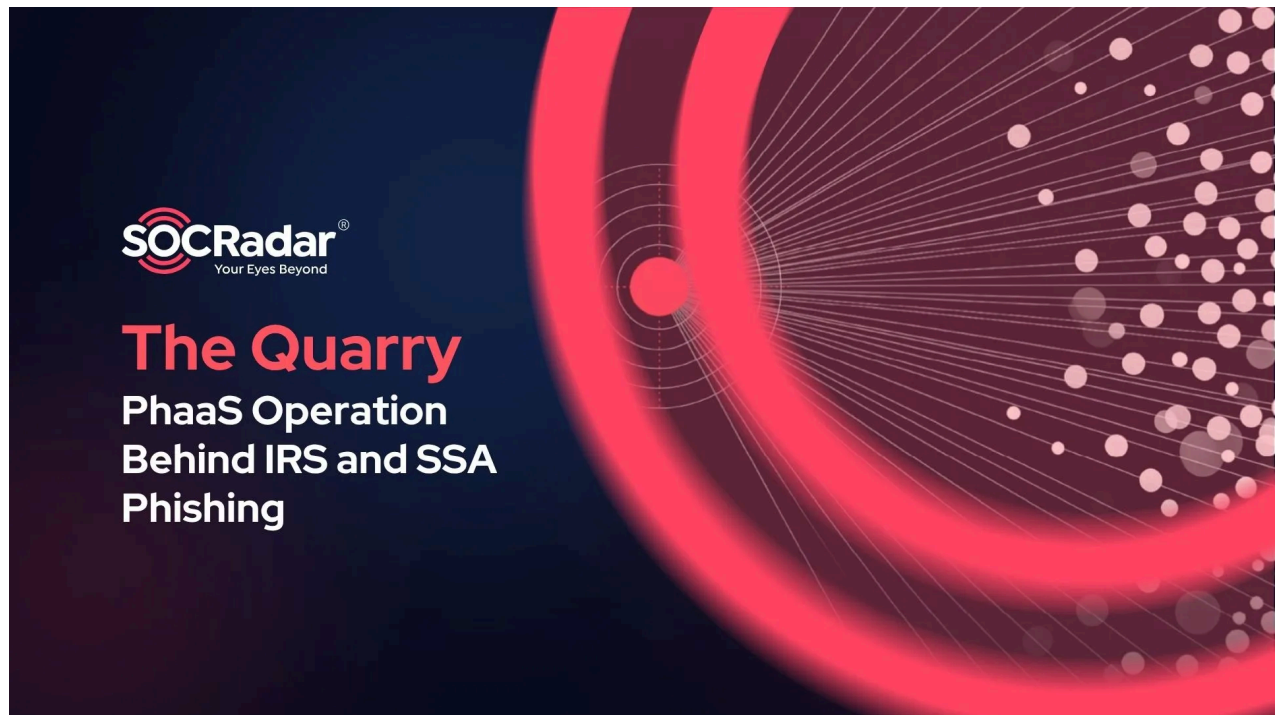


The Quarry: Inside the PhaaS Operation Behind Hundreds of IRS and SSA Phishing Campaigns

 socradar.io/blog/the-quarry-phaas-irs-ssa-phishing

Ameer Owda

June 15, 2026



Jun 15, 2026

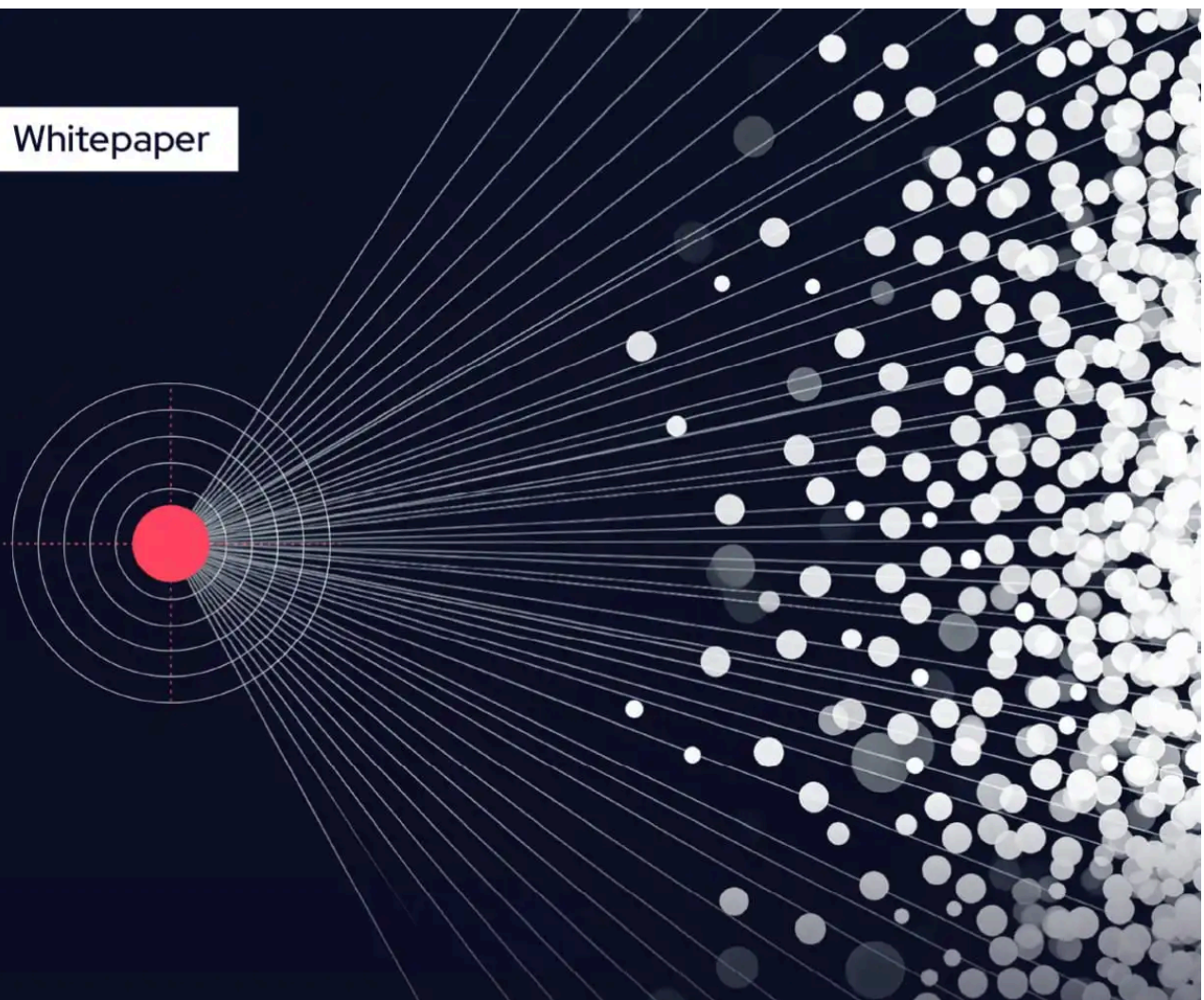
24 Mins Read

What looks like a wave of disconnected [phishing](#) incidents – some impersonating the IRS, others mimicking the Social Security Administration or DocuSign – can trace back to a single developer selling a Phishing-as-a-Service (PhaaS) toolkit to nearly 200 operators. SOCRadar's Threat has named this cybercrime ecosystem **The Quarry**, and it has been running since at least April 2025.

The developer behind it operates under the alias **RockyBelling** – also known as **Rockky**, **Rock**, and **Mike** – and runs a criminal service marketplace from Telegram. Operators who purchase the service receive phishing kits, cloaking infrastructure, self-hosted remote access panels, bulk email tools, and post-exploitation scripts. The operation adapts its lure themes to current events, with US tax season being the most heavily exploited window, but it runs year-round.

The operation remains active at the time of publication.

Whitepaper



The Quarry

Tracing a cybercriminal operation from government-themed phishing lures to developer attribution through hundreds of operators.



socradar.io

[Download the full whitepaper: The Quarry](#)

Key Findings

- A single developer – RockyBelling – built, maintains, and sells a modular [MaaS/PhaaS](#) toolkit to nearly **200 affiliates**, each running independent campaigns using shared infrastructure.
- The operation uses **legitimate RMM software** (primarily ConnectWise ScreenConnect) as its final payload, giving operators remote access to victim machines while avoiding the detection signatures associated with traditional [malware](#).
- **Traffic cloaking via Adspect** ensures that researchers, automated scanners, and sandboxes never see the phishing page – only real victims do.
- **Email lures impersonate the IRS and Social Security Administration**, alongside widely trusted platforms including Adobe, Microsoft, DocuSign, and Dropbox. Tax-themed lures are the most prevalent, but the operation pivots across pretexts year-round.
- **Telegram serves as C2 infrastructure**, with each affiliate receiving victim notifications in real time through dedicated bots. Over 90% of victims observed are located in the United States.
- A **VBS dropper with UAC bypass**, released in April 2026, introduced a second delivery path that bypasses the web-based kit entirely.
- Post-exploitation tools include PowerShell scripts for browser history extraction and W-2 document discovery, with exfiltration routed through Telegram.
- Evidence points to **potential Initial Access Broker (IAB) activity**, with stolen credentials and access possibly being resold to [ransomware](#) groups.
- **More than 80 domains, 40+ ScreenConnect panels, and 500+ distinct victim IP addresses** were identified across 14 countries during the research window (April 2025 through April 2026).

RockyBelling: The Threat Actor Behind The Quarry

Understanding The Quarry requires setting aside the instinct to treat each campaign as a separate operation. What looks like dozens of disconnected phishing incidents are in fact variations on a single toolkit sold by one person.

RockyBelling – also known as Rock, Rockky, and Mike runs a Telegram channel called **Rocky War Room**, which had 194 subscribers at the time of analysis and functions as a product catalog, announcement channel, and support desk for his criminal services. His profile bio reads “Anything Cyber!!!! Screenconnect always available,” which summarizes the service offering concisely.



[Dark Web Profile: Rock/RockyBelling](#)

Rock claims authorship of most tools in his catalog – a claim supported by code analysis. He offers onboarding support, infrastructure migration assistance, demonstration videos, and regular product updates. When the VBS dropper was released in April 2026, he announced it in the channel alongside a demo showing the UAC bypass in action. When ScreenConnect panels needed updates, he posted channel-wide notices. The operation functions with the consistency of a managed service.

His GitLab account was one of the pivoting endpoints that eventually led to attribution. The finder repository hosted there contained ScreenConnect MSI installers, post-exploitation scripts, decoy PDFs, and Telegram bot tokens linked directly to his Telegram channels.

The developer's country of origin remains unknown. Arabic comments were found embedded in multiple kit files – inside CSS blocks and PHP configuration sections. These may belong to the developer or to a specific operator who modified their kit instance. The service is global, and the operator population is diverse.

The Quarry's PhaaS and MaaS Service Catalog

The developer offers a tiered service. Entry-level purchases start around \$500 for tools like the **Rocky Gmail Sender**, a mass-mailing tool with multi-profile support, subject line randomization, HTML template support, attachment capability, and anti-detection features. A fully provisioned ScreenConnect setup costs approximately \$2,000, with a \$100 monthly

maintenance fee. Complete campaign setups – tailored to specific targets with the developer’s operational guidance – run approximately \$3,000.

The catalog includes:

Phishing kits – Customizable lure pages impersonating US government agencies and major SaaS brands, with Adspect cloaking integrated from the start. Each kit handles OS filtering, cloaking, lure delivery, payload staging, and Telegram-based victim logging.

VBS dropper with UAC bypass – Released in April 2026. Bypasses the web delivery flow entirely, executing the full infection chain from a single email attachment. No browser interaction required.

Self-hosted ScreenConnect panels – Provisioned individually per affiliate. More than 40 active instances were identified. Each panel connects to the corresponding MSI compiled for that instance, so every affiliate’s victims report to a separate panel.

Rocky Gmail Sender – Bulk email tool with randomization, template support, anti-detection features, and attachment capability.

Credential harvesting panel – A modified phishing framework for username and password collection, possibly derived from Evilginx, referenced in [Telegram channel](#) content.

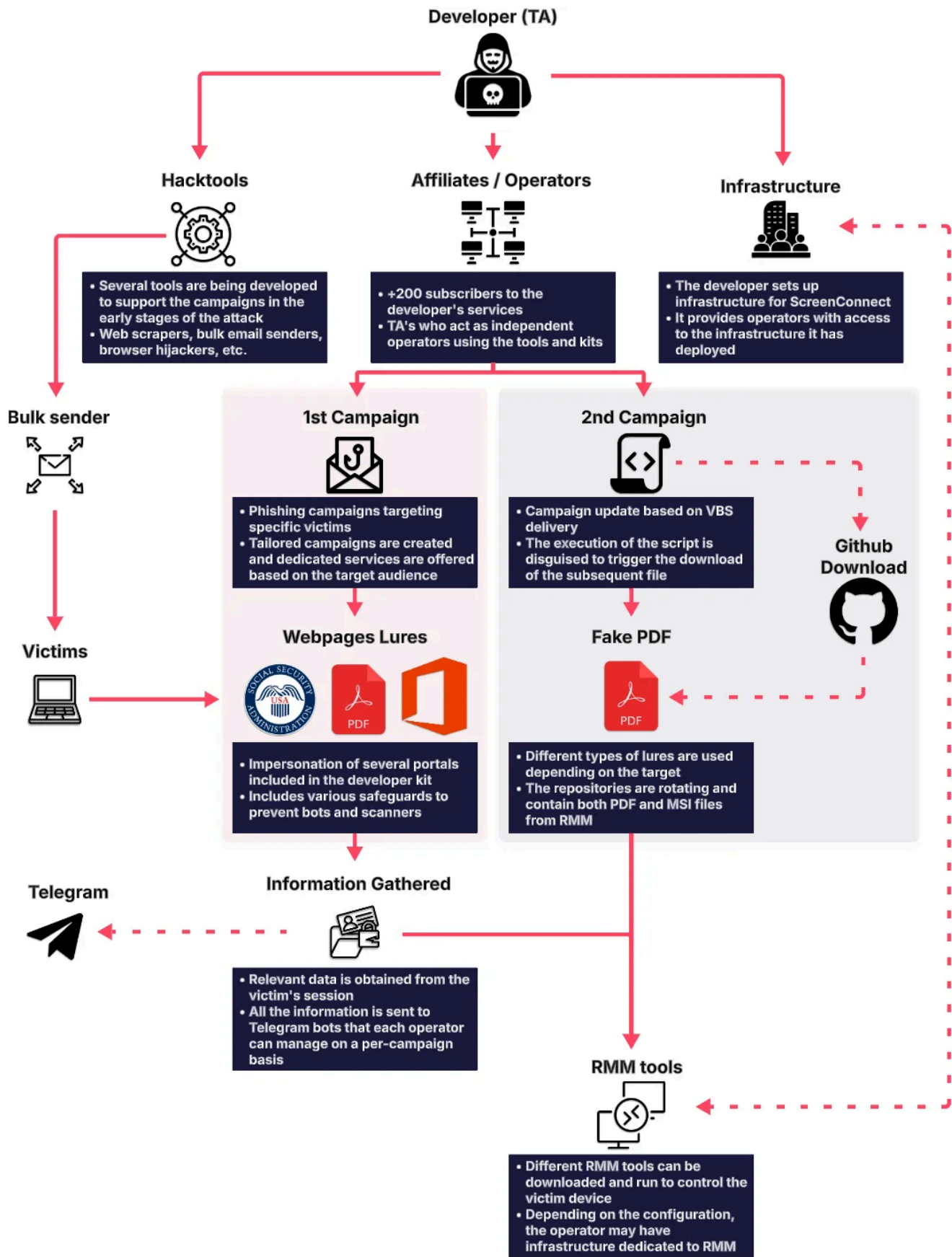
Post-exploitation PS1 scripts – A Chrome/Edge browser history stealer that forcibly closes the browser, accesses the locked SQLite database, and exfiltrates six months of history to Telegram. A second script performs a recursive scan of the user profile directory for filenames containing “w2,” then exfiltrates the paths. Both scripts are aimed at US tax season targets.

VioletRAT – A RAT promoted in the channel. Its relationship to the primary kit has not been confirmed, but the modular service model allows affiliates to integrate it into their own attack chains.

Rocky Email Sorter – Sorts email addresses by domain across Gmail, Yahoo, Hotmail, AOL, and more. A supporting tool for the pre-campaign stage.

How The Quarry Operates: A Six-Phase Attack Chain

The SOCRadar research team broke down The Quarry’s attack chain into six phases, each with measurable technical signatures that can support detection and response.



The Quarry PhaaS operation attack chain diagram from developer through affiliates to victims

Phase 0 – Scraping and Bulk Distribution

The operation can be initiated from different vectors depending on the nature of the operator. The tools available at this stage are modular and not mandatory – operators may use Rocky’s scraping and mailing tools, integrate third-party tools promoted in the channel such as MaDoO Blaster, or bring their own distribution infrastructure.

Within the ecosystem of tools the developer offers, scrapers and bulk email senders are available for operators who need them. These tools harvest email addresses sorted by domain and sector, then distribute lures through mass mailing with randomized subject lines, HTML templates, and attachment support.

The most prevalent lure theme is US tax season. Emails impersonate IRS refund notifications, SSA tax filing confirmations, and W-2 sharing workflows through Adobe, DocuSign, or Dropbox. The operation also supports other pretexts year-round – event invitations, VIP RSVPs, document review workflows – adapted by operators to their specific targets. The infrastructure accommodates whatever is most credible for the audience in question.

Phase 1 – Initial Filtering

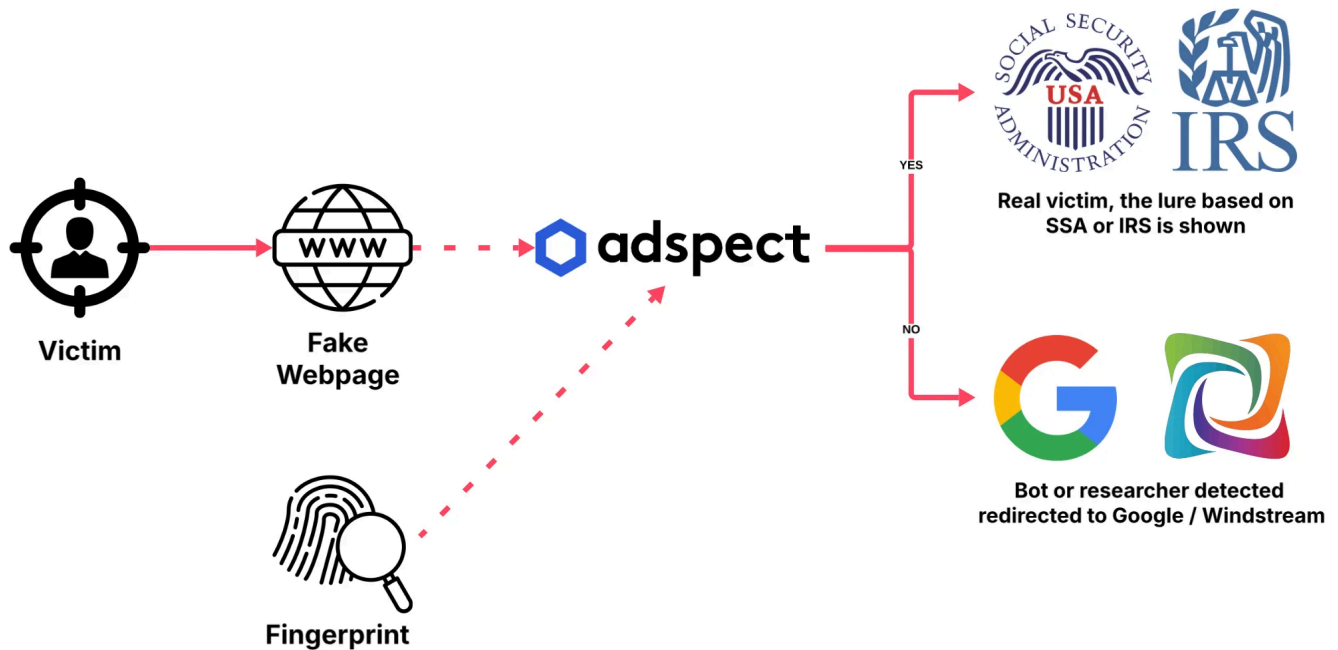
When a victim’s browser reaches the malicious domain, the first thing that runs is index.php. Before any lure content is shown, this file checks the visitor’s User-Agent string for the presence of “Windows.” If Windows is not detected – meaning macOS, Linux, mobile devices, or most automated crawlers – the server delivers a generic harmless page (errorPage.php) and stops execution.

This serves two purposes. The final payload is a Windows MSI or EXE, so non-Windows visitors are operationally useless. Filtering them out also acts as a first defensive layer against analysis environments that do not emulate a Windows browser.

For visitors who pass, the kit generates a random 300-character URL fragment and redirects to the next stage. URL fragments are not transmitted to the server in standard HTTP requests, meaning automated tools tracking domain requests cannot correlate sessions or identify what page they are viewing. Each visit generates a different fragment, complicating both analysis and blocklisting.

Phase 2 – Cloaking

The second filtering layer is where The Quarry separates itself from simpler phishing operations. PHP files with randomly generated 10-character names – referenced by the index file – run a browser fingerprinting routine using **Adspect**, a traffic filtering service used here as a cloaking layer.



Adspect cloaking decision flow showing real victims versus bots in The Quarry phishing operation

Adspect uses JavaScript to collect visitor telemetry before the phishing page is served. It checks:

- WebGL vendor and renderer, detecting virtual graphics cards typical of sandbox environments
- Timezone offset, flagging geographic inconsistencies
- Presence of standard browser objects (console, navigator, screen, window)
- Detection of nested frames that may indicate iframe-based analysis environments
- TouchEvent detection to distinguish desktop from mobile
- Behavior of `Array.prototype.includes` as an environment fingerprinting signal

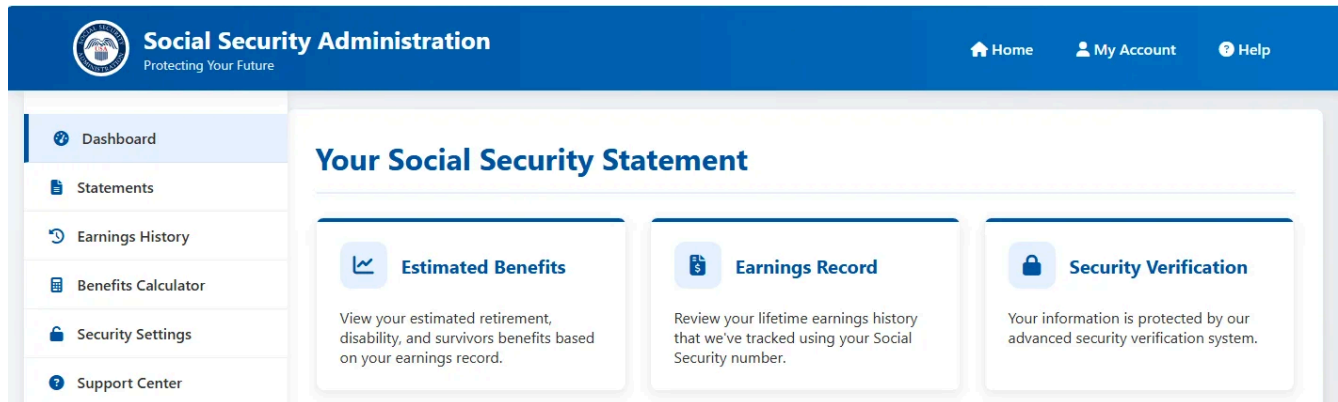
This data is sent via POST to Adspect's backend using a unique `stream_id` embedded in the PHP. Adspect returns a decision: serve the lure or redirect the visitor. If the visitor looks like a bot or researcher, the server sends a 301 redirect to a legitimate destination – in observed cases, often `webmail.windstream.net`, the login page for a real US telecommunications provider. If the visitor passes, the phishing page loads.

The same Windstream URL is reused as a post-download redirect in some kit versions, where victims are sent there three seconds after the RMM installer begins downloading. The developer's use of this domain at both ends of the chain – as a safe page for researchers and as a post-download decoy for victims – appears deliberate.

Adspect `stream_ids` are reused across multiple domains by the same operator, making them strong pivoting anchors. Identifying one `stream_id` allows clustering of all domains where that operator has deployed the same cloaking configuration.

Phase 3 – The Lure

Visitors who survive both filtering stages reach the impersonation page, served by docs.php (a filename that varies across campaigns). The primary version replicates the US Social Security Administration portal with high visual fidelity – copied colors, the SSA seal, footer elements, and section structure including “Estimated Benefits,” “Earnings Record,” and “Security Verification.”



Fake Social Security Administration portal used in The Quarry IRS SSA phishing campaign

The interaction is designed to minimize friction while maximizing credibility. It follows five steps:

Step 1 – Dashboard. The victim sees a government-style control panel with familiar-looking sections. Security messaging reinforces perceived legitimacy.

Step 2 – Download button. A “Download Your Statement” button is the only meaningful interactive element on the page.

Step 3 – OS selection. Clicking the button triggers an overlay asking the victim to select Windows or macOS. Both choices deliver the same payload. The selection exists only to reinforce the appearance of a legitimate, platform-aware service.

Step 4 – Loading spinner. A spinner plays for approximately 2.5 seconds. During this time, de.php is silently invoked in a hidden iframe, initiating the download without visible navigation.

Step 5 – Instruction popup. Once loading completes, a popup appears explaining that the victim must run the “Security Connector” they just downloaded to access their sensitive data. The exact message: “This tool establishes a secure link to our encrypted servers to unlock and display your full statement.”

This [social engineering](#) step normalizes the execution of a downloaded file in order to access a government document. The popup removes the cognitive gap between “I clicked a button on a government site” and “I am now running an executable.”

The same backend serves multiple lure themes. During pivoting, the same PHP infrastructure was observed presenting Adobe, Dropbox, DocuSign, and Messenger-style login panels. The structural elements – file paths, Telegram token, payload directories – remain consistent across themes. Only the frontend HTML changes.

Phase 4 – Payload Delivery via ScreenConnect

The file triggered by the hidden iframe – de.php – handles payload delivery in four steps.

1. **Payload selection.** The /sources/ directory on each server holds multiple RMM installer variants (EXE, MSI). de.php randomly selects one on each execution. This prevents a researcher who downloads the payload once from assuming they have captured the only sample in circulation.
2. **Unique download environment per victim.** For each visit, the kit creates a randomly named 12-character subdirectory inside /downloads/ and copies the selected payload into it. The download URL is unique per victim:

`https://[domain]/downloads/{RandomChars}/{VisibleName}`

This prevents static URL blocklisting. Across kit versions, a cleanup function (safe_cleanup()) also removes expired subdirectories automatically, erasing evidence after a TTL expires.

3. **Telegram notification.** Before the file is served, the server sends a notification to the affiliate's Telegram bot containing the victim's IP address, User-Agent, timestamp, source filename, and a direct link to the download. The affiliate can monitor victims in real time from a mobile device without needing any desktop infrastructure.
4. **File delivery.** The payload is served through a hidden iframe. The victim sees no additional navigation.

Three major kit versions were identified across campaigns:

Topic	Version X	Version Y	Version Z
Visible payload name	ScreenConnect.ClientSetup.exe	StatementID-{RandomChars}.exe	TRANVIEW2026-{RandomChars}.exe
Keepalive	No	No	Yes – pings keepalive.php every 5 seconds

Post-download redirect	No	No	Yes – to webmail.windstream.net after 3 seconds
Directory cleanup	No	No	Yes – safe_cleanup() removes expired entries
Telegram logging	IP, UA, filename	IP, UA, filename	IP, UA, filename, UTC timestamp, source file, direct link

Version Z represents the most operationally mature variant. The keepalive mechanism ensures the download subdirectory stays active long enough for the full file transfer to complete before the cleanup routine removes it.

VBS Dropper: An Alternative Delivery Method

In April 2026, Rock announced an alternative delivery path through the Telegram channel: a Visual Basic Script dropper with UAC bypass. Unlike the web-based kit – which requires the victim to navigate through the lure and click the download – the VBS chain executes autonomously the moment the victim opens the attached file.

The script follows three steps:

Privilege escalation: The VBS immediately requests administrator rights through ShellExecute using the runas verb. If the victim accepts the UAC prompt – which the government document context is designed to make likely – the script continues with elevated privileges.

Simultaneous download: The script downloads two files in parallel into the system TEMP directory: the RMM MSI installer, pulled from GitHub or GitLab repositories, and a decoy PDF (commonly social-security-statement-upd.pdf). Using GitHub and GitLab avoids the domain and IP blocklists that frequently flag attacker-controlled infrastructure.

Silent installation and cleanup: The MSI installs via /quiet ALLUSERS=2, suppressing any visible window. The decoy PDF opens in the default viewer. The victim sees a convincing SSA statement document while ScreenConnect installs silently in the background. After installation, the VBS deletes the MSI, removing the primary forensic artifact.

Three VBS variants were identified, ranging from fragmented Base64 concatenation to hexadecimal string encoding to a PS1 second-stage loader implementing AES decryption.

Obfuscation sophistication increases across versions. Shared traits across all variants include the same privilege escalation mechanism, the same COM objects, use of the TEMP directory as a staging location, the /quiet ALLUSERS=2 install parameter, and post-install self-cleanup.

Phase 5 – Exfiltration via Telegram

Exfiltration begins when a victim reaches the download stage. The kit compiles a notification containing at minimum: a status label (New Download, Download Started), the victim's IP address, the downloaded filename, the User-Agent string, and a timestamp. In more complete versions, this includes the source filename and a direct link to the generated download URL.

All of this is sent to the affiliate's Telegram bot via HTTPS POST to the Telegram API. The notification arrives in real time. The affiliate does not need panel access – a Telegram conversation on a phone is enough to monitor the campaign.

The Telegram tokens embedded in PHP files are strong attribution signals. The same token appearing in multiple campaign domains identifies them as belonging to the same operator regardless of differences in domain registrars, ASNs, or kit structure. Conversely, different affiliates using different tokens on the same underlying kit infrastructure appear as separate, unrelated campaigns to external observers.

Phase 6 – Post-Exploitation

Once ScreenConnect is installed, the affiliate has interactive remote access to the victim machine. What happens next is up to them. The developer does not impose a standardized post-exploitation workflow – the model is to sell the initial access and supporting tools, leaving subsequent operations to each buyer.

The post-exploitation toolkit in the developer's catalog and repositories includes:

Browser History Stealer (PS1) – Forcibly closes Chrome or Edge to unlock SQLite database files, exports six months of history to CSV using a SQLite instance downloaded at runtime, and sends the complete file to Telegram. The system username is used as an identifier.

W-2 Document Finder (PS1) – Recursively searches the user profile directory (C:\Users\{username}\) for files with "w2" in the name. Exfiltrates the full paths to Telegram. Within the context of US tax season targeting, these files may contain Social Security numbers, employer details, and salary information.

VioletRAT – A RAT promoted regularly in the channel as an alternative or complement to the ScreenConnect approach, with features including cookie recovery, credential dumping, and background control. Its direct relationship with the primary kit has not been confirmed.

AWS credential harvesting – Logs found in monitored bots confirm the exfiltration of AWS access keys and associated deployment regions, obtained through scraping of publicly accessible JavaScript files belonging to target organizations.

Based on the actor and operator profiles, targeted sectors, and linked incidents, the most likely downstream uses of this access include direct financial fraud through stolen identity and tax credentials, the sale of corporate access to other [threat actors](#), and ransomware deployment by affiliates operating as Initial Access Brokers.

Infrastructure

Hosting Patterns

The operation splits infrastructure across two domain categories. **Operator-registered domains** are created specifically for campaigns, using naming patterns that combine fiscal or government terms (tax, ssa, irs, estate, trust, inherit) with action words (portal, hub, archives, sync, guidance). Examples include estatetaxarchives.com, trusttaxportal.com, and hub.ssa-guidance.com. **Compromised domains** are legitimate websites whose infrastructure was hijacked to host the kit on a malicious subdomain. The owners of these domains are victims. Their primary sites continue operating normally.

Across more than 80 identified domains, pivoting was performed through three primary vectors:

Vector 1 – PHP filename patterns: The files de.php and docs.php are characteristic of this kit and rarely appear together on legitimate websites. Searching for these filenames in combination with the naming patterns above exposed dozens of additional domains hosting the same kit, including domains whose lure content was hidden behind active Adspect cloaking.

Vector 2 – Payload naming conventions: RMM installers follow consistent patterns tied to the campaign theme: ScreenConnect.ClientSetup.exe, TRANVIEW2026-{Random}.exe, 2025-TaxOrganizer_{Random}.msi, StatementID-{Random}.exe. Searching for these patterns across sandboxing and reputation platforms identified additional samples and traced them back to further domains.

Vector 3 – Infrastructure fingerprinting: Shared ASN ranges, Let's Encrypt certificate issuance dates in adjacent windows, JARM fingerprints, and page title patterns allowed clustering of related infrastructure beyond what was reachable through file analysis alone. This confirmed payload reuse across campaigns run by different operators.

ScreenConnect Panels

ScreenConnect panels represent the most persistent component of the infrastructure. Unlike phishing domains that rotate frequently, these panels are dedicated infrastructure provisioned by the developer for each affiliate and designed to stay operational across multiple campaign cycles.

The onboarding process, inferred from Telegram channel communications and the technical structure observed, works as follows: the affiliate pays approximately \$2,000. The developer deploys a self-hosted ScreenConnect instance, generates an RSA-4096 certificate, compiles a pre-configured MSI that connects to that specific panel, and delivers the installer to the affiliate for use in the /sources/ directory. Monthly maintenance costs \$100.

More than 40 active ScreenConnect instances were identified, concentrated in ASN 23470 (ReliableSite) and identifiable via the characteristic ScreenConnect JARM fingerprint. Many include IRS or SSA patterns in their hostname or page title. The panels display “Welcome To Live Support” as the default login message when no customization has been applied.

The phishing domain infrastructure and the ScreenConnect panel infrastructure are deliberately separated across different ASNs. A compromised phishing domain does not expose the panel, and vice versa.

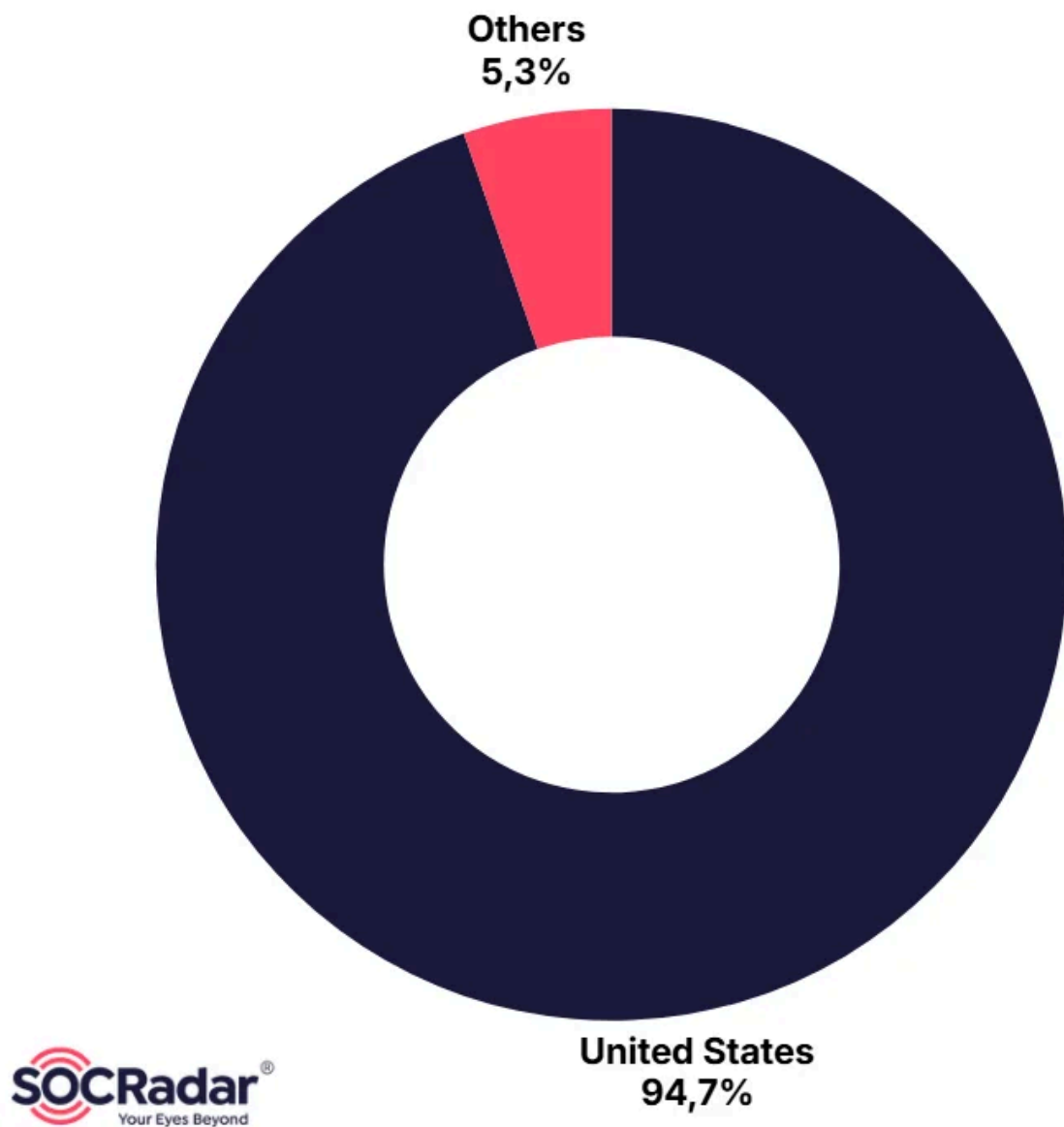
Telegram as C2 Infrastructure

Telegram functions as a Command and Control layer – victim logs flow in via HTTPS POST to the Telegram API, which is permitted in virtually all corporate environments and does not appear on standard blocklists. Each affiliate maintains an independent bot and chat ID. The developer uses the same pattern for his own operations, with hardcoded tokens found in GitLab repository files linking back to channels used for coordination and development.

Multiple bots linked to the same campaign infrastructure but operated by different affiliates were identified. This confirms that the infrastructure can support dozens of simultaneous campaigns reporting to different operators with no shared visibility between them.

Victimology

Victimology data was extracted from a subset of monitored Telegram bots. Because each operator likely maintains a dedicated bot, the observed dataset represents a fraction of the operation’s actual reach – nearly 200 users were identified within Rocky’s network, each potentially running campaigns against hundreds of targets.



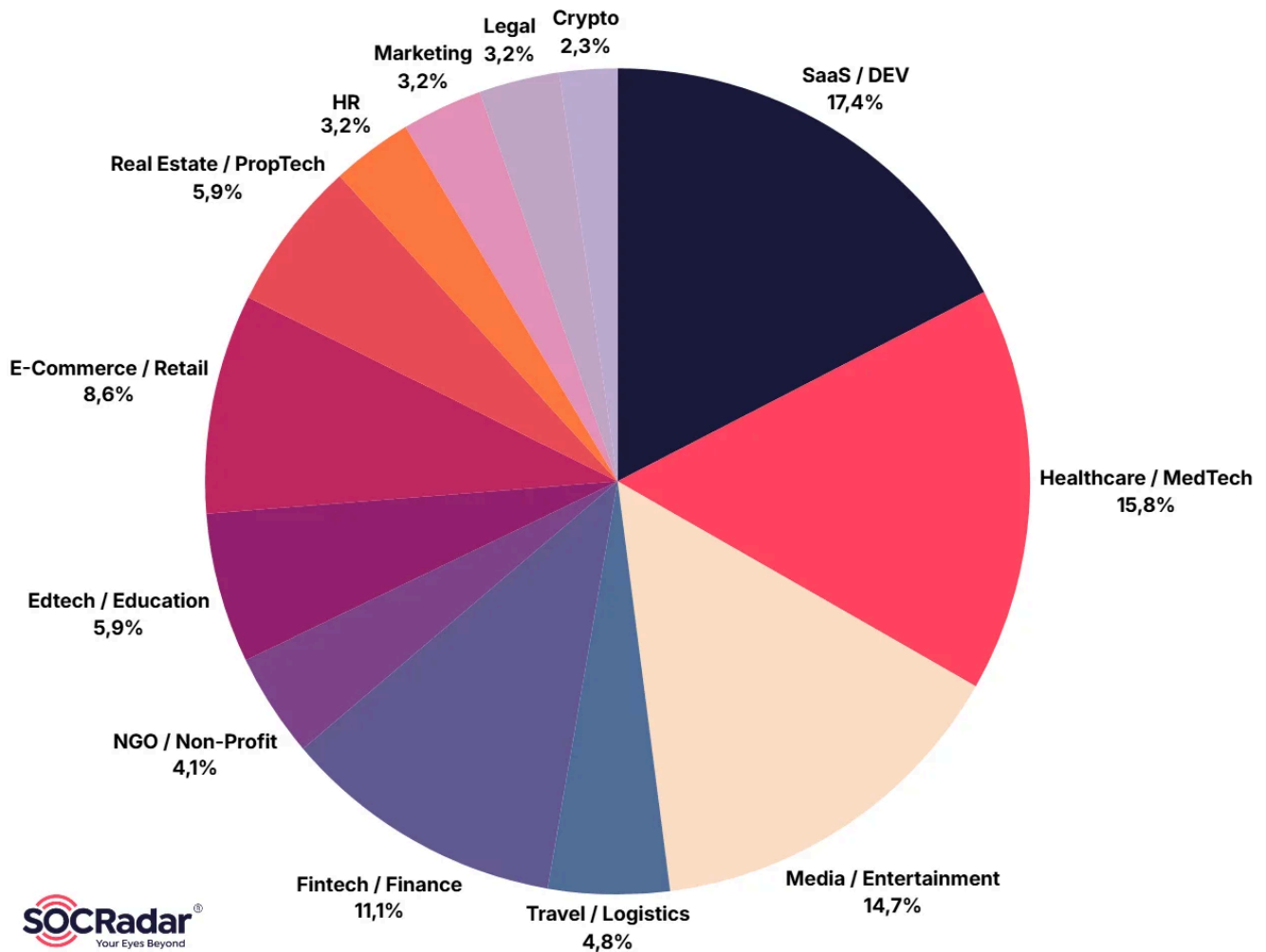
The Quarry victim geographic distribution showing 94.7% United States

Geographic Distribution

Among download events recorded in monitored bots, more than **90% of victims are located in the United States**. This aligns with the primary lure vector – tax-related communications impersonating US federal agencies. The remaining percentage likely includes US-based employees working remotely from other countries, individuals abroad with US tax obligations, and users behind VPN services. Countries where non-US victims were recorded include Egypt, Brazil, Germany, Japan, and Canada.

Additional lure themes identified during the research appear more globally oriented and could be adapted to target users in other countries.

Sector Distribution



The Quarry phishing campaign victim sector distribution pie chart

The most-targeted sectors reflect not just where tax-lured victims work, but where the operator's scraping and reconnaissance tools identified high-value credential exposure.

- SaaS / DEV – 17.4%
- Healthcare / MedTech – 15.8%
- Media / Entertainment – 14.7%
- Fintech / Finance – 11.1%
- E-Commerce / Retail – 8.6%
- Real Estate / PropTech – 5.9%
- EdTech / Education – 5.9%
- Travel / Logistics – 4.8%
- NGO / Non-Profit – 4.1%
- HR – 3.2%
- Marketing – 3.2%
- Legal – 3.2%

- Crypto – 2.3%

How to Detect The Quarry: Behavioral Indicators and IoCs

The Quarry is designed to resist analysis. The cloaking, randomized URLs, filename rotation, and Telegram-based exfiltration all reduce visibility. But consistent patterns exist across the infrastructure, and organizations monitoring for them have meaningful detection leverage.

Web and DNS signals: Domains combining fiscal terms (tax, ssa, irs, estate, trust, inherit) with portal-style terms (hub, guidance, archives, sync, portal) deserve scrutiny when they resolve to shared hosting infrastructure. The presence of de.php and docs.php on the same server is a strong indicator of kit deployment. Adspect stream_id values in PHP files cluster campaigns belonging to the same operator.

Endpoint signals: Unexpected ScreenConnect, Datto RMM, or Tiflux installation events – especially those with tax-themed MSI filenames (StatementID, TRANVIEW2026, TaxOrganizer) – should trigger investigation. Silent MSI installs via /quiet ALLUSERS=2 from temporary directories are unusual in legitimate workflows.

VBS-specific signals: The privilege escalation pattern (ShellExecute with runas and the /elevate argument), combined with use of MSXML2.ServerXMLHTTP.6.0 and ADODB.Stream for download and file writing, is consistent across all identified VBS variants. Downloads from GitHub raw content URLs followed immediately by MSI execution from the TEMP directory are a reliable behavioral indicator.

Network signals: HTTPS POST traffic to api.telegram.org from endpoints that do not ordinarily use Telegram is worth flagging, particularly when the destination chat ID and bot token are not associated with a sanctioned business integration. Blocking or alerting on this traffic can disrupt the operator's victim logging and exfiltration channel for that endpoint, though operators may adapt. Connections to ScreenConnect domains following RMM installer execution should be correlated against approved remote support tooling.

Email signals: Government agencies including the IRS and SSA do not initiate contact by email or send taxpayers executable downloads. Email security tools should be configured with rules targeting domains that match the fiscal-portal naming patterns above. SMTP log review for randomized subjects over short time windows from non-standard sending addresses can surface bulk distribution activity.

Indicators of Compromise

A partial list of indicators identified during research is included below. The complete IoC set is available on the [SOCRadar platform](#).

Domains

estatetaxarchives.com

hub.ssa-guidance.com

inherittaxpapers.site

verify.federal-docviewer.com

portal.federalverify-ssaclientportal.com

trusttaxportal.com

estatetaxrecords.com

tax-filecenter-irs.matthewtarwater.com

apps.docu-sign.net

secure.login-socialsecurity.com

hub.ssa-userstatus.com

secure.ssa-documentsync.com

MD5 hashes

8974830446d35e234881696092aded87

ef970697c5094c443f0456774cfee9bc

935413b08ef60cd819b2e1b573fc9050

2163afa18a3cdfa525b767e0e1baaba1

1827aa636cd86d1a4064e112aa197303

00b69eb7f44b5987f68667343aaafb6a

01ab231bcd9533f90e99651521b6e1bb

How to Defend Against PhaaS and RMM-Based Phishing Attacks

The Quarry succeeds through operational maturity, modular design, evasion depth, and the number of operators running variants of the same toolkit simultaneously. Defending against it requires attention to behaviors and infrastructure patterns rather than waiting for specific file hashes or domains to appear on a blocklist.

Restrict and monitor RMM tools: Maintain an approved list of remote access and monitoring tools permitted in your environment. Unauthorized ScreenConnect, Datto, Tiflux, or FleetDeck installations should generate an alert. Many organizations find that RMM tools are not monitored at the endpoint level.

Alert on Telegram API traffic from endpoints where it is not expected: Because Telegram is used for both victim logging and post-exploitation data exfiltration, unexpected HTTPS POST traffic to `api.telegram.org` from managed endpoints warrants investigation.

Harden email defenses against government impersonation: Government agencies like the IRS and SSA do not initiate contact by email or send taxpayers executable downloads. Employee awareness training should cover this explicitly. Email security tools should be configured with rules targeting domains that impersonate federal agency patterns.

Enforce application control to restrict unauthorized script execution: VBS execution from user-writable directories, particularly combined with elevated privileges, is not a typical administrative workflow. Policies that restrict VBScript execution by default – or that require signed scripts – would disrupt the VBS delivery chain.

Monitor GitHub and GitLab download traffic: RMM MSI installers pulled from raw GitHub or GitLab content URLs are unusual in legitimate enterprise environments. Endpoint monitoring rules that flag MSI downloads from code hosting platforms, particularly followed by silent install commands, are effective against the VBS delivery method.

Audit public-facing web properties for exposed credentials: The Layer 2 targeting in this campaign focuses on JavaScript files containing hardcoded cloud credentials. A periodic scan of externally facing web properties for embedded API keys and access tokens is a practical mitigation.

Deploy SOCRadar's [Extended Threat Intelligence](#): SOCRadar's XTI platform provides continuous monitoring for brand impersonation, domain spoofing, phishing infrastructure, and Dark Web credential exposure – all categories directly relevant to The Quarry's operation model.

Conclusion

The Quarry is what phishing looks like when it becomes a managed service. The developer built a platform – one that handles cloaking, delivery, payload staging, Telegram-based reporting, and post-exploitation tooling, then sold access to it at a price point that made it accessible to operators who would not have been capable of building any of it independently.

The result is a distributed, modular, persistent PhaaS operation that is difficult to attribute in any individual incident and difficult to disrupt by targeting any single component. The developer rotates infrastructure, issues updates, and onboards new affiliates. The attack surface scales with the number of active operators.

The operation remains active at the time of publication. New domains were registered in April and May 2026. Rocky War Room continues to post updates.

The full whitepaper – including the complete MITRE ATT&CK TTP table, backend code analysis, infrastructure maps, and extended IoC list – is available for download below. SOCRadar customers can access the full threat actor profile and indicator feed directly on the platform.

[\[Download the full whitepaper: The Quarry\]](#)



The banner features a red target icon on the left. To its right, the text "Cyber Threat Intelligence" is displayed in a large, bold font, with "Cyber Threat" in dark blue and "Intelligence" in red. On the right side of the banner, the text "Your Shield Against Cyber Adversaries is even stronger now!" is written in a smaller font, with "is even stronger now!" underlined. Below this text is a red button with the text "→ Get Free Access".