

# DEADLOCK

Ransomware operation that stayed dormant for 11 months after first appearing in July 2025, then surged to roughly 80 victims in June 2026 — briefly the world's second most active group — before collapsing to 22 the following month. Notable for hosting its command and control on the Polygon blockchain rather than traditional infrastructure.

Lynx/INC affiliate ties

Polygon blockchain C2

BYOVD kernel EDR kill

RISK RATING

High

ACTIVE SINCE

July 2025

(dormant 11 months)

BUSINESS MODEL

Partial RaaS,  
shared affiliate  
tooling

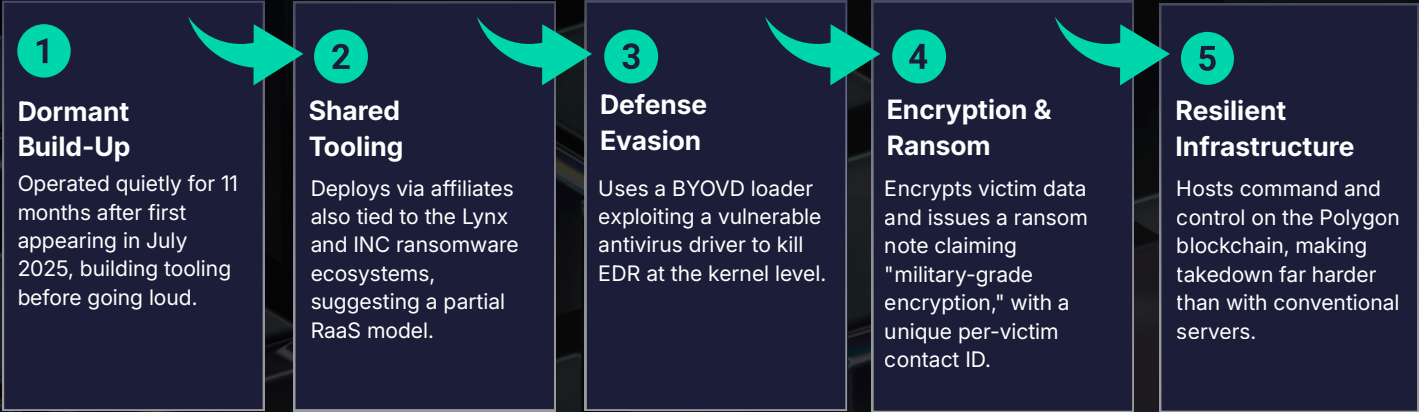
PRIMARY VECTOR

Unconfirmed;  
BYOVD used post-  
access

CLAIMED VICTIMS

81 peak (Jun '26),  
22 the next month

## ATTACK CHAIN



## MITRE ATT&CK MAPPING

| ID        | TECHNIQUE                                                           |
|-----------|---------------------------------------------------------------------|
| T1566     | Phishing (likely initial access, consistent with ecosystem norms)   |
| T1588.002 | Obtain capabilities: tool (affiliate ties to Lynx and INC builders) |
| T1583.006 | Acquire infrastructure: web services (blockchain-hosted C2)         |
| T1562.001 | Impair defenses (BYOVD, kernel-level EDR termination)               |
| T1486     | Data encrypted for impact                                           |
| T1657     | Financial theft (ransom demand via per-victim contact ID)           |

## SECTOR BY SECTOR Summary



**Manufacturing**

The majority of claimed victims fall here, consistent with the sector's tolerance for downtime-driven ransom pressure.



**IT & Technology**

A recurring target, likely valued for the downstream access these firms provide into client environments.



**Transportation & Logistics**

Named among the group's confirmed sectors, fitting a broad, opportunistic targeting pattern rather than a niche focus.

## ORIGIN & EVOLUTION

First observed in mid-2025, then went silent for 11 months with no public leak site before resurfacing in June 2026 with roughly 75 victims listed in a single month, a pace that briefly rivalled established operations. Microsoft has observed the malware deployed by affiliates also tied to the Lynx and INC ransomware ecosystems, pointing to a partial RaaS model rather than a single organized crew.

## THREAT LANDSCAPE CONTEXT

Shares affiliate tooling with the Lynx and INC ransomware ecosystems rather than running a clean, independent operation. Its 11-month dormancy before resurfacing suggests a small core team building capability quietly rather than an active criminal franchise the whole period.

## SIGNATURE TRADECRAFT

Deploys via affiliates also tied to Lynx and INC builders, then uses a BYOVD loader to kill EDR at the kernel level before encrypting. Its defining trait is hosting command and control on the Polygon blockchain rather than conventional servers, making takedown far harder than seizing a normal C2 host.

## ANALYST OUTLOOK

The June spike collapsed to 22 victims in July, so DeadLock's staying power as a brand is genuinely uncertain. The blockchain C2 technique it popularized is the more durable story, ReliaQuest already expects other groups like Cry0 to copy the approach.

## NOTABLE INCIDENTS

### West African Resources Ltd

July 2026

Claimed a breach of the Australian gold mining company, threatening to leak sensitive data.

### June 2026 mass listing debut

After 11 months of silence, DeadLock's leak site reappeared already populated with roughly 80 victims in a single month, briefly making it the world's second most active group by volume.

### Leak-site resilience test

When its clearnet mirror went offline, the Polygon blockchain-hosted backup and Session messenger infrastructure kept negotiations running, demonstrating the practical resilience of its unconventional infrastructure.