[ CLASSIFIED - INTERNAL USE ONLY ]

# dP Internal Operations Report

Q1 2026 - Infrastructure Status and Operational Review

**Document ID:** dP-OPS-2026-0041
**Classification:** INTERNAL - Level 3
**Prepared by:** d4rkm4tter (Infrastructure Lead)
**Reviewed by:** de4thPawn (Operations Director)
**Distribution:** Core team only
**Date:** 2026-01-28

## 1. Executive Summary

This report summarizes the current state of our operational infrastructure following the emergency shutdown initiated on 2026-01-15. All primary command and control servers have been successfully decommissioned. Secondary relay nodes in regions LATAM-3 and EU-7 were wiped per standard protocol DP-WIPE-9. Public-facing assets remain under monitoring to assess exposure risk.

As of this writing, no indicators of compromise have been detected on remaining infrastructure. However, the operations team has identified residual digital footprints across several public platforms that require immediate attention (see Section 4).

## 2. Infrastructure Status

| Asset | Region | Status | Last Contact |
|---|---|---|---|
| C2-PRIMARY | LATAM-3 | OFFLINE (wiped) | 2026-01-15 03:41 UTC |
| C2-BACKUP | EU-7 | OFFLINE (wiped) | 2026-01-15 04:02 UTC |
| RELAY-01 | APAC-2 | OFFLINE | 2026-01-14 22:15 UTC |
| RELAY-02 | NA-1 | OFFLINE | 2026-01-15 01:30 UTC |
| EXFIL-NODE | LATAM-3 | DESTROYED | 2026-01-15 03:55 UTC |
| WEB-FRONT | CDN | SUSPENDED | 2026-01-16 00:00 UTC |

All decommissioned assets followed the DP-WIPE-9 protocol: three-pass overwrite, key destruction, and physical disposal where applicable. Verification checksums have been archived in the secure vault

(access restricted to Level 4+).

## 3. Operational Personnel (Active)

| Handle | Role | Status | Clearance |
|---|---|---|---|
| de4thPawn | Operations Director | ACTIVE | Level 5 |
| d4rkm4tter | Infrastructure Lead | ACTIVE | Level 4 |
| sh4d0w_r00t | Exploit Development | ACTIVE | Level 4 |
| n1ghtcr4wl | SIGINT / Recon | STANDBY | Level 3 |
| v01d_k1ng | Logistics / Finance | ACTIVE | Level 3 |
| gh0st_pr0xy | Network Operations | RELOCATED | Level 4 |

All personnel have been instructed to maintain radio silence on primary channels. Communication is restricted to secondary encrypted channels only. Personal devices must not be used for any operational communication.

[ CLASSIFIED - INTERNAL USE ONLY ]

## 4. Digital Exposure Assessment

During the post-shutdown review, the SIGINT team identified several public digital artifacts that remain accessible and could be used to trace our operations. These represent an unacceptable risk to operational security and must be addressed within the next 72 hours.

### 4.1 Public Platform Accounts

The handle 'de4thPawn' was used across multiple platforms during recruitment operations in Q3-Q4 2025. While content has been partially scrubbed, cached versions and archived snapshots may still exist. The SIGINT team has confirmed that at least one image posted under this handle retains embedded EXIF metadata that was not stripped before upload. This is a critical oversight.

### 4.2 Code Repository Exposure

A GitHub account under the 'de4thPawn' handle contains several repositories. While no classified tools were uploaded, preliminary review indicates that configuration files in early commits may contain operational tokens that were not rotated before the account was deprioritized. Full audit pending.

### 4.3 Blog Infrastructure

The domain de4thpawn-log.com was used briefly as a dead-drop communication channel disguised as a personal blog. The domain has been suspended, but web archiving services (Wayback Machine, Google Cache) may have captured content before takedown. The deployment access code published on 2026-01-22 is of particular concern.

## 5. Recovery Protocol

The following recovery actions have been approved by Operations Director:

**Phase 1 (Immediate):** Scrub all remaining public accounts. Submit takedown requests to platform providers. Rotate all tokens and credentials referenced in any public or semi-public repository.

**Phase 2 (7 days):** Establish new infrastructure in regions LATAM-5 and APAC-4. New C2 channels will use rotating domain fronting through legitimate CDN providers. All new handles must follow the updated naming convention (ref: DP-OPSEC-12).

**Phase 3 (30 days):** Resume limited operations with new identities. Full operational capability expected by end of Q1 2026. Budget allocation for new infrastructure approved: see Appendix B.

---

## Appendix A: Emergency Access Credentials

The following credentials are to be used only in case of total infrastructure loss. These are one-time recovery codes and must be destroyed after use.

| System | Access Code |
|---|---|
| Backup vault | dP-vault-7x9K2mN |
| Recovery relay | relay-auth-Qp3vB8w |
| Emergency C2 | PWG{d0rk_y0ur_w4y_1n} |
| Secure comms | sc-init-Hn5jR4tL |

NOTE: If any of the above codes have been compromised, initiate protocol DP-BURN-ALL immediately and contact Operations Director via the tertiary channel.

---



*dP-OPS-2026-0041 | Generated: 2026-01-28 | Expires: 2026-04-28*