CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

January 23, 2025

“Crazy Evil” Cryptoscam Gang Infects Thousands with Infostealer Malware

Crazy Evil is a Russian-speaking “traffer team,” active on Telegram, that exploits NFTs, cryptocurrencies, and other digital assets with malware targeting influencers and tech professionals.

Insikt Group identified over ten active social media scams linked to Crazy Evil, likely infecting tens of thousands of devices with infostealer malware and generating millions in illicit revenue.

Crazy Evil leverages a diverse malware toolkit used in high-profile attacks — affecting both Windows and macOS — posing a significant threat to the decentralized finance ecosystem.

Analysis cut-off date: December 2, 2024

Executive Summary

Insikt Group has identified a versatile and adaptable Russian-speaking cybercriminal group engaged in digital asset theft, identity fraud, and the global proliferation of information stealer (hereafter "infostealer") malware, operating under the moniker "Crazy Evil". Crazy Evil is commonly referred to as a "traffer team" — a collective of social engineering specialists tasked with redirecting legitimate traffic to malicious landing pages. These "traffers" hunt for high-value victims, also referred to as "mammoths", to enable a pipeline of digital asset theft. This threat group has been active on low-tier dark web forums since 2021, amassing over 3,000 followers on its public Telegram (@CrazyEvilCorp) channel, with traffers divided among six subteams. These subteams are responsible for managing unique phishing pages associated with various scams aimed at infecting the devices of cryptocurrency influencers, gaming personalities, and technology professionals with malware. As of December 2, 2024, all of the scams linked to Crazy Evil are still active.

Crazy Evil is specifically interested in heists involving non-fungible tokens (NFTs) but has also been observed opportunistically capitalizing on other cryptocurrencies, payment cards, gaming accounts with auctionable and collectible assets, online banking accounts, and other financial targets. Insikt Group assesses that Crazy Evil has generated millions of dollars in illicit revenue and infected tens of thousands of devices with malware worldwide. Crazy Evil is one of dozens of traffer teams active on the dark web, growing significantly over the past three months as the likely result of a series of exit scams involving "Marko Polo" and another rival traffer team named "CryptoLove". Crazy Evil poses a significant threat to the decentralized finance (DeFi) and decentralized application (DApp) ecosystems, both of which continue to grow in popularity and are seeing increasingly wider incorporation into everyday life.

Insikt Group followed responsible disclosure procedures in advance of this publication per Recorded Future's notification policy.

Key Findings

- **Social Media Scams Identified**: Insikt Group has uncovered over ten active scams on social media linked to Crazy Evil and its six subteams. Several of these scams — such as Voxium, Rocket Galaxy, DeMeet, and Gatherum — have resulted in high-profile attacks. These scams represent a significant threat to both individual users and organizations, as many of them are still active as of this writing.
- **Targeting of Cryptocurrency Users and Influencers**: Crazy Evil explicitly victimizes the cryptocurrency space with bespoke spearphishing lures. Crazy Evil traffers sometimes take days or weeks of reconnaissance time to scope operations, identify targets, and initiate engagements. Insikt Group procured access to the Crazy Evil "worker manuals" that provide in-depth

descriptions of these tactics, which explicitly encourage a narrow focus on targets within the decentralized finance sector.

- **Diversified Malware Toolkit**: Crazy Evil conducts a cross-platform operation, affecting both Windows and macOS, that uses Stealc, Atomic macOS Stealer (AMOS), and Angel Drainer, among other tools. Previous submissions to Recorded Future Malware Intelligence indicate that scams linked to Crazy Evil at one point also delivered Rhadamanthys and Ducktail.
- **Reach and Impact**: Crazy Evil's sprawling operations have likely compromised tens of thousands of devices worldwide, resulting in millions of dollars in illicit revenue. Since its foundation in 2021, Crazy Evil has gone undetected and undeterred for almost four years while wreaking havoc on social media and messaging platforms like Telegram and Discord. The threat group's ability to operate on such a large scale poses a serious risk to both personal data security and the overall stability of the Web3 ecosystem.

Background

Insikt Group has been continuously monitoring a highly active traffer team named Crazy Evil for several months. Crazy Evil is a self-described "cryptoscam team" that has been primarily operating on various low-tier, Russian-language, Lolz-style sources — such as Lolz.Guru, LolzTeam, and Zelenka — since at least January 29, 2022. "Lolz-style sources" refer to dark web forums composed of rolling advertisement boards and chatboxes — a format popularized by LolzTeam. Insikt Group has also found identical advertisements for Crazy Evil on the Russian-language forums YouHack and Best Dark Forum, suggesting that Crazy Evil has significant marketing reach and is a well-known brand across the cybercriminal underground.

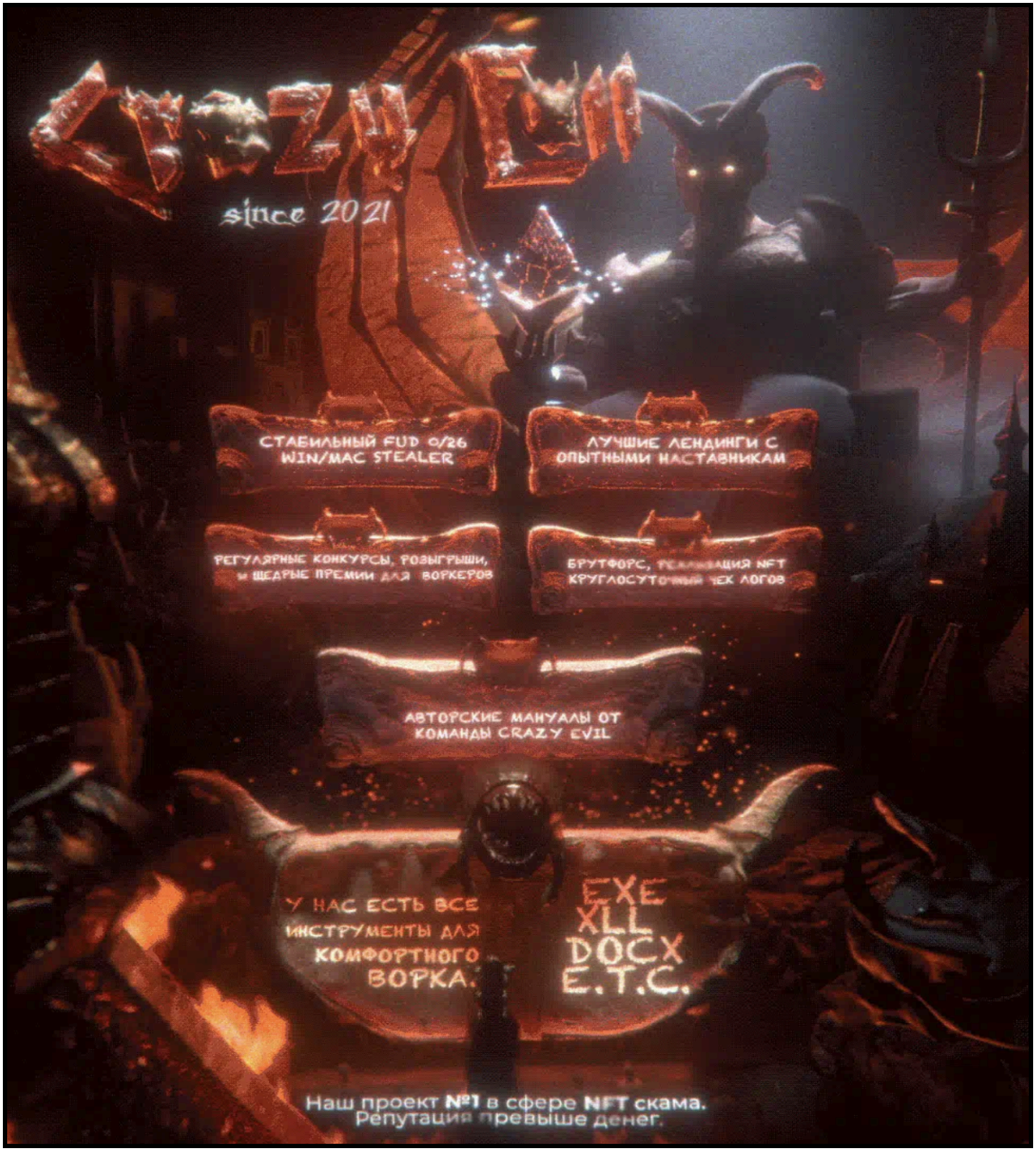

***Figure 1**: Crazy Evil advertisement, posted across at least five different dark web sources (Source: Recorded Future)*

Crazy Evil claims to have been operating since 2021, with its lifetime revenue exceeding $5 million. This is corroborated via Insikt Group access to private "payments" channels run by Crazy Evil, which announce affiliate and subteam earnings. Earnings fluctuate wildly per reporting period based on the total number of victims. For example, some Crazy Evil scams may only net $0.10 to $1,000 per victim. In other cases, Insikt Group has observed single infections resulting in losses exceeding $100,000. The Crazy Evil does not know if an attack has been successful until after the infostealer infection occurs; the group's success depends heavily on luck and persistence.

In its public advertisements, Crazy Evil outlines a general description of the team and lists some basic requirements regarding affiliate participation. Some of the most basic required "skills" are:

- The ability to operate fully undetectable (FUD) infostealers for both Windows and macOS
- An advanced understanding of hardware cryptocurrency wallets and tactics for wallet substitution (for example, address poisoning) — specifically affecting Ledger on macOS and Ledger or Trezor on Windows
- The ability to work with various FUD exploits; this requirement is not expanded upon further
- Experience with various landing pages, cryptocurrency wallet drainers, and other public and private tooling. For inexperienced cybercriminals, Crazy Evil has prepared manuals and may pair a new traffer with a "curator" for training.

Prospective affiliates are encouraged to submit detailed applications to Crazy Evil via a Telegram bot (@CrazyEvilNft_bot), which then unlocks access to subsequent applications and private channels.

The administrators of Crazy Evil claim to provide the "best traffer manuals" and "regular guidance" for its traffers. They also offer audio- and video-based training calls with native speakers, "checker" and "crypter" services for malware payloads, and channels dedicated to victim "lead-sharing".

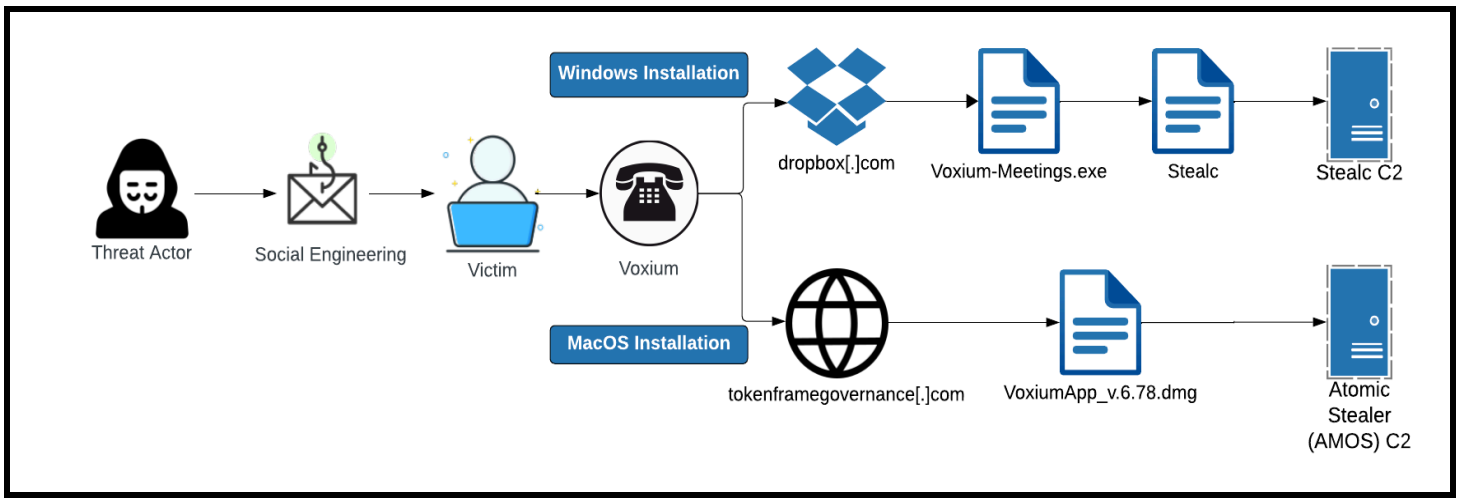

***Figure 2**: Standard Crazy Evil attack chain, using Voxium (CE-1) as an example (Source: Recorded Future)*

The affiliate application for Crazy Evil includes the following questions, listed below:

- Does an applicant have experience working with infostealer malware logs?
- How much time can the applicant dedicate to work?
- Does the applicant have access to social media accounts, or a budget to purchase them?
- Does the applicant have accounts on any dark web forums?
- Describe any skills or other relevant experience that can be useful to Crazy Evil.

Applications are likely vetted by Crazy Evil's alleged leader, a threat actor known on Telegram as "Abraham" (@AbrahamCrazyEvil).

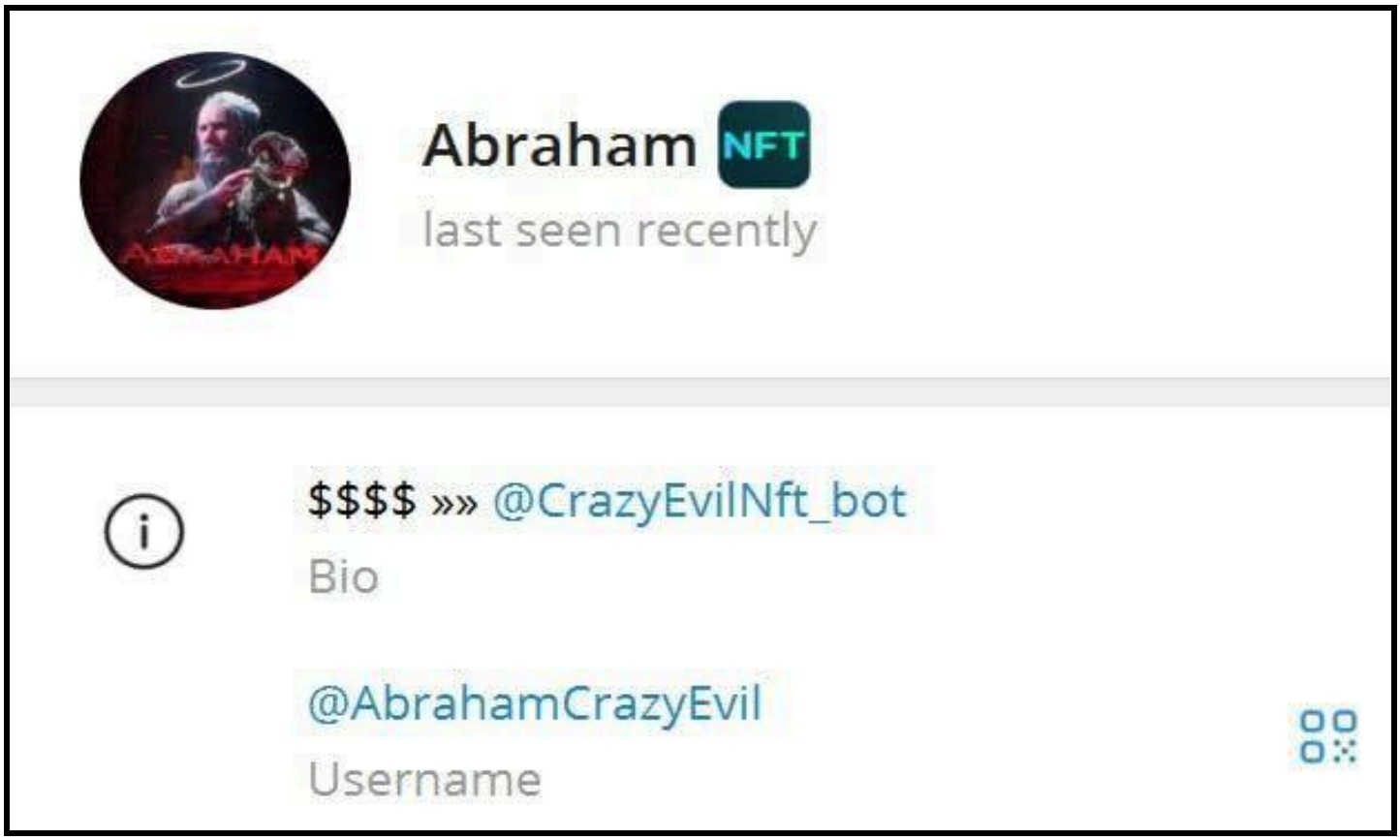

***Figure 3**: Telegram profile for Abraham — the alleged leader of Crazy Evil (Source: Recorded Future)*

Once accepted into Crazy Evil, the primary Telegram bot redirects new traffers to the following private channels that are only accessible to vetted members:

- Payments ("Выплаты")
- Information ("Инфо")
- "Logbar" ("Отстук")
- "Crazy Evil Corp"

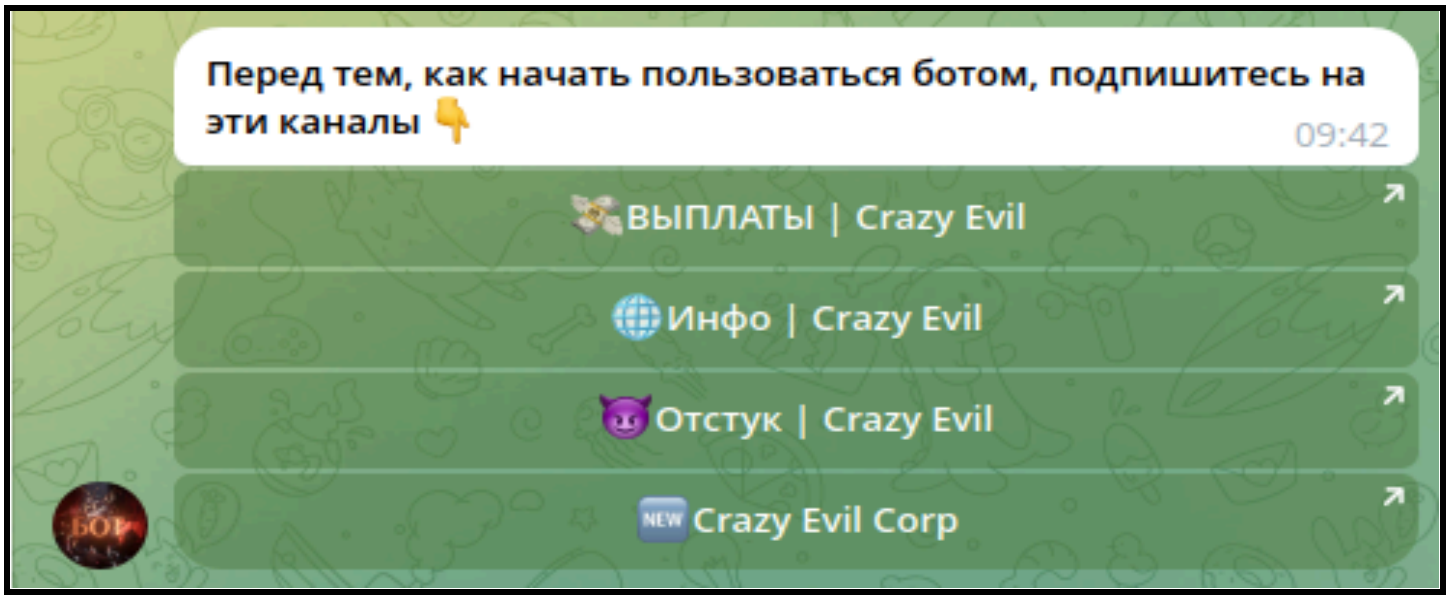

***Figure 4**: Crazy Evil's bot functionality, which redirects approved traffers to private channels (Source: Recorded Future)*

The two best sources of actionable intelligence linked to Crazy Evil include the **Payments** and **Logbar** channels. These channels name specific subteams and traffers responsible for attacks — allowing for clustering and attribution — and a detailed list of victims that includes IP addresses, geographical locations, malware build IDs, and more. These two channels are briefly described below, with screenshots in **Figure 5**.

Payments

The private channel named "**Payments | Crazy Evil**" has over 4,000 members as of this writing, and serves as proof of revenue for Crazy Evil traffers. Crazy Evil traffers are geographically diverse, speak many languages, and are hard to generalize demographically, but we believe that the overwhelming majority are Russian-speaking and located in Eastern Europe. This channel announces earnings — in both US dollars and Russian rubles — tagging the associated Crazy Evil subteam, the traffer responsible for the attack, their curator, and the date of infostealer log exfiltration.

Logbar

The private channel "**Logbar | Crazy Evil**" has over 3,000 members as of this writing, and displays a detailed victimology of Crazy Evil infostealer operations. This channel provides information about stolen data — including affected IP addresses, countries, build IDs, and the number of compromised cookies, passwords, and cryptocurrency wallets in the log. In some cases, Crazy Evil provides information on whether the victim was previously targeted, and how many times.

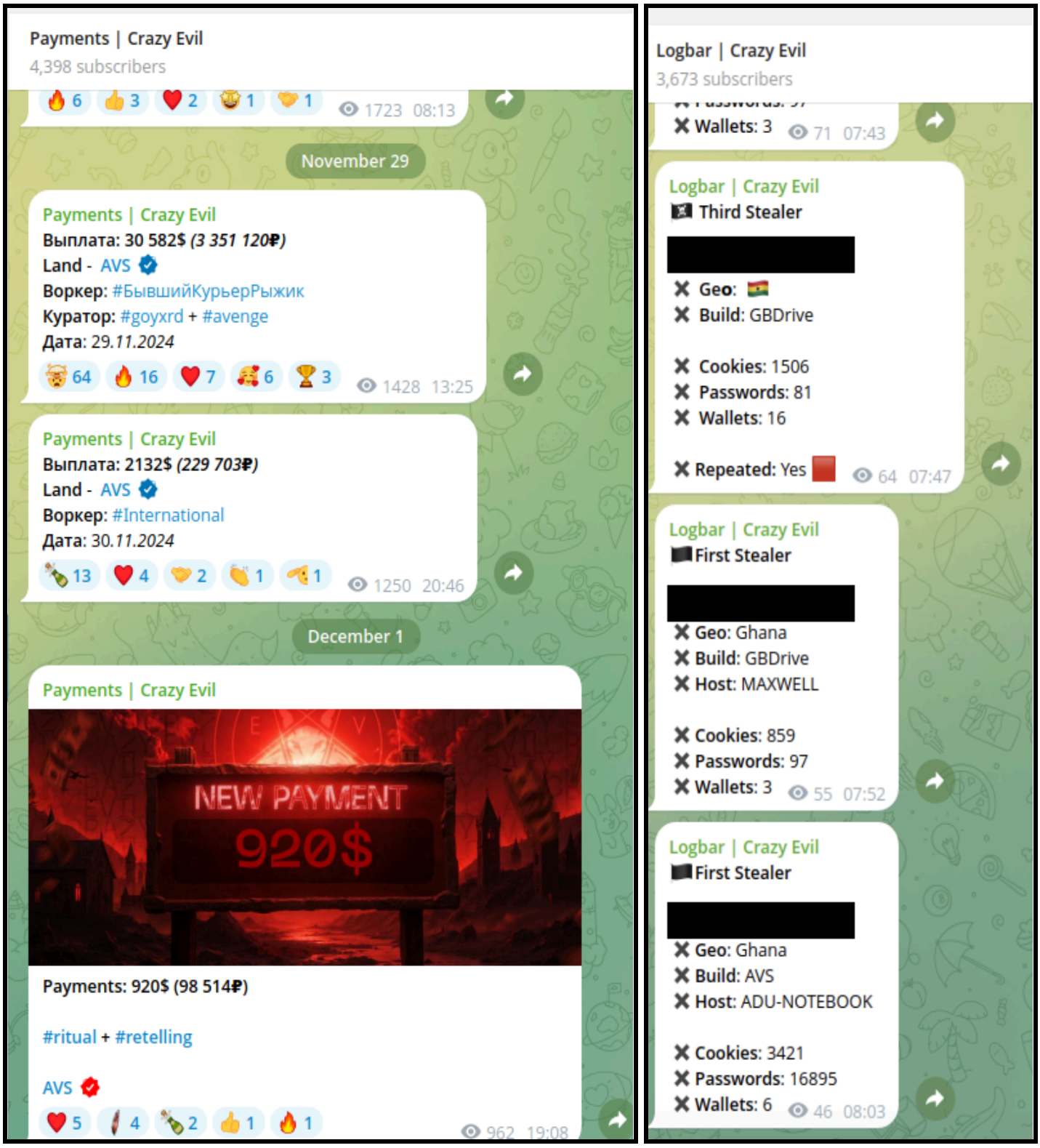

***Figure 5**: Crazy Evil's Payments (Left) and Logbar (Right) channels (Source: Recorded Future)*

Other Channels

In addition to the two Telegram channels described above, Crazy Evil operates two other primary informational channels and one private discussion group for its traffers:

- "**Crazy Evil | Corp**" (@CrazyEvilCorp), which serves as the central "hub" channel for Crazy Evil and has over 3,000 members, as of this writing
- "**Info | Crazy Evil**", which serves as an informational channel that provides regular administrative and technical updates for Crazy Evil traffers and has over 4,000 members, as of this writing.
- "**Global Chat | Crazy Evil**", which serves as the primary communication platform for Crazy Evil traffers; its discussion topics vary widely, from official work business to unrelated memes, and it has over 4,000 members as of this writing.

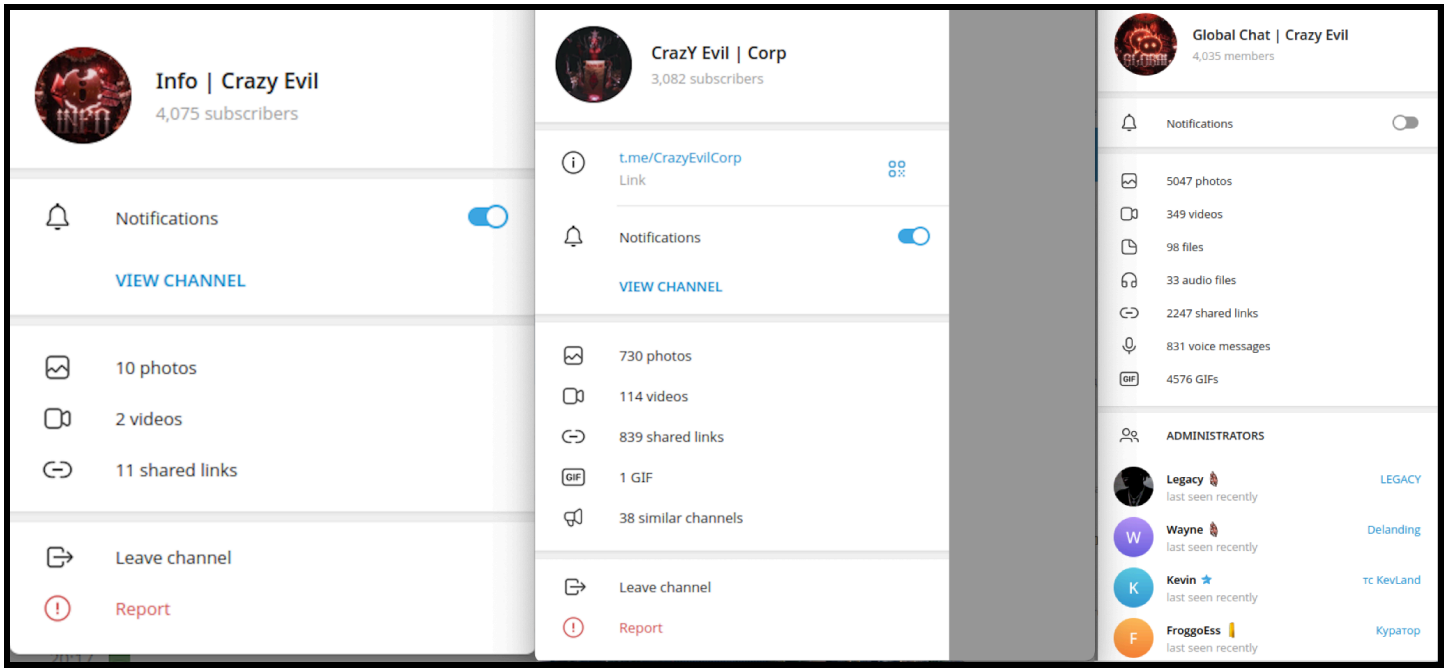

***Figure 6**: Additional Crazy Evil Telegram channels and groups (Source: Recorded Future)*

Work on Crazy Evil landing pages is divided equally among six traffer subteams, shown in **Table 1**. Each of these subteams has their own application process. These subteams — named **AVLAND**, **TYPED**, **DELAND**, **ZOOMLAND**, **DEFI**, and **KEVLAND** — are each assigned to a specific scam, making it relatively easy to cluster and attribute their activities. For the sake of simplicity, Insikt Group tracks Crazy Evil using the identifier "**CE**", followed by a number corresponding to the relevant Crazy Evil subteam. Insikt Group procured access to the private channels associated with each Crazy Evil subteam, providing deep insight into their administration and operations. All active scams associated with Crazy Evil are described at length in the following sections.

Crazy Evil Clustering

Insikt Group Identifier	Team Name	Attributed Scam
CE-1	**AVLAND**	Voxium, Rocket Galaxy
CE-2	**TYPED**	TyperDex
CE-3	**DELAND**	DeMeet
CE-4	**ZOOMLAND**	Various Zoom and WeChat impersonators
CE-5	**DEFI**	Selenium Finance
CE-6	**KEVLAND**	Gatherum

***Table 1**: Crazy Evil clustering referenced in this report (Source: Recorded Future)*

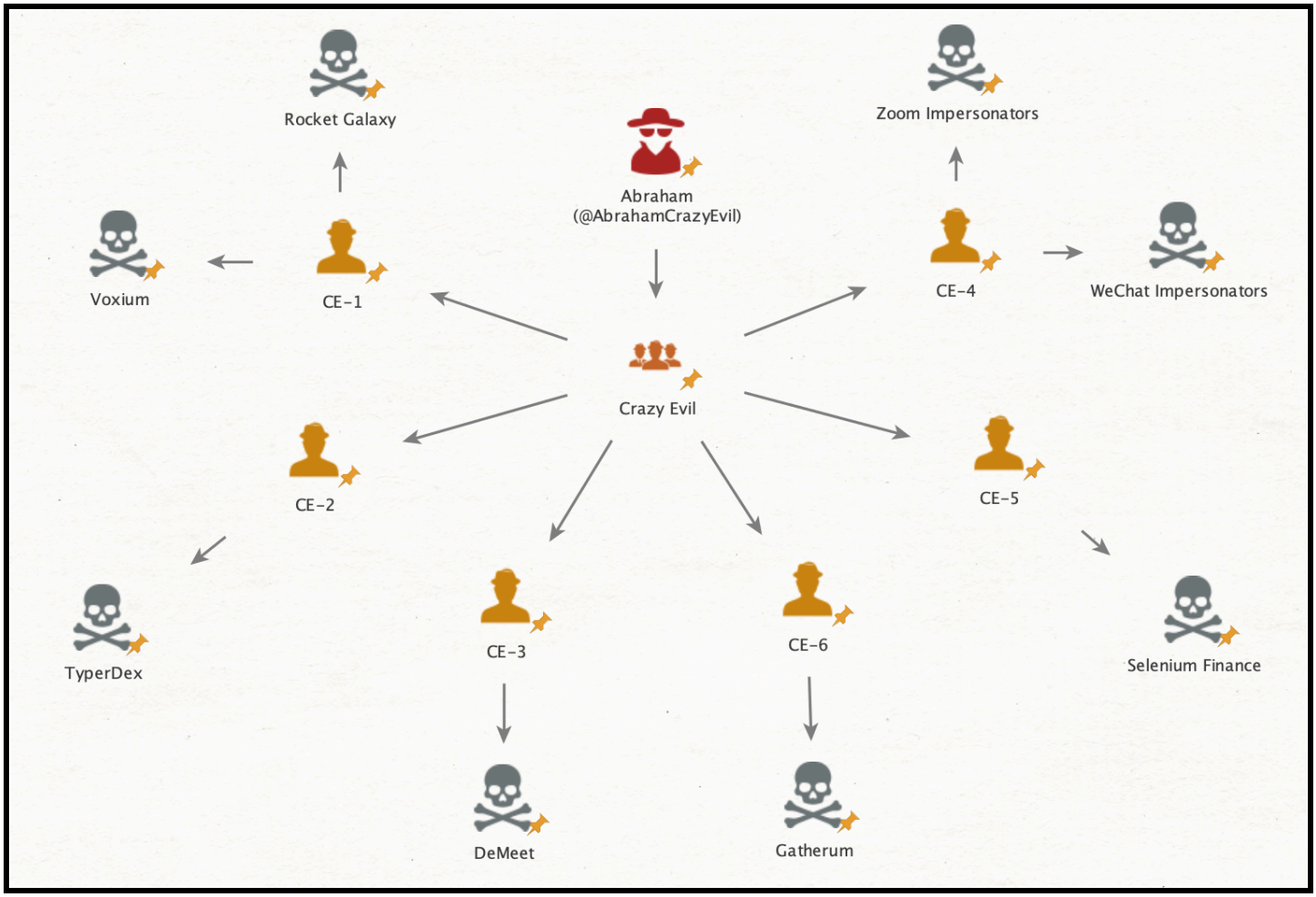

***Figure 7**: Crazy Evil subteam clustering referenced in this report (Source: Recorded Future)*

Scams Attributed to Crazy Evil

AVLAND (CE-1)

Voxium is a self-proclaimed decentralized communication tool built on Solana, which is primarily marketed via social media (@voxiumcalls; @voxiumapp) and Telegram (@voxiumnews). Traffers associated with Voxium are supplied with an AI-generated whitepaper on the project (*voxium[.]eu/whitepaper*), a manual for engaging with victims, and a rulebook for proper work conduct. Voxium is operated by the Crazy Evil subteam **AVS | RG** — often referred to internally as **AV**, **AVLand**, or **AVENGE** — that Insikt Group tracks as the cluster **CE-1**.

CE-1 traffers are instructed to leverage ChatGPT to create convincing English-language phishing lures for their mammoths — a Russian cybercriminal slang term used to describe high-priority social engineering victims. According to Crazy Evil's traffer manuals, the ideal mammoth is "older" and "less experienced with social media" than the average user. CE-1 traffers pose as project managers, recruiters, and start-up founders on social media. Voxium's stated goal is to widely propagate job offer and investment scams within the Web3 ecosystem using infostealers, creating a pipeline for cryptocurrency and NFT theft. CE-1 traffers frequently state that "time is the most valuable resource" to Crazy Evil, implying that the success of Voxium relies heavily on quick-win attacks. CE-1 traffers advise swift turnarounds in victim engagements, encouraging traffers to abandon conversations that fail to result in "quick and easy" infections.

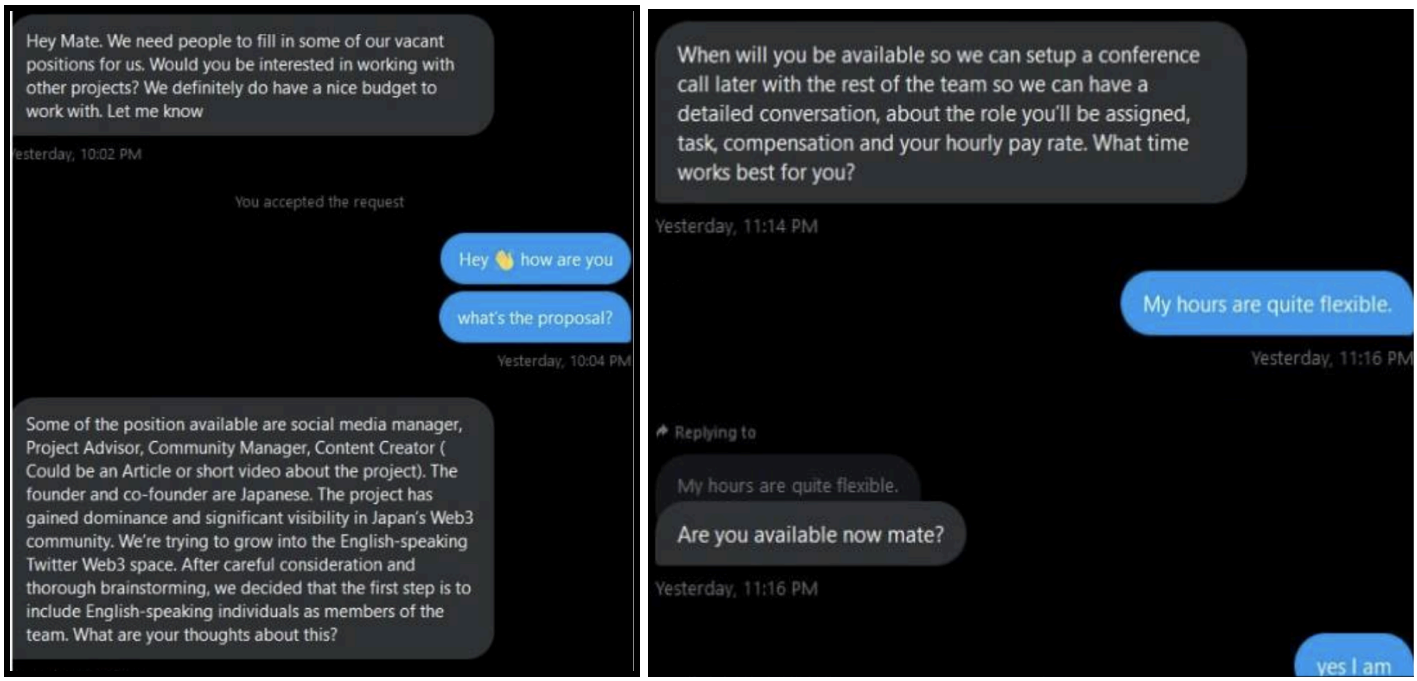

***Figure 8**: Sample conversations of Voxium engagements, taken from the AVS | RG traffer manuals (Source: Recorded Future)*

Figure 9: *Voxium landing page at voxiumcalls[.]com (Source: Recorded Future)*

Upon visiting a Voxium website (**Table 3**) — for example, *voxiumcalls[.]com* — victims are prompted to input a "meeting code" before downloading the Voxium installer for either Windows OS or macOS. These meeting codes are assigned to traffers via the Voxium administrator. Insikt Group procured several meeting codes in order to successfully download and install Voxium.

For Windows OS users, the Voxium website contacts Dropbox (*dropbox[.]com/scl/fi/j2942ad5hlnheby7pc2rz/Voxium-Meetings.exe?rlkey=5vxdh3tx3fhh9aqmq1ujdqrns&st=hc267s5f&dl=1*) to download the `Voxium-Meetings.exe` client. For macOS users, the Voxium website contacts *tokenframegovernance[.]com* and runs the script `kusaka.php?call=av` before downloading `VoxiumApp_v.6.78.dmg`. Insikt Group notes that the Voxium website checks the validity of meeting codes by placing a request to IPinfo using the token `41c9400467d8df` and contacting a Telegram bot (`bot7035066518:AAEiKOY_kY8zNWnsH0ik7FxC_fLrcfvS__Q`). Querying this bot via the Telegram API returns the username @voxcodes_bot.

Filename	Malware Tags	C2	Malware Intelligence
`Voxium-Meetings.exe`	Stealc	178.22.31[.]97	Triage
`VoxiumApp_v.6.78.dmg`	N/A (AMOS)	141.98.9[.]20	Triage

Table 2*: Sandbox analyses of Voxium Windows OS and macOS builds (Source: Recorded Future)*

Domain	ASN	First Seen	Last Seen	Status
voxiumcalls[.]com	AS-HOSTINGER, CY (AS47583)	2024-10-14	2024-12-02	Active
voxium[.]eu	AS-HOSTINGER, CY (AS47583)	2020-01-10	2024-12-02	Active
voxiumhub[.]com	AS-HOSTINGER, CY (AS47583)	2024-08-31	2024-11-28	Inactive
voxium[.]cloud	RU-AEZA-AS, RU (AS216246)	2024-10-15	2024-11-21	Inactive

***Table 3**: Voxium website infrastructure (Source: Recorded Future)*

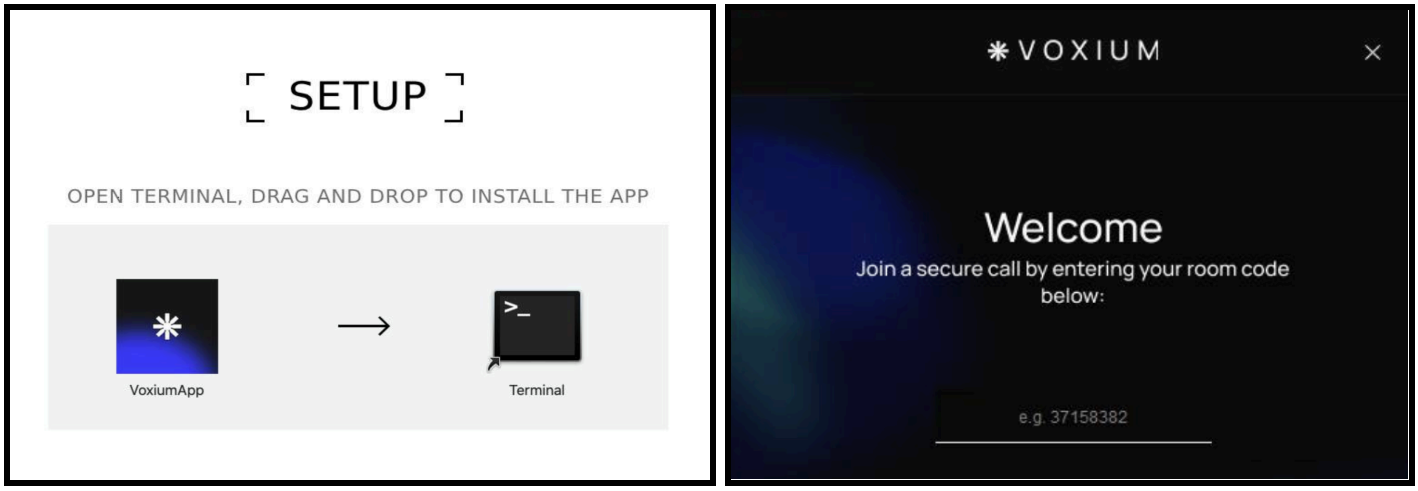

***Figure 10**: Voxium installers on macOS (Left) and Windows (Right) (Source: Recorded Future)*

While **AVS | RG** (**CE-1**) does not presently claim responsibility for any scams other than Voxium, Insikt Group identified several overlaps in landing page design and traffer activity with different scams that warrant further investigation. For example, we believe that the "**RG**" in the team name "**AVS | RG**" almost certainly refers to the scam game **Rocket Galaxy** (@rocketglxworld) — formerly **Rocket Legacy** (@rocketlegacynft) — despite CE-1 currently not claiming responsibility for operating Rocket Galaxy in any public or private communications. This suspected link between Voxium and Rocket Galaxy is substantiated in forensic evidence by the use of the unique IPinfo webhook token `41c9400467d8df` — described in the Voxium website above — which is also observed in the landing pages for Rocket Galaxy. Insikt Group further identified unique text- and artifact-based overlaps identified in the DOM content of both the Voxium and Rocket Galaxy websites. These include strings like "`getUserIpAddressAndCountry`", which is found in both websites. At the present time, Insikt Group is not able to procure malware samples associated with Rocket Galaxy or Rocket Legacy, as the websites' (**Table 4**) code-checking functionality is inoperable.

Domain	ASN	First Seen	Last Seen	Status
rocketgalaxy[.]io	AS-HOSTINGER, CY (AS47583)	2024-11-15	2024-11-21	Inactive
rocketgalaxy[.]xyz	AS-HOSTINGER, CY (AS47583)	2024-09-09	2024-11-14	Inactive
rocketgalaxyworld[.]com	AS-HOSTINGER, CY (AS47583)	2024-07-05	2024-12-01	Inactive
playrocketgalaxy[.]com	AS-HOSTINGER, CY (AS47583)	2024-02-08	2024-07-23	Inactive
rocketlegacy[.]xyz	DDOS-GUARD, RU (AS57724)	2024-11-11	2024-12-02	Active

***Table 4**: Rocket Galaxy website infrastructure (Source: Recorded Future)*

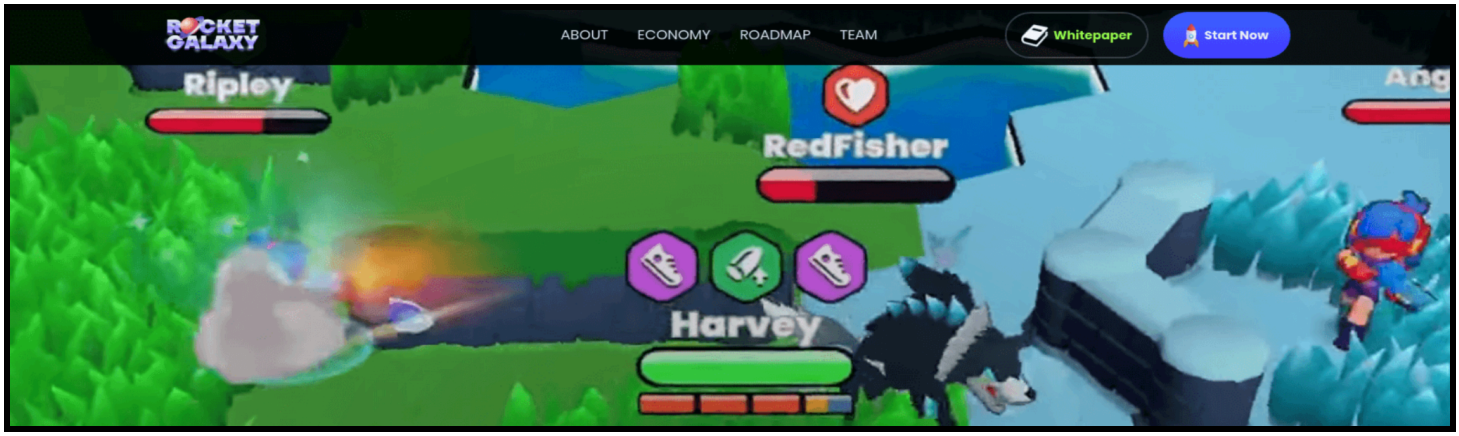

***Figure 11**: Rocket Galaxy landing page at rocketgalaxy[.]io (Source: Recorded Future)*

Insikt Group also identified approximately six instances of suspicious activity on social media that further suggest a direct link between Voxium and Rocket Galaxy. We identified several sock puppet accounts operated by CE-1 Voxium traffers amplifying Rocket Galaxy, or publicly claiming a relationship with Rocket Galaxy in their profiles.

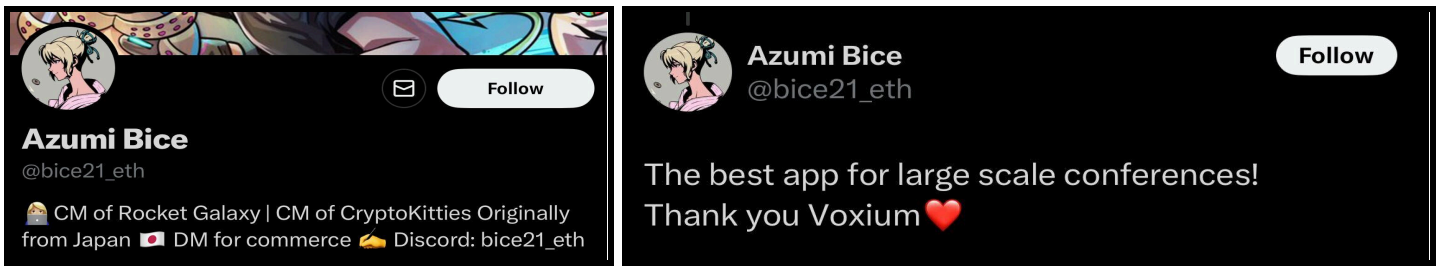

***Figure 12**: Known Voxium traffers also claiming a link to Rocket Galaxy (Source: Recorded Future)*

Further pivoting on the Google Tag `GTM-5BWVXJQ` used by the Voxium website unearths five additional websites that are possibly linked to CE-1 threat activity: **CCD**, **Ultima**, **Solana SMS**, **WatcherBot**, and **Secretum**. We note that Solana SMS and Secretum share the same logo and favicon as Voxium. Insikt Group was not able to identify any malware samples associated with these projects but did identify many cryptocurrency and NFT theft reports on social media that suggested that these landing pages either delivered malware or drained wallets at some point. Insikt Group is unable to confirm any relationship between these websites and Crazy Evil at this time, but we assess that this warrants further investigation. As of December 2, 2024, all of these websites (**Table 5**) are defunct.

Domain	ASN	First Seen	Last Seen	Status
ccdcompany[.]online	TIMEWEB-AS, RU (AS9123)	2023-01-04	2024-02-08	Inactive
ultima-dapp[.]online	BEGET-AS, RU (AS198610)	2022-12-17	2024-01-21	Inactive
ultimadapp[.]online	BEGET-AS, RU (AS198610)	2022-11-14	2023-01-07	Inactive
solanasms[.]com	CLOUDFLARENET, US (AS13335)	2023-02-14	2024-06-14	Inactive
watcherbot[.]xyz	CLOUDFLARENET, US (AS13335)	2022-01-08	2024-12-01	Inactive
secretum[.]io	CLOUDFLARENET, US (AS13335)	2021-05-20	2024-12-01	Inactive

***Table 5**: Defunct websites that use the same Google Tag as Voxium, also referenced in cryptocurrency scam reports on social media (Source: Recorded Future)*

***Figure 13**: Solana SMS, a defunct website that bears the same logo, favicon, and Google Tag as Voxium. The relationship between CE-1 and Solana SMS is currently unclear. (Source: Recorded Future)*

TYPED (CE-2)

TyperDex is a self-proclaimed AI-assisted productivity software that is primarily marketed via social media (@typerdexapp) and an AI-generated Medium blog (*medium[.]com/@typerdexapp*). Traffers associated with TyperDex receive a manual for engaging with prospective victims. TyperDex is associated with the Crazy Evil subteam **TYPED** — also stylized as "**TypeD**" — which is managed by Telegram user @dvllu. Insikt Group tracks this cluster of activity as **CE-2**.

Unlike Voxium, the TyperDex launcher does not require a code to download. This means that TyperDex is openly accessible to any website visitor who happens to stumble across it. TyperDex is indexed by most major search engines, as is every other Crazy Evil phishing page, suggesting that Crazy Evil likely employs SEO poisoning as one of its tactics.

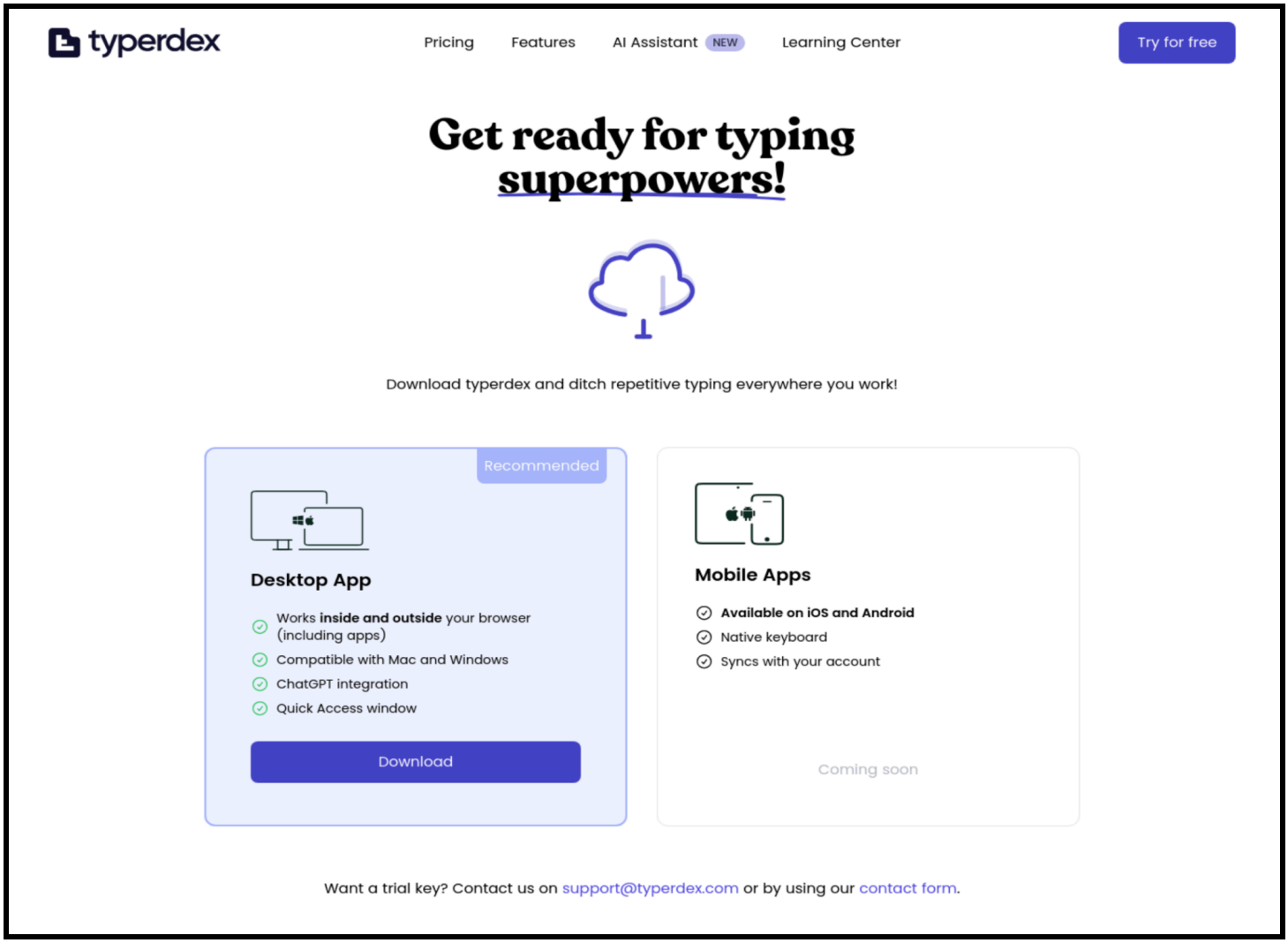

***Figure 14**: TyperDex landing page at typerdex[.]ai (Source: Recorded Future)*

For Windows users, the TyperDex website redirects to Dropbox (*dropbox[.]com/scl/fi/loqgll5mweihyz18zop97/TyperDexSetup.exe?rlkey=5glhygglqa5hipe7yjyvz2ez8&st=ex6×4ear&dl=1*) to download `TyperDexSetup.exe`. For macOS users, the TyperDex website redirects to *iiyoiiyo[.]com* and runs the script `kusaka.php?call=typer` before downloading `TyperDexSetup_v.4.85.dmg`. Insikt Group notes that this same `kusaka.php` was observed in the Voxium case above, but used a different `call` parameter to download TyperDex.

As of December 2, 2024, the TyperDex Windows build has been removed from Dropbox. For the existing Windows builds that Insikt Group has obtained, the access codes found in open sources and obtained via proprietary means no longer function. This prevents the TyperDex Windows build from downloading its second-stage infostealer payloads and communicating with its command-and-control (C2) at the present time. However, we note that the TyperDex macOS build still functions properly and provides valuable insights into the CE-2 operation, sharing its C2 with Voxium. While AMOS administrative panels and C2s are often recycled between unrelated customers, we note that traffer teams openly acknowledge that they share AMOS panels, C2s, and builds between each subteam for easier collaboration. This also enables the automation of team-specific "logbar" channels, described above.

Filename	Malware Tags	C2	Malware Intelligence
`TyperDexSetup.exe`	N/A	N/A	Triage
`TyperDexSetup_v.4.85.dmg`	N/A (AMOS)	141.98.9[.]20	Triage

***Table 6**: Sandbox analyses of TyperDex Windows and macOS builds (Source: Recorded Future)*

Domain	ASN	First Seen	Last Seen	Status
typerdex[.]ai	NAMECHEAP-NET, US (AS22612)	2024-09-22	2024-12-02	Active
typerdex[.]io	NAMECHEAP-NET, US (AS22612)	2024-03-30	2024-11-17	Inactive
typerdex[.]team	NAMECHEAP-NET, US (AS22612)	2024-07-03	2024-07-08	Inactive
typerdex[.]com	NAMECHEAP-NET, US (AS22612)	2024-01-14	2024-12-02	Active

***Table 7**: TyperDex website infrastructure (Source: Recorded Future)*

DELAND (CE-3)

DeMeet is a self-proclaimed "community development" platform with message- and audio-based chat, event planning, and brand loyalty functionalities. However, it does not perform any of these functions and instead delivers an infostealer payload. DeMeet is primarily advertised on social media (@demeetapp) and Telegram (@demeetapp). Traffers associated with DeMeet are provided with a whitepaper on the project (*demeet[.]gitbook[.]io*) and Linktree page (*linktr[.]ee/demeetapp*) to further legitimize the scam. DeMeet is operated by the Crazy Evil subteam **DELAND** — also stylized as "**DeLand**", "**Deland**", or "**DeLanding**" — which Insikt Group tracks as **CE-3**. This subteam has several administrators, curators, and support members, including Telegram users @wmwrk, @workersupport, @NameOfLucky, and @letosnay, among others.

Similar to **TyperDex** (**CE-2**), DeMeet does not require an access code to initiate a download. DeMeet also allows landing page visitors to generate their own access codes via the "create room" function, thus bypassing restrictions on unauthorized access to the DeMeet payload. Insikt Group was able to easily procure access to both the Windows and macOS builds of DeMeet; however, as of December 2, 2024, the Windows version of DeMeet is inoperable. The build will stall indefinitely and crash before it has a chance to download its second-stage payload and establish communication with its C2. The Windows build repeatedly contacts *connectcall[.]top* in an attempt to retrieve suspected infostealer payloads named `RIntelInstallator-AKdaAB.exe` and `SIntelInstallator-LAsjC2D.exe`, but fails to do so. It is possible that these builds have been moved. Recorded Future Malware Intelligence reports for the Windows build of DeMeet can be found in **Table 8**.

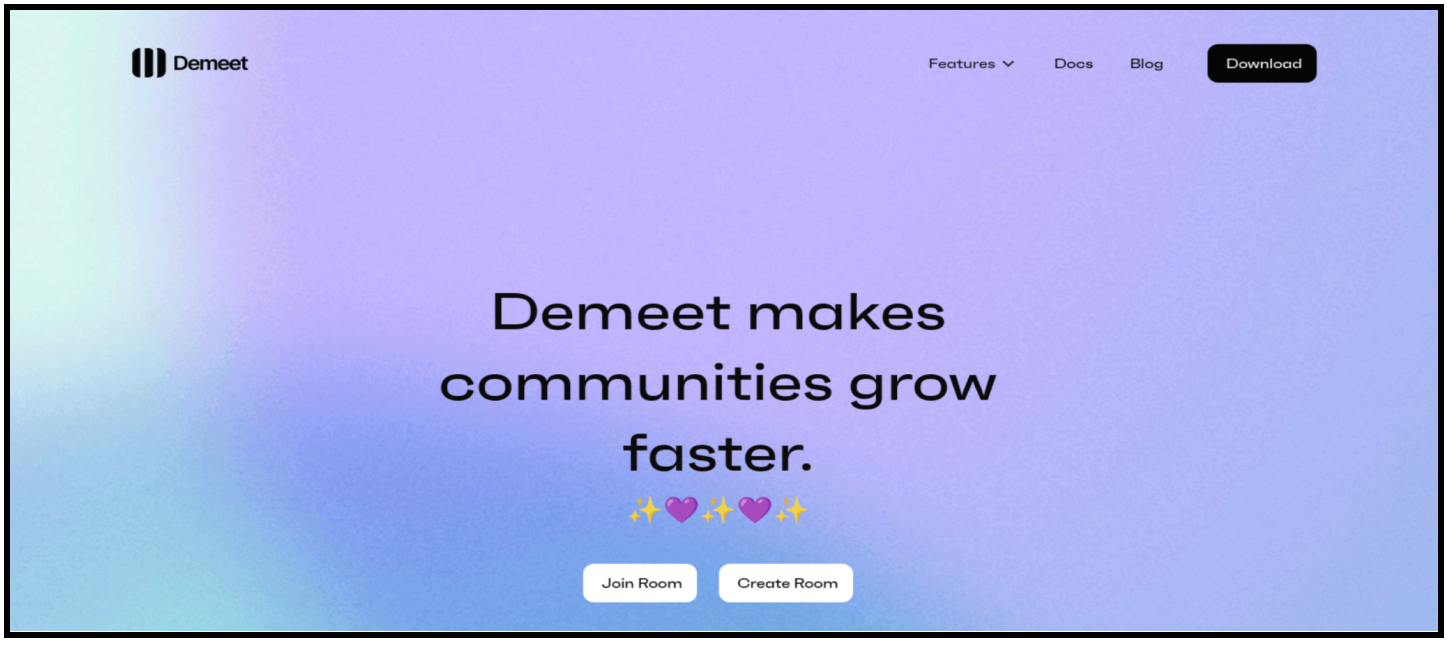

***Figure 15**: DeMeet landing page at demeet[.]app (Source: Recorded Future)*

For Windows users, the DeMeet website redirects to Dropbox (*dropbox[.]com/scl/fi/wvcmuli543l3l1nmjxwya/DemeetApp.exe?rlkey=dwpyays8uaky25hrrijhwgzfa&st=54msfi5l&dl=1*) to download `DemeetApp.exe`. For macOS users, the DeMeet website redirects to the same *iiyoiiyo[.]com* domain — observed in the TyperDex scam above — and runs the same `kusaka.php` script with the parameter `call=demeet`. This downloads `DemeetApp_v.5.42.dmg`, another build of AMOS that communicates with the same *141.98.9[.]20* C2 seen in both the Voxium and TyperDex scams above.

Filename	Malware Tags	C2	Malware Intelligence
`DemeetApp.exe`	N/A	N/A	Triage
`DemeetApp_v.5.42.dmg`	N/A (AMOS)	141.98.9[.]20	Triage

***Table 8**: Sandbox analyses of DeMeet Windows and macOS builds (Source: Recorded Future)*

Domain	ASN	First Seen	Last Seen	Status
demeet[.]app	AS-REGRU (AS197695)	2024-07-24	2024-12-02	Active
demeetapp[.]com	AS-REGRU (AS197695)	2024-10-01	2024-11-19	Defunct
demeet[.]site	EXIMIUS-AS, RU (AS207027)	2022-11-17	2024-12-02	Active
demeet[.]online	CLOUDFLARENET, US (AS13335)	2024-10-15	2024-12-02	Active

***Table 9**: Websites attributed to the DeMeet scam (Source: Recorded Future)*

ZOOMLAND (CE-4)

Crazy Evil subteam **ZOOMLAND** — tracked by Insikt Group as **CE-4** — is responsible for running various generic scams impersonating the Zoom meeting software (for English-speaking targets) and WeChat (for Chinese-speaking targets). Insikt Group notes that CE-4 is the only cluster of Crazy Evil threat activity we observed that explicitly targets Chinese victims. It is a common practice among traffer teams to have at least one subteam dedicated to casting a wide net by impersonating legitimate software like Zoom, WeChat, Google Meet, Microsoft Teams, Slack, and so forth. These scams capitalize on well-established brands to build trust but are less resilient and more prone to takedowns.

Insikt Group notes that ZOOMLAND is operated by the Telegram user @dvllu, who also runs **TYPED** (**CE-2**), described above. It is unclear why "dvllu" runs two separate teams, but it is clear that this threat actor has a significant amount of influence over Crazy Evil's operations.

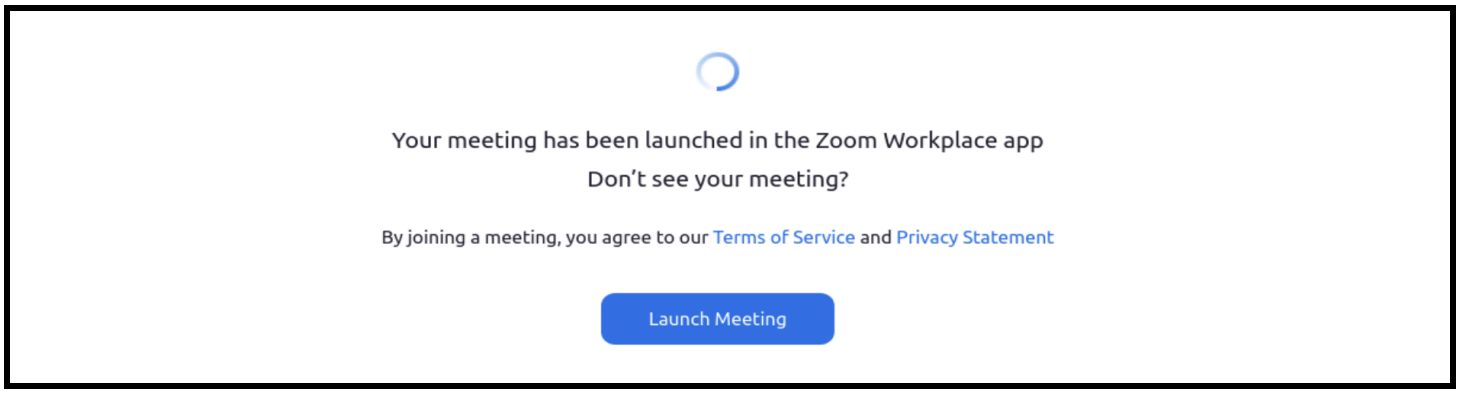

***Figure 16**: Zoom impersonator landing page at app.us4zoom[.]us (Source: Recorded Future)*

For Windows users, the Zoom landing page redirects to Dropbox (*dropbox[.]com/scl/fi/cufs9mlcndluscjovrl53/ZoomInstallerFull.exe?rlkey=fwjxifn34i3tj7hcv44jrsy4c&st=8powy1e8&dl=1*) to download `ZoomInstallerFull.exe`. For macOS users, the Zoom landing page redirects to the same *iiyoiiyo[.]com* observed above and runs the same `kusaka.php?call=prv` to download `Zoom_v.4.83.dmg`. Insikt Group was not able to identify any valid codes shared in open sources to initiate the Windows build installer, but notes that the AMOS C2 on macOS is the same as observed in all of the scams above.

As of December 2, 2024, the landing page for the WeChat scam is offline at *app-whechat[.]com*. Insikt Group was not able to identify any mirrors or related domains; therefore, we were not able to procure any downloads associated with this scam. The most recent active link known to Insikt Group used the access code `5732-1467`. It is currently unclear whether CE-4 plans to relaunch or rebrand its WeChat scam, but Insikt Group could not identify any malware submissions or open-source reports that overlap with this activity.

Filename	Malware Tags	C2	Malware Intelligence
`ZoomInstallerFull.exe`	N/A	N/A	Triage
`Zoom_v.4.83.dmg`	N/A (AMOS)	141.98.9[.]20	Triage

***Table 10**: Sandbox analyses of Zoom impersonator Windows and macOS builds (Source: Recorded Future)*

Domain	ASN	First Seen	Last Seen	Status
app.us4zoom[.]us	CLOUDFLARENET, US (AS13335)	2024-11-23	2024-12-02	Active

***Table 11**: Zoom impersonator website infrastructure (Source: Recorded Future)*

DEFI (CE-5)

Selenium Finance is a self-proclaimed digital asset management platform that is primarily advertised on social media (@seleniumfinance) and an AI-generated Medium blog (*medium[.]com/@defiselenium*). Traffers assigned to Selenium Finance receive Russian-language manuals on scamming, the concept of being a traffer, and strategies for working victims. Selenium Finance also has its own ERC-20 token to further increase legitimacy. Selenium Finance is managed by **DEFI** — also stylized as "**DeFi**", which is a reference to "decentralized finance" and the type of scams that this subteam operates — which Insikt Group tracks internally as **CE-5.** CE-5 is operated by Telegram users @shivag0d and @goyxard.

As of December 2, 2024, the Windows build of Selenium Finance has been removed from Dropbox. CE-5 has not provided an alternative download link, and Insikt Group has not observed any discussions in open sources or submissions to Recorded Future Malware Intelligence resembling a Windows build for Selenium Finance. The macOS version is active and can be downloaded at the same domain described several times above — *iiyoiiyo[.]com*. For this build, the domain uses the script `kusaka.php?call=defi` to retrieve `DeFi_Run_Bot_v.4.89.dmg`.

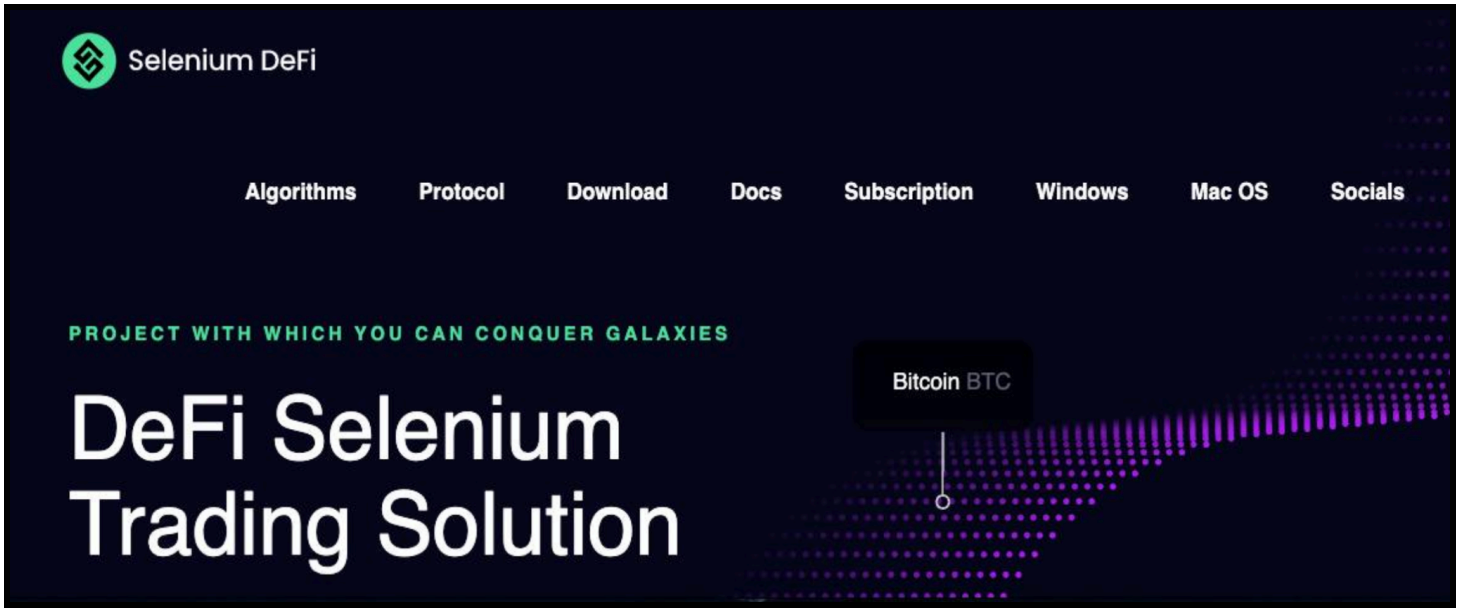

***Figure 17**: Selenium Finance landing page at selenium[.]fi (Source: Recorded Future)*

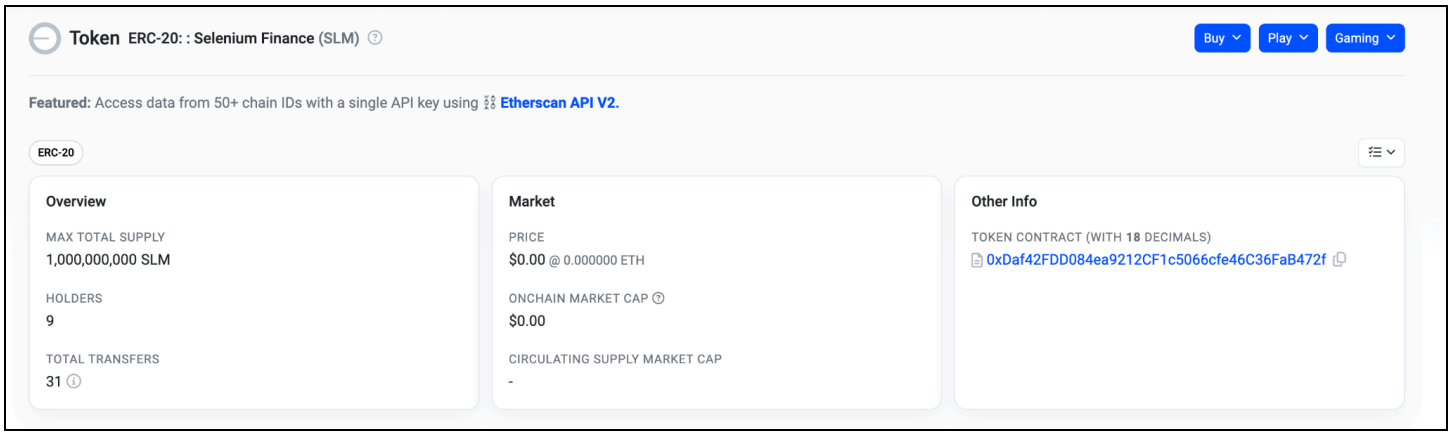

***Figure 18**: Selenium Finance ERC-20 token (Source: BaseScan)*

Filename	Malware Tags	C2	Malware Intelligence
`DeFi_Run_Bot_v.4.89.dmg`	N/A (AMOS)	141.98.9[.]20	Triage

***Table 12**: Selenium Finance macOS builds (Source: Recorded Future)*

Domain	ASN	First Seen	Last Seen	Status
selenium[.]fi	CLOUDFLARENET, US (AS13335)	2024-10-23	2024-12-02	Active

***Table 13**: Websites attributed to the Selenium Finance scam (Source: Recorded Future)*

KEVLAND (CE-6)

Gatherum is a self-proclaimed AI-enhanced virtual meeting software that is primarily advertised on social media (@GatherumAI) and an AI-generated Medium blog (*medium[.]com/@GatherumApp*). Traffers assigned to Gatherum are provided with a manual for working the scam. Gatherum is managed by Crazy Evil subteam **KEVLAND**, tracked internally by Insikt Group as **CE-6**.

In order to download the Gatherum builds for Windows and macOS, a user needs to input an access code on the Gatherum landing page to “join a room” — similar to Voxium. CE-6 maintains specific channels on Telegram that issue and generate access codes for traffers. However, we note that this access code functionality is currently broken on the landing page, allowing users to download Gatherum without inputting anything. This allowed Insikt Group to download builds for both Windows and macOS.

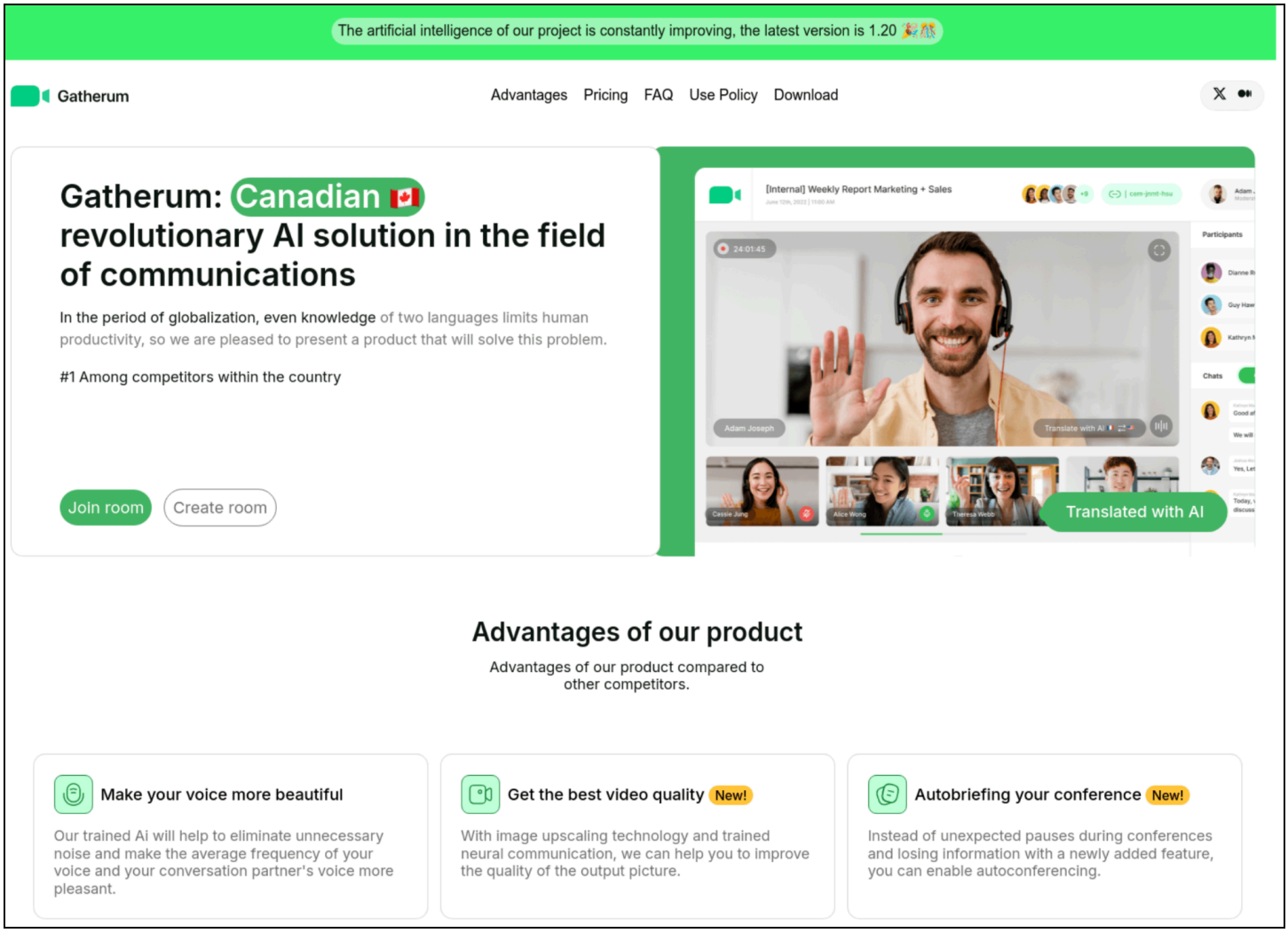

***Figure 19**: Gatherum landing page at gatherum[.]ca (Source: Recorded Future)*

For Windows users, the Gatherum website redirects to Dropbox (*dropbox[.]com/scl/fi/x896zkpxljpx426shp515/GatherumSetup.exe?rlkey=hjptce7ftkbr98gjkwdl8xy4h&st=k2e4u0xf&dl=1*) to download `GatherumSetup.exe`. For macOS users, the Gatherum website redirects to *iiyoiiyo[.]com* and runs the script `kusaka.php?call=gatherum` to download `Gatherum_v.6.97.dmg`. Insikt Group notes that the macOS build of Gatherum uses the same *141.98.9[.]20* C2 seen throughout this report, with every AMOS build attributed to Crazy Evil.

As of December 2, 2024, the Windows build of Gatherum is inoperable and does not download its second-stage infostealer payloads; therefore, it does not establish a connection with its C2.

Filename	Malware Tags	C2	Malware Intelligence
`GatherumSetup.exe`	N/A	N/A	Triage
`Gatherum_v.6.97.dmg`	N/A (AMOS)	141.98.9[.]20	Triage

***Table 14**: Gatherum Windows and macOS builds (Source: Recorded Future)*

Domain	ASN	First Seen	Last Seen	Status
gatherum[.]ca	CLOUDFLARENET, US (AS13335)	2024-09-16	2024-12-02	Active
gatherum[.]net	CLOUDFLARENET, US (AS13335)	2018-08-01	2024-09-06	Inactive
gatherum[.]one	CLOUDFLARENET, US (AS13335)	2024-07-26	2024-12-02	Active
gatherum[.]cc	AEZA-AS, GB (AS210644)	2024-07-16	2024-11-11	Inactive

***Table 15**: Gatherum website infrastructure (Source: Recorded Future)*

Mitigations

- **Enhance Endpoint Protection**: Deploy advanced endpoint detection and response (EDR) solutions to monitor for and block the execution of known malware families associated with Crazy Evil — such as Rhadamanthys, Stealc, and AMOS. These specific tools, in combination with social media scams, are immediate indicators of a Crazy Evil attack.
- **Web Filtering and Monitoring**: Deploy web filtering solutions to block access to known malicious domains linked to Crazy Evil — including all of the domains listed in this report — as well as suspicious downloads, especially those related to cracked “freemium” software.
- **Continuous Threat Intelligence Monitoring**: Regularly update threat intelligence feeds with the latest indicators of compromise (IoCs) related to Crazy Evil. Ensure that security teams are aware of the latest tactics, techniques, and procedures (TTPs) employed by the group.
- **User Awareness and Training**: Implement ongoing cybersecurity awareness training for employees, emphasizing the risks associated with phishing, social engineering, and suspicious downloads. Include specific modules on the risks posed by cryptocurrency-targeted attacks used by Crazy Evil.
- **Collaboration and Information Sharing**: Collaborate with industry peers, threat intelligence organizations, and law enforcement agencies to share information on Crazy Evil and similar threats. Engage in cross-sector initiatives to improve collective defenses against advanced cybercriminal groups.
- **Enhanced Regulatory Compliance**: Stay ahead of evolving regulatory requirements related to data protection and cybersecurity. Ensure that your organization’s practices align with both

domestic and international standards, particularly in industries like finance, where Crazy Evil's attacks could have severe consequences.

- **Recorded Future**: Insikt Group recommends using Recorded Future Malware Intelligence to identify build IDs, C2 infrastructure, staging domains, and other malicious indicators associated with the Crazy Evil scams described above. Using both Recorded Future Malware Intelligence and Recorded Future Network Intelligence can better identify and cluster infostealer activity, providing initial indications of infections, victimology, and pivoting scams.

Outlook

In the short term, individuals and organizations will face a surge in credential theft, unauthorized transactions, and digital asset losses as cybercriminal groups like Crazy Evil hone their social engineering tactics. Cryptocurrency enthusiasts, NFT traders, and gaming professionals — who often use platforms with minimal regulatory oversight — are prime targets. As Crazy Evil continues to achieve success, other cybercriminal entities are likely to emulate its methods, compelling security teams to remain perpetually vigilant to prevent widespread breaches and erosion of trust within the cryptocurrency, gaming, and software sectors.

Looking ahead to the medium and long term, the rise of Web3 technologies and decentralized finance will fundamentally transform the global cybersecurity landscape. As these technologies become increasingly mainstream and incorporated into everyday life, especially in business, cybercriminal groups that exclusively work in this space will become uniquely positioned to capitalize on wider adoption. Traffer teams like Crazy Evil are well-equipped to exploit these emerging ecosystems by utilizing advanced tools, resilient infrastructures, and sophisticated phishing schemes tailored to specific platforms and user bases. Crazy Evil has spent several years directly targeting the Web3 and decentralized finance ecosystem, discussing major developments, related news, emerging start-ups, and other topics in its private team chats.

Crazy Evil's strong presence on dark web forums, its alliances with rival gangs and malware developers, and the robust obfuscation techniques it incorporates into its scams will likely result in more enduring threats that are difficult to detect and neutralize. Threat groups like Crazy Evil are resilient to identification and disruption — the biggest threat to their operations comes from internal strife. When threat groups like Crazy Evil increase in membership and expand operations, exit scamming and splintering are more likely to be their downfall, as seen with Marko Polo and CryptoLove.

Appendix A — Indicators of Compromise

Domains:

tokenframegovernance[.]com
voxiumcalls[.]com
voxium[.]eu
voxiumhub[.]com
voxium[.]cloud
rocketgalaxy[.]io
rocketgalaxy[.]xyz
rocketgalaxyworld[.]com
playrocketgalaxy[.]com
rocketlegacy[.]xyz
ccdcompany[.]online
ultima-dapp[.]online
ultimadapp[.]online
solanasms[.]com
watcherbot[.]xyz
secretum[.]io
iiyoiiyo[.]com
typerdex[.]ai
typerdex[.]io
typerdex[.]team
typerdex[.]com
demeet[.]app
demeetapp[.]com
demeet[.]site
demeet[.]online
app.us4zoom[.]us
app-whechat[.]com
selenium[.]fi
gatherum[.]ca
gatherum[.]net
gatherum[.]one
gatherum[.]cc

IP Addresses:

178.22.31[.]97
141.98.9[.]20

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access: Spearphishing Attachment	T1566.001
Initial Access: Spearphishing Link	T1566.002
Initial Access: Drive-by Compromise	T1189
Execution: User Execution - Malicious File	T1204.002
Defense Evasion: Obfuscated Files or Information	T1027
Credential Access: OS Credential Dumping	T1003
Discovery: System Information Discovery	T1082
Collection: Data from Local System	T1005
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Exfiltration: Exfiltration Over C2 Channel	T1041
Exfiltration: Automated Exfiltration	T1020

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com