INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-11 18:20 UTC

Operation Atlantic: Multinational Law Enforcement Disrupts Global Crypto Fraud Networks, 20,000 Victims Identified

THREAT CAMPAIGN | **MEDIUM** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0167
Type	Threat Campaign
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	No specific products or vendors; individual cryptocurrency wallet holders in Canada, United Kingdom, and United States
Published	2026-04-11T10:20:40
Discovery Source	Rss

Executive Summary

UK, US, and Canadian law enforcement disrupted a multinational cryptocurrency fraud network under Operation Atlantic, identifying over 20,000 victims and freezing $12 million in criminal proceeds from an estimated $45 million stolen globally. The operation targeted approval phishing and pig butchering schemes that manipulate individuals into granting attackers control over cryptocurrency wallets. Organizations with employees or customers who hold cryptocurrency assets face indirect reputational and fraud exposure; enterprises that custody or transact in crypto face irreversible financial loss risk if approval transactions are compromised.

Technical Analysis

Operation Atlantic targeted two primary fraud mechanisms: approval phishing, where victims are socially engineered into signing wallet approval transactions granting attacker-controlled addresses unlimited spend permissions over ERC-20 or similar tokens; and pig butchering, a long-con investment fraud variant where victims are cultivated over weeks before being directed to fraudulent platforms. Technically, approval phishing exploits the legitimate token approval function in smart contract ecosystems, no vulnerability in underlying protocol code is required. Attackers misuse standard functionality. Applicable weaknesses include CWE-358 (Impersonation) covering identity deception used to build victim trust, and CWE-1021 (Improper Restriction of Rendered UI Layers) covering fraudulent dApp and wallet interfaces that obscure transaction scope. MITRE ATT&CK techniques observed: T1566 and T1566.002 (Spearphishing Link/Attachment for initial contact), T1204

(User Execution, victim must sign the approval transaction), T1583 and T1583.001 (Acquire Infrastructure/Domains for fraudulent platforms), T1588 (Obtain Capabilities), and T1657 (Financial Theft as the terminal objective). No CVE applies; this is a social engineering and financial fraud campaign, not a software vulnerability. No patch exists, the attack surface is human behavior and wallet permission hygiene.

Action Checklist

1. Containment: If your organization custodies cryptocurrency on behalf of clients or employees, review active token approvals on all associated wallet addresses using on-chain tools such as Revoke.cash or Etherscan's token approval checker. Revoke any approvals granted to unrecognized or untrusted addresses immediately.
2. Detection: Monitor for anomalous outbound cryptocurrency transfers, particularly bulk ERC-20 token movements initiated shortly after wallet approval transactions. Review access logs for employee interactions with unsolicited investment platforms or wallet-connection prompts. Flag any approval transactions signed outside of established internal workflows.
3. Eradication: Revoke outstanding token approvals that cannot be traced to a known, authorized internal process. Invalidate any wallet connections to third-party dApps that were not explicitly approved through a documented procurement or onboarding process.
4. Recovery: Validate that wallet approval inventories are clean post-revocation. Implement a recurring approval audit cadence (monthly minimum) for any organization-controlled wallets. Notify affected individuals if employee wallets were compromised and coordinate with legal on any mandatory disclosure obligations.
5. Post-Incident: Conduct targeted security awareness training focused on cryptocurrency wallet hygiene: what a token approval transaction does, how to read approval prompts, and how to identify fraudulent investment solicitations. Establish a policy requiring approval of any wallet connections to external platforms before an employee or system may sign a transaction.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to immediate priority if any organization-controlled wallet holding custodied client funds shows a completed unauthorized TransferFrom transaction, if total losses exceed regulatory materiality thresholds triggering mandatory breach notification under PIPEDA, UK GDPR (ICO 72-hour window), or applicable US state law, or if the organization lacks the wallet signing keys required to execute revocations independently.
Recovery Notes	Post-revocation, verify clean approval state on all organization-controlled wallet addresses via a second independent Etherscan or Revoke.cash audit within 24 hours of revocation, retaining both pre- and post-revocation snapshots as paired evidence. Monitor on-chain transaction history for each affected wallet for a minimum of 30 days post-revocation for any new unauthorized approval transactions, which would indicate the compromise vector (social engineering lure, compromised device, or exposed seed phrase) remains active. If any drain transactions were completed before containment, coordinate with a blockchain analytics provider (e.g., Chainalysis Reactor or free alternatives such as Breadcrumbs.app) to trace fund flows, as Operation Atlantic demonstrated that law enforcement can freeze proceeds when tracing is initiated promptly.

Forensic Artifacts	On-chain ERC-20 Approval event logs (event signature: Approval(address owner, address spender, uint256 value)) for all organization-controlled wallet addresses — captures the exact block timestamp, spender address, and approval amount granted during the approval phishing interaction, which is the primary evidence of exploitation in this campaign | On-chain TransferFrom transaction records for each victim wallet — documents the attacker's drain transactions after approval was granted, including the drainer contract address and destination wallet, which are the direct evidence of financial loss and link to the criminal infrastructure disrupted under Operation Atlantic | Web proxy or DNS query logs from employee endpoints showing connections to fraudulent investment platforms or wallet-connector phishing pages in the 24–72 hours before any suspicious on-chain approval transaction — identifies the social engineering delivery vector (pig butchering lure site or fake dApp) | Browser history SQLite databases from affected employee endpoints (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\History; Firefox: %APPDATA%\Mozilla\Firefox\Profiles*.default\places.sqlite) — recovers visits to fraudulent investment platforms or wallet-connection prompts that preceded the approval transaction | Internal communication records (email, SMS, messaging app logs) showing the unsolicited investment solicitation or romantic grooming contact that initiated the pig butchering scheme — establishes the social engineering timeline and may contain the fraudulent dApp URL or attacker contact identifiers relevant to law enforcement referral under Operation Atlantic

Per-Action IR Details

Containment — If your organization custodies cryptocurrency on behalf of clients or employees, audit active token approvals on all associated wallet addresses using on-chain tools such as Revoke.cash or Etherscan's token approval checker. Revoke any approvals granted to unrecognized or untrusted addresses immediately.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected assets and prevent further damage while preserving evidence

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management) — treat wallet approval grants as privileged delegations requiring inventory and revocation, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — organization-controlled wallet addresses must appear in the asset inventory before approvals can be audited, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — token approvals are delegated permissions equivalent to account-level access grants and must be tracked

Compensating: For a 2-person team with no SIEM: use Etherscan's free Token Approval Checker (etherscan.io/tokenapprovalchecker) or Revoke.cash by pasting each organization-controlled wallet address. Export the approval list to a CSV by copying the rendered table. For wallets on networks other than Ethereum mainnet, use the equivalent block explorer (e.g., polygonscan.com, bscscan.com). Cross-reference each spender address against your internal authorized-dApp list. Flag any spender with an approval amount of 'Unlimited' or any spender address that does not appear in internal records. Revoke directly from Revoke.cash (requires wallet signature) or manually submit a zero-value approval transaction via MetaMask to the token contract's 'approve' function setting allowance to 0.

Evidence: Before revoking approvals, capture a full timestamped snapshot of all active ERC-20/ERC-721 token approvals for each wallet address via Etherscan or Revoke.cash — record spender contract address, token contract address, approval amount (unlimited vs. specific), and the block number and timestamp of the original approval transaction. Export the on-chain transaction history for each approval event (event signature: Approval(address indexed owner, address indexed spender, uint256 value)) from the token contract's event log. This approval transaction hash is the primary forensic artifact linking the victim wallet to the fraudulent spender address used in the pig butchering or approval phishing scheme.

Detection — Monitor for anomalous outbound cryptocurrency transfers, particularly bulk ERC-20 token movements initiated shortly after wallet approval transactions. Review access logs for employee interactions

with unsolicited investment platforms or wallet-connection prompts. Flag any approval transactions signed outside of established internal workflows.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across sources to understand scope and establish timeline

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring) — track and document each approval and transfer event as an incident record, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review web proxy and DNS logs at defined frequency for connections to known fraudulent investment platforms, NIST SI-4 (System Monitoring) — monitor for wallet-connection prompts delivered via phishing lures or fraudulent dApp sites, CIS 8.2 (Collect Audit Logs) — ensure DNS query logs, web proxy logs, and browser history are collected from employee endpoints before they are overwritten

Compensating: For a 2-person team: enable DNS query logging on your internal resolver (e.g., bind query log or Windows DNS debug log) and grep for domains associated with known pig butchering lure sites — cross-reference against CISA's known-bad domain feeds and the blockchain analytics community's published Operation Atlantic IOC lists. On Windows endpoints, query browser history SQLite databases directly: for Chrome, run 'Copy-Item $env:LOCALAPPDATA\Google\Chrome\User Data\Default\History $dest' then query with sqlite3 'SELECT url, last_visit_time FROM urls WHERE url LIKE "%connect%wallet%" OR url LIKE "%approve%"'. For ERC-20 TransferFrom events (the on-chain signal of approval abuse), set up a free Etherscan or Alchemy webhook alert on organization wallet addresses to notify on any outbound TransferFrom call — this detects the attacker draining tokens after approval was granted.

Evidence: Capture web proxy or DNS logs showing employee connections to fraudulent investment platforms or wallet-connector phishing pages in the 24–72 hours preceding any suspicious approval transaction. Retrieve browser history from affected employee endpoints — specifically look for visits to domains mimicking legitimate DeFi platforms (e.g., typosquatted Uniswap, fake Coinbase Wallet connect pages) that prompted a wallet signature. On-chain, pull the full event log for any TransferFrom transactions originating from the victim wallet address that were not initiated by the wallet owner's own signing key — these are the direct evidence of approval phishing exploitation. Capture internal email or messaging platform records showing the social engineering lure (the 'pig butchering' grooming messages or unsolicited investment opportunity that led to wallet connection).

Eradication — Revoke outstanding token approvals that cannot be traced to a known, authorized internal process. Invalidate any wallet connections to third-party dApps that were not explicitly approved through a documented procurement or onboarding process.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all components of the threat from the environment and verify removal

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation) — revoking unauthorized approvals is the direct remediation action equivalent to patching; the 'flaw' is the standing delegated permission, NIST AC-2 (Account Management) — approval grants to unauthorized spender addresses are delegated access rights that must be revoked on the same basis as unauthorized account access, CIS 5.3 (Disable Dormant Accounts) — treat wallet approvals to unrecognized spender addresses as dormant/unauthorized delegations and revoke within the same 45-day-or-sooner standard, CIS 6.2 (Establish an Access Revoking Process) — apply the organization's access revocation process to token approval grants; treat spender addresses as principals subject to access lifecycle management

Compensating: For a 2-person team: use Revoke.cash connected to each affected wallet (requires the wallet's signing key or hardware wallet) to batch-revoke all flagged approvals. For wallets where the signing key is unavailable (e.g., custodied keys), submit a manual approval transaction setting allowance to 0 via the token contract's approve(spenderAddress, 0) call using ethers.js or web3.py: 'contract.functions.approve(spender_address, 0).transact({"from": wallet_address})'. Document each revocation with the transaction hash, block number, token contract, and spender address revoked. For WalletConnect sessions specifically, disconnecting from the dApp interface revokes the session — instruct affected employees to open their wallet app, navigate to connected sites, and disconnect all unrecognized sessions.

Evidence: Before executing revocations, preserve the complete pre-revocation approval state as a timestamped record: spender address, token contract, approval amount, originating transaction hash, and block timestamp for each approval being revoked. This record is required for any law enforcement referral consistent with Operation Atlantic's victim identification process and for insurance or legal proceedings. Also capture any WalletConnect session metadata (session topic, peer metadata including dApp name and URL) from the wallet application logs before disconnecting — this may identify the specific fraudulent dApp used in the attack.

Recovery — Validate that wallet approval inventories are clean post-revocation. Implement a recurring approval audit cadence (monthly minimum) for any organization-controlled wallets. Notify affected individuals if employee wallets were compromised and coordinate with legal on any mandatory disclosure obligations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation, verify integrity, and confirm no residual threat remains

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting) — report confirmed employee wallet compromises to organizational IR capability and coordinate with legal on notification obligations, particularly where custodied client funds were affected, NIST IR-8 (Incident Response Plan) — the recovery step validates that IR plan execution was effective; the monthly audit cadence is the sustained monitoring component of the plan, NIST SI-7 (Software, Firmware, and Information Integrity) — verify wallet approval state post-revocation matches the expected clean baseline, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — recurring monthly approval audits are the ongoing vulnerability management cadence for organization-controlled wallets, CIS 7.2 (Establish and Maintain a Remediation Process) — document the monthly approval audit as a formal remediation tracking item with assigned ownership

Compensating: For a 2-person team: create a monthly cron job or calendar reminder to re-run Revoke.cash or Etherscan approval checks on all organization wallet addresses and compare output against your documented authorized-approvals baseline CSV. Automate post-revocation validation by scripting an Etherscan API call (free tier, 5 calls/second) against each wallet: 'curl "https://api.etherscan.io/api?module=account&action=tokentx&address=WALLET_ADDRESS&apikey=YOUR_KEY"' and filter for any TransferFrom events post-revocation date — any hit indicates residual unauthorized access. For breach notification scoping, use the Operation Atlantic victim identification criteria published by CISA and partner agencies to assess whether affected individuals meet regulatory notification thresholds in Canada (PIPEDA), UK (UK GDPR/ICO), or US (state breach notification laws).

Evidence: Post-revocation, capture a second full approval snapshot from Etherscan/Revoke.cash to confirm all targeted approvals now show 0 allowance — retain both the pre- and post-revocation snapshots as paired evidence records. Review on-chain transaction history for the 30 days following revocation to confirm no new unauthorized approval transactions were signed, which would indicate the social engineering lure is ongoing or the employee's device/seed phrase is still compromised. Document the clean-state validation timestamp and analyst signature for audit trail purposes per NIST AU-10 (Non-Repudiation).

Post-Incident — Conduct targeted security awareness training focused on cryptocurrency wallet hygiene: what a token approval transaction does, how to read approval prompts, and how to identify fraudulent investment solicitations. Establish a policy requiring approval of any wallet connections to external platforms before an employee or system may sign a transaction.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned, policy updates, and detection improvement to prevent recurrence

Controls: NIST IR-2 (Incident Response Training) — deliver targeted training on approval phishing and pig butchering mechanics to all personnel with cryptocurrency wallet access within the post-incident training window, NIST IR-8 (Incident Response Plan) — update the IR plan to include cryptocurrency wallet approval abuse as a named incident category with specific detection, containment, and revocation procedures, NIST SI-5 (Security Alerts, Advisories, and Directives) — incorporate Operation Atlantic advisories from CISA, FCA (UK), and RCMP/CAFC (Canada) into the organization's security advisory dissemination process, CIS 6.1 (Establish an Access Granting Process) — formalize

wallet-to-dApp connection requests as an access granting workflow requiring documented approval before any signing event, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — include cryptocurrency approval abuse as a recurring item in the vulnerability management process given the sustained nature of pig butchering campaigns

Compensating: For a 2-person team with no LMS or security awareness platform: develop a one-page visual explainer showing the difference between a legitimate ERC-20 approval prompt and a fraudulent one — use real screenshots from MetaMask's approval dialog annotating the spender address field, the token amount field (flag 'Unlimited'), and the contract verification status. Distribute via email with a mandatory acknowledgment reply. For the wallet-connection approval policy, implement a simple Google Form or ServiceNow-lite (free Jira) ticket as the pre-approval gate — require employees to submit the dApp name, contract address, and business justification before signing any wallet connection. Post the CISA and FCA pig butchering awareness bulletins (from Operation Atlantic public releases) as mandatory reading in the acknowledgment workflow.

Evidence: Preserve the complete incident timeline — from the first social engineering contact (if recoverable from email/messaging logs) through the approval grant, any drain transactions, and the revocation — as the primary lessons-learned input. This timeline should be used to update the detection hypothesis library: specifically, create a new hunting hypothesis for 'ERC-20 unlimited approval followed by TransferFrom within 72 hours to a first-seen spender address' as a standing detection rule. Retain Operation Atlantic IOC sets (fraudulent dApp domains, known drainer contract addresses) published by CISA, the FCA, and RCMP/CAFC for integration into DNS blocklists and future threat hunts.

Detection Guidance

No network-layer IOCs are available from public reporting on this operation. Detection is behavioral and on-chain. For organizations with crypto custody operations: (1) Query on-chain approval logs for any approval transaction (e.g., ERC-20 'approve' or 'setApprovalForAll' events) where the approved spender address is not on an internal allowlist. (2) Alert on token transfers from organizational wallets to addresses with no prior transaction history with the organization. (3) In endpoint and email security tooling, flag inbound messages containing wallet connection links or unsolicited investment platform invitations. (4) Monitor employee-facing web proxies for access to domains registered within the past 90 days that match cryptocurrency exchange or investment platform patterns. For general enterprise environments with no direct crypto custody, the primary detection surface is phishing: apply standard T1566 detection logic to inbound email, SMS gateway logs, and collaboration platform messages targeting employees.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Not available from public reporting`	No specific attacker-controlled domains, wallet addresses, or infrastructure indicators were released in public Operation Atlantic disclosures as of this item's sources	LOW

Framework Mappings

MITRE-ATTACK

- **T1204** — User Execution
- **T1583** — Acquire Infrastructure

- **T1566** — Phishing
- **T1583.001** — Domains
- **T1657** — Financial Theft
- **T1566.002** — Spearphishing Link
- **T1588** — Obtain Capabilities

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1204	User Execution	Execution
T1583	Acquire Infrastructure	Resource-Development
T1566	Phishing	Initial-Access
T1583.001	Domains	Resource-Development
T1657	Financial Theft	Impact
T1566.002	Spearphishing Link	Initial-Access
T1588	Obtain Capabilities	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/police-identifies-20...	T3

Source	URL	Tier
	https://www.bleepingcomputer.com/news/security/police-identifies-20...	T3
	https://www.bleepingcomputer.com/news/security/uk-warns-of-iranian-...	T3
	https://www.bleepingcomputer.com/news/security/india-targets-micros...	T3
US, UK, Canadian cops disrupt $45M global crypto scam	https://www.theregister.com/2026/04/09/crypto_fraud_scam_45_million/	T3

Generated 2026-04-11 18:20 UTC by TJS Security Command Center