EDP ECOSYSTEM DEEP-DIVE

MODULE 04: CALLERS AND SPAMMERS

Social Engineering and Human-Layer Access: Vishing, Call Centers, and Email Bombing

HANDLING: INTERAGENCY | April 2026 | EDP Deep-Dive Series

MODULE HEADER	
Module Number	**04**
Module Name	**Callers and Spammers (Social Engineering and Human-Layer Access)**
EDP Node Reference	**No dedicated Dependency Map node -- cross-reference to Node 04 (IAB Markets, HIGH tier) as downstream access recipient; Node 05 (Botnet/Loader Ecosystems, HIGH tier) as parallel/substitute delivery mechanism; Node 10 (Credential/Stealer-Log Markets, MEDIUM tier) as contact data supplier. See Section 8 for Dependency Map annotation recommendation.**
Ecosystem Layer	**Human-Layer Access Generation (cross-cutting; supplements and substitutes for technical initial access across stealer, loader, IAB, and ransomware chains)**
Upstream Connections	**Feeds from: Stealer-log and credential markets (Module 01/Module 05) for target contact data; Underground Forums (Module 10) for tooling and service procurement**
Downstream Connections	**Feeds into: Initial Access Brokers (Module 05) -- caller-generated access sold as footholds; Ransomware Groups/RaaS (Module 07) -- direct escalation from social-engineering entry to ransomware deployment; Loaders (Module 02) -- call-center campaigns deliver loader payloads directly**
Research Date	**April 2026**
Primary Researcher	**Reno**
Source Tools Used	**Perplexity (raw research, Sections 1-7) + Claude (synthesis, EDP integration, Section 8 Analyst Assessment)**

SECTION 1: WHAT IT IS

Definition

Callers and spammers are threat actors and services that use voice, messaging, and email-volume operations to manipulate human targets into surrendering credentials, approving MFA requests, granting remote access, or executing malware. Unlike technical initial access methods that exploit software vulnerabilities, this module covers human-layer exploitation: social engineering that weaponizes trust, urgency, and institutional process familiarity to bypass security controls that cannot be defeated technically. **[CONFIRMED]**

Scope includes: vishing and fake IT/helpdesk calls; call-center-directed malware delivery (subscription cancellation pretexts); email bombing used as a social engineering amplifier; bulk SMS and email spam for credential harvesting; and AI-assisted vishing platforms sold as a service. Purely technical phishing kits are outside scope except where tightly coupled with telephone-based operations. **[CONFIRMED]**

How It Functions

Pattern A -- Vishing and fake IT/helpdesk (LAPSUS$/Scattered Spider model): Actors obtain target organization data through OSINT (LinkedIn, corporate directories, stealer logs) and identify helpdesk staff, IT administrators, or high-value employees. The caller impersonates IT support, a vendor, or a bank representative. The objective is to convince the target to reset MFA, provide a one-time passcode, install remote access software, or approve an account change. Native-accent English and deep knowledge of corporate processes are key differentiators for high-capability operators. **[CONFIRMED]**

Pattern B -- Call-center malware delivery (BazarCall / subscription cancellation model): Actors send emails claiming the recipient has been billed for a subscription service (antivirus, software, streaming). The email contains no malicious link; the only action item is a callback phone number. When the target calls, a call-center operator guides them to download a "cancellation tool" from a controlled website. The tool is a loader, RAT, or ransomware stager. This model defeats email security gateways entirely because no malicious link exists in the email. **[CONFIRMED]**

Pattern C -- Email bombing plus fake IT support (Black Basta/RaaS affiliate model): Step 1: scripts or rented tooling sign the target's email address up to thousands of newsletter and subscription forms simultaneously, flooding the inbox within minutes. Step 2: an actor calls the target posing as IT support offering to help with the "email problem." Step 3: the caller convinces the target to install a remote access tool (Teams, AnyDesk, TeamViewer). Step 4: the operator deploys a C2 framework (Cobalt Strike, Havoc) and begins hands-on intrusion. Step 5: data exfiltration or ransomware deployment. **[CONFIRMED]**

Pattern D -- AI vishing-as-a-service (PlugValley and similar): Vishing-as-a-Service (VaaS) platforms provide threat actors with AI-generated voice bots, spoofed caller IDs, customizable scripts, and real-time call management through a web dashboard. This eliminates the need for human callers and allows campaign scaling across languages and geographies. The model represents commoditization of vishing capability analogous to CaaS for malware evasion. **[CREDIBLE]**

Role in Ecosystem

Callers and spammers are a human-layer bypass for technical controls. They are most valuable where technical exploitation is constrained: when MFA is enabled, when credentials alone are insufficient, when targets have strong endpoint security, or when the attacker needs to escalate from basic access to administrative privileges without triggering EDR. The caller function fills the gap that technical initial access methods cannot always fill reliably. **[CONFIRMED]**

What it enables: Credential and MFA token harvest; helpdesk-authorized account changes (password resets, phone number changes, MFA bypass); remote access session establishment via legitimate remote-support tools; loader and malware delivery without malicious links in email (evades gateway scanning). **[CONFIRMED]**

What degrades without it: Ransomware and data-extortion operators dependent on this method must revert to purely technical initial access, which is more detectable, slower, and requires higher technical capability per victim. The email bomb plus fake IT support chain specifically requires both the social engineering component and the email delivery component to function -- removing either degrades the attack. **[CREDIBLE]**

EDP ecosystem position: Unlike stealers, loaders, and crypters (which occupy defined sequential stages in the kill chain), callers and spammers are a cross-cutting alternative initial access mechanism. They can substitute for loaders when technical delivery is blocked, augment stealer-derived access for privilege escalation, or directly feed IABs with high-value corporate credentials. No dedicated Dependency Map node exists; this module recommends one in Section 8. **[ANALYST INFERENCE]**

Business Model

Revenue Stream	Description	Pricing (Approximate)
In-house call-center operations (BazarCall, email-bomb teams)	RaaS affiliate or operator maintains its own call-center staff and campaign infrastructure. Callers are paid wages or a share of ransom proceeds. Campaigns are run against targeted victim sets from stealer logs or purchased data.	Operational cost model; wages paid to call-center staff; revenue from ransom or access sales
Vishing-as-a-Service (VaaS) subscriptions	Platforms like PlugValley sell subscription access to AI voice bots, number spoofing, and script management. Customers are threat actors who lack their own callers. Analogous to CaaS subscription model.	Subscription pricing; specific figures not available in open sources as of April 2026

Email bombing as a rented service	Email bombing campaigns can be rented from darknet service providers; scripts and tooling abuse legitimate newsletter signup forms. Low cost per campaign.	As low as $5 per campaign per academic analysis (ATHENE center); commodity pricing
Access brokering (LAPSUS$/Scattered Spider model)	Groups like LAPSUS$ and Scattered Spider use social engineering primarily for data extortion or corporate access. Access may be used directly or sold. Model is not strictly a paid service -- it is primary exploitation activity.	Revenue from ransom, data sale, or corporate extortion; not a service pricing model

Variants and Subtypes

Human-staffed call centers (BazarCall, subscription cancellation): Call centers with trained human operators. Operators follow scripts tailored to the pretext (subscription cancellation, bank fraud alert, IT support). Human operators can respond to off-script questions and adapt to resistant targets. Used by BazarCall-lineage campaigns documented by Microsoft and CyberScoop. **[CONFIRMED]**

Helpdesk impersonation by skilled individual operators (LAPSUS$, Scattered Spider): Small groups or individuals with high linguistic and social skills impersonate corporate IT/helpdesk. Requires OSINT on the target organization, knowledge of corporate identity verification processes, and the ability to convincingly role-play helpdesk personnel. Higher capability per actor; does not scale to mass campaigns but effective against high-value individual targets. **[CONFIRMED]**

AI vishing platforms (PlugValley and successors): Automated vishing using AI-generated voices, spoofed caller IDs, and pre-scripted call flows. Reduces dependency on human callers; enables multilingual and multinational scaling. Represents the industrialization endpoint for this category. **[CREDIBLE]**

Email bombing (standalone or as vishing amplifier): High-volume subscription email flood generated by scripts abusing legitimate website signup forms. Used as a standalone harassment tool or as a precondition for a fake IT support call. Documented cost as low as $5 for a bombing campaign on darknet markets. **[CONFIRMED]**

SIM swapping (supporting tactic): SIM swap attacks against mobile carriers, combined with social engineering of carrier staff, enable phone number hijacking -- used by LAPSUS$ and Scattered Spider to take over victim MFA-enrolled phone numbers. A high-impact variant that provides account takeover capability independent of credential knowledge. **[CONFIRMED]**

SECTION 2: KEY ACTORS AND EXAMPLES

Named Actors and Patterns

Actor / Pattern	Type	Tactics	Targets	Confidence
LAPSUS$ (DEV-0537)	Data-extortion group; phone-based social engineering specialist	Bribed or manipulated helpdesk and insider staff; phone-based social engineering; SIM swapping; impersonates employees with native-accent English; answers knowledge-based authentication (KBA) to trigger MFA resets.	Big tech (Microsoft, Samsung, Okta, Nvidia); telcos; IT outsourcers; 2021-22 peak; multiple major brand compromises	**CONFIRMED**
Scattered Spider (UNC3944 / Muddled Libra / Scatter Swine)	Financially motivated group; hybrid phishing and vishing; overlaps with RaaS affiliates	Impersonates IT/helpdesk via SMS, phone, and email; uses Evilginx/adversary-in-the-middle for	Tech, finance, retail, MSPs; US and Western focus; high-value admin and service accounts	**CONFIRMED**

		credential and MFA capture; targets service accounts and admin credentials; overlaps with ALPHV/BlackCat ransomware affiliate activity.		
BazarCall / call-center malware delivery (Conti/Ryuk heritage; Black Basta affiliates)	RaaS-linked call centers delivering loader payloads via subscription cancellation pretext	"Subscription cancellation" emails with no malicious link; call-center directs victim to download a cancellation tool (loader/stager); documented as BazarCall delivery for Conti and Ryuk heritage groups; associated with Black Basta affiliate activity.	SMBs and enterprises in US and EU; cross-sector	**CONFIRMED**
Email-bomb plus fake IT support (Black Basta affiliates; multiple RaaS crews)	TTP set used by RaaS affiliates; combines email-bombing with Teams/AnyDesk/TeamViewer remote access	Five-step chain: mass subscription signup flood; fake IT support call; remote access via Teams/AnyDesk; C2 deployment (Cobalt Strike, Havoc); exfiltration or ransomware. Huntress documented at least 5 organizations hit with this pattern as of early 2026.	SMBs and enterprises globally; sectors with high remote-support reliance	**CONFIRMED**
PlugValley (AI Vishing-as-a-Service)	Commoditized VaaS platform sold to threat actors; AI voice bots with spoofed numbers and scripted call flows	Provides AI voice bots, caller ID spoofing, customizable scripts, and real-time call management via web dashboard. Customers are downstream threat actors lacking their own call capacity. Fortra exposure documented the platform and its capabilities.	Any sector where phone numbers are available; credential harvesting and MFA bypass at scale	**CREDIBLE (Fortra reporting)**

Notable Examples and Case Studies

LAPSUS$ -- helpdesk-based MFA bypass at scale (2021-22): LAPSUS$ compromised Microsoft, Samsung, Okta, Nvidia, and other major brands using phone-based social engineering that bypassed MFA and privileged account controls. Key TTPs included calling carrier helpdesks to perform SIM swaps, calling corporate IT helpdesks to trigger password resets while impersonating employees, and bribing insiders at outsourced IT firms with access to target systems. The group demonstrated that MFA alone does not prevent access if the enrollment and reset process is vulnerable to social engineering. **[CONFIRMED]**

Scattered Spider -- Caesars and MGM Resorts (2023): Scattered Spider compromised Caesars Entertainment and MGM Resorts in September 2023 using helpdesk vishing. In the MGM case, the group called the IT helpdesk, impersonated an employee whose LinkedIn profile they had located, and obtained password reset and MFA modification assistance. MGM estimated $100 million in losses from the subsequent ransomware deployment by ALPHV/BlackCat. This is the highest-documented-impact single vishing-initiated incident. **[CONFIRMED]**

BazarCall campaign lineage (2020-present): The BazarCall model -- fake subscription billing email with a callback number leading to a call center that delivers malware -- originated in Conti/Ryuk affiliate operations circa 2020-21 and has persisted through multiple brand evolutions. Black Basta affiliates are documented as continuing this technique. The persistence of this model despite broad public reporting demonstrates structural resilience: there is no email link to block, and the social engineering layer is inherently difficult to automate detection of. **[CONFIRMED]**

Email bomb plus Teams-based remote access (Huntress 2025-26): Huntress documented a pattern affecting at least five organizations where mass subscription email bombing was followed by a fake IT support call directing the victim to accept a Teams meeting or install AnyDesk. The attackers then used the remote access session to deploy Cobalt Strike and Havoc C2 frameworks. The email bombing component caused the victim's inbox to be effectively non-functional, increasing their susceptibility to the support call that immediately followed. **[CONFIRMED]**

Actor Pool Distinction: Western/English-Language vs. RU-Language Ecosystem

This module spans two distinct actor pools that require separate analytical treatment: **[CONFIRMED]**

Western/English-language actors (LAPSUS$, Scattered Spider): Financially motivated groups primarily composed of English-speaking individuals, some in the UK, US, and South America. No confirmed Russian state link. Not subject to the Dark Covenant controlled-impunity framework. Motivation is financial and reputational. Subject to Western LE jurisdiction -- several LAPSUS$ and Scattered Spider members have been arrested. These actors use social engineering as their primary attack vector, not as a supplement to technical intrusion. **[CONFIRMED]**

RU-language ecosystem affiliates (BazarCall lineage, Black Basta, email-bomb teams): Call-center operations run by or associated with Conti/Ryuk heritage groups and their successors, including Black Basta. These actors use phone-based social engineering as one element of a broader RaaS kill chain that includes loaders, crypters, and ransomware deployment. They are part of the Russia/CIS-centric ecosystem this EDP project primarily addresses and are subject to controlled-impunity dynamics. The call-center function for these groups is an operational component, not their primary identity. **[CONFIRMED]**

EDP framework relevance is highest for the RU-language ecosystem affiliates. The Western actors (LAPSUS$, Scattered Spider) are documented here for completeness and because their TTPs are widely adopted but are not the primary focus of this module's EDP integration in Section 8. **[ANALYST INFERENCE]**

Scale and Volume

Metric	Estimate	Confidence
Social engineering as initial access vector (industry)	Multiple industry reports (Microsoft Digital Defense Report, others) list social engineering (email, phone, SMS) among the top initial access vectors for ransomware and data-extortion campaigns; no precise global percentage available	HIGH for direction; no global quantification available
Email bombing cost on darknet	As low as $5 per bombing campaign; scripts and rented tooling abuse legitimate subscription forms	CONFIRMED (ATHENE academic analysis)
MGM Resorts estimated losses from Scattered Spider vishing entry (2023)	~$100 million disclosed loss; ransomware deployed by ALPHV/BlackCat following vishing-initiated access	CONFIRMED (SEC disclosure)
LAPSUS$ incident count (2021-22)	Confirmed compromises at Microsoft, Samsung, Okta, Nvidia, T-Mobile, and others; multiple major brand names in approximately 12 months of activity	CONFIRMED (vendor disclosures, KrebsOnSecurity)

Huntress email-bomb plus fake IT support incidents (2025-26)	At least 5 documented organizations; pattern attributed to multiple RaaS affiliate crews using email-bomb plus Teams/AnyDesk remote access chain	CONFIRMED (Huntress)
Scattered Spider sector concentration	~70% of observed Scattered Spider targets are in tech, finance, and retail; helpdesks and MSPs are key entry points	CREDIBLE (Rapid7/ReliaQuest)
Global vishing/fake-IT incident volume	No reliable global count; incident data is case-study based and relies on voluntary reporting; significant underreporting expected	NOT AVAILABLE in OSINT

SECTION 3: INFRASTRUCTURE DEPENDENCIES

Telephony and VoIP Infrastructure

VoIP providers and caller-ID spoofing: High-volume vishing campaigns depend on VoIP infrastructure that allows programmatic call placement and caller-ID manipulation. Actors use VoIP providers with weak or absent KYC, SIM-box equipment for mobile-number generation, or residential number leasing to make calls appear to originate domestically. **[CONFIRMED]**

AI vishing platform infrastructure (PlugValley model): VaaS platforms integrate AI voice synthesis, VoIP APIs, and web-based script management into a turnkey dashboard. Platform operators maintain VoIP provider accounts, voice synthesis compute, and customer-facing infrastructure. The platform model separates infrastructure operation from campaign execution. **[CREDIBLE]**

SIM-swapping enablement: LAPSUS$ and Scattered Spider use insider access at mobile carriers or social engineering of carrier helpdesks to port victim phone numbers to attacker-controlled SIMs. This requires either insider contacts within carrier organizations or documented social engineering scripts for carrier identity verification. **[CONFIRMED]**

Contact Data and Target Intelligence

Stealer logs and credential databases: Call-center operations and vishing groups use stealer-log data to identify target phone numbers, email addresses, job titles, and organizational context. Stealer-derived data provides the OSINT foundation for convincing pretexts -- knowing a victim's name, employer, and role makes a fake IT support call significantly more credible. **[CREDIBLE]**

EDP cross-reference: Contact data dependency maps directly to Module 01 (Stealers) and Dependency Map Node 10 (Credential/Stealer-Log Markets, MEDIUM tier). This is a confirmed upstream dependency for RU-language ecosystem call-center operations. **[ANALYST INFERENCE]**

OSINT collection (helpdesk-focused groups): LAPSUS$ and Scattered Spider rely heavily on LinkedIn, corporate org charts, and public HR data to identify helpdesk staff, IT administrators, and employees with elevated privileges. This OSINT layer provides the specific targeting data needed for high-success social engineering. **[CONFIRMED]**

Purchased data broker lists: Bulk email and phone list acquisition from data brokers, credential dumps, or underground market purchases provides targeting data for mass-scale campaigns. Quality of targeting data directly affects vishing success rates. **[CREDIBLE]**

Email Infrastructure for Bombing and Pretexting

Newsletter and subscription form abuse: Email bombing attacks do not require controlled email infrastructure. Scripts automatically submit target email addresses to legitimate newsletter signup and account registration forms across thousands of websites. The resulting flood is composed of legitimate emails from real senders, which bypass spam filters. **[CONFIRMED]**

Rented email bombing tooling: Email bombing campaigns can be rented as a service on darknet markets for as little as $5. The commodity pricing reflects the low technical barrier and the reuse of legitimate website infrastructure as an amplifier. No criminal email sending infrastructure is required. **[CONFIRMED]**

Pretexting email for callback delivery (BazarCall): The subscription cancellation email is the delivery mechanism for BazarCall-style campaigns. These emails are designed to appear as legitimate billing notices.

They do not contain malicious links or attachments -- only a phone number. This design is deliberate: it defeats email security gateway scanning. **[CONFIRMED]**

Remote Access and Collaboration Tool Abuse

Legitimate remote-support tools as C2 entry points: Fake IT support campaigns specifically request that victims install or allow access via Teams, AnyDesk, TeamViewer, or similar tools. These are legitimate, widely deployed enterprise applications. Their legitimate status makes them difficult to block without operational disruption, and their use generates minimal security alerts compared to custom C2 implants. **[CONFIRMED]**

C2 framework deployment post-access: Once remote access is established via legitimate tools, actors deploy Cobalt Strike or Havoc C2 frameworks for persistent, flexible access that is independent of the remote-support session. This transitions the access from social-engineering-established to technically maintained. **[CONFIRMED]**

EDP cross-reference: C2 deployment dependency maps to Module 02 (Loaders) and Module 07 (Ransomware Groups/RaaS) for the payload delivery phase following remote access establishment. **[ANALYST INFERENCE]**

Cross-Module Linkages

Module	Linkage	Coupling	Confidence
Module 01 -- Stealers	Stealer logs provide phone numbers, email addresses, job titles, and organizational data used for targeting. Caller operations are partially dependent on stealer-derived targeting data for credible pretexts.	MEDIUM (upstream data)	**CREDIBLE**
Module 02 -- Loaders	BazarCall-style call centers deliver loader payloads directly. Call-center operations are an alternative initial delivery mechanism to spam-based loader distribution, used when technical delivery is blocked.	HIGH (parallel delivery)	**CONFIRMED**
Module 05 -- Initial Access Brokers (IABs)	Access generated through vishing and fake IT support is monetized through IAB channels -- helpdesk-established remote access sessions and MFA-bypassed accounts are sold as corporate footholds.	HIGH (downstream access)	**CREDIBLE**
Module 07 -- Ransomware Groups / RaaS	Scattered Spider-established access was directly used for ALPHV/BlackCat ransomware deployment (MGM 2023). BazarCall delivery chains are documented Conti/Black Basta ransomware precursors. Direct downstream pathway.	CRITICAL (downstream)	**CONFIRMED**
Module 10 -- Underground Forums	Forums provide the procurement channel for email bombing services, VaaS subscriptions, and call-center tooling. Contact data is purchased through forum markets.	MEDIUM (market procurement)	**CREDIBLE**

SECTION 4: DISRUPTION LEVERAGE POINTS

Primary Leverage Points

Hardening helpdesk and identity verification workflows (highest-ROI lever): The structural vulnerability exploited by LAPSUS$, Scattered Spider, and BazarCall is not a software flaw -- it is a procedural gap in helpdesk identity verification. Requiring out-of-band, cryptographic, or multi-party verification for any IT action taken over the phone (especially MFA resets, phone number changes, and remote access grants) eliminates the

primary attack surface. This is the highest-ROI lever because it affects all phone-based social engineering simultaneously, requires no LE access, and has no backfire risk. **[CONFIRMED]**

Email provider cooperation for bombing detection: Email providers can detect sudden spikes in subscription confirmation emails from many diverse domains to a single mailbox and temporarily quarantine excess messages. This disrupts the email bombing precondition for the fake IT support pattern. Implemented correctly, the bombing attack loses its effectiveness without affecting normal email delivery. **[CONFIRMED]**

VoIP KYC and number-spoofing controls: Requiring real KYC from VoIP customers and implementing anti-spoofing protections (STIR/SHAKEN framework for US carriers) raises the friction for bulk vishing campaign infrastructure provisioning. VoIP providers with weak KYC are exploitable; those with strong KYC force actors to use more expensive or detectable alternatives. **[CREDIBLE]**

Infiltration and takedown of AI vishing platforms: VaaS platforms like PlugValley represent a concentrated target for LE. Unlike distributed call centers that can be relocated, VaaS platform infrastructure is centralized and has identifiable hosting, payment rails, and customer lists. Building an attribution package on VaaS operators -- via infiltration and payment trail analysis -- creates a takedown target that, if removed, degrades capability for all downstream customers simultaneously. **[CREDIBLE]**

Arrest and prosecution of call-center operators: Unlike Russian-infrastructure-dependent actors, many call-center operators are accessible to Western LE jurisdiction (several LAPSUS$ and Scattered Spider members are US/UK nationals who have been arrested). BazarCall-lineage operators are harder to reach but their call-center staff (often in non-Russian jurisdictions) may be accessible. Each arrest removes trained operators who carry institutional knowledge of successful scripts and pretexts. **[CREDIBLE]**

Who Owns Disruption

Actor	Role and Authority	Method
Target organizations (primary defensive lever)	Hardening helpdesk workflows, implementing MFA reset verification procedures, and training staff to recognize email bomb plus fake IT patterns is the highest-impact lever and is entirely within organizational control.	Policy: out-of-band verification, multi-party approval for MFA/access changes, remote-support tool controls
Email/collaboration platform providers (Microsoft 365, Google Workspace)	Email bombing detection and quarantine; Teams misuse detection (external account initiating IT support sessions); abuse enforcement on BazarCall-style pretexting emails.	Rate limiting, subscription flood detection, external-meeting trust controls
Mobile carriers and VoIP providers	STIR/SHAKEN implementation, stricter KYC for VoIP number provisioning, SIM swap fraud controls, and call pattern analytics for vishing campaign detection.	Anti-spoofing, KYC enforcement, carrier-level campaign detection
FBI / DOJ (Western actor arrests)	Primary LE authority for LAPSUS$ and Scattered Spider prosecutions (US/UK nationals). Extradition and prosecution feasibility is higher for this actor pool than for Russia-based operators.	Arrest, indictment, asset seizure, extradition
Europol EC3 / NCA (cross-border coordination)	Coordination for arrests and infrastructure seizures where call-center operations span jurisdictions. UK NCA active in LAPSUS$ prosecutions.	Coordination, warrants, infrastructure seizure
OFAC / Treasury (underutilized)	Designation authority not applied to call-center operations associated with designated ransomware groups, despite documented linkage between BazarCall/Black Basta and ransomware proceeds. Nexus exists for designation extension.	Designation of call-center operators/services serving designated RaaS groups

Best Disruption Method

Defensive hardening is the primary lever -- not LE action: Unlike loaders, stealers, or BPH, caller/spammer operations cannot be meaningfully disrupted through infrastructure seizure alone. The attack surface is

procedural and human. The most effective disruption method is universal implementation of identity verification standards for all helpdesk actions -- particularly MFA resets, account recovery, and remote access authorization. This is independent of any LE operation, applies globally, and does not trigger any backfire dynamics. The CISA-aligned guidance is clear: no MFA reset or privileged action over the phone without cryptographic or multi-party verification. **[CONFIRMED]**

Email bombing countermeasures as the secondary lever: Subscription flooding detection by email providers disrupts the precondition for the email-bomb plus fake IT support attack chain. This is a platform-level control that requires coordination with major email providers and subscription form operators. Website-level CAPTCHA and rate limiting on subscription forms reduces the availability of bombing amplifiers. **[CONFIRMED]**

VaaS platform takedowns as the highest-impact LE target in this category: Traditional call centers can be relocated quickly. AI VaaS platforms are more concentrated and more disruptable. An infiltration and takedown operation against a major VaaS platform removes capability for all downstream customers simultaneously and sets a precedent that deters future platform development. This is the LE investment that produces the broadest per-action impact in this module. **[CREDIBLE]**

Backfire Risk

Shift to more targeted, insider-enriched pretexts: As generic vishing faces more skepticism, higher-capability groups will invest in inside information (HR data, partner access, stealer-log details) to craft highly specific pretexts. LAPSUS$-style insider bribery is evidence that this escalation is already underway. **[CREDIBLE]**

AI vishing acceleration: Enforcement against low-end human call centers may accelerate adoption of AI vishing platforms that scale more cheaply and are harder to attribute. PlugValley and successors represent this trajectory. LE actions that disrupt human operators without also targeting the VaaS platform layer may produce net negative outcomes by accelerating the shift to AI. **[CREDIBLE]**

Helpdesk friction on legitimate operations: Stricter KBA and MFA reset verification procedures will create operational friction for legitimate helpdesk support. If poorly implemented, this may generate internal pressure to relax the controls -- the exact dynamic that LAPSUS$ and Scattered Spider exploited. Security improvements must be accompanied by process design that keeps legitimate support workable. **[CONFIRMED]**

False positives from email bombing detection: Aggressive subscription flood detection could quarantine legitimate transactional email. Threshold calibration is required to avoid disrupting normal mail delivery. **[CREDIBLE]**

Compounding Actions

- **Stealer log market disruption (Module 01, Node 10):** Degrading stealer log markets reduces the targeting data available for vishing pretexts. Caller operations that rely on stealer-derived contact and organizational data become less specific and therefore less convincing. Amplification: MEDIUM.
- **IAB market pressure (Module 05, Node 04):** Reducing the market for caller-generated access (helpdesk-granted footholds, MFA-bypassed accounts) reduces the monetization incentive for phone-based access generation. Amplification: MEDIUM.
- **Underground forum disruption (Module 10, Node 07):** Email bombing services and VaaS subscriptions are procured through underground forum markets. Forum disruption raises procurement friction. Amplification: LOW-MEDIUM.
- **Ransomware group disruption (Module 07, Node indirect):** Disrupting the RaaS affiliates that commission call-center operations removes the primary financial sponsor for BazarCall-lineage campaigns. Without RaaS revenue flow, maintaining call-center staff becomes economically unviable. Amplification: HIGH (for RU-language ecosystem call centers).

SECTION 5: RESILIENCE AND REPLACE DIFFICULTY

Replace Difficulty

Infrastructure level: LOW. VoIP numbers, email accounts, and call-center locations can be replaced quickly. Email bombing scripts are available cheaply on darknet markets. No specialized or scarce technical infrastructure is required. Infrastructure replace difficulty is lower than any other module in the EDP framework. **[CONFIRMED]**

Human skill level: MODERATE. Effective vishing (LAPSUS$, Scattered Spider quality) requires language skills, accent authenticity, deep knowledge of corporate processes, and improvisational ability for off-script conversations. These skills are not universally available but are widely distributed in global call-center labor

markets. Call-center campaigns at the lower end (BazarCall scripts) require less skill but are still human-dependent. **[CREDIBLE]**

Playbook and pretext level: LOW. Once effective pretexts are documented and publicized (fake subscription cancellation, email bomb plus IT support), they can be replicated by new actors with minimal adaptation. Published reporting on LAPSUS$ and BazarCall TTPs has functioned as effective documentation for adoption by successor groups. **[CONFIRMED]**

AI vishing capability level: LOW (decreasing barrier). AI vishing platforms reduce the human skill requirement to near zero for scripted call scenarios. As these platforms mature, the replace difficulty for this module approaches zero at the commodity level. **[CREDIBLE]**

Redundancy

Call method redundancy: HIGH. Multiple calling approaches are available: human operators, AI platforms, SIM boxes, VoIP providers. If one provider is disrupted, alternatives are immediately available. No single infrastructure dependency creates a bottleneck. **[CONFIRMED]**

Pretext redundancy: HIGH. Multiple documented pretexts exist (subscription cancellation, IT support, bank fraud alert, email bomb + IT support). If one is widely recognized, actors shift to another. **[CONFIRMED]**

Actor redundancy: MEDIUM. High-capability groups (LAPSUS$, Scattered Spider) are harder to replace because their effectiveness depends on specific skills and OSINT capabilities. Lower-capability BazarCall-style campaigns are easily replaced. The overall function is redundant; specific high-capability actors are somewhat more difficult to replace. **[CREDIBLE]**

Historical Reconstitution

Case	Reconstitution Pattern	Rebuild Time
LAPSUS$ arrests (2022-23)	Multiple arrests of LAPSUS$ members in UK, Brazil, and US. Group activity declined significantly. However, the TTPs were adopted by other groups (Scattered Spider, others). The technique survived even as the specific group was disrupted.	Weeks for TTP adoption by successor groups; individual group disruption achieved but function persisted
BazarCall / call-center malware delivery (2020-present)	Despite broad public documentation starting in 2021, BazarCall-style campaigns continued through 2022, 2023, 2024, and 2025 under Black Basta and other affiliates. No LE action specifically targeting the call-center infrastructure has been publicly disclosed. The model has proven highly durable.	No sustained disruption achieved; model persists 5+ years after initial documentation
Scattered Spider (ongoing as of April 2026)	Multiple Scattered Spider members arrested (2023-24) after the MGM and Caesars incidents. Activity has continued under overlapping actors and affiliated groups. FBI and DOJ have charged multiple individuals. The group demonstrates that arrests do not eliminate the capability when it is distributed across multiple individuals.	Partial disruption; activity continues under successor/affiliated actors

The caller/spammer function is among the most resilient in the EDP framework because it depends primarily on human skills and publicly documented techniques rather than specialized technical infrastructure. Disrupting the function requires either sustained universal defensive hardening (victim-side) or elimination of the financial incentive structure (removing the RaaS affiliate commissions that fund call-center operations). **[CONFIRMED]**

Durability Assessment

Level	Assessment	Rating
Function level (phone-based social engineering)	Disruption durability is LOW. The function is technique-based and human-dependent; no infrastructure seizure can eliminate it. Success is measured in reduced success rate per attempt, not function elimination.	**LOW**

Specific actor/group level	Arrests (LAPSUS$, Scattered Spider) produce MEDIUM disruption. The group is degraded; the technique is adopted by others. Individual group elimination is feasible; function elimination is not.	**MEDIUM (specific actors)**
Defensive hardening effectiveness (victim-side)	MEDIUM-HIGH for organizations that implement strict out-of-band verification for helpdesk actions. This is the most durable mitigation available and is independent of LE action. Universal adoption would effectively eliminate the primary attack surface for this module.	**MEDIUM-HIGH (defensive)**

SECTION 6: INDICATORS AND KPIs

Health Indicators

Indicator	Normal (Operating)	Under Pressure
Volume of reported vishing/fake-IT attempts	Consistent level of vishing incident reports; helpdesk staff encountering suspicious calls regularly; new pretext variants appearing in threat intel feeds	Significant decline in reported attempts across monitored organizations; or shift to entirely new pretexts/scripts not matching known patterns
Email bombing events detected	Periodic email bombing events detectable in email security logs as subscription flood spikes; new campaigns documented in threat intel	Reduction in email bombing events; or migration to bombing methods that evade current detection (e.g., more distributed flood sources)
BazarCall / subscription-pretext email volume	Steady volume of fake billing/subscription emails in commercial email security telemetry; recurring callback-number campaigns	Significant drop in callback-based pretext emails; or shift to new pretext types not covered by current detection rules
AI vishing platform activity	VaaS platforms active and advertising on forums/Telegram; AI-generated call indicators appearing in threat intel	Platform takedowns confirmed; activity migrates to new, less-mature platforms; reduced AI-call indicator frequency
Helpdesk-authorized changes linked to subsequent incidents	Periodic incident timelines confirm phone-based access changes as precursors; pattern visible in DFIR casework	Reduction in incident timelines showing phone-initiated helpdesk changes as the initial access event; shift to other initial access vectors in DFIR casework

Disruption KPIs

KPI	Baseline (2024-25)	Post-Disruption Target
Helpdesk-verified identity procedure adoption rate	No standardized global baseline; adoption is organization-by-organization; major enterprises post-LAPSUS$/Scattered Spider have improved; SMBs largely unimproved	Primary metric for this module: % of organizations requiring out-of-band cryptographic or multi-party verification for all helpdesk-mediated MFA and account changes
Email bombing event volume and containment time	No formal global baseline; Huntress 2025-26 documents active campaigns; email security vendors report periodic bombing events in telemetry	After email provider cooperation program: measurable reduction in email bombing events that bypass

		spam filters; median containment time < 15 minutes from flood onset
Vishing/social-engineering attributed initial access (% of ransomware cases)	Multiple sources indicate social engineering is top-tier initial access vector; exact ransomware % not formally established in open sources	After sustained helpdesk hardening campaign: measurable reduction in DFIR incident timelines attributing initial access to phone-based social engineering across monitored sector populations
VaaS platform enforcement outputs	No major VaaS platform LE action publicly documented as of April 2026; PlugValley and similar platforms active	Track: platforms identified, investigated, taken down; customers disrupted; follow-on platform emergence time
Call-center arrests and prosecutions	LAPSUS$ and Scattered Spider arrests documented (2022-24); BazarCall-lineage call-center staff no confirmed arrests to date	Track arrests per year; include call-center staff in Russia/Eastern Europe who may be reachable through partner jurisdiction coordination

Collection Methods

DFIR casework root-cause tagging: Incident response investigations that log initial access vector provide the most accurate measurement of phone-based social engineering prevalence in ransomware timelines. Systematic tagging across IR firms and CERTs for "vishing," "helpdesk impersonation," and "call-center malware delivery" as initial access vectors would enable statistical tracking. **[CREDIBLE]**

Email security telemetry: Email security platforms (Microsoft Defender, Proofpoint, Mimecast) detect subscription flood patterns, callback-number pretext emails, and fake billing notices. Aggregate telemetry provides trend data on BazarCall-style campaign volume. **[CONFIRMED]**

Forum and dark web monitoring: Monitoring of underground forum listings for email bombing services, VaaS subscriptions, and call-center tooling provides market health data. Actor discussions following LE actions provide reconnaissance intelligence on disruption impact. **[CREDIBLE]**

Threat intelligence from victim organizations: Vishing attempts are frequently reported to security teams and IR firms but rarely enter public databases. Coordinated private sector sharing (ISACs, FS-ISAC, H-ISAC) provides the best available quantitative data on attempt volume and success rates. **[CONFIRMED]**

Baseline Data

Metric	Value	Source/Confidence
MGM Resorts incident losses (Scattered Spider, 2023)	~$100 million disclosed losses; access established via single vishing call to IT helpdesk	CONFIRMED (SEC disclosure)
Email bombing darknet pricing	As low as $5 per campaign; scripts abuse legitimate newsletter signup forms across thousands of websites	CONFIRMED (ATHENE academic analysis)
LAPSUS$ confirmed victim organizations	Microsoft, Samsung, Okta, Nvidia, T-Mobile, and others; multiple major brands in approximately 12-month active period 2021-22	CONFIRMED (vendor disclosures)
Scattered Spider sector targeting	~70% of observed targets in tech, finance, and retail; helpdesks and MSPs documented as primary entry points	CREDIBLE (Rapid7/ReliaQuest)
Huntress email-bomb plus fake IT incidents (2025-26)	At least 5 documented organizations; Black Basta and RaaS affiliate attribution	CONFIRMED (Huntress)

Global vishing incident count	No reliable global database; significant underreporting; no census estimate available	NOT AVAILABLE in OSINT
BazarCall campaign longevity	Active model from ~2020 through at least 2025-26; documented across Conti, Ryuk, Black Basta, and affiliated operations; 5+ years without effective disruption	CONFIRMED (Microsoft, CyberScoop, Huntress)

SECTION 7: SOURCES AND CONFIDENCE

Primary Sources

Group-specific threat intelligence:

- KrebsOnSecurity -- LAPSUS$ reporting (2021-22): helpdesk bribery, SIM swap techniques, MFA bypass via social engineering; primary source for LAPSUS$ TTPs and victim list.
- Microsoft Security Blog -- LAPSUS$ and DEV-0537 analysis; BazarCall call-center malware delivery documentation.
- Rapid7 and ReliaQuest -- Scattered Spider (UNC3944 / Muddled Libra) analysis; vishing plus phishing hybrid model; sector targeting data.
- CyberScoop -- BazarCall call-center delivery model coverage; subscription cancellation pretext documentation.

Email bombing and campaign documentation:

- ATHENE Center -- "Diving into Email Bomb Attacks" academic analysis; $5 darknet pricing; subscription-form abuse mechanics; primary quantitative source for email bombing cost and delivery.
- Darktrace -- 2025 incident analysis: email bomb combined with vishing and remote access deployment; real-world operational chain documentation.
- Huntress -- 2025-26 email-bomb plus Teams/AnyDesk remote access pattern; 5+ confirmed victim organizations; attribution to RaaS affiliate crews.

AI vishing and commoditization:

- Fortra -- PlugValley AI Vishing-as-a-Service exposure documentation; platform capabilities, API-integrated VoIP, script management.

Incident case studies:

- SEC filing / news reporting -- MGM Resorts $100M loss from Scattered Spider vishing-initiated ALPHV/BlackCat ransomware deployment (2023); highest-documented single vishing incident.
- Rubrik -- fake IT support pattern documentation; remote-support tool abuse in social engineering chains.

Ecosystem context:

- Recorded Future -- Dark Covenant 3.0 (2025) -- controlled impunity framework; applicable to RU-language call-center operators affiliated with Black Basta and RaaS crews.
- GlobalSign and Microsoft Digital Defense Report -- social engineering as top-tier initial access vector for modern ransomware and data-extortion campaigns.

Secondary Sources

- Grandlinux / Saeree ERP analysis -- email bomb plus fake IT support 5-step attack chain documentation
- ReliaQuest -- Muddled Libra/Scattered Spider behavioral analysis and sector targeting
- Rubrik -- vishing and remote-support tool abuse in enterprise environments

Gaps and Uncertainties

No global vishing incident database: Unlike malware detections (sandbox telemetry) or loader operations (Endgame LE outputs), there is no systematic global database of vishing or social engineering incidents. Available data is case-study based and relies on voluntary organizational reporting. Significant underreporting is expected. All prevalence estimates should be treated as lower bounds. **[CONFIRMED]**

RaaS ecosystem call-center linkage quantification: Multiple reports suggest and several confirm that vishing and call-center operations are now standard tools in RaaS affiliate playbooks. However, no study has quantified

what proportion of ransomware incidents include a phone-based social engineering component in the pre-intrusion timeline. Establishing this ratio is a key research gap. **[CONFIRMED]**

AI vishing platform scale: PlugValley is the most publicly documented VaaS platform. Whether there are comparable platforms not yet publicly documented is unknown. The scale of AI vishing adoption by criminal operators is not quantified in open sources as of April 2026. **[CONFIRMED]**

BazarCall call-center geography and staffing: While the BazarCall model and its connection to Conti/Black Basta lineage are confirmed, the geographic location of call-center staff, their recruitment and compensation model, and the specific individuals running current campaigns are not publicly documented. This limits the precision of LE targeting for this actor set. **[CONFIRMED]**

Attribution for RU-language call-center operators: Unlike LAPSUS$ and Scattered Spider (where individual arrests have confirmed identities), the operators of BazarCall-style call centers linked to Russian RaaS groups have not been publicly attributed. State adjacency for this population is inferred from group affiliation, not direct evidence. **[CONFIRMED]**

Confidence Notes

Finding Area	Assessment	Confidence
Social engineering as top-tier initial access vector	Multiple independent industry and academic sources confirm. Direction is unambiguous; global quantification is not available.	**HIGH**
LAPSUS$ TTPs and victims	Confirmed through vendor disclosures, LE prosecution documents, and contemporaneous reporting. High-quality corroboration.	**CONFIRMED**
Scattered Spider TTPs and MGM/Caesars incidents	Confirmed from SEC disclosures, vendor analysis, and DOJ charges. MGM $100M loss figure is SEC-disclosed.	**CONFIRMED**
BazarCall / subscription cancellation model (operational)	Confirmed from multiple vendor analyses since 2020. Continued operation under Black Basta and affiliates is confirmed.	**CONFIRMED**
Email bombing cost and mechanism	ATHENE academic analysis provides confirmed pricing ($5) and mechanism (subscription form abuse). Strong primary source.	**CONFIRMED**
AI vishing platform (PlugValley)	Single primary source (Fortra). Capabilities and existence confirmed; scale of adoption and customer base not independently corroborated.	**CREDIBLE**
Global vishing incident volume and RaaS linkage rate	No global database; case-study based only; significant underreporting. Rate of RaaS incidents with phone-based component is unquantified.	**LOW-MODERATE**
RU-language call-center geography and operator identities	Group-level affiliation inferred; individual operators not publicly attributed; geographic location of call-center staff not confirmed.	**LOW-MODERATE**

SECTION 8: ANALYST ASSESSMENT

This section was generated by Claude based on synthesis of Perplexity research (Sections 1-7) and integration with EDP framework documents: Ransomware Ecosystem Dependency Map Refined v01, Ransomware Ecosystem Disruption Playbook v03, and Russian Government Protection Framework v03.

Key Takeaway

The EDP Dependency Map has no dedicated node for caller/spammer infrastructure. This is an analytical gap that Module 04 is designed to surface. Callers and spammers occupy a structurally distinct position in the ransomware supply chain: they are a human-layer bypass mechanism that substitutes for or augments technical initial access when technical methods are blocked. They are cross-cutting across multiple nodes (feeding Node 04 IAB Markets with access, serving as an alternative to Node 05 Botnet/Loader Ecosystems for delivery, directly enabling ransomware deployment). The absence from the Dependency Map understates the function's operational relevance. **[CONFIRMED]**

The analytically most significant characteristic of this module is that the primary disruption lever is defensive hardening -- not LE action against infrastructure. Unlike every other module in this series, where the principal disruption method involves seizure of servers, designation of operators, or takedown of market infrastructure, caller/spammer disruption is achieved primarily by making the attack surface inaccessible through victim-side procedural controls. This is a fundamentally different disruption logic and requires a different investment model. **[CONFIRMED]**

A critical analytical distinction must be maintained: this module covers two actor pools with different LE accessibility. LAPSUS$ and Scattered Spider are Western/English-language actors partially within Western LE jurisdiction -- arrests have occurred and should continue. BazarCall-lineage call centers affiliated with RU-language RaaS groups operate under the controlled-impunity framework and are substantially harder to reach directly. Conflating these pools produces incorrect disruption prioritization. **[CONFIRMED]**

Priority Recommendation

Two parallel actions, sequenced differently:

Action 1 -- Universal helpdesk hardening (immediate, no dependency on LE): Issue sector-specific guidance requiring cryptographic or multi-party verification for all helpdesk-mediated MFA resets, phone number changes, and remote access grants. Frame this as mandatory post-LAPSUS$/Scattered Spider remediation for financial, technology, healthcare, and retail sectors. This single control eliminates the attack surface for the highest-impact social engineering pattern documented in this module. It is the MGM lesson applied at scale: if Caesars implemented strict callback-number verification, LAPSUS$-style social engineering would not have succeeded. No LE action needed; no Russian infrastructure access needed; zero backfire risk.

Action 2 -- VaaS platform targeting (intelligence build-out for LE): AI Vishing-as-a-Service platforms are the highest-concentration and most scalable LE target in this category. PlugValley and emerging successors are centralized infrastructure with identifiable hosting, payment rails, and customer lists -- unlike distributed human call centers. An infiltration program targeting VaaS operators using the same model applied to CaaS in Module 03 (honeypot subscriber accounts, payment trail analysis, customer list acquisition) provides an actionable disruption target. Removing a VaaS platform degrades capability for all downstream customers simultaneously, which is the highest per-action impact available in this module from the LE side.

Connection to EDP Playbook

Module 04 does not map to a current Playbook phase because there is no Dependency Map node for it. The Section 8 recommendation is to add one. Proposed framing:

Proposed Node 04-A (Caller/Spammer Infrastructure) -- MEDIUM tier, LOW replace difficulty, LOW-MEDIUM backfire risk: The tier should be MEDIUM because replace difficulty is LOW and the function can be disrupted but not eliminated. Replace difficulty is LOW because infrastructure and pretexts are easily replaced; the constraint is human skill, which is widely available. Backfire risk is LOW-MEDIUM: hardening actions have no backfire; VaaS takedowns carry the standard risk of pushing actors to more closed, harder-to-monitor alternatives. Primary owner would be split: victim organizations (defensive hardening, no LE needed) and FBI/DOJ + Europol (for VaaS operator and Western-actor prosecution).

Playbook integration: Caller/spammer hardening actions are best timed to coincide with Phase B (Node 04 IAB Markets) pressure. The logic: IAB market disruption reduces the monetization value of caller-generated access. If helpdesk-established footholds cannot be sold because the IAB market is under simultaneous pressure, the economic incentive for maintaining call-center operations declines. Synchronizing defensive hardening campaigns (reducing successful call-center intrusions) with IAB market pressure (reducing monetization of successful ones) produces a two-sided demand-and-supply squeeze on this function.

Dark Covenant calibration: For RU-language call-center operators affiliated with Black Basta and similar groups, the Dark Covenant controlled-impunity framework applies indirectly -- they operate within the tolerant environment but are lower-profile than ransomware operators or major loader developers. BazarCall staff in Russia are unlikely to attract direct FSB protection unless their scale reaches a level that warrants state interest.

Western call-center operators (LAPSUS$, Scattered Spider) are outside the Dark Covenant framework entirely and should be treated as conventional criminal LE targets without state-protection screening requirements.

Dependency Map Update Recommendations

Node	Field	Current Entry	Recommended Update
New node recommendation: Caller/Spammer Infrastructure	Tier	Not present	Add Node 04-A (or equivalent): MEDIUM tier. Rationale: cross-cutting human-layer access generation; cannot be eliminated but can be made significantly more expensive and less successful through defensive hardening. Distinct from technical initial access nodes because primary leverage is victim-side, not infrastructure seizure.
New node recommendation: Caller/Spammer Infrastructure	Replace Difficulty	Not present	LOW for infrastructure and pretexts; MODERATE for high-capability individual operators (LAPSUS$/Scattered Spider quality). Distinguish in annotation: commodity replace difficulty is LOW; high-capability operator replace difficulty is MODERATE.
New node recommendation: Caller/Spammer Infrastructure	Primary Owner	Not present	Dual-track ownership: (1) Target organizations via CISA/sector guidance for defensive hardening -- no LE dependency; (2) FBI/DOJ + Europol for Western-actor prosecution; IC for VaaS platform targeting. Split ownership reflects the defensive-primary, LE-secondary disruption logic unique to this module.
New node recommendation: Caller/Spammer Infrastructure	Backfire Risk	Not present	LOW for defensive hardening actions. LOW-MEDIUM for VaaS takedowns (migration to more closed AI platforms). MEDIUM for public attribution of RU-language call-center operators (Dark Covenant screening recommended for any Black Basta-affiliated operators).

Follow-On Research

The highest-priority research gap is quantifying the proportion of ransomware incidents with phone-based social engineering in the pre-intrusion timeline. If a systematic DFIR casework tagging program across major IR firms (Mandiant, CrowdStrike, Secureworks, Palo Alto Unit 42) produced this ratio, it would allow precise measurement

of the ecosystem impact of caller/spammer disruption -- the data that currently does not exist and that this module cannot provide from open sources.

Secondary priorities: (1) Map BazarCall-lineage call-center infrastructure to specific RaaS affiliate operations. Connecting specific call-center IP ranges, VoIP accounts, and pretext emails to confirmed Black Basta or successor group attribution would enable LE action against an actor set that is currently described at the group level but not at the infrastructure level. (2) Assess AI vishing platform adoption rate: is PlugValley an isolated example or one of multiple active platforms? Forum and Telegram monitoring should focus specifically on VaaS advertising to characterize the current platform landscape before the next enforcement cycle.