Z E R O T R A C E L A B S

A T T A C K C A S E S T U D Y

Monkey Drainer NFT Phishing Campaign: Anatomy of a Phishing-as-a-Service Operation That Extracted $16M from the Ethereum Ecosystem

How a commoditized drainer kit deployed across hundreds of fake mint sites systematically harvested NFTs, ETH, and ERC-20 tokens from thousands of victims.

Attack Snapshot

victim	Thousands of individual NFT holders and crypto users across the Ethereum ecosystem; high-value targets included holders of Bored Ape Yacht Club, Azuki, and other blue-chip NFT collections
date	Active approximately June 2022 – February 2023; peak activity Q4 2022
loss	$16,000,000+ in ETH, NFTs (including BAYC and Azuki assets), and ERC-20 tokens across thousands of victim wallets
attack Type	Phishing-as-a-Service (PhaaS) / Malicious transaction approval / Permit signature abuse
chain	Ethereum (EVM)
attribution	Monkey Drainer — pseudonymous threat actor(s) operating a drainer kit subscription service; announced voluntary retirement February 2023 via on-chain message and Telegram; no confirmed real-world identity as of publication

Executive Summary

Monkey Drainer was a professional-grade phishing-as-a-service operation that sold or leased a wallet-draining toolkit to affiliate operators who deployed it across hundreds of

counterfeit NFT mint and brand impersonation sites. Victims were lured via targeted social media campaigns and search engine manipulation into connecting wallets and signing malicious setApprovalForAll or EIP-2612 permit transactions, which transferred asset control to attacker-controlled addresses without requiring private key compromise. The operation grossed over $16 million across its roughly eight-month lifespan, demonstrating that the threat surface in Web3 is not primarily cryptographic but social and UX-layer. The incident validated the industrialization of crypto phishing: low technical barrier for affiliates, high yield per victim, and near-zero attribution risk for operators.

What Happened

Monkey Drainer emerged in approximately mid-2022 as one of several drainer-kit services operating in the Ethereum NFT ecosystem, distinguished by its polished infrastructure, active Telegram marketing channel, and a reported revenue-sharing model in which the operator took a percentage cut (commonly cited as 20–30%) of all assets drained by affiliates. The toolkit provided affiliate operators with templated phishing site code, backend wallet-draining smart contract infrastructure, and operational guidance — effectively lowering the technical floor for conducting high-yield crypto phishing to near zero.

Affiliate operators deployed the kit across hundreds of phishing domains impersonating high-profile NFT projects and trusted crypto brands. Confirmed impersonation targets included Premint (a legitimate NFT allowlist platform that itself suffered a separate breach in July 2022), Ledger, and numerous NFT collection mint pages. Attack infrastructure was rotated frequently, with domains registered days before campaigns launched and abandoned or replaced after takedown pressure. Attackers exploited the frictionless nature of NFT culture — where connecting a wallet to an unfamiliar site is normalized behavior — to maximize victim throughput.

The kill chain in each individual attack was operationally simple but technically precise. Victims arrived at convincing counterfeit sites via malicious links distributed through compromised Twitter accounts, Discord servers, and paid search advertisements. On-site, they were prompted to connect their MetaMask or WalletConnect-compatible wallet, after which the drainer front-end automatically assessed wallet holdings using on-chain queries, prioritized the highest-value assets, and presented a crafted transaction request. The critical transaction was typically a setApprovalForAll call granting the attacker's contract unlimited authority over all ERC-721 or ERC-1155 tokens in the victim's wallet, or an EIP-2612 off-chain permit signature enabling ERC-20 token transfers without an on-chain approval step.

Two incidents in October 2022 brought significant public attention to Monkey Drainer's operation. On-chain investigator ZachXBT documented attacks that drained a single wallet of approximately $370,000 in assets including Azuki NFTs and ETH, and identified another victim losing assets worth roughly $300,000 in the same campaign wave. ZachXBT's analysis traced fund flows through multiple intermediate wallets and

identified the Monkey Drainer Telegram channel as the operational hub for the service. These findings were amplified widely in the NFT community, triggering coordinated reporting efforts but not operational disruption.

Monkey Drainer continued operating through late 2022, with total losses aggregating to over $16 million across thousands of victims. In February 2023, the operator posted a retirement announcement, citing increasing competition from rival drainer services (specifically naming Venom Drainer) and the operational burden of running the service. The announcement was delivered via Telegram and included a recommendation to competitors, underscoring the professionalized, business-like posture of the operation. No arrests or confirmed de-anonymization of the operator have been publicly reported. The toolkit and its successors — Venom Drainer, Inferno Drainer, Pink Drainer — continued operating and collectively extracted hundreds of millions of dollars from the ecosystem throughout 2023.

Kill Chain

1. **Infrastructure deployment and lure distribution**

   Affiliate operators registered domains impersonating legitimate NFT projects or brands (e.g., premint-nft[.]xyz variants, ledger-nft[.]io patterns). Phishing links were seeded through compromised high-follower Twitter accounts, Discord server compromises, and in some cases paid Google and Twitter search advertisements that appeared above legitimate project results. Targets were self-selected: users actively seeking NFT mint access, allowlist registration, or hardware wallet support were the primary audience.

2. **Wallet connection and asset reconnaissance**

   Victims landed on convincing clones of legitimate sites and were prompted to connect their wallets via MetaMask or WalletConnect. Upon connection, the drainer's front-end JavaScript automatically queried the victim's address for ERC-721, ERC-1155, and ERC-20 holdings using on-chain calls. Assets were ranked by floor price or estimated value using NFT marketplace API data, enabling the drainer to prioritize the most valuable approval transaction to present first.

3. **Malicious transaction presentation and signing**

   The drainer presented the victim with a transaction or signature request framed as a required step — 'verify wallet,' 'claim NFT,' 'complete mint,' or similar pretextual UI. The underlying request was either a setApprovalForAll transaction granting unlimited ERC-721/1155 transfer rights to an attacker-controlled contract, or an EIP-2612 permit signature for ERC-20 tokens (off-chain, gasless, and displaying minimal contextual information in wallet UIs). Victims signed without recognizing the scope of authorization being granted. Wallet interfaces at the time provided inadequate plain-language disclosure of what setApprovalForAll or permit signatures actually authorize.

4. **Asset extraction and laundering**

   Following signature, the drainer contract executed transfer calls to move NFTs and tokens to staging wallets under attacker control. High-value NFTs were listed or sold rapidly on secondary markets (OpenSea, Blur) before victims could flag them. ETH proceeds and ERC-20 tokens were routed through multiple intermediate addresses and mixed using services including Tornado Cash. Proceeds were then split between affiliates and the Monkey Drainer operator per

the revenue-sharing agreement. The speed of extraction — often within minutes of signing — rendered reversal impossible.

Where Users Failed Themselves

— Signing setApprovalForAll without understanding the permission scope: Victims approved unlimited transfer rights over entire NFT collections in a single transaction. This is categorically different from approving a single NFT transfer, but wallet UIs presented it without adequate risk differentiation, and users had not educated themselves on what the call does.

— Normalized wallet-connection behavior in NFT culture: The community habit of routinely connecting wallets to unfamiliar mint sites, allowlist registrars, and promotional pages conditioned users to treat wallet connection as low-risk. This cultural norm was precisely the attack surface Monkey Drainer exploited — victims connected without applying meaningful skepticism to site legitimacy.

— Failure to verify site authenticity before connecting: Victims did not cross-reference URLs against official project sources, check domain registration dates, or confirm site legitimacy via official project Discord or Twitter before connecting. Many phishing sites were live for 48–72 hours — long enough to harvest significant victims but short enough to evade extended scrutiny.

— Holding high-value assets in hot wallets used for active minting: Victims with BAYC, Azuki, and other blue-chip NFTs worth tens or hundreds of thousands of dollars were actively connecting those same wallets to unknown sites. High-value long-term holdings were co-mingled with active minting wallets, maximizing loss exposure when a signing error occurred.

— Ignoring or misreading transaction confirmation details: Even where wallet UIs displayed the contract address or function name being called, victims proceeded without decoding the transaction data or querying the contract address on Etherscan to assess legitimacy. Signing velocity — the impulse to complete a mint quickly — overrode due diligence.

Prevention Checklist

FOR INDIVIDUAL USERS

☐ Implement strict wallet segmentation: maintain a dedicated 'hot' minting wallet funded with only the ETH required for the immediate transaction, entirely separate from any wallet holding high-value NFTs or significant ERC-20 balances. Never connect a cold or high-value wallet to an unfamiliar site.

☐ Before signing any setApprovalForAll, permit, or non-standard approval transaction, decode the calldata on Etherscan or use a transaction simulator (e.g., Tenderly, Pocket Universe, Fire browser extension) to understand exactly what the transaction authorizes. If the authorization scope exceeds what the stated action requires, reject and exit.

☐ Verify every site URL character-by-character against the official project URL sourced from a pinned post on the project's verified official Twitter account or official Discord announcement channel — not from a link provided in any DM, ad, or search result. Register legitimate project URLs as browser bookmarks.

☐ Periodically audit active wallet approvals using tools such as Revoke.cash or Etherscan's token approval checker. Revoke any setApprovalForAll grants to contracts you do not actively and currently need. Treat dormant unlimited approvals as open attack surface.

☐ Enable transaction simulation in MetaMask's experimental settings or install a browser extension that provides pre-signing simulation and risk scoring (Pocket Universe, Stelo, Fire). These tools surface what a transaction will actually do before you sign.

FOR PROTOCOLS & PROJECTS

☐ NFT projects and brands must implement and publicize a verified official URL registry — a canonical, signed list of legitimate domains associated with the project — and communicate proactively when impersonation sites are identified. Treat domain monitoring as an ongoing security function, not a reactive one.

☐ Wallet providers (MetaMask, Coinbase Wallet, etc.) must display plain-language, high-visibility risk warnings for setApprovalForAll and EIP-2612 permit transactions that explicitly state 'This grants unlimited transfer rights over all assets in collection X to an external contract' before the user can confirm. The current technical display is insufficient for non-expert users.

☐ NFT marketplace platforms (OpenSea, Blur) should implement real-time flagging and listing delays for NFTs whose ownership changed within a short window following an unusual approval transaction, creating a friction buffer that reduces the liquidity value of freshly drained assets and buys victims time to report.

FOR THE ECOSYSTEM

☐ Establish a cross-platform rapid-response blacklist infrastructure for phishing domains that feeds directly into wallet provider block lists, browser extension warning systems, and DNS-layer filtering services. The current lag between domain identification and user-facing warnings measured in hours is unacceptable when victim throughput is measured in minutes.

☐ Fund and formalize on-chain threat intelligence sharing. ZachXBT's identification of Monkey Drainer's infrastructure was performed as independent research. Ecosystem participants — major protocols, wallet providers, security firms — should operate a shared threat intelligence pool with defined contribution and consumption standards analogous to ISAC models in traditional finance.

☐ Pursue regulatory and legal frameworks that treat phishing-as-a-service operators as criminal enterprises subject to cross-jurisdictional prosecution, and that impose legal liability on infrastructure providers (domain registrars, hosting providers) who fail to act on documented abuse reports within defined time windows. The voluntary retirement of Monkey Drainer without legal consequence is an open invitation to successors.

Key Takeaway

Monkey Drainer did not break any cryptography. It exploited a single behavioral vulnerability at scale: users signing transactions they did not understand, on sites they did not verify, with wallets they could not afford to compromise. Every dollar lost was preceded by a signature — a deliberate, irreversible user action. Until wallet UIs provide transaction transparency that matches the risk level of what is being authorized, and until users treat every approval signature as a potential total-loss event, phishing-as-a-service operations will remain the highest-yield, lowest-risk attack vector in the ecosystem.

S O U R C E S

— ZachXBT on-chain investigation thread, Twitter/X, October 2022 — original public attribution of Monkey Drainer activity and victim wallet analysis

— Bleeping Computer: 'Monkey Drainer phishing service stole $16 million before retiring' — February 2023 coverage of retirement announcement and aggregate loss estimates

— Premint NFT breach post-mortem, July 2022 — documented baseline for brand impersonation attack surface exploited by Monkey Drainer affiliates

— Dune Analytics community dashboards tracking Monkey Drainer contract activity and victim wallet counts, Q4 2022

— EIP-2612 specification (eips.ethereum.org) — technical reference for permit signature mechanism abused in ERC-20 token drain attacks

— Revoke.cash educational documentation on setApprovalForAll risks and approval audit methodology