etugen.io

June 28, 2026

THREAT HUNTING REPORT

HUNT MALICIOUS INFRASTRUCTURE
BEFORE IT HUNTS YOU.

Table of Contents

INTRODUCTION 3

Naming Mappings 5

AT A GLANCE 7

EXECUTIVE SUMMARY 10

SECTION 1: THREAT ACTOR PROFILE 11

AI Agent Architecture 12

Timeline 13

SECTION 2: CAMPAIGN ANALYSIS 14

TECHNICAL INFRASTRUCTURE - C2 17

TECHNICAL INFRASTRUCTURE - TOOLS 18

VICTIM ANALYSIS 19

MITRE ATT&CK MAPPING 20

INDICATORS (IOC) 21

DEFENSIVE RECOMMENDATIONS 22

ETG-2026-001 · CONCLUSION 23

Introduction

The cyber threat landscape is undergoing the fastest transformation in its history. The traditional attack lifecycle is now being replaced by a scalable, AI-powered model focused on operational efficiency. This next-generation threat actor systematically automates target selection, content generation, infrastructure management, and victim tracking, reaching a velocity and scale that far exceeds individual technical capabilities. The cases analyzed in this report are a tangible reflection of this transformation.

The core challenge in threat intelligence remains unchanged: staying one step ahead of the adversary. However, as their tools and methodologies rapidly evolve, it is becoming increasingly difficult for defense teams to match this pace using only reactive measures. etugen.io bridges this gap by combining proactive threat hunting, first-hand technical analysis, and field intelligence. This report is based on the full mirror analysis of an active C2 server and relies entirely on evidence observed in the field-not simulations or theoretical assessments.

Today's adversaries are intimately familiar with the boundaries of enterprise security platforms; they repeatedly test and bypass the behavioral detection mechanisms of endpoint security software and utilize human psychology as a primary attack vector, now predominantly amplified by AI-driven social engineering techniques.

The etugen.io Threat Intelligence Center monitors threat actors in real-time during their operations by integrating its first-hand technical analysis capabilities with field threat hunting. The analysis team employs a multi-layered research methodology, including the mirror analysis of active C2 infrastructure, source-code-level inspection of phishing campaigns, and telemetry evaluation of victim systems. The case upon which this report is built is a direct output of this methodology.

The focal actor of this report, **FISCAL PHANTOM**, represents the most remarkable eCrime case we have observed in the first half of 2026. The primary distinguishing feature of this actor is that it manages the majority of its attack lifecycle through a **Large Language Model (LLM)-based autonomous agent**. This agent executes tasks such as target harvesting, email personalization, AV bypass development, and victim management without requiring operator intervention. The result: an attack system that enables a single operator to generate 47,719 personalized phishing targets and expand their target pool by 41% within two weeks.

IN THE FISCAL PHANTOM OPERATION OBSERVED IN THE FIRST HALF OF 2026, THE AI-POWERED PIPELINE PROCESSED 131,035 RAW EMAIL ADDRESSES; FOLLOWING MX VERIFICATION AND CONTENT FILTERING, PERSONALIZED PHISHING CONTENT WAS GENERATED FOR 47,719 TARGETS



The accounting and taxation sector is becoming an increasingly attractive target for eCrime actors. The appeal of this sector stems from a combination of several factors: the sensitive financial data that CPAs manage on behalf of their clients, a lowered threshold of skepticism due to increased workload pressure during tax seasons, and a business structure that requires constant correspondence with regulatory bodies. This final characteristic provides a perfect breeding ground for impersonation attacks; for instance, an email containing a threat such as "your license will be suspended" severely impairs the recipient's capacity for immediate, rational decision-making.

Credential theft attacks have crossed a new threshold in terms of scale and complexity. The model we observed in the **FISCAL PHANTOM** case demonstrates that a single adversary can establish a multi-channel, autonomous attack pipeline. This pipeline involves target harvesting using a GMaps scraper, generating personalized phishing content with AI, credential exfiltration via a custom-encrypted C2, and the parallel utilization of the same list for M365 credential spraying. This indicates an operational maturity that goes far beyond the traditional "send a phishing email and wait" model.

The offensive use of artificial intelligence is gaining momentum. The case documented in our report reveals that eCrime operators actively utilize LLM tools not only for content generation, but also for AV bypass development, debugging, and operational decision-making processes. This trend alters the core dynamic of the threat landscape faced by defense teams: it is now necessary to detect not just malicious software, but **continuously self-optimizing, autonomous attack systems**.

This report covers the May-June 2026 period. During the analysis process, **the etugen.io Threat Intelligence Center** documented the following findings:

- Real-time observation of an active C2 infrastructure within a live operation
- Comprehensive documentation of the AI-powered phishing pipeline, containing 47,719 targets, along with all its components
- Validation of the cross-utilization relationship between scraper-based target harvesting and M365 credential spraying on the same target
- Source-code-level analysis of the LNK > VBS > PowerShell chain and 5 distinct AV bypass techniques
- Identification of the simultaneous execution of three parallel campaigns impersonating NASBA, AICPA, and IRS identities
- Determination that two systems connected to the C2 are associated with the actor's infrastructure, and documentation of the actor storing their own credential database on the C2 (an OPSEC failure)



Naming Mappings

The **etugen.io** team assigns a two-component codename to tracked threat actors: the adjective defines the actor's targeting focus or operational behavior, while the category suffix indicates the actor's general classification. This system is designed to prevent confusion arising from the same actor being referred to by different names across various sources, and to facilitate analyst tracking.

THREAT ACTOR	CLASS	DESCRIPTION
PHANTOM	eCrime	Financially motivated cybercrime
SHADOW	APT	Nation-state linked crime
GHOST	HACKTIVIST	Ideologically, politically motivated crime
VIPER	INSIDER THREAT	Misuse of trusted access

etugen.io codenames do not imply the identity, nationality, or country affiliation of the actors. The codename is assigned solely to facilitate analysis and to avoid using the actor's self-chosen aliases.

Actors in This Report

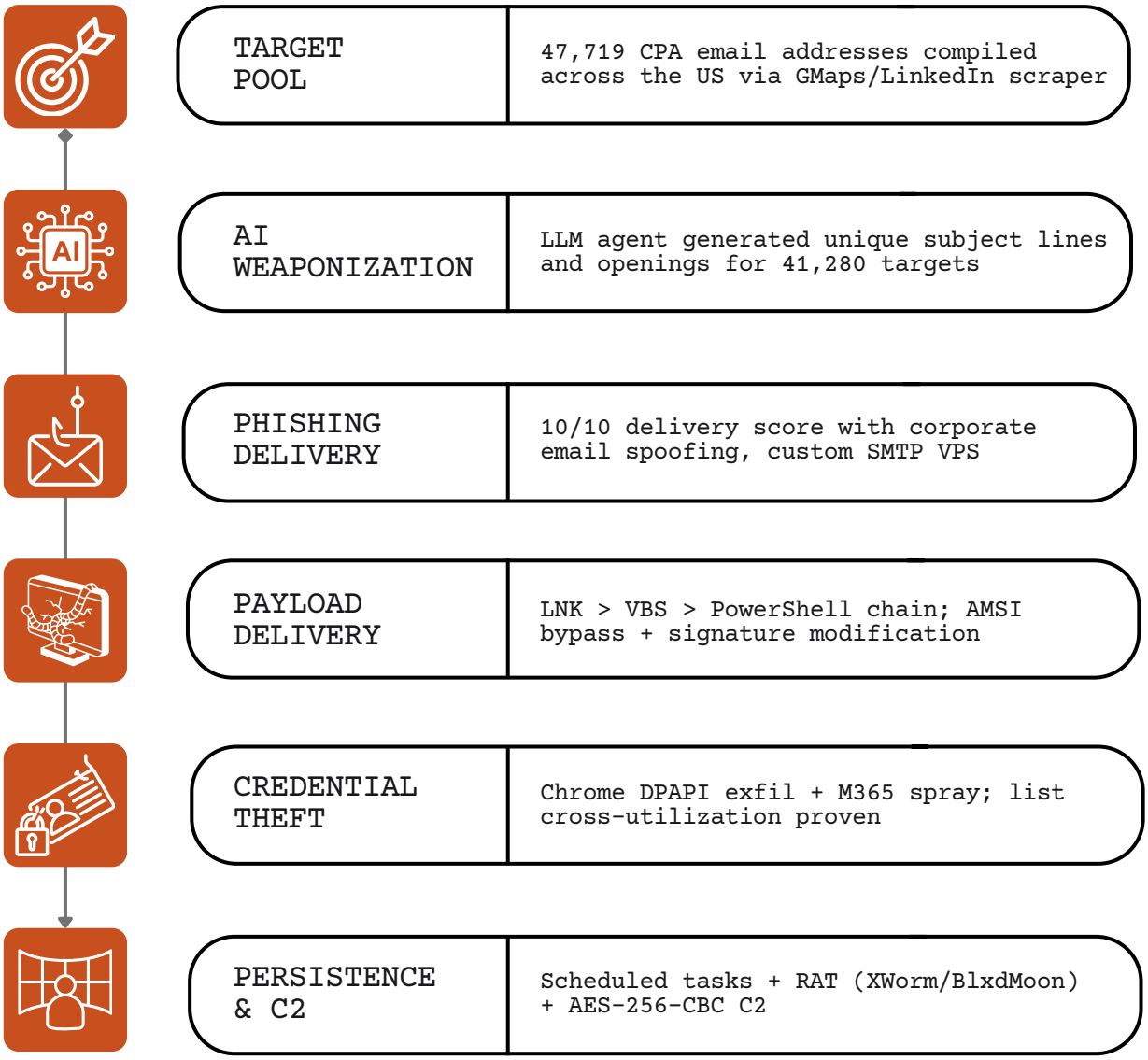
ALIAS	ATTRIBUTE	SUFFIX	DESCRIPTION
FISCAL PHANTOM	PHANTOM	FISCAL	Accounting and taxation sector-focused targeting (FISCAL) + financially motivated eCrime category (PHANTOM)

etugen.io codenames do not imply the identity, nationality, or country affiliation of the actors. The codename is assigned solely to facilitate analysis and to avoid using the actor's self-chosen aliases.

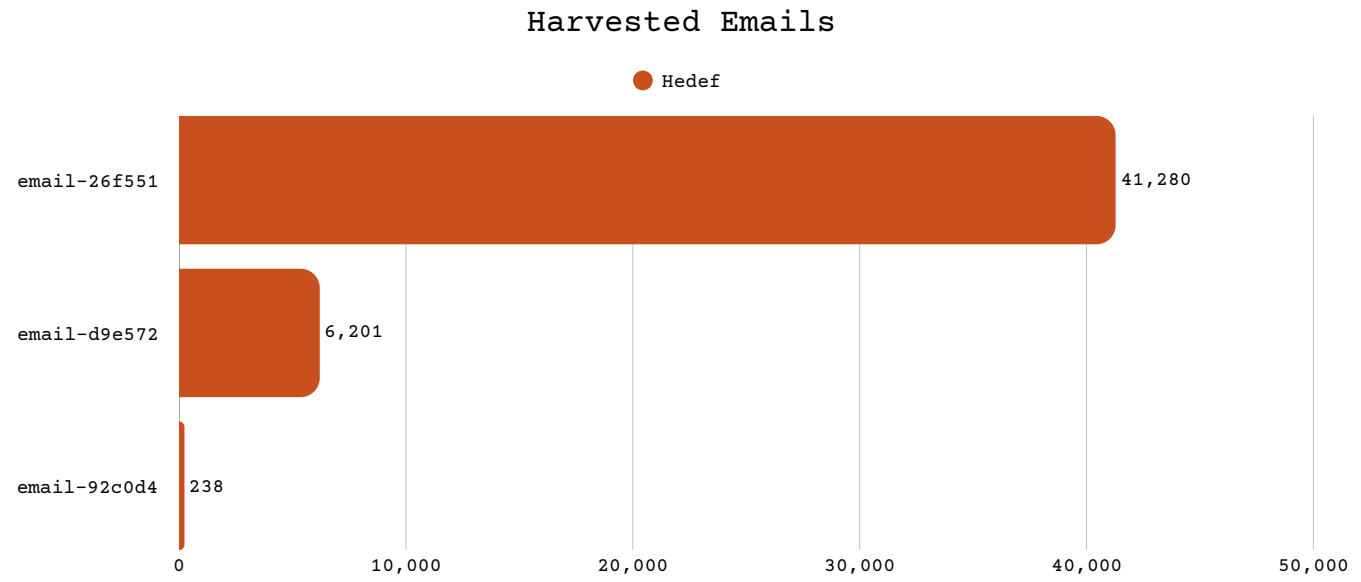
At a Glance

This AI-powered eCrime operation was observed during the May–June 2026 period through the analysis of an active C2 infrastructure. The findings document the scale of impact achieved by a single operator utilizing AI.

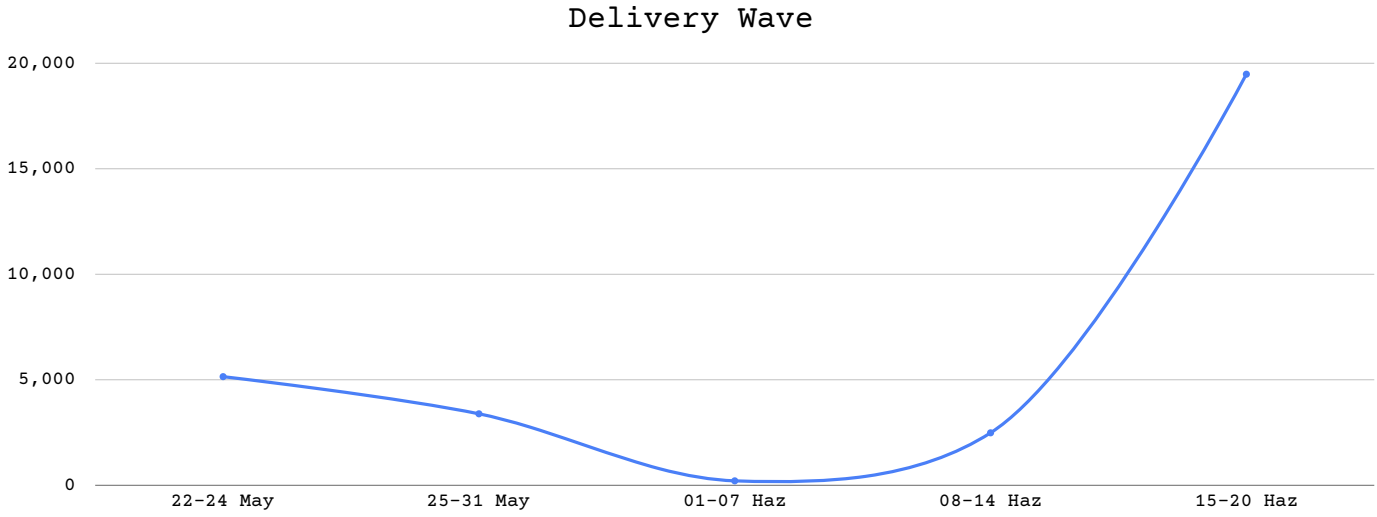
Anatomy of the Fiscal Phantom Attack



The actor's GMaps/LinkedIn scraper infrastructure initially gathered 131,035 raw emails; these were subjected to MX verification and web content scraping across 63,603 unique domains. Following a tax/CPA keyword filter, 47,719 targets were refined from the domains and exported as three CSV batches. The **Dennis King** list grew from **29,265** records in mid-June to **41,280** within two weeks (+41%), validating an active and expanding campaign.

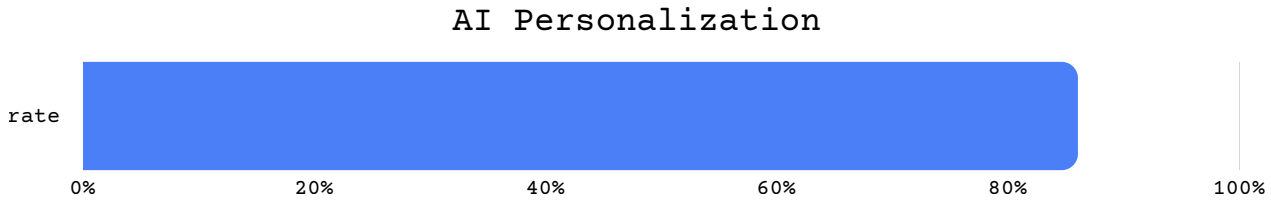


The combined weekly delivery volume of the **Dennis King BEC and NASBA** campaigns was calculated using delivery logs. A significant operational acceleration was observed during the week of June 15-20.



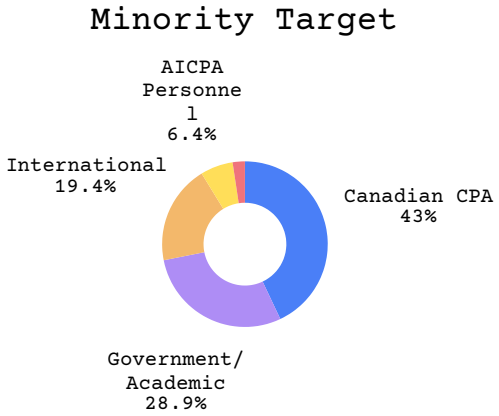
AI Operation Scope

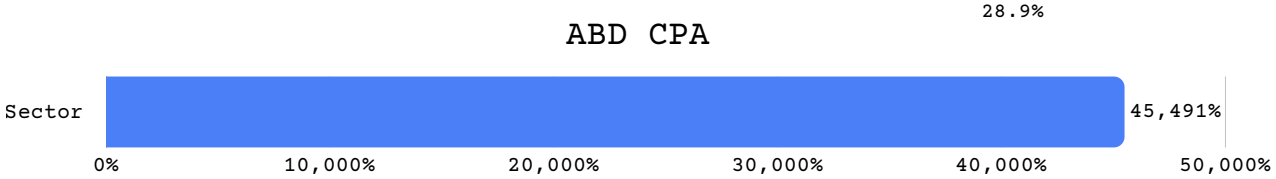
For 41,280 targets, the LLM generated a unique subject line and introductory paragraph for each email using recipient names and firm information (rotating through 10 subject templates × 6 body templates). Not limited to bulk delivery, the AI agent concurrently managed active BEC conversations replied to by more than 30 CPAs, conducted price negotiations, defended a Virginia license appeal, and consistently maintained the fraudulent **Dennis F. King** persona in every response. The result: a **mail-tester.com** score of 10/10 zero spam filter detection.



Targeted Sectors

A domain regex analysis was performed on 45,868 records; it was verified by count that 99.2% of the targets were US-based small and medium-sized CPA firms. Conversely, the minority targets comprising 0.8% of the pool carry strategic weight: AICPA corporate emails signify direct access to the professional association's internal communication channels, Big 4 addresses point to the sector's audit and consulting backbone, and government/academic addresses represent direct access to public institutions. The fact that the actor passed these addresses through the scrape filter reflects an opportunistic scanning strategy rather than discriminatory targeting.





The actor's TTPs and targeting profile point solely to a financially motivated (eCrime) motivation; no state-sponsored or hacktivist indicators were detected.

Executive Summary

This report contains the findings of an active threat hunting operation conducted by **the etugen.io Threat Intelligence Center**. The analysis examines the May-June 2026 operations of a financially motivated threat actor, codenamed FISCAL PHANTOM, which systematically targets accounting and taxation professionals in the United States.

> **FISCAL PHANTOM** adopts an approach rarely seen in the industry, executing the majority of its attack lifecycle through an autonomous agent based on Large Language Models (LLMs). The actor carries out target harvesting, email personalization, AV bypass development, and victim management via this agent. This methodology propels the speed and scale of the attack far beyond the capacity of a human operator.

Key Findings

- The active phishing infrastructure executes three parallel campaigns impersonating NASBA, AICPA, and IRS identities.
- Personalized email content was generated for 47,719 CPA/accounting targets through the AI pipeline.
- The target pool expanded by 41% within two weeks (from 29,265 to 41,280 active targets).
- Target scraping lists are cross-utilized with M365 credential spraying operations.
- Two systems actively connected to the C2 were detected, both assessed to be associated with the actor's network; the 388-piece credential database found in the C2 mirror has been reclassified as the actor's own OPSEC failure rather than external victims.
- The tool arsenal encompasses a custom Python C2, BlxdMoon RAT, XWorm v5.6, QuasarRAT, and Sliver C2.

Sectors Impacted: Accounting / Tax Advisory, Finance, Public Institutions (Secondary)

MITRE ATT&CK: T1566.001, T1059.001, T1059.005, T1053.005, T1555.003, T1113, T1125, T1071.001, T1573.001, T1562.001

Section 1: Threat Actor Profile – FISCAL PHANTOM

FISCAL PHANTOM is a threat actor categorized under financially motivated cybercrime (eCrime), operated by a single actor or a small team. The actor maintains operations via a Kali Linux-based cloud server, utilizing an LLM agent as the primary execution layer, and manages the system through an instant messaging application using English commands.

Attribute	Assessment
Motivation	Financial (Credential theft)
Country of Origin	Undetermined [Likely (Origin: Nigeria, Residence: America)]
Target Geography	Primary: US, Secondary: Canada, Ireland, Hong Kong
Target Sector	CPA / Accounting / Tax Advisory
Technical Maturity	Medium-High (Custom tool development, AV bypass, AI integration)
First Observed	May 2026
Last Activity	June 2026 (Active at the time of analysis)
Distinguishing Feature	Use of an LLM-powered autonomous attack agent

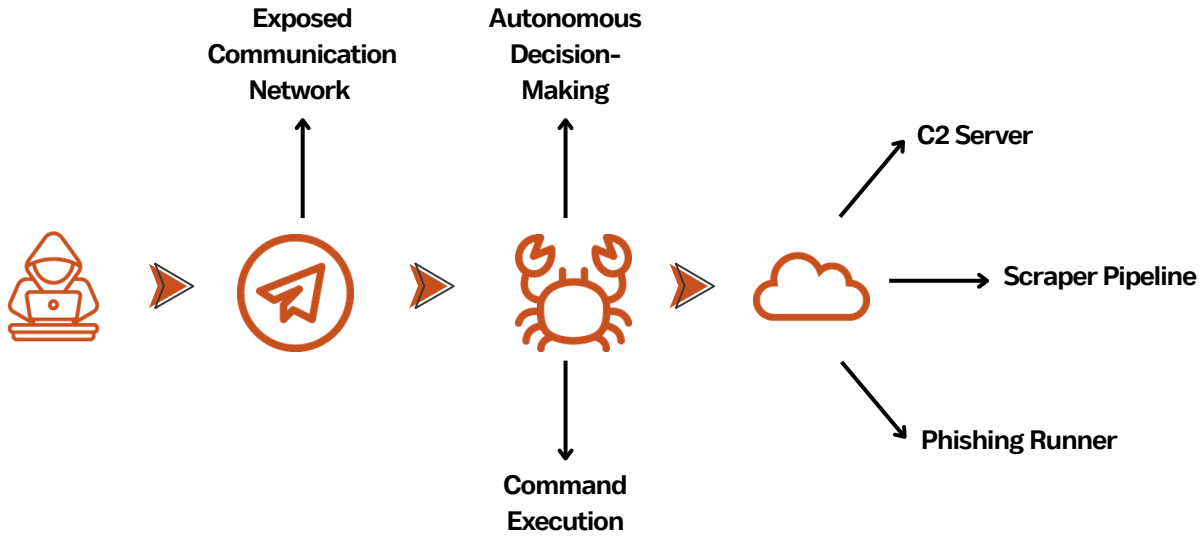
> ***The LLM agent usage by this actor represents an operational model that is rare among eCrime groups as of 2026, but shows a growing trend.***

The most remarkable feature of **FISCAL PHANTOM** is that it manages the attack lifecycle through an autonomous artificial intelligence agent. This agent:

- Operates on a Large Language Model (LLM)-based framework
- Receives natural language commands in English from the operator via an instant messaging application
- Independently executes tool utilization, code writing, debugging, and operational decision-making processes
- Performs file system read/write operations, network access, and process management without operator intervention

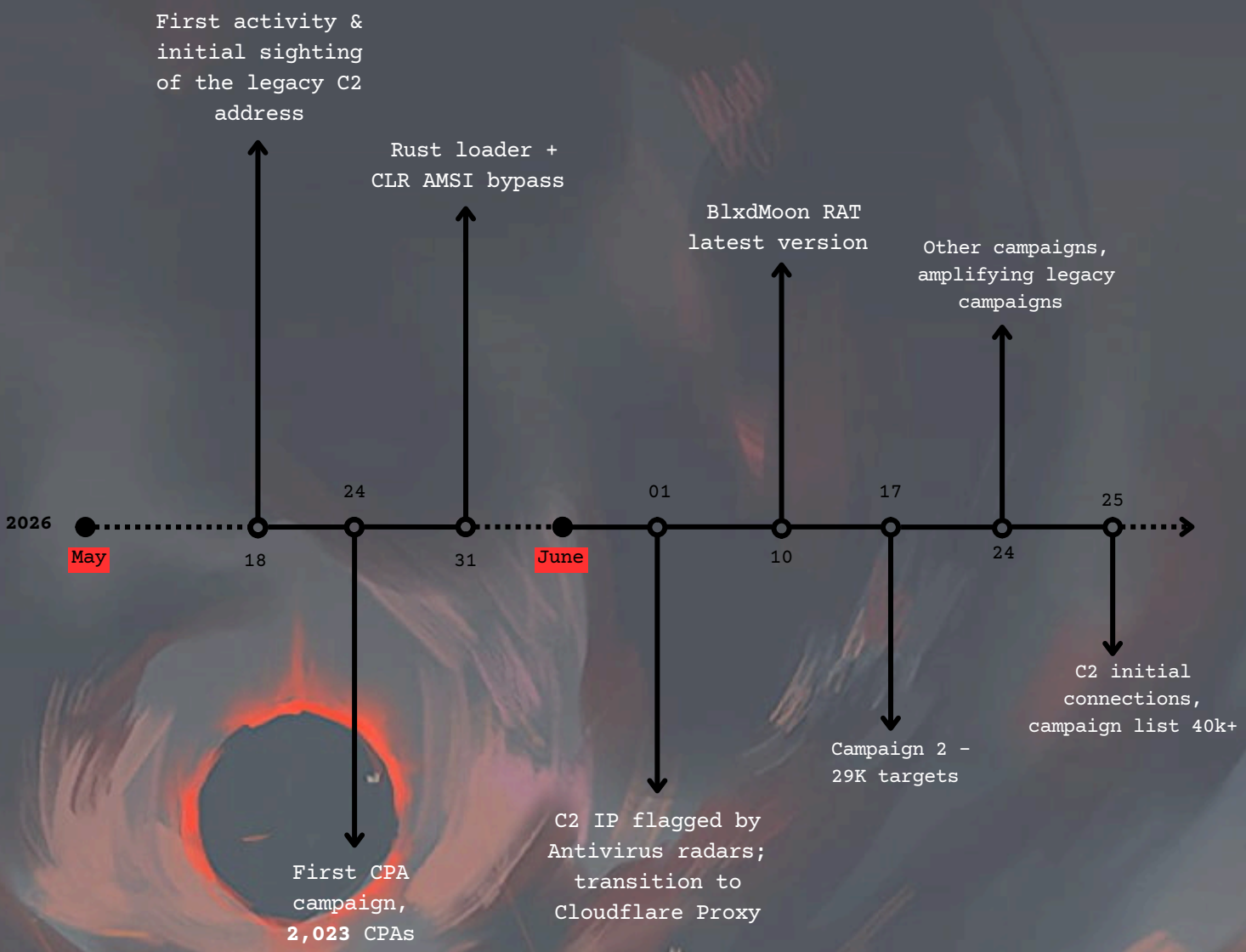
AI Agent Architecture

FISCAL PHANTOM is a threat actor categorized under financially motivated cybercrime (eCrime), operated by a single actor or a small team. The actor maintains operations via a Kali Linux-based cloud server, utilizing an LLM agent as the primary execution layer, and manages the system through an instant messaging application using English commands.



This architecture significantly lowers the operator's technical skill threshold and provides a much higher operational tempo compared to traditional human operators.

Timeline



FISCAL PHANTOM is one of the most technically remarkable eCrime actors tracked by **etugen.io** in 2026. The primary characteristic that distinguishes the actor from its peers in the industry is that it executes its attack lifecycle largely through an autonomous artificial intelligence agent.

Section 2: Campaign Analysis

Campaign 1 – NASBA ETHICS: Regulatory Impersonation Attack

FISCAL PHANTOM's primary campaign targets Certified Public Accountants (CPAs) in the United States with fraudulent "ethics violation" notices sent on behalf of NASBA (National Association of State Boards of Accountancy) and the AICPA.

The campaign is built upon a potent social engineering framework that directly exploits the professional anxieties of accountants: a warning email threatening their professional license severely diminishes the recipients' capacity for critical thinking.

> *The actor utilizes the typosquat domain **nasba-board.org** instead of the legitimate **nasba.org**. The addition of the word "board" creates the false impression that it is a natural component of the institution's official name. Example: **complaint@nasba-board.org***

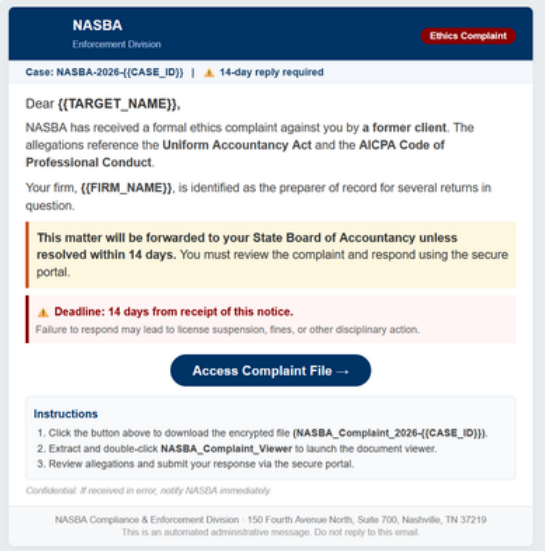
The phishing email is crafted using professional HTML templating and impersonates the AICPA corporate identity (dark blue header, gold badge). The template simultaneously deploys four distinct high-pressure elements:

The combination of elements visible in the image creates a sense of urgency, forcing the target to act quickly and significantly increasing the likelihood of a link click or file download.

Submissions are scheduled for the start of business hours (09:00 AM) based on US time zones, with separate cron jobs created for each respective UTC time zone.

The landing page implements a three-layered defense mechanism:

- IP geo-filtering - blocks access from outside the US
- Virtual machine detection - prevents sandbox analysis
- Bot filtering - blocks automated scanners



Email Template Example 1

A daily volume of 250 submissions is scheduled for each of the email addresses complaint@nasba-board.org and compliance@nasba-board.org.

Total daily = 500

Target = 2023 CPA/Accountant

Estimated time of completion = ~4 days

Campaign 2 – DENNIS KING: AI-Personalized BEC Operation

The "Dennis King" operation stands as **FISCAL PHANTOM**'s most comprehensive campaign. In this campaign, the actor poses as a fraudulent accounting consultant offering workload-sharing assistance during a tax season. The defining characteristic of this campaign is the delivery of AI-generated, personalized email content to all 41,280 targets.

This approach is designed to bypass spam filters: because every email features a unique subject line and introductory paragraph, signature-based filtering mechanisms are rendered ineffective.

The actor's lead generation pipeline consists of four distinct phases. In the first phase, Google Maps and web scraping tools harvest corporate data by scanning for the keywords "CPA, Accounting, Tax," with a maximum cap of 10 email addresses extracted per firm. During the second phase, an AI personalization engine generates a recipient-specific subject line and introductory paragraph for each collected target. These generated assets are then exported to the **leads.fileshearing.com/history** platform. In the final phase, the Dennis King campaign runner utilizes this output directly to execute the deployment.

Template	Sample Output
Streamlining Tax Process for [Name]	Streamlining Tax Process for [Target]@[cpa-firm]
Compliance Services for [Name]	Compliance Services for [Target]@[cpa-firm]
Tax Season Preparation - [Name]	Tax Season Preparation - [Target]
Question About [Name]'s Tax Needs	Question About [Target]@[Organization]'s Tax Needs
Partnering with [Name]	Partnering with [Target]

The same logic applies to the introductory paragraphs: 6 different templates are used in rotation, with the recipient's name and corporate context dynamically injected into the text for each target.

The email volume increase over approximately 2 weeks exceeds 12,000.

This growth rate demonstrates that the automated scraper is continuously operational and that the campaign is actively expanding.

An executive email account of a US CPA firm listed in the lead generation database was simultaneously targeted by an M365 credential spraying operation:

This overlap proves that the actor utilizes the scraped output concurrently for both phishing and credential stuffing. Consequently, the lead list serves not as a passive target database, but as a direct input for an active, multi-channel attack infrastructure.

Campaign 3 – IRS/PTIN: Individual Tax Professional Targeting

The IRS/PTIN campaign is an independent phishing operation conducted in parallel with the NASBA campaign. The target audience consists of individual tax consultants who are required by the IRS to hold a PTIN (Preparer Tax Identification Number). Given the professional legal status of the PTIN preparing paid tax returns without a PTIN is illegal-an email themed around "Your PTIN has been invalidated" constitutes a highly potent social engineering vector.

The IRS lure incorporates two technical differences compared to the NASBA campaign:

1. **PDF Decoy Mechanism:** When the recipient executes the payload, a legitimate IRS Form 1040 is downloaded and opened in the background. Convinced that they are viewing a legitimate document, the user does not suspect anything and keeps the session open.
2. **LNK Masking:** The IRS_Dashboard.pdf.lnk file is an LNK shortcut that utilizes a PDF icon as its system icon. The attack chain is initiated when the target double-clicks the file, believing it to be a PDF document.

> *The accounting and tax consultancy sector has become a primary target for eCrime actors as of 2026. The FISCAL PHANTOM case is a concrete reflection of this trend.*

The highest priority risk for accounting firms is the credential chain scenario: the theft of credentials belonging to a single CPA firm employee opens the door to pivoting into dozens of client accounts. In this specific case, where FISCAL PHANTOM cross-referenced phishing lists with M365 spraying lists, it was verified that the **admin@[CPA-FIRM-A].com** account was targeted across both vectors.

Why the Accounting Sector ?

Several structural factors underlie why eCrime actors target accounting and CPA firms:

Risk Factor	Description
High density of sensitive financial data	CPAs manage client bank accounts, tax returns, and SSNs-a single credential opens the door to a secondary victim chain.
High volume of regulatory correspondence	Continuous official communication with the IRS, NASBA, and AICPA legitimizes impersonation attacks.
Tax season pressure	Lowered skepticism threshold during peak periods-messages requiring "immediate action" are scrutinized less.
Small and medium-sized firm structure	The vast majority are 1-10 person firms lacking a dedicated security team.
High transaction authority	Accountants can initiate wire transfers on behalf of clients-making BEC attacks highly likely to succeed.

TECHNICAL INFRASTRUCTURE – C2

Instead of commercial C2, FISCAL PHANTOM utilizes a custom-developed Python C2; this neutralizes detection based on known signatures. C2 infrastructure components:

Component	Detail
Birincil C2	c2.fileshearing[.]com:443
Protocol	Custom TCP / AES-256-CBC
Payload server	177.7.55[.]165:8080
ScreenConnect relay	instance-hzso12-relay.screenconnect.com
SMTP / VPS	Google Workspace (smtp:587) · IT WEB LTD (NL)
leads.fileshearing.com	Scraper infrastructure
fileshearing.com	Phishing landing
c2.fileshearing.com:443	Primary C2

POWERSHELL BEACON

The PowerShell beacon connects to the C2 via an AES-CBC encrypted channel and executes commands using **cmd /c.**

Connection sequence:

Target > C2 'ok\0' (3 bytes) > C2 ack > 'AUTH:BZc2k9qy' > 16-byte confirmation > command loop. The beacon reconnects every 10 seconds.

TECHNICAL INFRASTRUCTURE – TOOLS

The actor's AV/EDR bypass development process demonstrates a capacity for building resilience through trial-and-error and is accelerated by an AI agent. Bypass evolution:

Method	Result
Direct VBS execution	Blocked by EDR
.NET CreateNoWindow + Hidden	Fully stealth
powershell -NoP -NonI -W H -Ex Byp	Policy bypass
BlxdMoon RAT (MinGW x64)	149KB, custom
XWorm v5.6 / Sliver C2 / donut	Arsenal

TOOL ARSENAL

Custom Python C2 (AES-256-CBC), BlxdMoon RAT, PowerShell beacon, XWorm v5.6, AsyncRAT, QuasarRAT (hex-patch), Havoc (abandoned), Sliver C2, ScreenConnect (dual-use/legitimate tool abuse), lnk-it-up, donut v1.1, GMaps scraper, and email_pipeline.py (131K > MX > CPA filter).

VICTIM ANALYSIS

During the analysis period, a victim actively and live-connected to the C2 (Victim A) was identified. The second machine is the actor's own test environment.

Value	Property
South Africa / Metrofibre	Geography / ISP
ASUS Zenbook Duo (Win 11)	System
Norton 360 (active)	Security software
102.33.220[.]53	Egress IP

SIZDIRILAN VERI & TEST ORTAMI

En kritik bulgu: 388 parçaya bölünmüş Chrome kimlik bilgileri veritabanı; DPAPI çözülüp AES-256-CBC ile yeniden şifrelenerek aktarılmıştır. Chrome cookie, Edge hesap veritabanı, periyodik ekran görüntüsü ve keylogger çıktısı da sızdırılmıştır - Norton 360 kurulu sistemde başarılı. Test ortamı aynı çıkış IP'sini kullanır (zayıf OPSEC).

MITRE ATT&CK MAPPING

The FISCAL PHANTOM attack chain proceeded in four phases; MITRE ATT&CK mapping:

- ✕ Initial Access
- ✕ Execution & Persistence
- ✕ Credential Access
- ✕ C2 & Exfiltration

MITRE ATT&CK MAPPING

Tactic	Technique (ID)	Observed
Initial Access	Spearphishing (T1566.001)	NASBA/IRS email
Execution	PowerShell (T1059.001)	upd.ps1 beacon
Persistence	Scheduled Task (T1053.005)	EdgeUpdate (15 min)
Credential Access	Browser Creds (T1555.003)	Chrome/Edge DPAPI

Analyst Note: FISCAL PHANTOM manages its attack lifecycle via an LLM-based autonomous agent; it utilizes a custom Python C2 (AES-256-CBC), BlxdMoon RAT, XWorm v5.6, and Sliver C2. It bypasses EDR through AMSI patching and stealthy PowerShell, and beacons back to the encrypted C2 every 10 seconds.

INDICATORS OF COMPROMISE –IOCS

The following indicators have been defanged for safe handling. Verify with your own telemetry before blocking. The full list is contained within the ETG-2026-001 report.

Indicator	Type
fileshearing[.]com	Primary infrastructure
nasba-board[.]org	NASBA typosquat
c2.fileshearing[.]com:443	C2 endpoint (AES-256)
%APPDATA%\upd.ps1	PowerShell beacon

DEFENSE RECOMMENDATIONS

Immediate actions: nasba-board[.]org and fileshearing[.]com (including all subdomains) should be blocked on the email gateway and DNS. EdgeUpdate/WindowsUpdate scheduled tasks, as well as %APPDATA%\upd.ps1 / eu.vbs, must be scanned. Stealthy PowerShell and 'wscript.exe -B' should be flagged in the EDR. The C2 signature (6f 6b 00 + AUTH:) should be added to the IDS. CPA/accountant awareness training and typosquat monitoring are highly recommended.

DEFENSE RECOMMENDATIONS

IMMEDIATE ACTIONS (0–24H):

- Block the **nasba-board[.]org** domain on the email gateway.
- Route **fileshearing[.]com** and all of its subdomains to a DNS sinkhole.
- Audit EdgeUpdate / WindowsUpdate scheduled tasks.
- Scan for the presence of **%APPDATA%\upd.ps1** and **eu.vbs**.
- Reset Chrome/Edge credentials on affected systems.

MEDIUM–TERM & STRATEGIC:

- EDR: Flag %APPDATA%*.ps1 + hidden PowerShell execution.
- EDR: Alert on the 'wscript.exe -B' argument.
- IDS: Add the C2 signature 6f 6b 00 + AUTH:.
- M365: Analyze the redirect and credential spray patterns.
- CPA awareness training + typosquat monitoring for nasba-* and irs-*.

ETG-2026-001 · Conclusion

FISCAL PHANTOM is one of the most technically remarkable eCrime actors observed in the first half of 2026. The actor's use of an LLM-based autonomous agent is not merely a technical novelty; it represents a paradigm shift that fundamentally alters attack velocity, scale, and personalization capacity.

ASSESSMENT

A scrape pipeline reaching over 47,000 targets, a 10/10 email delivery score, ten distinct AV bypass attempts, and an active victim C2 connection collectively demonstrate that AI-backed eCrime is now a mature threat category.