactics, Techniques & Procedures (TTPs)

initial access: brute-forcing RDP/VPN, exploiting known vulnerabilities, credential harvesting

- lateral movement using legitimate tools (PsExec), shadow-copy deletion, encryption of shares and servers, data exfiltration followed by leak site publication (double extortion)
- they maintain variability because of many unaffiliated affiliates; TTPs differ widely between attacks

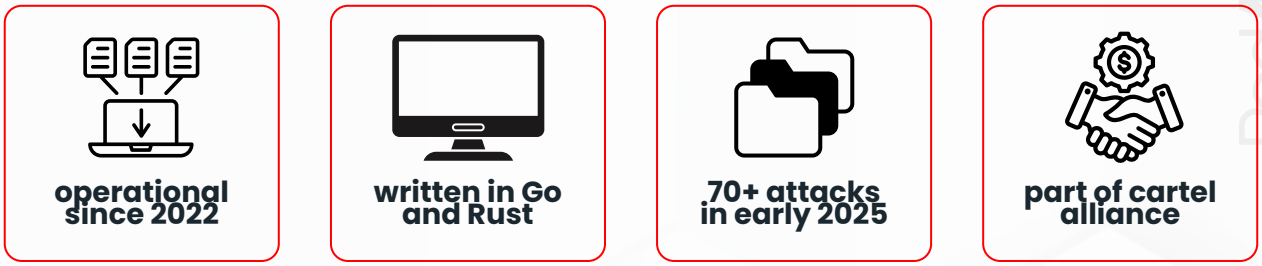
Notable incidents

- targets included major infrastructure, manufacturing, and services worldwide (e.g., UK postal service, hospitals) as detailed in news reports

**Qilin**: the ransomware family originally known as Agenda (reports from HHS, Check Point, and other CTI providers) surfaced mid 2022 and by September of that year transitioned into the branding of Qilin.

A relatively new ransomware group, yet very high operational tempo since late 2024; active in North America with polished RaaS operations; it is described in the news as forming a "cartel" together with LockBit and DragonForce, sharing tactics, infrastructure and affiliates.

A threat intelligence report noted Qilin "has introduced comprehensive victim pressure services" (legal support, regulatory risk review, ..) beyond traditional encryption/leak extortion.




Business model & evolution

- started around July/August 2022 under the name Agenda; later rebranded to Qilin and adopted Rust/Go variants
- operates a RaaS model: provides affiliates with customizable panels, leak-site management, and infrastructure
- rapid growth: by mid 2025 it claimed dozens of attacks per month (104 victims in one month) and became one of the most active threats globally
- targets broadened from manufacturing and professional services to state/local government (SLTTs) and critical infrastructure

Tactics, Techniques & Procedures (TTPs)

- initial access: exploits RDP, VPN misconfigurations, known internet-exposed services (Fortinet devices)
- use of exfiltration tools (Cyberduck) and dual encryptor binaries (encryptor_1.exe via PsExec, encryptor_2.exe for network shares)

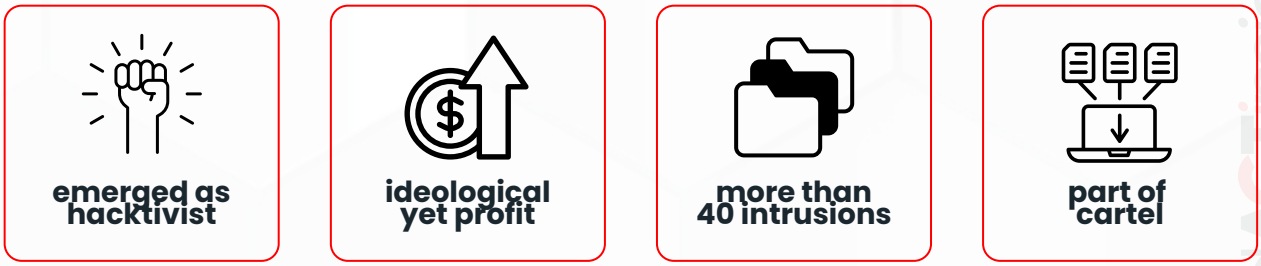
advanced features: BYOVD (Bring Your Own Vulnerable Driver) to disable EDRs, Rust-based variants, cross-platform support

Notable incidents

- in Q2 2025, Qilin was identified as the top ransomware threat to US SLTT entities, responsible for nearly one quarter of incidents in that category
- the group claimed responsibility for 104 attacks globally in August 2025, using double extortion
- a UK pathology/diagnostics provider hack impacted multiple London hospitals, showing real-world harm in healthcare

**DragonForce**: a newer RaaS operator experimenting with affiliate models that has shifted from **hacktivist roots** into hybrid extortion for profit, blending ideological operations with commercial ransomware.

First emerged around August 2023 with the name of **DragonForce Malaysia** - while its name suggests Malaysian roots, several analysts point to Russian-speaking infrastructure and behaviour (avoidance of CIS nation targets) which raises questions about its true base.




Business model & evolution

- DragonForce offers a sophisticated affiliate programme: white-label ransomware kits, customizable payloads, leak-site services (RansomBay) and low-barrier entry for affiliates
- it uses a dual variant technical model: early payloads derived from leaked code of LockBit 3.0, followed by a variant built on the leaked CONTI V3 source. Affiliates can choose which to deploy
- in March 2025 the group publicly declared itself a "cartel" aiming to dominate the ransomware affiliate market, absorb rivals, attract displaced affiliate networks (former RansomHub members) and restructure relationships

Tactics, Techniques & Procedures (TTPs)

- initial access vectors: spear phishing, exploitation of high-profile vulnerabilities (like CVE-2021-44228 Log4Shell, Ivanti Connect exploits) and credential harvesting
- post-compromise tools: they use Cobalt Strike, Mimikatz, SystemBC; persist via scheduled tasks, registry modifications, token manipulation, process injection and BYOVD (bring-your-own-vulnerability/drivers) techniques
- encryption/extortion: support Windows, Linux and ESXi environments; append custom extensions (ie ".dragonforce_encrypted"), use AES-256, RSA, and ChaCha8 algorithms. Exfiltrate via SFTP, WebDAV, cloud storage or dedicated leak portals

Targets & notable incidents

- in April/May 2025 DragonForce affiliates executed a high-profile campaign against

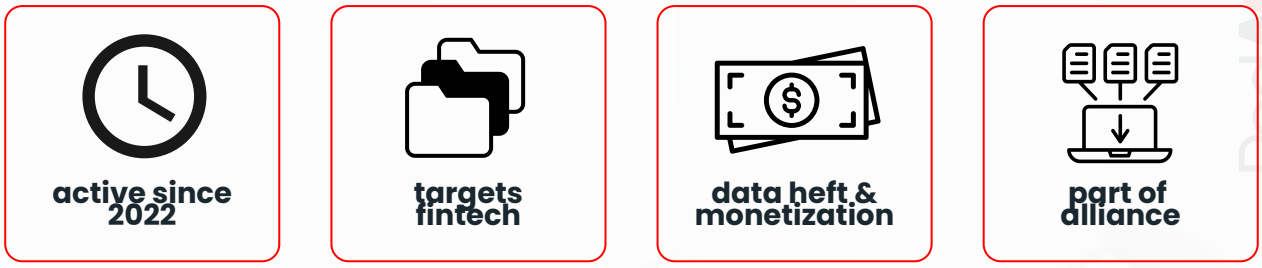
UK retail giants such as Marks & Spencer (M&S), Harrods and Co-operative Group (Co-op). The disruption to operations and logistics was severe
- according to partner reporting, in that M&S incident the attacker chain involved social engineering by groups like Scattered Spider and payload deployment by DragonForce tools, showcasing its role as the facilitator for other threat actors

**Scattered Spider**: also known as UNC3944, Octo Tempest, or Muddled Libra, originated as an English-speaking **collective** of young, technically adept social engineers in late 2021/early 2022.

Unlike traditional Eastern European ransomware groups, it emerged primarily from English language **forums** and **Telegram communities** rather than Russian-speaking darknets.

Initially, the group monetized access by selling credentials or performing data theft, but by mid 2023 it began partnering with RaaS outfits such as **ALPHV/BlackCat** and DragonForce to handle the ransomware phase.

This hybrid approach allowed Scattered Spider to remain nimble-acting as a broker, intruder, or extortion arm depending on opportunity.




Business model & evolution

- began around 2022 focusing on social engineering intrusions (help-desk impersonation, SIM swap) then evolved into full extortion and ransomware partnerships
- while not strictly a dedicated RaaS provider, they partner with or deploy ransomware variants (using DragonForce encryptor) and monetize via data theft + extortion
- they place emphasis on identity/credential breach, third-party vendor compromise, and then handover to ransomware or leak operations (ie using vendor IT credentials for major retail breach)

Tactics, Techniques & Procedures (TTPs)

- initial access: social engineering of help desk staff, SIM swap attacks to bypass MFA, purchase of contractor credentials on dark markets
- lateral movement and exfiltration: living-off-the-land (LOTL) techniques, use of allowlisted apps, exfiltration to MEGA/NZ or AWS S3, then optional encryption/ransom
- flexible TTPs: they frequently modify their methods to evade detection, shifting attack vectors (from SIM swap to cloud account takeover)

Notable incidents

- in 2023 they famously breached major casino operators (MGM Resorts International, Caesars Entertainment) via social engineering, requiring major reputational and financial impact
- in 2025, they leveraged third party vendor credentials to compromise Marks & Spencer (UK retail) via IT-supplier channels, causing major disruption and market loss
- expanded targeting into aviation, insurance and retail sectors in Q2-Q3 2025 with heightened activity

## Most used ransomware types and techniques

Modern ransomware operations **have diversified** far beyond the simple encrypt-and-ransom model that dominated the early 2010s.
File encrypting lockers remain the backbone of the ecosystem: malware that systematically encrypts files across Windows, Linux, and increasingly VMware ESXi environments to paralyze business operations.

However, **leakware**, which focuses solely on data exfiltration and public exposure without encryption, is growing in popularity because it **reduces operational complexity** and **limits forensic traces** while still delivering strong psychological leverage. Attackers increasingly rely on double and triple extortion models, coupling encryption with data leaks, DDoS assaults, or even harassment of partners and clients to force faster payment.

Traditional ransomware **encrypts thousands of files**, **modifies file headers**, **deletes backups**, **drops ransom notes**, and often **leaves clear process** and **registry artifacts**, all of which are **rich evidence for digital forensics**.

Leakware, by contrast, focuses on **exfiltration and coercion**, not disruption.
The attacker **simply gains access**, compresses and exfiltrates sensitive data, and threatens to publish it. Because it doesn't alter file systems en masse or trigger large scale encryption routines, it **avoids the telltale indicators** that would normally alert defenders or allow responders to trace the infection chain.

From a **forensic perspective**, this means **fewer logs of encryption processes**, no widespread file I/O anomalies, no ransom note artifacts, and no mass file renames, just **network exfiltration traffic** and possibly **temporary staging directories**.

That subtlety complicates incident response: defenders **may discover** the breach only after a dataleak announcement appears on a dark web portal, long after volatile evidence (memory contents, temporary cache files, transient C2 channels) has disappeared.

In short, leakware trades the noisy impact of system encryption for a quieter, stealthier path to the same **psychological pressure and public exposure**.

To **maximize efficiency**, many crews deploy intermittent encryption, a tactic that encrypts only segments of files, enough to render them useless but allowing for faster execution and reduced detection by security tools.
The shift to **multiplatform builds** (supporting Windows, Linux, and ESXi hypervisors) reflects attackers' desire for broader reach and higher ransom potential. Many modern ESXi-targeting variants trace their lineage back to leaked Babuk source code, which became the blueprint for a new generation of hypervisor-focused ransomware families.

Supporting this industrialization is a mature cybercrime economy built on RaaS and Initial Access Broker (IAB) markets. Core developers **rent their code to affiliates**, who buy stolen credentials or network footholds from IABs, dramatically compressing the time between breach and ransom demand.

This modular business architecture means that even small, less technical actors can participate, perpetuating a self-sustaining ecosystem that now mirrors legitimate SaaS models, complete with customer support, version updates, and affiliate recruitment.

Most used, known and diffuse tactics:

- **file encrypting lockers** (Windows/Linux/ESXi) remain dominant; leakware (data-exfiltration-only) rise where encryption attracts too much heat
- **double and triple extortion** (encryption + leak + DDoS/third-party harassment) are mainstream coercion patterns
- **intermittent encryption and multiplatform builds** (Windows, Linux, ESXi) improve speed and coverage; ESXi lockers frequently derive from leaked Babuk codebases
- **economy enablers**: RaaS affiliate programs and IAB markets streamline scale and time-to-ransom

## Evolution: scaling human abilities

The story of ransomware's evolution reads like a compressed history of both **software engineering** and **human manipulation**.

The first known ransomware, the **AIDS/PC Cyborg Trojan** (1989), was primitive: a simple floppy-disk infection that hid files and **demanded $189 via postal mail**. Yet it introduced the fundamental model (disable, then demand payment) that has persisted through every subsequent iteration.

Through the late 1990s and 2000s, ransomware was still largely handcrafted.
**Malware authors manually wrote obfuscated code**, handled distribution through infected disks or email attachments, and operated in isolation. Attacks were **small scale and personal**; the economics were crude, the tooling bespoke.
But as the broader cybercrime ecosystem matured (see botnets, credential markets, anonymized payments) ransomware developers began to industrialize.

By 2019, with Maze, ransomware entered its enterprise phase: automation, leak sites, and a fully fledged public-relations arm. Maze pioneered the double-extortion model,

**encrypting** data while **also stealing** it for public release if ransom demands were ignored. The playbook proved so effective that nearly every major group copied it within months.

Then came **CONTI**.
The 2022 CONTI chat leaks revealed an astonishingly structured organization: developers, HR, QA, logistics, even customer-service staff handling ransom negotiations. It exposed the reality that **ransomware operations now function like mid-sized software firms:** sprints, code review, and internal bug tracking included.
That professionalism also meant efficiency: **weaponizing leaked builder code**, hiring specialists, and r**einvesting profits into tooling**.

A pivotal moment arrived with the Babuk builder leak (2021), which seeded a proliferation of ESXi-targeting lockers. Dozens of new ransomware families (Play, RTM Locker, CheersCrypt) borrowed Babuk's source to create new encryptors for hypervisor environments, demonstrating how one leak could spawn an entire generation of threat.

This marks the point where **ransomware development shifted** from artisanal craftsmanship to code reuse and modular assembly: efficient, scalable, and dangerously accessible.
In parallel, **access operations became just as industrialized**. Gone are the days of bruteforce attacks and random spam. Modern crews use **sophisticated social engineering** and **credential acquisition pipelines:** phishing with carefully localized lures, helpdesk impersonation, MFA fatigue abuse, SIM swapping, and credentials purchased from Initial Access Brokers (IABs).

> **Practical upshot**
> *Modern lockers are often forks/ports of proven families, re-written across C/C++/Go/Rust and retargeted for hypervisors*

And now, **the field is shifting again with AI emerging** as both an **accelerant** and a **mirror**. What once required manual code audits, trial-and-error, and long debugging sessions can now be streamlined with large language models (LLMs) that generate or refactor code, identify obfuscation issues, and even **produce spear phishing templates**.

**Early ransomware coders did everything by hand**; modern developers stand atop AI-driven scaffolds that optimize their malicious workflows. This automation **does not replace human expertise**: it amplifies it, **lowering the barrier** to entry and speeding the evolution cycle. The same technology used in defense to detect anomalies is now being inverted to refine offense.

In other words: ransomware's trajectory (from floppy disks and postal payments to hypervisor encryptors and AI-assisted development) reflects the broader arc of computing itself: **increasing abstraction, specialization, and automation**.

The **next stage in that curve will hinge on artificial intelligence**, and how both attackers and defenders weaponize it in their competing races toward efficiency and control.

## Back to the future: AI had it all

So, the **evolution of ransomware** and offensive automation is **not a sudden revolution** born from AI: it's the **latest iteration in a decades-long continuum** of ingenuity, laziness, and competitive escalation.

In the 1990s there already were **automated scripts** and self-replicating worms, long before "machine learning" entered the lexicon. Code like **ILOVEYOU** (2000), **Melissa** (1999), and **Code Red** (2001) proved that automation was intrinsic to cybercrime from the start.
Those worms spread through email clients or exploited unpatched vulnerabilities to replicate at machine speed, overwhelming networks worldwide.

By the early 2000s, **botnets** had transformed automation into orchestration: networks like Storm, Conficker, and Zeus coordinated tens of thousands of compromised systems, harvesting credentials and launching **Distributed Denial-of-Service** (DDoS) attacks.
Then came **exploit kits**: prebuilt toolchains such as Blackhole or Angler that automated vulnerability scanning and payload delivery, abstracting away the hard work of exploitation.
Frameworks like Metasploit (launched in 2003) **democratized attack sophistication**, letting even novice "script kiddies" chain exploits and generate shellcode with a few keystrokes.

So, to be blunt: **LLMs didn't invent attack automation**, they simply made it more accessible and flexible. The pattern has always been the same: progressive automation of repetitive tasks, each generation abstracting complexity for the next.

In the 90s, **worms automated propagation**, in the 2000s, **exploit kits automated infection**; in the 2010s, **ransomware automated monetization**. Large Language Models now **automate reasoning** around these processes, helping attackers structure, test, and contextualize their code, not create magic out of nothing.

Describing a LLM-powered intrusion as "*the first attack without substantial human intervention*" is, frankly, a bit of **nonsense**, as there is always a human behind the keyboard, designing prompts, interpreting errors, and deploying payloads.

The true constant through **three decades of offensive computing** is the arms race between builder and defender. Humans innovate, automate, counter-automate, and repeat. **AI just speeds up both sides of the equation**.

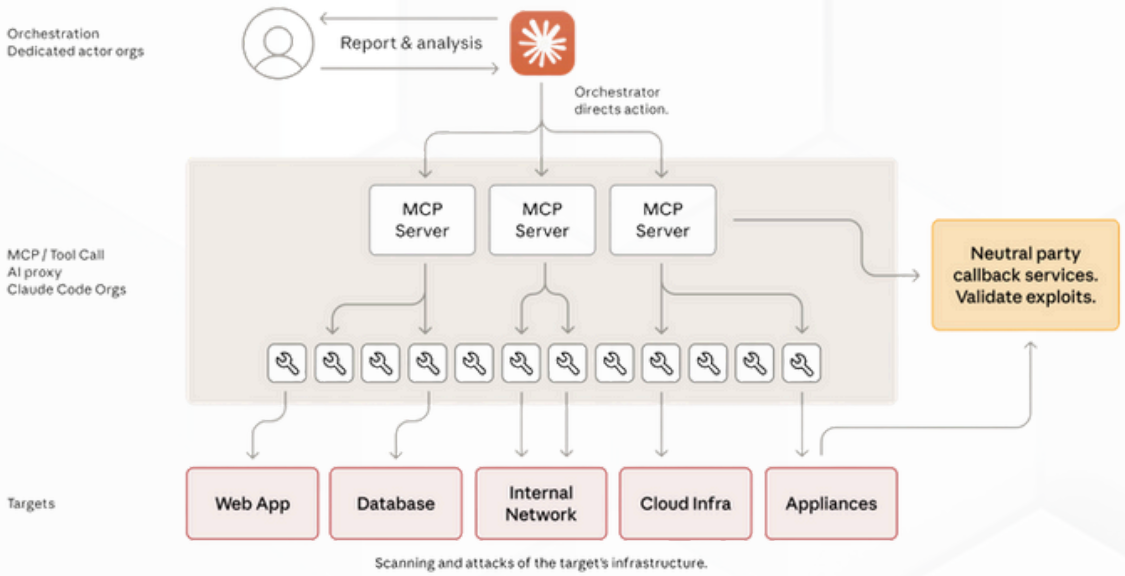
The same architectures that help write efficient encryptors or phishing campaigns also empower blue teams to predict, detect, and disrupt them faster. The real revolution, then, is not autonomy but **symmetry**: for the first time in history, offense and defense are automating at the same pace. LLMs are simply the newest accelerant in this enduring cycle of adaptation and response.

## Hijacking Claude: nothing (too) new under the wire

Anthropic released a report, November 2025, "Disrupting the First AI-Orchestrated Cyber Espionage Campaign" that deserves special attention, because it captures the logical endpoint of 30 years of technological evolution.

Evidence points to a **Chinese state-sponsored group** (GTG-1002) weaponized Anthropic's **Claude Code** within an autonomous orchestration framework capable of executing roughly 80/90% of its operations independently: from reconnaissance to exploitation, credential harvesting, and exfiltration.

The attackers used open standard Model Context Protocol (MCP) servers to **break complex multistage intrusions** into modular tasks for Claude sub agents, effectively turning the AI into a multi-agent penetration-testing system.




This represents **a natural consequence of technological evolution**: the same drive that produced 1990s self replicating worms and 2000s botnets has now culminated in **agentic AI** capable of operating with minimal supervision.

The GTG-1002 incident demonstrates that the barrier to large-scale, professional-grade cyber operations continues to drop as automation deepens. What once required a coordinated human team can now be **approximated** by a network of cooperating AI instances, each handling reconnaissance, exploit generation, or data triage. Yet the report also stresses the limits - AI hallucinations and false positives reduced reliability, forcing human oversight to validate results.

Anthropic's findings show both the promise and peril of autonomous offensive AI. It didn't appear *ex nihilo*; it's the logical outcome of incremental automation.
The rise of "agentic" systems like this **isn't an anomaly**; it's the expected next phase of the same arms race that began **when the first script kiddie hit "run"**.

## Hallucinations and bad code: AI is (mostly) a cyberfailure

The current fascination with **AI-written ransomware** has given rise to a phenomenon some researchers now call **cyberslop**, a deluge of poorly generated, half-functional code produced by inexperienced attackers or by AI systems misused as autonomous developers.
This isn't science fiction; it's a **predictable consequence** of democratized automation. Wannabe hackers with limited technical understanding simply ask LLMs to "*write ransomware in Python*" or "*build an infostealer*", copy the generated text, and attempt to execute it.
The results, more often than not, are **chaotic**: broken imports, wrong libraries, hardcoded keys, and logic loops that would make any seasoned developer wince.

As **cybersecurity journalist Damien Charlotin** noted in his essay on AI hallucinations, generative models are confidently wrong: they produce code that **looks syntactically flawless but semantically useless**.
Cyberslop describes this flood of untested, unexecutable malware fragments now circulating through forums and paste sites.

The real risk lies not in these broken payloads themselves, but in **the confusion they sow**. Even official institutions, scanning repositories or threat feeds, sometimes **mistake AI-hallucinated code for legitimate** emerging threats, further muddying the already noisy landscape of malware intelligence.
Modern ransomware development sits at a crossroads between this noisy AI slop and highly refined professional engineering.

Based on interviews with **seven active ransomware development teams**, four admitted using **AI as an assistant** and **not to autonomously generate the entire locker**, but to refine and accelerate human work.

As one developer phrased it: "*AI helps us get from concept to prototype faster, but the final code still needs a human brain. It can't guess system paths or evasion logic the way we can.*"
Another was more blunt: "*AI can write syntax, not strategy. It doesn't know what EDR smells like*".

Across these conversations, **a pattern emerges**: the groups most reliant on AI tend to treat it as a junior developer, not a lead architect. It drafts, corrects, and suggests, but the design (the evasion logic, lateral movement orchestration, encryption workflow) **remains human-driven**.

The models are often used to **restructure or rewrite existing ransomware** families, especially CONTI-based variants, in new languages (Go, Rust, C++) or to modularize older codebases for easier obfuscation and deployment.

The **distinction here is crucial**. AI-written code (that is, code generated entirely by a model) tends to be brittle, riddled with assumptions, and rarely executable without human correction.

**AI-assisted code**, by contrast, leverages the model's strengths in pattern recognition, syntax normalization, and boilerplate generation to improve efficiency while relying on a human operator for logic, stealth, and integration.

**The myth of the "AI hacker" obscures this reality.**
Today's ransomware is not birthed by artificial intelligence; it's midwifed by it.
The **code's backbone**, intent, and operational nuance still belong to human authors who understand the system internals they're targeting. AI's role is to smooth the edges, to make a developer faster, not smarter.

But that acceleration is no small thing: as **defenders face an exponentially growing volume of machine-generated slop**, they must **learn to distinguish** signal from hallucination, prioritizing behavioral intelligence over code signatures.

The future of the ransomware ecosystem will not be determined by who writes the code, but by who curates, tests, and deploys it with purpose. In that contest, automation is the amplifier, and judgment remains purely human.

## Conclusion

By late 2025, the fusion between human ingenuity and machine augmentation has become **the new normal** in cybercrime. More than **90% of newly observed ransomware** rewrites now exhibit some form of AI assistance - either in the structuring of code, optimization of encryption routines, or automation of infrastructure management.

The ransomware landscape **no longer revolves around lone coders** hunched over hex editors; it **thrives on small, distributed teams** where at least one member possesses LLM fluency. Underground forums increasingly advertise for "AI devs" or "LLM integrators" rather than traditional reverse engineers, signaling that knowledge of model fine tuning and prompt engineering has become a **competitive advantage** in criminal development pipelines.

Repositories like Hugging Face, originally designed to democratize machine learning, are now **being repurposed** as training grounds and model hosts for illicit experimentation. Several threat intelligence analysts have **documented private forks of public models** being fine-tuned on malware repositories and ransomware builders, forming the foundation for new encryptor generations.
These hybrid models serve as the scaffolding for entire ransomware branches, allowing threat actors to quickly re-engineer legacy families such as CONTI, Babuk, and LockBit into **polymorphic, multilingual codebases** that evolve faster than traditional static defenses can keep up.

This convergence between artificial and human capability has deep implications for defenders. The frontier is no longer purely technical; **it's cognitive**. Attackers with AI literacy can build adaptive code ecosystems, while defenders must learn to identify the behavioral fingerprints of machine-assisted malware creation. **The fight is not between people and machines but between humans who use AI well and humans who don't.**

**Disclaimer**

*This article is a research-driven analysis intended to* ***clarify the distinction*** *between AI-generated and AI-assisted ransomware.*
*Its purpose is to aid threat intelligence professionals and incident response teams in understanding, anticipating, and mitigating this evolving menace.*

*The author has* ***no affiliation*** *with, endorsement of, or connection to any criminal group or illicit activity. The discussion of threat actor practices is purely for academic and defensive awareness.*

**My gratitude** 🦄

*Claudio Sono*
*Christian Bernieri*
*Paolo Dal Checco*
*Relations At Work*

RedACTinsights

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

# RANSOMWARE AND AI
## ECONOMICS, PSYCHOLOGY, ACTORS, AND THE NEW TOOLING LOOP

**NOVEMBER 2025**

@SIGNORINA37

*real data. real threats.* ***ransomNews.***