

# DIREWOLF

Human-operated, double-extortion ransomware group active since April 2025, now past 100 leak-site victims across 32 countries by deliberately destroying backups before encrypting. No confirmed ties to any established ransomware family.

Golang/UPX

ChaCha20 encryption

Windows

RISK RATING

High

ACTIVE SINCE

2025

MOTIVATION

Financial extortion

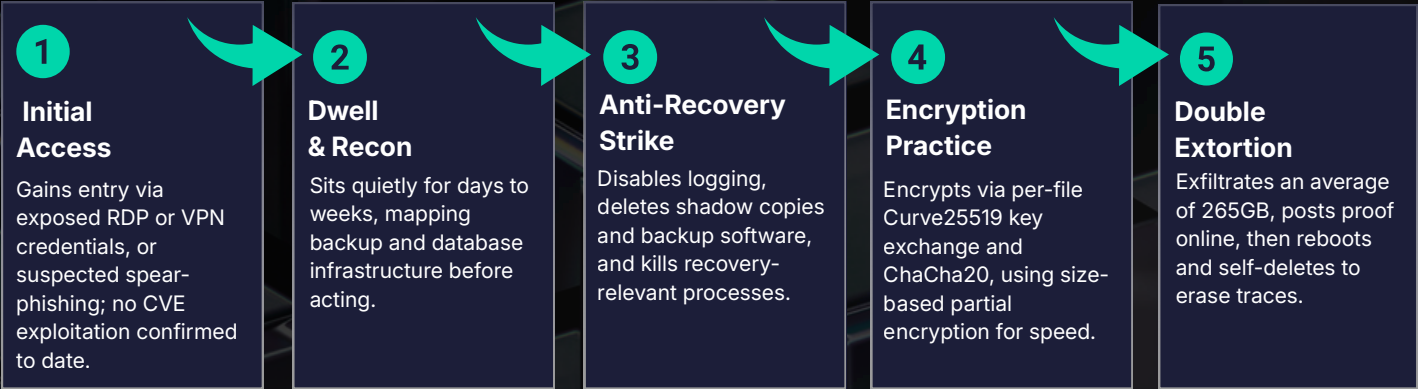
PRIMARY VECTOR

Credential-based access, suspected phishing

RANSOMWARE TIES

None confirmed, independent operation

## ATTACK CHAIN



## MITRE ATT&CK MAPPING

| ID        | TECHNIQUE                                                 |
|-----------|-----------------------------------------------------------|
| T1078     | Valid accounts (stolen RDP/VPN credentials)               |
| T1566     | Phishing (suspected spear-phishing entry)                 |
| T1489     | Service stop (backup, security, database services)        |
| T1490     | Inhibit system recovery (shadow copy and backup deletion) |
| T1486     | Data encrypted for impact (Curve25519 + ChaCha20)         |
| T1070.004 | Indicator removal: file deletion (self-delete after run)  |

## SECTOR BY SECTOR Summary



Healthcare

Now the most-claimed sector, with recent hits showing how fast infostealer-leaked credentials become an intrusion.



Technology

A founding target since the group's first campaigns, prized for the downstream access it gives into customer environments.



Manufacturing

Hit hardest by the backup-destruction chain, where operational downtime creates outsized ransom pressure.

## ORIGIN & EVOLUTION

Emerged independently in April 2025 with no confirmed infrastructure or affiliate overlap with Akira, Fog, Qilin, or SafePay, despite operating in the same crowded market. Its leak-site tagline, "We only seek money, no morals, no political stance," reinforces the purely financial framing it uses to distance itself from more ideologically branded groups.

## THREAT LANDSCAPE CONTEXT

Operates with no confirmed ties to any established ransomware family, unusual in a market where most groups share code, wallets, or affiliates with at least one other operation. That independence, paired with its financial-only messaging, positions it as a clean-slate actor in a field of splinters and rebrands.

## SIGNATURE TRADecraft

Gains entry through exposed RDP or VPN credentials, or suspected spear-phishing, then sits quietly for days or weeks mapping backup and database infrastructure before striking. Its hallmark is destroying recovery options first, disabling logging, deleting shadow copies, and killing backup software, then encrypting with a Curve25519/ChaCha20 combination before self-deleting to erase its tracks.

## ANALYST OUTLOOK

DireWolf's speed from credential exposure to active breach is its most dangerous trait, not its encryption. Expect continued expansion into new sectors like education as it hunts wherever infostealer logs put fresh credentials up for sale.

## NOTABLE INCIDENTS

### Arizona State University

2026

Claimed as DireWolf's first US higher-education victim, marking a sector expansion beyond its usual healthcare and technology targets.

### National Kidney Registry

A corporate credential appeared in infostealer logs; DireWolf listed the organization as a victim just three days later, showing how fast leaked credentials become an active intrusion.

### Quironsalud, Spain

Breached the Spanish healthcare provider, consistent with the group's heavy healthcare targeting and backup-destruction playbook.