05/03/2026

THRIVE
Cyber Security Incident Response Team:

Adversary Operations Group (AOG)

Finance, Financial Services & Banking Sector Report

Quarterly Threat Intelligence Assessment

Empowering Our Clients to Harness the Promise of Technology

Contents

Report ID	CTI-AOG-2026-003
Title	Finance, Financial Services & Banking Sector — Quarterly Threat Intelligence Assessment
Reporting Period	03 February 2026 – 05 March 2026
Date Produced	05 March 2026
Classification	TLP: White
Overall Sector Risk	**HIGH**
Produced By	Cyber Security Incident Response Team: Adversary Operations Group (AOG)
Author	Simon White
Sources	Thrive Intelligence Platforms, Infoblox, ThreatFabric, Wiz Research, Proofpoint, Microsoft
Revision	0.2

1. EXECUTIVE SUMMARY

The finance, financial services, and banking sector faces a sustained HIGH threat environment during the 30-day reporting period (03 Feb – 05 Mar 2026). Reports from Thrive Intelligence platforms and corroborating open sources identifies six converging threat categories directly targeting the sector: (1) OAuth redirect abuse enabling malware delivery and credential bypass; (2) AI-driven investment fraud campaigns operating across 23,000+ algorithmically generated domains; (3) Massiv — a newly identified Android banking trojan with Device Takeover capability; (4) Malware-as-a-Service (MaaS) credential stealers and RATs (Arkanix, TrustConnect) targeting banking credentials and financial data; (5) DNS-evasive fake investment platforms (Savvy Seahorse) routing victims' funds to Russian-linked accounts; and (6) a broad cloud threat landscape highlighting ransomware, credential theft, and third-party risks escalating across cloud-hosted financial infrastructure.

Recommended immediate posture: HEIGHTENED VIGILANCE.

Priority actions: block OAuth redirect abuse vectors, audit Entra ID application consents, deploy mobile fraud detection for DTO patterns, and block confirmed malicious domain infrastructure listed in Section 5.

2. THREAT LANDSCAPE OVERVIEW

During the 30-day reporting period, the financial sector experienced sustained multi-vector threat activity. The threat landscape is characterized by the commoditization of attack tooling through MaaS platforms, the integration of AI capabilities into fraud operations, an escalating identity and cloud attack surface, and the continued evolution of mobile banking fraud. Nine primary threat categories are assessed as active against the sector:

Threat Category	Primary Vector	Severity	Trend
OAuth Redirect Abuse / Malware Delivery	Phishing / Identity	CRITICAL	↑ Escalating (Mar 2026)
AI-Driven Investment Fraud (Pig Butchering)	Social Engineering	CRITICAL	↑ Expanding globally
Massiv Android Banking Trojan (NEW)	Mobile / Sideloading	HIGH	↑ Newly identified Feb 2026

MaaS Credential Stealers (Arkanix, TrustConnect)	Email / MaaS	HIGH	→ Persistent
Malicious OAuth Apps in Entra ID	Identity / Cloud	HIGH	↑ Escalating campaign
Savvy Seahorse Fake Investment Platforms	DNS / social media	HIGH	→ Persistent since 2021
Cloud Infrastructure Threats	Misconfiguration / Cloud Abuse	HIGH	↑ Expanding attack surface
Cryptocurrency Scam Infrastructure	Domain / YouTube Hijacking	MEDIUM	→ Persistent
Calendar Phishing (Credential Harvest)	Email / Calendar Apps	MEDIUM	↑ Growing adoption by actors

3. TECHNICAL THREAT ANALYSIS

3.1 OAuth Redirect Abuse Enabling Malware Delivery and Credential Bypass

Published: 04 Mar 2026
Source: Microsoft Warns OAuth Redirect Abuse Delivers Malware to Government Targets
Confidence: HIGH Microsoft Defender Security Research Team primary source, corroborated by existing Entra ID OAuth campaign intelligence (8e0a733b).

Microsoft has disclosed active phishing campaigns exploiting a by-design feature of OAuth to redirect victims to attacker-controlled infrastructure without requiring credential or token theft. This technique represents a significant evolution in identity-based attacks, as it bypasses conventional email and browser phishing defenses by crafting URLs through legitimate identity providers including Entra ID and Google Workspace.

Attack Chain:

- Threat actor creates a malicious application in a tenant under their control
- Application is configured with a redirect URL pointing to an attacker-controlled domain hosting malware
- OAuth phishing link is distributed via email, using financial, e-signature, social security, Teams recording, and political lures
- Victim clicks link — intentionally invalid OAuth scope triggers redirect to attacker domain
- Victim downloads a ZIP archive containing a Windows shortcut (LNK) file
- LNK executes PowerShell, conducting host reconnaissance, then extracts an MSI installer
- MSI drops a decoy document while sideloading a malicious DLL (crashhandler.dll) via steam_monitor.exe
- DLL decrypts crashlog.dat and executes final payload in memory, establishing C2 channel

- Some campaigns additionally route victims to AitM phishing frameworks (EvilProxy) to harvest session cookies

Finance Sector Relevance:

Lure themes include financial and social security content, making finance sector employees and customers high-value targets. Post-exploitation activity includes pre-ransomware staging and hands-on-keyboard operations. Email distribution uses mass-sending tools and custom Python/Node.js solutions on scale.

AOG Analyst Comment:

This report represents a critical development in identity-based attack tradecraft. The exploitation of OAuth's native redirect behavior rather than vulnerabilities means this technique is inherently resistant to patches and will persist as long as OAuth remains in use. The direct overlap with the existing malicious OAuth app campaign (Report 8e0a733b) confirms a broader adversary focus on Entra ID as a persistent access vector into financial organizations. AOG recommends immediate review of: (1) application consent policies to restrict user-initiated OAuth authorizations; (2) conditional access policies to block unknown application redirects; and (3) email gateway rules to identify OAuth URL patterns in inbound phishing lures. Threat hunting teams should prioritize reviewing Entra ID audit logs for newly consented applications and unusual OAuth redirect activity. Escalation to Tier 2 is warranted given the active nature of this campaign and its overlap with financial sector lure themes.

3.2 AI-Driven Pig Butchering: Investment Fraud at Scale

Source: Banners, Bots and Butchers: The AI-Driven Long Con in Asia
Confidence: HIGH — Infoblox and Group-IB joint investigation with technical domain analysis.

A sophisticated hybrid campaign combines social media malvertising with AI-powered chatbot engagement to conduct cryptocurrency investment fraud targeting users in Asia, with confirmed indicators of global expansion. The campaign operates across 23,000+ algorithmically generated domains and employs AI chatbots for sustained, convincing victim engagement throughout the fraud lifecycle.

Finance Sector Relevance:

Victims are induced to transfer funds — often from bank accounts — into fabricated investment platforms. Compromised victim accounts are subsequently used for money mule activity, directly impacting financial institutions' fraud detection and AML compliance obligations. The scale of the infrastructure (23,000+ domains) presents a significant challenge for perimeter-based IOC blocking alone.

AOG Analyst Comment:

The integration of AI chatbot technology into pig-butchering fraud infrastructure marks an architectural shift in the threat landscape. Traditional fraud detection patterns based on brief initial contact followed by exit are no longer reliable — AI-sustained engagement can extend victim interactions for weeks or months, significantly increasing average fraud losses. Financial institutions should review AML monitoring rules for patterns consistent with mule account activity originating from this campaign typology. Customer-facing advisory communications are

recommended. AOG also flags the global expansion indicator: while primarily Asia-focused, Infoblox note signs of geographic spread which could include UK and European financial sector customers.

3.3 Cloud Threat Hunting and Defense Landscape - Financial Sector Relevance

Source: 2025 Cloud Threat Hunting and Defense Landscape
Confidence: HIGH - Recorded Future annual research report corroborated by AlienVault OTX pulse.

Recorded Future's 2025 annual cloud threat intelligence report identifies key trends highly relevant to financial sector cloud infrastructure. The report documents a material shift toward cloud-native attack methods that abuse built-in functionality rather than relying on traditional malware, a pattern directly aligned with the OAuth abuse campaigns observed in this reporting period.

Key Findings Relevant to Financial Services:

- Threat actors increasingly registering their own cloud tenants to legitimize malicious OAuth applications and command infrastructure
- Exploitation of misconfigurations remains the primary initial access vector for cloud breaches
- Credential theft via cloud-native tools (ACR Stealer, FatalRAT, SaltWater, SeaSpy, Lamehug, Seaside) directly targeting financial sector organizations
- Ransomware groups increasingly incorporating cloud storage exfiltration prior to encryption
- Third-party risk escalating — supply chain attacks via compromised cloud-hosted services
- AI and ML cloud services identified as emerging targets, with threat actors probing financial sector AI implementations
- DDoS attack effectiveness against cloud environments decreasing, with attackers pivoting to identity and credential-based intrusion

AOG Analyst Comment:

This report provides essential strategic context for the tactical threat activity observed throughout this reporting period. The documented shift to cloud-native attack methods directly explains the OAuth redirect abuse and malicious Entra ID application campaigns these are not isolated incidents but part of a broader adversary strategy to abuse legitimate cloud functionality. For financial sector organizations, the convergence of cloud-native attacks, credential theft tooling, and third-party risks creates a compound risk posture. AOG recommends financial institutions review their cloud security posture management (CSPM) controls, prioritize service account and OAuth application auditing, and ensure third-party SaaS integrations are subject to periodic security review. The AI/ML cloud service targeting finding warrants particular attention for financial institutions deploying AI in trading, fraud detection, or customer service contexts these represent emerging high-value targets.

3.4 Massiv Android Banking Trojan

Source: When your IPTV app terminates your savings
Confidence: HIGH ThreatFabric technical malware analysis. Newly identified February 2026.

Massiv is a newly identified Android banking trojan distributed through side-loaded IPTV applications that enables Device Takeover (DTO) attacks, allowing threat actors to initiate fraudulent banking transactions directly from

compromised devices. Its ability to bypass Android's FLAG_SECURE screen capture protection via UI-tree mode represents a meaningful capability uplift over comparable malware families.

Key Capabilities:

- Full Device Takeover (DTO) via screen streaming and UI-tree interaction
- Overlay attacks to capture credentials on banking and financial apps
- Keylogging for credential and PIN capture
- SMS and push notification interception (OTP bypass)
- Screen capture with FLAG_SECURE bypass via UI-tree mode
- Accessibility Service abuse for persistent device control
- Targets government applications and digital identity wallets (confirmed: Portugal)

AOG Analyst Comment:

Massiv's Device Takeover capability is of direct concern to financial institutions offering mobile banking services. Unlike overlay-only malware, DTO enables actors to initiate transactions invisibly to the victim — on-device fraud that circumvents transaction monitoring systems that rely on detecting access from unusual devices or locations, since fraud occurs on the victim's own enrolled device. The FLAG_SECURE bypass is a notable technical development. AOG recommends financial institutions review mobile banking app RASP (Runtime Application Self-Protection) controls, implement anomaly detection for accessibility service usage patterns, and consider biometric step-up authentication for high-value transfers. Customer advisory communication regarding unofficial IPTV applications is recommended.

3.5 Arkanix Stealer — MaaS Credential Theft

Source: Arkanix Stealer targets a variety of data, offers a MaaS referral program

Confidence: HIGH - Securelist technical analysis. C2 infrastructure disrupted Dec 2025; samples and techniques persist in wild.

Arkanix is a MaaS credential stealer targeting online banking credentials, cryptocurrency wallets, VPN authentication, and financial platform session tokens. Available in Python and C++ variants, Arkanix implements a referral program to attract buyers with a commoditization model that increases operator numbers and complicates attribution.

Financial Data Targeted:

- Online banking credentials from all major browsers (saved passwords and session cookies)
- Cryptocurrency wallets: MetaMask, Exodus, Coinbase, Trust Wallet
- VPN credentials: OpenVPN, NordVPN, ProtonVPN (enabling network access resale)
- RDP connection details (enabling initial access brokerage)
- Desktop screenshots (operational intelligence for follow-on attacks)

AOG Analyst Comment:

While Arkanix's primary C2 infrastructure was reportedly disrupted in December 2025, the Kaspersky analysis confirms samples continue to circulate. The financial credential focus encompassing both banking and cryptocurrency makes Arkanix a high-relevance stealer for this sector. SOC teams should review EDR telemetry for indicators of browser credential dump activity, MetaMask extension directory access, VPN configuration file reads, and anomalous screenshot capture processes. Any harvested Arkanix credential sets are likely in circulation on dark

web markets, raising the probability of follow-on credential-stuffing attacks against financial institution authentication systems. AOG recommends reviewing authentication logs for anomalous credential reuse patterns.

3.6 TrustConnect RAT - MaaS Remote Access Trojan

Source: (Don't) TrustConnect: It's a RAT in an RMM hat

Confidence: HIGH Proofpoint Threat Research. New MaaS RAT identified February 2026. Linked to prior Redline Stealer operators.

TrustConnect is a newly identified MaaS Remote Access Trojan priced at $300/month that masquerades as a legitimate Remote Monitoring and Management (RMM) tool. Its fake business website serves as both its public-facing C2 dashboard and its MaaS purchasing portal. Links to prior Redline Stealer operators suggest experienced actors behind its development.

Key Capabilities:

- Web-based C2 dashboard with buyer and operator interfaces
- Automated digitally signed payload generation (bypasses application allow lists)
- Full remote desktop capability — enabling hands-on-keyboard operations in victim environments
- Email-distributed, often bundled alongside legitimate RMM tool installers as a lure

AOG Analyst Comment:

TrustConnect's lineage from Redline Stealer operators is significant. Redline was responsible for widespread banking credential theft campaigns, and its successor tooling inheriting a full RAT capability represents an escalation in operator sophistication. The digitally signed payload generation capability is a direct counter to endpoint application allow listing a control commonly deployed in financial environments. Financial sector IT security teams should validate that EDR solutions have behavioral detection for RMM-impersonating RATs and review email gateway policies for lures using RMM product names. The $300/month price point ensures broad operator adoption, making this a widely deployed threat in the near term.

3.7 Malicious OAuth Application Campaigns in Entra ID

Source: Uncovering Malicious OAuth Campaigns in Entra ID

Confidence: HIGH — Wiz Research with automated OAuth Apps Scout detection pipeline. Confirmed 19-app campaign with named IOCs.

Wiz Research has identified and documented a sustained campaign of malicious OAuth applications registered in Microsoft Entra ID, designed to blend in with legitimate enterprise SaaS integrations. These applications impersonate well-known brands including DocuSign, Adobe, OneDrive, and Microsoft Teams, requesting high-privilege scopes that enable persistent access to M365 environments independent of user credential changes.

Confirmed High-Privilege Scopes Abused:

- Mail.ReadWrite full email access and manipulation
- Files.ReadWrite.All full SharePoint/OneDrive access
- User.Read.All organizational directory enumeration

- Calendars.ReadWrite calendar access (supporting calendar phishing)

Finance Sector Relevance:

OAuth token-based persistence survives password resets, MFA re-enrollment, and conditional access policy changes. For financial sector organizations, malicious OAuth applications with mail and file access scopes represent a covert persistent access vector into M365 environments housing financial communications, SWIFT correspondence, customer data, and regulatory documentation.

AOG Analyst Comment:

This report is directly linked to the OAuth redirect abuse campaign disclosed by Microsoft (Report 6176f775) and should be reviewed in conjunction with it. Together, they confirm a systematic adversary focus on the Microsoft identity and cloud platform as a primary attack surface. The malicious OAuth app technique is particularly dangerous because: it does not require ongoing phishing success; it is invisible to users who consented; standard password-reset incident response processes do not remediate it; and granted scopes may enable lateral movement to other connected applications. AOG strongly recommends conducting an immediate full audit of all third-party OAuth application consents in Entra ID, prioritizing revocation of any unverified, newly registered, or unexpectedly privileged applications. The OAuth Apps Scout methodology described in the Wiz report should be evaluated for adoption.

3.8 Savvy Seahorse — DNS-Evasive Fake Investment Platforms

Source: DNS Used to Hide Fake Investment Platform Schemes
Confidence: HIGH Infoblox threat research with DNS infrastructure analysis. Active since August 2021.

Savvy Seahorse is a persistent DNS threat actor operating fake investment platforms via Facebook advertising. The actor employs a sophisticated DNS CNAME-based Traffic Distribution System (TDS) to dynamically update IP addresses, rapidly cycle subdomains, and evade conventional detection. Funds collected from victims are routed to Russian-linked bank accounts.

Key Infrastructure:

- 4,200+ base domains with CNAME records pointing to b36cname[.]site subdomains
- DNS TDS enables real-time IP rotation and subdomain cycling every 5-10 days
- Fake ChatGPT and WhatsApp bots used for victim interaction
- Multi-language targeting across European and Asian language groups

AOG Analyst Comment:

Savvy Seahorse demonstrates how DNS infrastructure can be weaponized to create large-scale, evasion-resilient fraud campaigns. The CNAME TDS architecture means that blocking individual IP addresses or downstream domains is largely ineffective — the root domain b36cname[.]site is the primary blocking target. For financial institutions, the fraud pipeline directly draws from retail banking customer funds, and money mule accounts associated with this campaign may appear in transaction monitoring. AOG recommends adding b36cname[.]site (all subdomains) as a priority DNS block across all outbound resolvers, email gateways, and web proxies.

3.9 Calendar Phishing — Credential Harvesting via Spoofed Invitations

Source: Invitation to Trouble: The Rise of Calendar Phishing Attacks
Confidence: MEDIUM-HIGH — Multiple corroborating sources. Technique is increasingly observed in enterprise targeting.

Spoofed Microsoft and Google Calendar invitations are being used to deliver credential phishing campaigns. By exploiting routine business scheduling behavior, actors achieve high click-through rates. Calendar invites containing meeting links redirect employees to fake M365 or Google login pages, harvesting credentials for subsequent enterprise access.

AOG Analyst Comment:

Calendar phishing is a growing complement to traditional email phishing. The technique is effective precisely because calendar invitations are expected to contain external links, bypassing the scepticism employees may apply to email links. For financial sector organizations, harvested M365 credentials feed directly into the broader OAuth and identity threat picture an actor with stolen credentials can consent to malicious OAuth apps, access SWIFT correspondence, and establish persistence before credential-based controls can respond. AOG recommends staff security awareness advisories specifically covering calendar-based phishing lures and recommends reviewing conditional access policies to ensure MFA cannot be bypassed via credential theft alone.

3.10 Cryptocurrency Scam Infrastructure - Domain and YouTube Campaign

Source: Uncovering Malicious Cryptocurrency Scam Domains and Hacked YouTube Channels
Confidence: HIGH — Infoblox domain infrastructure analysis with confirmed IOCs.

Infoblox researchers have identified a cluster of malicious domains under the CryptDesignBot infrastructure hosting cryptocurrency scams, supplemented by hijacked YouTube channels hosting fake celebrity livestreams (Elon Musk, Tesla, crypto exchange impersonations). Lookalike domains impersonate legitimate brands and frequently change registrars to evade detection.

AOG Analyst Comment: While assessed at MEDIUM severity for institutional financial sector clients, this campaign directly impacts the retail banking customer base through cryptocurrency fraud. Financial institutions should monitor for unusual customer fund outflows to cryptocurrency exchange destinations correlated with this infrastructure. Customer fraud communications should include warnings about fake celebrity cryptocurrency livestream scams.

4. INDICATORS OF COMPROMISE (IOCs)

4.1 Malicious Domains — Priority Block List

The following domains are confirmed as malicious and should be blocked at DNS resolver, email gateway, and web proxy layers.

Domain / Indicator	Threat	Notes
b36cname[.]site (ALL subdomains)	Savvy Seahorse	CNAME TDS hub — blocking this root neutralizes 4,200+ downstream domains
capitals-investment[.]live	Investment Fraud	Fake investment platform
capitalai-investment[.]com	Investment Fraud	AI-themed fake investment lure
finance-3885899[.]world	Investment Fraud	Pig-butchering campaign domain
finance818[.]online	Investment Fraud	Pig-butchering campaign domain
vtb-finance[.]com	Brand Impersonation	VTB Bank impersonation
vtb-finance[.]online	Brand Impersonation	VTB Bank impersonation variant
cryptocurrencyworld[.]online	Crypto Scam	CryptDesignBot infrastructure
cryptocurrencys[.]site	Crypto Scam	CryptDesignBot infrastructure
cryptocurrency[.]legal	Crypto Scam	CryptDesignBot infrastructure
cryptocurrencyexpress[.]xyz	Crypto Scam	CryptDesignBot infrastructure

4.2 OAuth Application Indicators — Malicious Entra ID Apps

The following application characteristics should be used to identify and revoke malicious OAuth consents in Microsoft Entra ID. Review all applications matching these patterns.

Indicator Type	Value	Action
Impersonated Brand Names	DocuSign, Adobe, OneDrive, Zoom,	Review any app using these names from unverified publishers

	Teams, Microsoft 365	
High-Privilege Scopes	Mail.ReadWrite, Files.ReadWrite.All, User.Read.All, Calendars.ReadWrite	IMMEDIATE REVIEW — revoke if publisher unverified or unexpected
Publisher Status	Unverified / Recently Registered	Treat as high-risk; revoke unless positively verified
OAuth Redirect Patterns	Redirects to non-corporate / unknown domains	Block at conditional access layer; investigate endpoint
Tenant Registration Age	Newly registered tenants (< 30 days)	Treat as indicator of malicious registration pattern

4.3 Massiv Android Trojan Behavioral IOCs

Indicator	Detail
Distribution Method	Side-loaded APK via unofficial IPTV streaming sites
Lure Application Type	IPTV / media streaming applications
Abused Android API	Accessibility Services (persistent device control)
C2 Method	Screen streaming and UI-tree API
Evasion Technique	UI-tree mode bypasses FLAG_SECURE screen capture protection
Confirmed Target Geography	Portugal (government digital ID wallet apps) — global expansion suspected
OTP Bypass Method	SMS and push notification interception

4.4 TrustConnect / Arkanix - Endpoint and Network IOCs

Malware	IOC Type	Detail
TrustConnect	C2 Infrastructure	Fake RMM vendor website used as C2 dashboard and MaaS portal
TrustConnect	Delivery Vector	Email campaigns with RMM tool lures; bundled with legitimate RMM installers
TrustConnect	Payload Characteristic	Auto-generated digitally signed executables (bypasses allowlisting)
TrustConnect	Attribution Link	Linked to prior Redline Stealer operators
Arkanix	Data Target	Browser saved credentials, session cookies, crypto wallet extensions
Arkanix	Data Target	VPN config files (OpenVPN, NordVPN, ProtonVPN)
Arkanix	Behavior	Desktop screenshot capture; RDP connection detail exfiltration

5. MITRE ATT&CK MAPPING

The following techniques have been observed or are strongly indicated across the threats documented in this report. Confidence ratings reflect the strength of evidence supporting each technique.

Technique ID	Technique Name	Priority	Observed In
T1528	Steal Application Access Token (OAuth)	CRITICAL	OAuth Redirect Abuse, Malicious Entra ID Apps
T1657	Financial Theft	CRITICAL	Pig Butchering, Savvy Seahorse, Massiv DTO
T1566.002	Phishing: Spearphishing Link	HIGH	OAuth Redirect Abuse, Calendar Phishing, Arkanix

T1566.003	Phishing via Service (Calendar Invite)	HIGH	Calendar Phishing Campaign
T1098.001	Additional Cloud Credentials	HIGH	Malicious OAuth App consents in Entra ID
T1539	Steal Web Session Cookie	HIGH	OAuth AitM (EvilProxy), Arkanix Stealer
T1555.003	Credentials from Browser	HIGH	Arkanix Stealer, TrustConnect RAT
T1219	Remote Access Software / RMM Abuse	HIGH	TrustConnect RAT (masquerading as RMM)
T1404	Mobile Privilege Escalation (Accessibility)	HIGH	Massiv Android Banking Trojan
T1056.001	Keylogging	HIGH	Massiv, Arkanix, TrustConnect
T1056.002	GUI Input Capture / Overlay Attack	HIGH	Massiv Android Banking Trojan
T1113	Screen Capture	HIGH	Massiv (FLAG_SECURE bypass), Arkanix, TrustConnect
T1041	Exfiltration Over C2 Channel	HIGH	Arkanix Stealer, TrustConnect RAT
T1189	Drive-By Compromise / Malvertising	MEDIUM	Pig Butchering, Savvy Seahorse Facebook Ads
T1568.001	DNS-Based Evasion (CNAME TDS)	MEDIUM	Savvy Seahorse Infrastructure
T1486	Data Encrypted for Impact (Ransomware)	HIGH	Cloud Threat Landscape — residual ransomware risk

6. RISK ASSESSMENT

Risk Scenario	Likelihood	Impact	Overall Risk	Primary Threat Driver
M365 environment compromise via OAuth redirect / malicious app consent	HIGH	CRITICAL	CRITICAL	OAuth Redirect Abuse + Malicious Entra ID Apps
Mobile banking fraud via Massiv Device Takeover	HIGH	CRITICAL	CRITICAL	Massiv Android Banking Trojan
Customer investment fraud losses / mule account activity	HIGH	HIGH	HIGH	Pig Butchering / Savvy Seahorse
Enterprise credential theft feeding IAB / ransomware pre-staging	HIGH	HIGH	HIGH	Arkanix + TrustConnect
Cloud misconfiguration exploitation leading to data breach	HIGH	HIGH	HIGH	Cloud Threat Landscape Report
SWIFT / payment system fraud via RAT with full remote desktop access	MEDIUM	CRITICAL	HIGH	TrustConnect RAT
Ransomware attack on cloud-hosted financial infrastructure	MEDIUM	CRITICAL	HIGH	Cloud Threat Landscape Report
Regulatory non-compliance / brand damage from consumer fraud	HIGH	MEDIUM	HIGH	Fraud campaigns across multiple vectors

7. DETECTION & MITIGATION RECOMMENDATIONS

7.1 Immediate Actions (0–72 Hours)

Priority	Action	Rationale
P1	Block b36cname[.]site and all subdomains at DNS resolver, email gateway, and web proxy	Neutralizes 4,200+ Savvy Seahorse downstream domains in single block
P1	Conduct emergency Entra ID OAuth application audit — revoke all unverified or newly registered apps holding Mail.ReadWrite, Files.ReadWrite.All, or User.Read.All scopes	Addresses both malicious OAuth app and OAuth redirect abuse campaigns
P1	Block all IOC domains listed in Section 4.1 at DNS, proxy, and email gateway layers	Direct block of confirmed malicious infrastructure
P2	Hunt EDR telemetry for: browser credential dump processes, MetaMask/wallet extension directory access, VPN config file reads by anomalous processes, desktop screenshot capture	Arkanix Stealer and TrustConnect RAT behavioral indicators
P2	Issue staff security advisory covering OAuth phishing links (e-signature, Teams recording, financial lures) and calendar invitation phishing	Active campaigns using these delivery mechanisms
P2	Configure Entra ID Conditional Access to require admin approval for all new third-party OAuth app consents requesting privileged scopes	Prevents new malicious OAuth app consents while audit is in progress

7.2 Identity, Cloud, and OAuth Security

- Implement OAuth application consent policies requiring admin approval for all apps requesting high-privilege scopes
- Deploy continuous OAuth application monitoring using automated detection pipelines (reference: OAuth Apps Scout methodology from Wiz Research)
- Conduct quarterly audit of all OAuth consent grants across all Entra ID tenants
- Enable Conditional Access policies enforcing MFA for all M365 access and blocking legacy authentication protocols
- Review and harden CSPM controls for all cloud-hosted financial infrastructure
- Enforce just-in-time (JIT) and just-enough-access (JEA) for cloud service accounts
- Review third-party SaaS integrations — revoke or restrict integrations that are no longer actively required

7.3 Mobile Banking Security

- Issue customer advisory warning against side-loading applications from unofficial sources, specifically IPTV and media streaming apps
- Implement mobile fraud detection analytics capable of identifying Device Takeover patterns: transactions initiated via accessibility service interaction anomalies and UI-tree API usage
- Review mobile banking app FLAG_SECURE implementation — evaluate RASP controls for Massiv's UI-tree bypass technique
- Enforce biometric re-authentication for high-value transfers originating from enrolled devices
- Monitor for transactions from devices exhibiting abnormal accessibility service usage

7.4 Investment Fraud and Customer Protection

- Add all IOC domains from Section 4.1 to online banking and mobile app URL filtering for customer-protection
- Deploy customer-facing alerts regarding AI-powered investment fraud, pig-butchering scams, and fake celebrity cryptocurrency livestreams
- Review AML monitoring rules for patterns consistent with money mule recruitment and operation: unusual outbound cryptocurrency transfers, sudden account funding followed by rapid transfers
- Enhance due diligence triggers for mule-recruitment behavioral patterns in transaction monitoring

7.5 Cloud Ransomware Readiness

- Verify integrity of offline/immutable backups and validate restoration procedures for cloud-hosted systems
- Ensure SWIFT infrastructure is network-segmented with hardware token MFA and monitored for anomalous access
- Review and test data breach notification procedures in the context of potential cloud data exfiltration prior to encryption
- Ensure cloud storage buckets and repositories holding sensitive financial data are not publicly exposed (misconfiguration remains primary initial access vector)

8. INTELLIGENCE GAPS

The following collection gaps are identified. Priority collection requests are raised for Tier 2 / senior analyst action:

Gap	Detail
OAuth Redirect Abuse — Attribution	No attributed threat actor group for the Microsoft-disclosed OAuth redirect campaigns. Attribution would enable pattern matching against known TTPs and better predict targeting.
Massiv C2 Infrastructure	Server addresses, domain patterns, and full C2 communication protocol are not yet publicly characterized for Massiv. Required for network-layer detection.

Arkanix Credential Circulation	Extent of harvested financial credential sets in circulation on dark web markets following C2 takedown is unquantified. Dark web monitoring required.
TrustConnect Deployment Scale	Number of active financial sector infections and current operator campaign targeting is unknown.
Savvy Seahorse Full Attribution	Nationality and full Russian bank account network incompletely characterized. Incomplete picture limits sanctions screening effectiveness.
Cloud Misconfiguration Incident Data	Recorded Future report notes escalating cloud breach activity, but specific financial sector incident telemetry is not available internally. Threat hunting collection required.

9. ESCALATION CRITERIA

The following events require IMMEDIATE escalation to Tier 2 / Senior Analyst:

- Detection of any IOC domain from Section 4.1 in DNS, proxy, or email gateway logs
- Identification of any unverified or newly registered OAuth application with Mail.ReadWrite, Files.ReadWrite.All, or equivalent high-privilege scopes in Entra ID
- Detection of OAuth redirect patterns (non-corporate OAuth error-state redirects) in email gateway or proxy logs
- Customer report of unauthorized mobile banking transactions from device with no user-initiated action (potential Massiv DTO)
- Employee report of calendar invitation containing unusual login page (potential calendar phishing)
- EDR detection of browser credential dump / wallet extension directory access / VPN config file read by anomalous process / mass screenshot capture (Arkanix / TrustConnect indicators)
- Mass customer reports of account compromise within a short window (harvested credential batch deployment)
- Detection of unusual SWIFT message patterns or outbound wires outside business hours from workstations without established SWIFT access
- VSS deletion, MBR write operations, or mass file encryption events across cloud or on-premises infrastructure

10. AOG ANALYST COMMENT

AOG Analyst Comment — Assessment Summary

This 30-day assessment identifies a threat environment characterized by the convergence of three strategic trends: the systematic targeting of the Microsoft identity and cloud platform (OAuth redirect abuse, malicious Entra ID app consents, credential phishing campaigns); the industrialization of financial fraud through AI integration and MaaS commoditization (pig butchering chatbots, Arkanix, TrustConnect); and the evolution of mobile banking fraud into full Device Takeover capability (Massiv). The most significant development in this reporting period is the OAuth redirect abuse disclosure from Microsoft, which taken together with the Wiz Research malicious OAuth app campaign confirms that adversaries have adopted a systematic strategy of abusing Microsoft's own identity infrastructure to establish persistent, credential-resilient access to enterprise M365 environments. For financial sector organizations, this creates a particularly dangerous attack surface: M365 environments house SWIFT correspondence, customer financial data, regulatory communications, and internal treasury operations.

The second most significant finding is the Massiv Android banking trojan. The Device Takeover capability with FLAG_SECURE bypass represents a meaningful capability uplift that renders several conventional mobile fraud controls less effective. Financial institutions should treat Massiv as a near-term threat requiring proactive RASP control review rather than a watch-and-wait risk.

Assessment Confidence: MEDIUM-HIGH. Primary limitations are the attribution gaps identified in Section 8 and the absence of internal telemetry confirming active campaigns against specific client environments. This report should be refreshed within 14 days given the active and evolving nature of the OAuth-related campaigns.

Prepared by: Thrive Adversary Operations Group (AOG) Tier 1 CTI Analyst | 05 March 2026