WHITE PAPER

Democratizing Destruction: The Business Structure of RaaS and the Rise of Affiliate Networks

How ransomware became an industry - and what the professionalisation of cybercrime means for every organisation's threat model

A Digital Resilience Strategic Advisory Report

Digital Resilience | www.digitalresilience.co.za | April 2025
Target Audience: CISOs, SOC Teams, Risk and Compliance Leaders

EXECUTIVE SUMMARY

Ransomware-as-a-Service has fundamentally restructured the economics of cybercrime. What was once the exclusive domain of highly skilled technical operatives has been reduced to a commercial transaction: an affiliate pays an upfront fee or agrees to a revenue split, receives access to battle-tested ransomware infrastructure, and targets victims with the same tools used by nation-state threat actors. The barrier to entry for a devastating ransomware attack has fallen to near zero in terms of technical skill - what remains is ambition and access to a cryptocurrency wallet.

The consequences are quantifiable. Total ransomware payments in 2023 exceeded USD 1.1 billion - a single-year record - and represented only a fraction of total economic impact when operational downtime, remediation costs, reputational damage, and regulatory exposure are included. Between 70 and 80 percent of all ransomware incidents now involve an affiliate-based delivery model. The number of organisations willing to pay has declined as resilience has improved, but the number of attacks has continued to rise, with attackers targeting smaller organisations, critical infrastructure, and healthcare providers precisely because these sectors have historically underinvested in defensive controls.

This white paper maps the full RaaS ecosystem: how it is structured, who the participants are, how attacks are executed, which groups are most active, and - critically - how defenders can interrupt the kill chain at each stage. Understanding the adversary's business model is the prerequisite for defeating it.

USD 1.1B+ Ransomware payments recorded in 2023 - a single-year global record	**70–80%** Proportion of ransomware incidents now using the affiliate delivery model
4,000+ Ransomware attacks detected per day globally across all sectors in 2024	**22 days** Average business downtime following a ransomware incident in 2023

> *"The RaaS model did not just lower the barrier to ransomware - it created a marketplace where almost anyone can rent the infrastructure of a sophisticated criminal enterprise for a percentage of the take. Defending against it requires understanding it as a business, not just a technical attack."*
>
> **- Yaron Assabi**

THE RAAS BUSINESS MODEL – FROM HACKER ART TO CRIMINAL INDUSTRY

To understand the RaaS threat, it is necessary to understand how dramatically the economics of ransomware have changed over the past decade. Early ransomware campaigns - CryptoLocker in 2013, WannaCry in 2017 - were conducted by relatively small, technically cohesive groups. Development, distribution, targeting, negotiation, and money laundering all resided within a single organisation. This created a natural ceiling on scale: the number of simultaneous attacks was constrained by the number of skilled operatives a group could recruit and manage.

The shift to the affiliate model dissolved this constraint entirely. By separating the creation of ransomware tooling from its deployment, RaaS groups could scale horizontally across dozens or hundreds of independent operators simultaneously - each pursuing their own targets, each applying their own social engineering and access techniques, and each returning a percentage of ransom revenue to the core development group.

The Affiliate Revenue Model

The financial mechanics of RaaS are directly modelled on legitimate software-as-a-service franchise structures. Core developers maintain the ransomware payload, the payment portal, the negotiation interface, and the technical infrastructure. Affiliates - often recruited via dark web forums with explicit screening processes - pay to access this infrastructure and deploy it against targets of their own selection.

Revenue splits vary by group but typically follow one of two structures:

Model	Structure	Typical Split	Used By
Standard affiliate	Affiliate pays no upfront fee; core dev takes percentage of each ransom	Core dev: 20-30% / Affiliate: 70-80%	LockBit, BlackCat/ALPHV, Royal
Tiered affiliate	Higher-volume affiliates earn a better split over time	Scaling from 70/30 to 90/10 based on output	LockBit 3.0 (Black)
Access fee model	Affiliates pay recurring subscription fee plus percentage	Fee + 15-20% per payment	Smaller, emerging RaaS groups
Private group	No external affiliates; all attacks conducted internally	100% retained internally	Cl0p, some state-nexus groups

The Professionalisation of Ransomware Operations

RaaS groups have adopted the operational structures and cultural norms of legitimate software businesses with remarkable fidelity. Leading groups maintain:

- **Affiliate recruitment portals** with formal vetting processes, requiring demonstrated technical capability and in some cases references from existing affiliate networks.
- **Technical support teams** who assist affiliates with deployment issues, provide updated encryption payloads, and troubleshoot victim negotiation infrastructure.
- **Brand management** - groups like LockBit maintained public-facing reputations for reliability (paying affiliates promptly, honouring decryption agreements with paying victims) as a business strategy to encourage ransom payment.
- **Legal clauses and rules of engagement** - many groups prohibit attacks on hospitals, schools, and critical infrastructure in certain jurisdictions to avoid triggering coordinated law enforcement responses.
- **Bug bounty programmes** - LockBit 3.0 explicitly offered cryptocurrency rewards for reporting vulnerabilities in their own ransomware and infrastructure, directly replicating legitimate security industry practices.

> **RaaS as a Franchising Model**
> The parallels between RaaS and conventional franchising are deliberate and operationally significant. A franchise model allows a brand and its core intellectual property to scale rapidly by leveraging third-party capital and effort. The franchisor (RaaS developer) provides the product, infrastructure, and brand; the franchisee (affiliate) provides the market access and operational execution. Defenders who understand this structure can target the franchisor's infrastructure to degrade the entire affiliate network simultaneously - as demonstrated by law enforcement operations against LockBit and ALPHV in 2024.

THE RAAS ECOSYSTEM – ROLES, PLAYERS, AND SUPPLY CHAIN

A modern ransomware attack does not involve a single threat actor. It involves an interconnected supply chain of specialists, each contributing a discrete function to the overall operation and each taking a cut of the eventual ransom. Understanding each role is essential for mapping the defensive countermeasures that can interrupt the chain.

Core Roles in the RaaS Supply Chain

Role	Function	Technical Skill Required	Primary Motivation
RaaS Developer	Writes and maintains the ransomware payload, encryption engine, payment portal, and affiliate management panel	Very High - requires deep malware dev, cryptography, and infra skills	Recurring revenue from affiliate percentage; reputational dominance
Affiliate Operator	Deploys ransomware against selected targets; manages victim communication and negotiation	Medium - requires network intrusion skill; payload deployment is automated	Per-incident profit (70-80% of ransom)
Initial Access Broker (IAB)	Specialists who breach corporate networks and sell persistent access to ransomware affiliates	High - specialised in phishing, credential stuffing, VPN exploit	Per-access sale (USD 500-USD 100,000+ depending on organisation size)
Negotiation Specialist	Manages ransom negotiation on behalf of affiliate; sets and justifies ransom quantum, manages payment timeline	Low-Medium - primarily social engineering and business acumen	Percentage of negotiated ransom
Cryptomixer / Launderer	Converts ransom cryptocurrency through mixing services, chain-hopping, and cash-out channels	Medium - requires cryptocurrency and operational security expertise	Service fee (3-8% of funds laundered)
Data Extortion Specialist	Manages stolen data publication on Dedicated Leak Sites (DLS); handles third-party victim notification for additional leverage	Low-Medium - primarily operational and OSINT skills	Percentage of ransom or flat fee per campaign

Initial Access Brokers - The Ransomware Supply Chain's Wholesalers

Initial Access Brokers represent one of the most significant structural developments in the cybercrime economy. Rather than requiring ransomware affiliates to possess network intrusion skills, IABs provide a market where established network footholds are bought and sold like commodities. An IAB who successfully exploits a vulnerable VPN appliance or phishes corporate credentials has no need to deploy ransomware themselves - they can sell persistent access to multiple buyers on dark web marketplaces.

The IAB market has grown dramatically in step with RaaS adoption. Access listings on dark web forums grew by over 100% between 2021 and 2023, with prices ranging from a few hundred dollars for low-value SME access to tens of thousands for access to Fortune 500 organisations, government agencies, and critical infrastructure providers. IABs frequently specialise by geography, sector, or access type, creating structured submarkets within the broader criminal ecosystem.

Dedicated Leak Sites and the Data Extortion Layer

Dedicated Leak Sites are dark web platforms maintained by RaaS groups to publish stolen data from non-paying victims. The existence of a DLS fundamentally changes the threat calculus for victims: even organisations with robust backup infrastructure who can restore operations without paying now face a second, separate threat - the publication of exfiltrated data.

DLS operations have become increasingly sophisticated. Groups time publications for maximum impact (before earnings announcements, regulatory deadlines, or pending contract renewals), selectively release partial data sets to demonstrate authenticity and increase pressure, and in some cases directly notify the victim's customers, regulators, and business partners of the breach - creating a third layer of leverage independent of the encryption event itself.

> *"Paying a ransom does not restore trust in your data. It funds the next attack. The only reliable answer to RaaS is building an environment where encryption does not constitute a crisis - and exfiltration cannot be weaponised."*
>
> **- Yaron Assabi**

ATTACK ANATOMY – ENCRYPTION, EXFILTRATION, AND TRIPLE EXTORTION

Modern RaaS attacks follow a structured kill chain that has evolved significantly beyond the simple encrypt-and-demand model of early ransomware. Understanding each phase is essential for mapping defensive controls to the points where they are most effective.

The Modern RaaS Kill Chain

Phase	Attacker Activity	Typical Duration	Defender Opportunity
1. Initial Access	Exploit public-facing apps (VPN, RDP, Exchange), phishing, credential stuffing, or purchase from IAB	Hours to days	Patch management, MFA enforcement, exposure monitoring
2. Persistence and Lateral Movement	Establish C2 beaconing, escalate privileges, map internal network, identify backup systems and domain controllers	Days to weeks (avg. 17 days dwell time)	EDR/XDR detection, network segmentation, anomaly alerting
3. Data Exfiltration	Identify and stage high-value data (financial records, PII, IP); exfiltrate to attacker-controlled infrastructure	Days (often parallel to reconnaissance)	DLP, egress monitoring, data classification
4. Backup Destruction	Target and destroy or encrypt backup systems, shadow copies, and recovery infrastructure to maximise leverage	Hours (often final step before encryption)	Immutable offline/air-gapped backups; backup access controls
5. Encryption Deployment	Deploy ransomware payload across all accessible systems simultaneously via GPO, PSExec, or scheduled tasks	Minutes to hours	Application allowlisting; rapid network isolation
6. Extortion and Negotiation	Deliver ransom note; open negotiation channel; leverage DLS and third-party notification as additional pressure	Days to months	Incident response plan; legal and PR counsel; cyber insurance

Double and Triple Extortion

Single extortion - encrypt and demand payment for the decryption key - is now the exception rather than the rule. The Maze group pioneered double extortion in 2019, combining encryption with data exfiltration and threatening to publish stolen data on a Dedicated Leak Site. This model has been universally adopted across the RaaS ecosystem because it negates the primary defensive strategy of robust backup infrastructure: even if the victim restores operations from backup, they still face the data publication threat.

Triple extortion adds a third pressure vector: direct outreach to the victim's customers, employees, regulators, business partners, or insurers. Some groups conduct distributed denial-of-service attacks against the victim's public infrastructure simultaneously, preventing normal business operations while negotiation continues. Each additional extortion layer is designed to fracture the victim organisation's internal consensus on whether to pay - creating pressure from customers, shareholders, and regulators simultaneously.

> **The Negotiation Dynamic**
> RaaS groups have professionalised the negotiation process to maximise payment rates. Affiliates typically begin with a ransom demand calibrated to the victim's estimated annual revenue (often 1-5%), then negotiate downward to create a sense of compromise and urgency. Many groups offer a short-term 'early payment discount' of 20-30% to accelerate decisions. Organisations without a pre-prepared incident response plan and negotiation protocol are at a significant disadvantage in this dynamic - making pre-incident preparation the single most important investment in this threat category.

NOTABLE RAAS GROUPS AND CASE STUDIES

The RaaS ecosystem is characterised by constant evolution: groups emerge, rebrand, splinter, and are disrupted by law enforcement in rapid cycles. Understanding the leading groups - their targeting profiles, technical capabilities, and operational security - provides actionable threat intelligence for defenders and illustrates the overall trajectory of the ecosystem.

Major Active and Recent RaaS Groups

Group	Also Known As	Active Since	Key Characteristics	Notable Incidents
LockBit	LockBit 2.0 / LockBit 3.0 (Black)	2019	Largest affiliate network; fastest encryption speed; Linux/ESXi variants; bug bounty programme; disrupted by Operation Cronos (Feb 2024) but partially rebuilt	Royal Mail UK, ICBC, Boeing, Allen and Overy
BlackCat / ALPHV	Noberus	2021	First major RaaS written in Rust; triple extortion standard; highly customisable affiliate panel; FBI operation and exit-scam collapse in early 2024	MGM Resorts (USD 100M impact), Change Healthcare (USD 22M paid)

Group	Also Known As	Active Since	Key Characteristics	Notable Incidents
Cl0p	TA505	2019	Primarily data extortion (no encryption in some campaigns); exploits zero-days in managed file transfer software; mass-exploitation model targeting hundreds simultaneously	MOVEit MFT (600+ organisations), GoAnywhere MFT
Royal / BlackSuit	BlackSuit (post-2023)	2022	No formal affiliate programme; private group; rebranded as BlackSuit after law enforcement attention; partial Conti codebase lineage	City of Dallas, Dish Network, multiple healthcare providers
Play	PlayCrypt	2022	Intermittent affiliate use; no negotiation on DLS publications; advanced lateral movement techniques; targets MSPs to access multiple victims simultaneously	City of Oakland, Rackspace, multiple law firms
Dark Angels	Dunghill Leak	2022	Ultra-selective targeting of single large organisations; manually operated; record-setting ransom payments; minimal public exposure by design	USD 75M ransom payment (2024) - largest ever recorded

Case Study: Operation Cronos and the LockBit Disruption

In February 2024, a coordinated law enforcement operation involving agencies from the United Kingdom, United States, Europol, and nine other countries seized LockBit's infrastructure, took control of its affiliate panel, and arrested key operatives. At its peak, LockBit was responsible for an estimated 25% of all ransomware attacks globally, with over 200 active affiliates and a victim count exceeding 2,000 organisations. The operation demonstrated several critical insights about the RaaS ecosystem:

- **Centralised infrastructure is a systemic vulnerability.** Seizing the developer's infrastructure disabled the entire affiliate network simultaneously - demonstrating the value of targeting the franchisor rather than individual affiliates.
- **Affiliate data is operationally valuable.** Law enforcement obtained the affiliate management panel, revealing the identities, profits, and technical details of affiliates across dozens of countries.
- **Disruption is not permanent.** LockBit rebuilt partially within weeks, demonstrating the resilience of decentralised criminal ecosystems and the challenge of sustained disruption without comprehensive arrests of all key personnel.

- **Financial intelligence is central.** Cryptocurrency tracing enabled law enforcement to follow ransom payments through mixing services, ultimately identifying cash-out points and real-world identities.

200+ Active affiliates in the LockBit 3.0 network at peak - generating attacks across 120+ countries	**USD 75M** Largest single ransomware payment recorded - Dark Angels group, 2024
17 days Average attacker dwell time in victim networks before ransomware deployment	**600+** Organisations compromised in the MOVEit MFT zero-day campaign by Cl0p in 2023

DISRUPTING THE KILL CHAIN – A DEFENSIVE FRAMEWORK

Effective defence against RaaS does not require stopping every attack - it requires making your organisation an unattractive target, interrupting the kill chain before irreversible damage occurs, and ensuring that when an attack does land, your recovery capability renders the business impact manageable. The following framework addresses each phase of the modern RaaS kill chain with proportionate, evidence-based controls.

Priority Control Areas and Implementation Guidance

Control Area	Specific Actions	Kill Chain Phase Addressed	Maturity Level
Identity and Access Management	Enforce MFA on all remote access (VPN, RDP, email); implement privileged access workstations (PAWs) for admin; adopt just-in-time privileged access; monitor for credential-based anomalies	Initial Access, Lateral Movement	Foundational

Control Area	Specific Actions	Kill Chain Phase Addressed	Maturity Level
Patch and Exposure Management	Prioritise internet-facing systems (VPN appliances, MFT tools, RDP gateways, Exchange) with 24-48hr critical patch SLA; maintain continuous external attack surface monitoring	Initial Access	Foundational
Endpoint Detection and Response	Deploy EDR/XDR with behavioural analytics and rollback capability; enable tamper protection; integrate with SIEM for correlated alerting; implement application allowlisting on critical servers	Lateral Movement, Encryption Deployment	Intermediate
Network Segmentation	Implement micro-segmentation between business units; isolate OT/IoT from corporate network; restrict lateral movement via host-based firewall policy; monitor east-west traffic for anomalous behaviour	Lateral Movement, Backup Destruction	Intermediate
Backup Architecture	Implement 3-2-1-1-0 backup rule (3 copies, 2 media, 1 offsite, 1 air-gapped/immutable, 0 errors verified); test restoration quarterly; restrict backup system access to dedicated non-privileged accounts	Backup Destruction, Encryption Deployment	Foundational
Data Classification and DLP	Classify data by sensitivity and regulatory exposure; implement egress controls for sensitive data categories; monitor and alert on bulk data staging or unusual egress volumes	Data Exfiltration	Intermediate
Incident Response Planning	Maintain a tested ransomware-specific IR playbook; pre-negotiate retainer with a specialist IR firm; conduct tabletop exercises annually; define pre-approved decision authority for ransom decisions	All phases - recovery	Intermediate

Control Area	Specific Actions	Kill Chain Phase Addressed	Maturity Level
Threat Intelligence	Subscribe to sector-specific threat feeds; monitor dark web IAB marketplaces for your organisation's access listings; participate in information sharing platforms (ISACs, CERT alerts)	Initial Access prevention	Advanced

The Cyber Insurance Consideration

Cyber insurance has become a significant and sometimes misunderstood component of ransomware response strategy. Insurers have responded to the surge in ransomware claims by dramatically tightening underwriting requirements, increasing premiums, and introducing sub-limits and exclusions specific to ransomware. Organisations that view cyber insurance as a substitute for security controls will find that coverage is denied or insufficient when a claim arises.

- **Insurers now require demonstrated security controls** as a condition of coverage, including MFA on remote access, EDR deployment, offline backup testing, and board-level security governance.
- **Ransom payments are not automatically covered.** Many policies now require insurer approval before payment is made, with payments subject to sanctions screening. Payments to sanctioned entities (including some RaaS groups) may be prohibited regardless of insurance coverage.
- **Business interruption coverage** is frequently the largest component of a ransomware claim and is subject to sub-limits, waiting periods, and proof-of-loss requirements that are often not understood until a claim is made.
- **Treat cyber insurance as risk transfer, not risk elimination.** The retention period before coverage activates and the documentation burden during a live incident mean that insurance complements - and does not replace - operational resilience.

> **The Ransom Payment Decision**
> Whether to pay a ransom is one of the most consequential decisions an organisation faces during a ransomware incident. The calculus involves legal risk (sanctions exposure; varying national prohibitions), operational risk (decryptors frequently fail; paying does not prevent DLS publication or re-targeting), reputational risk, and insurance implications. This decision should be made within a pre-defined governance framework that includes legal counsel, the insurer, and an experienced IR partner - never in the heat of a live incident without prior preparation.

SOURCES AND FURTHER READING

[1] Chainalysis. (2024). The Chainalysis 2024 Crypto Crime Report: Ransomware Hits Record USD 1.1 Billion in Payments. Chainalysis Inc.

[2] Coveware. (2024). Q4 2023 Ransomware Marketplace Report: Ransom Payment Trends and Affiliate Model Analysis. Coveware Inc.

[3] Mandiant / Google Cloud. (2024). M-Trends 2024 Special Report: Attacker Dwell Time and Initial Access Vector Analysis.

[4] National Cyber Security Centre (NCSC-UK). (2023). Ransomware, Extortion and the Cyber Crime Ecosystem. NCSC.

[5] FBI Internet Crime Complaint Center (IC3). (2024). 2023 Internet Crime Report. Federal Bureau of Investigation.

[6] CISA. (2024). #StopRansomware Advisory: LockBit 3.0 Ransomware Affiliates Exploit CVE-2023-4966 Citrix Bleed. Cybersecurity and Infrastructure Security Agency.

[7] Europol. (2024). Operation Cronos: LockBit Infrastructure Takedown - Press Release and Technical Summary. European Union Agency for Law Enforcement Cooperation.

[8] Palo Alto Unit 42. (2024). Ransomware and Extortion Report 2024: Threat Actor Profiles and Ransom Demand Analysis. Palo Alto Networks.

[9] Recorded Future. (2024). Initial Access Broker Marketplace Report: Dark Web Listings and Pricing Analysis 2023-2024.

[10] Sophos. (2024). The State of Ransomware 2024: Survey of 5,000 IT and Security Leaders on Ransomware Incidents, Recovery Costs, and Cyber Insurance. Sophos Ltd.

This white paper is intended for informational and strategic planning purposes. All statistics are sourced from publicly available research and industry reports. Digital Resilience does not endorse any specific vendor product referenced herein.

Strengthen Your Ransomware Resilience

Ransomware-as-a-Service has turned cybercrime into a scalable, low-skill franchise. The organisations that survive are not those that hoped they would be spared - they are those that built the controls, playbooks, and recovery capabilities to render an attack a recoverable incident rather than an existential event. Digital Resilience partners with organisations to close the gaps that RaaS affiliates exploit.

What Digital Resilience Offers:

RaaS Threat Simulation - realistic affiliate-model attack simulations testing your detection, response, and recovery against current threat actor TTPs. Ransomware Readiness Assessment - structured evaluation of backup architecture, identity controls, and incident response maturity against NIST CSF and CIS Controls. Incident Response Retainer - pre-negotiated, on-call IR support available within hours of a ransomware event. Tabletop Exercises - facilitated ransomware scenario exercises for executive, technical, and board-level stakeholders. Dark Web Monitoring - continuous monitoring of IAB marketplaces and Dedicated Leak Sites for your organisation's data and access listings.

Protecting your Business Ecosystem

yaron@digitalresilience.co.za | www.digitalresilience.co.za