CRAZY EVIL

[/ˈkreɪzi ˈiːvəl/]

A financially motivated, Russian-speaking traffer team active since 2021, CrazyEvil specializes in cryptocurrency theft, credential harvesting, and identity fraud — deploying infostealers through fake job scams and social media impersonation across global Web3 ecosystems.

IDENTITY

Attribution	: Russian-speaking cybercriminal traffer team.
Active Since	: 2021.
Aliases	: CrazyEvilCorp, Kevland (subgroup behind GrassCall).
Motivation	: Financial gain via digital asset theft, credential harvesting, NFT/crypto fraud, large-scale infostealer operations.

TTPs

Initial Access	- Social engineering (fake NFT airdrops, influencer outreach, fraudulent collaboration messages) - Malicious links shared via Telegram, Discord, X, Instagram - Fake job recruitment schemes (GrassCall campaign) - Malvertising and phishing landing pages targeting crypto users
Persistence	- Auto-start registry modifications (Windows) - Launch agents / persistence daemons (macOS) - Browser session hijacking - Cloud session token theft
Command & Control (C2)	- Telegram channels and bots for coordination - Encrypted web-based panels for malware tasking - Domain rotation and fast-flux infrastructure for phishing pages
Tools & Malware	**Infostealers:** RedLine, Lumma, Rhadamanthys, MetaStealer **Stealer variants for multi-OS:** Windows + macOS payloads **Phishing kits:** NFT airdrop pages, wallet drainer scripts **Browser extensions:** Session theft and reinfection mechanisms
Techniques	- Credential harvesting from browsers and crypto wallets - Data exfiltration (wallet.dat, seed phrases, browser cookies) - Social engineering targeting high-value victims (“mammoths”) - Fake Web3 project pages to lure influencers and developers

TARGET PROFILE

Target Sectors	- Cryptocurrency / Web3 platforms - Financial and fintech services - Technology and developer communities - Gaming ecosystems with tradable assets - Social media influencers with large followings
Geographies Targeted	- United States - Europe (particularly EU crypto communities) - Asia (notably Web3 and gaming markets) - Global opportunistic targeting of individuals and small businesses

THREAT ASSESSMENT

Risk Level	: High .
Most Recent Activity	: Ongoing large-scale NFT/crypto scams; GrassCall job recruitment operations; multi-platform infostealer distribution.
Evolution	: Shift from niche NFT scams to sophisticated, multi-vector Web3 exploitation campaigns; increased use of subteams and automated infrastructure.

NOTABLE OPERATIONS

- **2021:** Emergence on dark web forums; early NFT drainer campaigns.
- **2022–2023:** Expansion of traffer teams; growth of Telegram channels; increased infostealer distribution.
- **2024:** Large-scale influencer-targeted scams; multi-OS malware adoption; tens of thousands of infections.
- **2025:** GrassCall job recruitment scam delivering malware to crypto job seekers; rapid growth following rival traffer team disruptions.