THREAT INTELLIGENCE REPORT

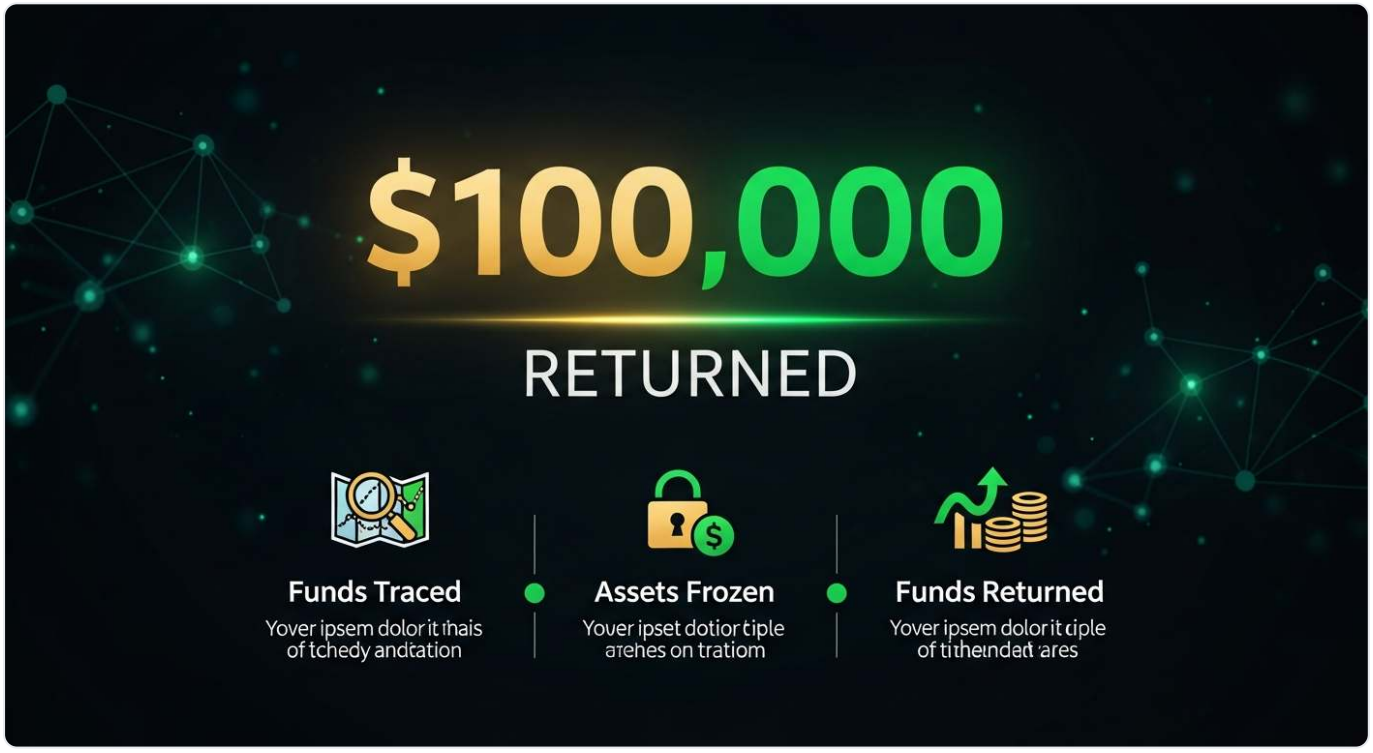
$100K Returned — Malvertising Scam Foiled

Ref. **PD-TI-2026-94138** Published **10 July 2026** Source **phishdestroy.io/100k-returned-malvertising**

Investigation • 5—7 min read

Russian scammers impersonated a crypto project via malvertising and stealer malware. We detected the operation, restored wallet access, and returned over $100K. The extra recovered funds were donated to @_SEAL_Org. Below: breakdown, IOCs, and lessons.

4 min read · Updated **March 2026** · PhishDestroy Intelligence



$100,000 returned to victim - funds traced, assets frozen, funds returned infographic

Originally published on Medium — PhishDestroy

Overview

A cryptocurrency project fell victim to a social engineering attack disguised as a legitimate advertising partnership. PhishDestroy restored wallet access and recovered **over $100,000** in compromised funds, then redirected the offered reward to an external organization to maintain independence.

What You Need to Know

- The wallet was already compromised; funds had already been moved.
- Access was restored and **$100K+** was prevented from remaining with the attacker.

- The project offered a reward, which was declined and directed to @_SEAL_Org instead.
- This work is conducted independently as a operator effort, not as paid employment.

How the Scam Operated

- Victim received a partnership/advertising proposal for a crypto game.
- Attack appeared credible: professional website, established X (Twitter) presence, legitimate-seeming video calls.
- During calls, attackers requested installation of a "workplace viewer" to access materials.
- The "viewer" was **stealer malware** .
- Attackers withdrew funds, swapped tokens across chains, and moved assets to their own wallet.

Response Actions Taken

1. Confirmed compromise and halted further movement.
2. Restored wallet access for the rightful owner.
3. Secured and reassigned control of attacker's receiving wallet to victim team.
4. Coordinated follow-up steps to reduce residual risk.

Result: Access restored, control returned, attacker locked out.

Post-Incident Hardening

Device Security

- Step-by-step guidance for handling infected devices safely
- Network isolation, session revocation, credential/key rotation, clean rebuild plan

Operational Setup

- New, clean workstation dedicated to wallet operations
- Fresh OS, vendor-only downloads, hardware wallet, minimal extensions, separate browser profile, 2FA

Forensics Preparation

- Disk snapshots and system/app log collection guidance
- Evidence preservation for potential legal investigation

Understanding "Adverting"

Adverting is business-style social engineering where criminals imitate normal workflows (ad buys, partnerships, PR) to trick installation of malicious "clients."

Common warning signs:

- "Install our ad manager/helper to sync creatives"
- "Use our custom Zoom/Telegram client for the call"

- "Open our media kit/NDA via a secure viewer"

Key rule: If a workflow from unknown parties requires a special client/viewer/updater, assume hostility by default. Use only official vendor downloads.

The Reward and Independence

- The project offered a reward because recovery exceeded the initial loss.
- PhishDestroy declined to keep the reward.
- The entire surplus was directed to @_SEAL_Org .
- This maintains independence — no funding streams or obligations.

Core Principles

- Independence only — no budgets or strings attached.
- Results-focused approach over discussion.
- Opposition to any "special clients" or unverified software.
- Selective disclosure that helps victims, not threat actors.
- Direct pressure on attacker infrastructure.

Practical Recommendations

For Projects & Teams

- Never install workplace viewers/clients/updaters from unverified third parties.
- Obtain Zoom/Telegram only from official vendor sites.
- Avoid sponsored links for wallets, bridges, airdrops.
- Prefer hardware wallets with offline seed storage.
- If compromised: revoke sessions, move funds, rotate keys, re-issue secrets, seek help immediately.

For the Community

- Report suspicious activity via our Telegram bot .
- Access critical action guidance and resources at phishdestroy.io/critical-action .

Conclusion

Despite funds already being moved, PhishDestroy **restored access** and ensured the attacker could not retain the stolen assets. By declining the reward and directing surplus funds elsewhere, the organization maintains its unpaid, independent operational model focused on rapid, effective incident response.

Quick Links

- Report via Telegram bot
- Critical Action — what to do if hacked
- Anatomy of a Takedown

- Crypto Security Guide

If your wallet is compromised: revoke sessions, rotate keys, contact us immediately.

Need Urgent Help?

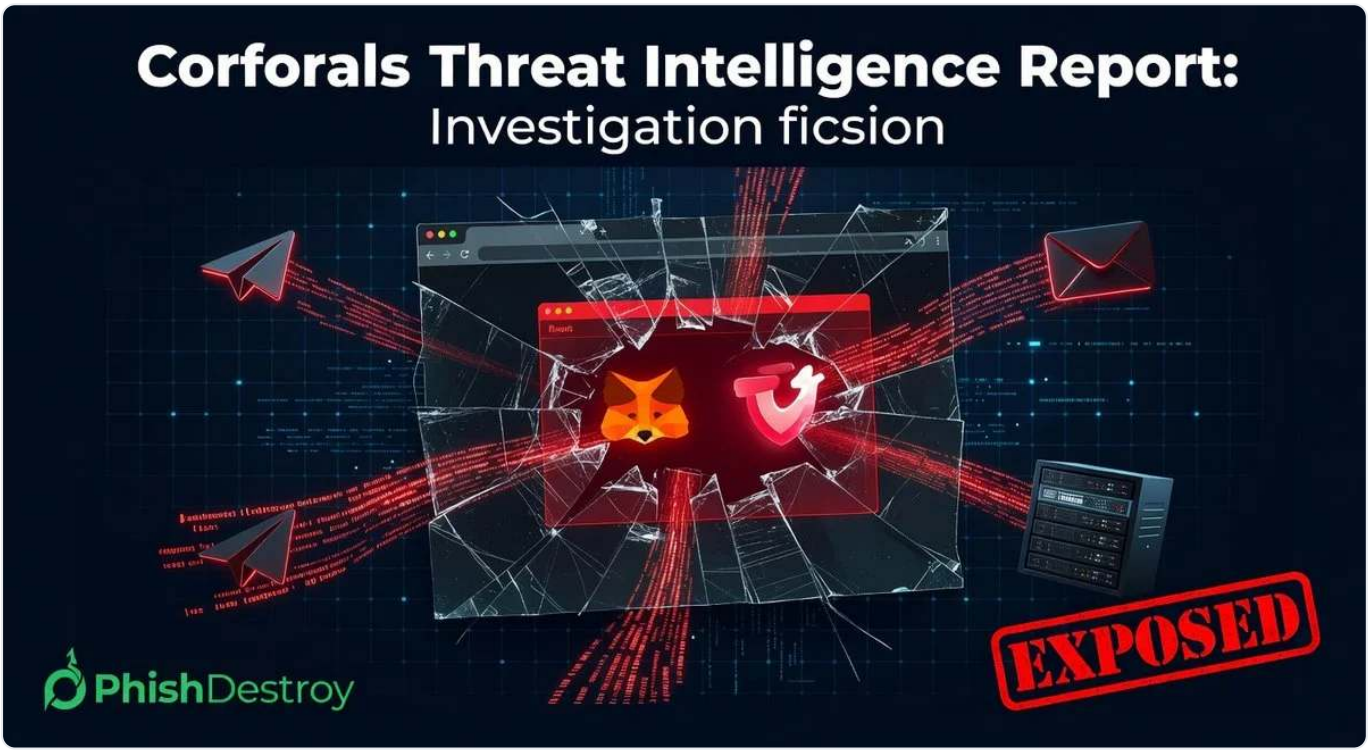
Telegram Bot contact@phishdestroy.io

#Adverting #WalletRecovery #StealerMalware #SocialEngineering #CryptoSecurity

Share This Investigation

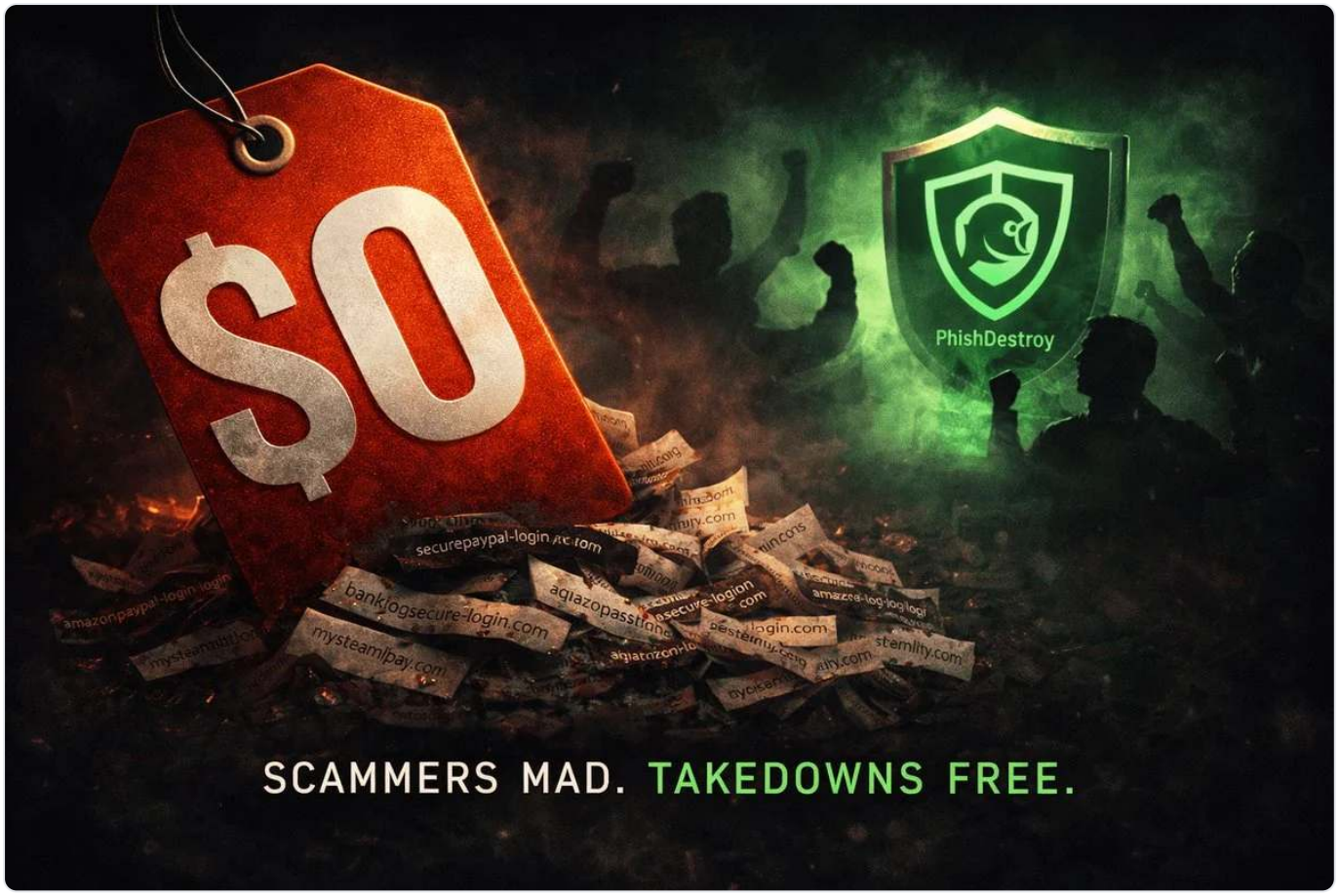
X / Twitter Telegram Reddit LinkedIn

Related Investigations



DEEP INVESTIGATION

Anatomy of Crypto Phishing: 8 Real Seed Phrase Stealers Reverse-Engineered



INVESTIGATION

$0 Takedowns: How We Disrupt Phishing Infrastructure