2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

UNMASKING GRASSCALL CAMPAIGN: THE HACKERS BEHIND JOB RECRUITMENT CYBER SCAMS

Dixit Panchal & Soumen Burma

Quick Heal Technologies, India

dixit.panchal@quickheal.com
soumen.burma@quickheal.com

ABSTRACT

The 'GrassCall' campaign exploits the job recruitment process to execute cyber scams, primarily targeting individuals in the cryptocurrency and Web3 sectors. Orchestrated by the Russian-speaking threat actor 'Crazy Evil', this campaign leverages a combination of social engineering, malicious software, and advanced information-stealing tactics to compromise victims' systems and access sensitive data.

We have analysed the campaign in detail. The operation begins with the creation of fraudulent companies, complete with authentic-looking websites and active profiles on professional platforms like *LinkedIn*. These entities post high-quality job listings to lure candidates. Once victims engage, communication transitions to encrypted messaging platforms like *Telegram*, where candidates are directed to download a custom video-conferencing application named 'GrassCall' from malicious domains (e.g. 'grasscall[.]net').

INTRODUCTION

The GrassCall malware campaign represents an advanced social engineering attack carried out by a Russian-speaking cybercriminal organization referred to as Crazy Evil, with its subgroup, 'kevland', leading the operation. The campaign specifically targets job seekers in the cryptocurrency and Web3 sectors, using fake job interview schemes to compromise victims' systems and steal their cryptocurrency assets.

Hundreds of people have been impacted by the scam, with some reporting having their wallets drained in the attacks.

OVERVIEW OF THREAT ACTOR

Crazy Evil is a Russian-speaking cybercriminal organization that has evolved rapidly since its inception in 2021, becoming one of the most prolific groups targeting digital assets. The group specializes in identity fraud, cryptocurrency theft, and the deployment of information-stealing malware. Their operations are characterized by sophisticated social engineering tactics, often involving the use of 'traffers' – social engineering experts who redirect legitimate traffic to malicious phishing pages.

Potential affiliates are invited to apply through the Crazy Evil *Telegram* bot (@CrazyEvilNft_bot), which grants them access to further application steps and exclusive private channels. According to its administrators, Crazy Evil offers top-tier manuals and ongoing support specifically tailored for its traffers. The group also provides training sessions in audio and video formats led by native speakers, along with services like malware 'checkers' and 'crypters' to help prepare malicious payloads. Additionally, there are dedicated channels for sharing information on potential victims.

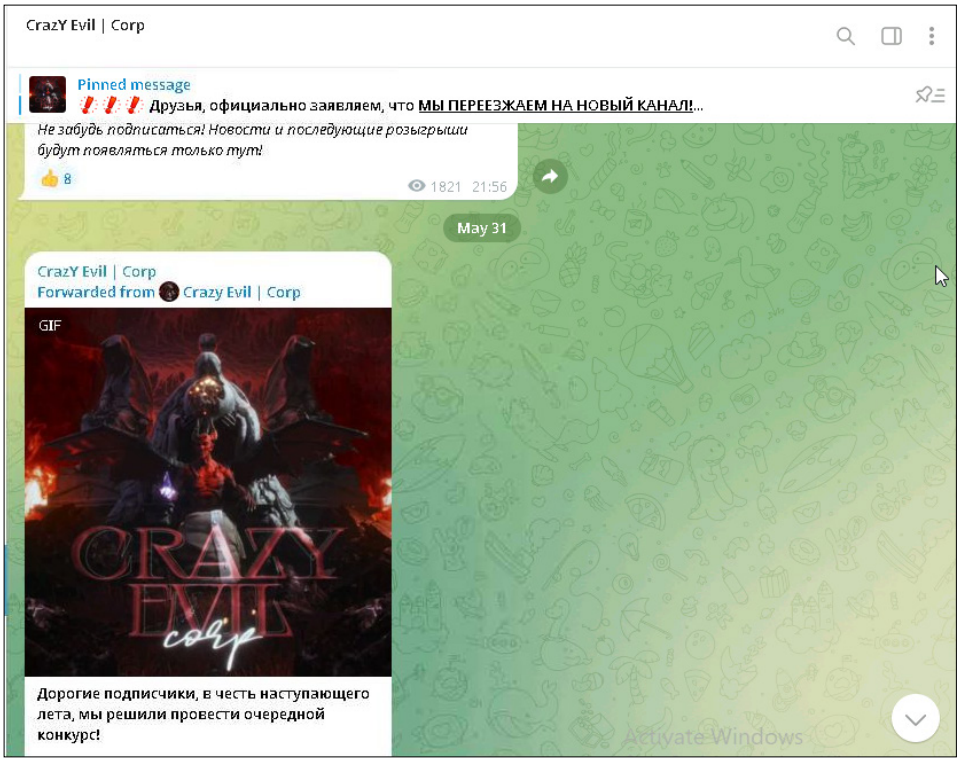


Figure 1: Crazy Evil Corp Telegram channel.

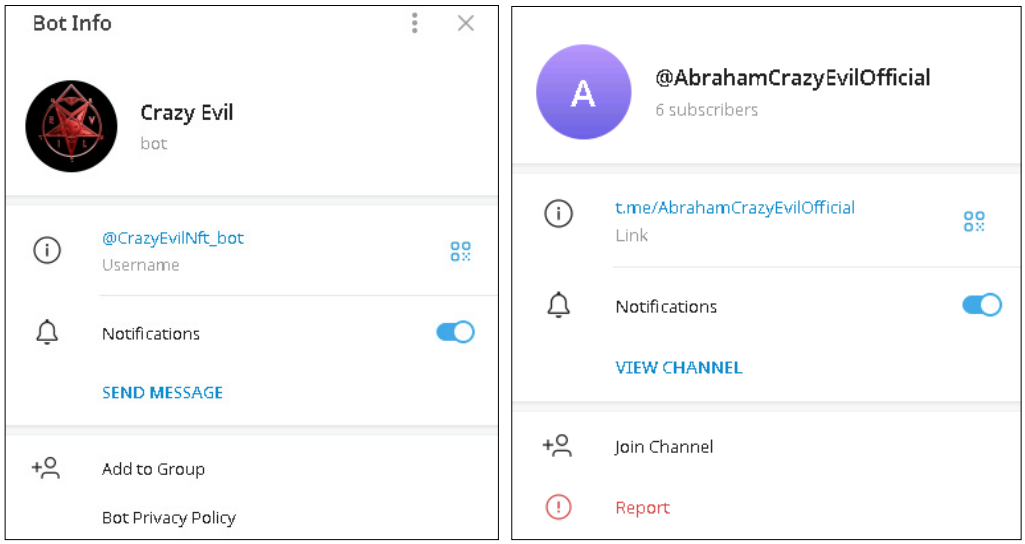


Figure 2: Telegram profiles of the Crazy Evil bot (left) and Abraham, the alleged leader of Crazy Evil (right).

Beyond its main *Telegram* channels, Crazy Evil also manages two primary information-focused channels and a private discussion group for its traffers:

- 'Crazy Evil | Corp' (@CrazyEvilCorp): This functions as the organization's central hub, with a membership of over 3,000 at the time of writing.
- 'Info | Crazy Evil': A dedicated update channel that delivers frequent administrative and technical news to the group's traffers. It currently has more than 4,000 subscribers.
- 'Global Chat | Crazy Evil': The main discussion space for traffers, where conversations range from official work matters to casual meme sharing. This group also has a member count exceeding 4,000.

INFECTION CHAIN

Figure 3 shows the chain of execution in the GrassCall malware campaign.

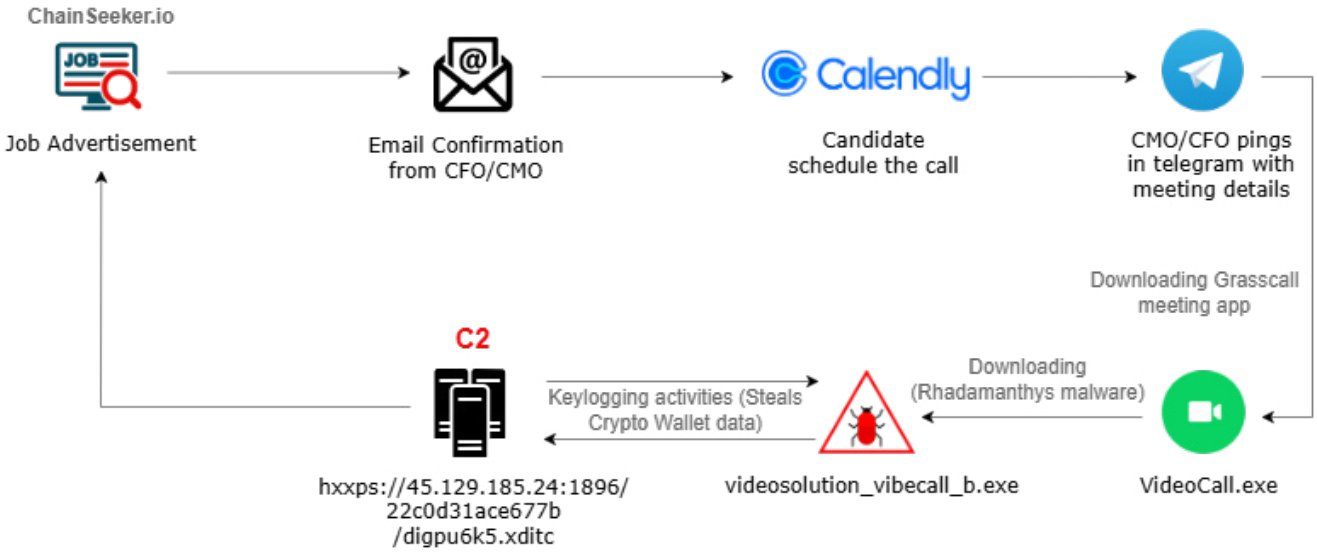


Figure 3: Chain of execution.

ATTACK TACTICS AND APPROACH

First, the attackers set up a fabricated business, such as 'ChainSeeker.io', for which they create a professional-looking website and active social media accounts on platforms like *LinkedIn* and *X* (formerly *Twitter*).

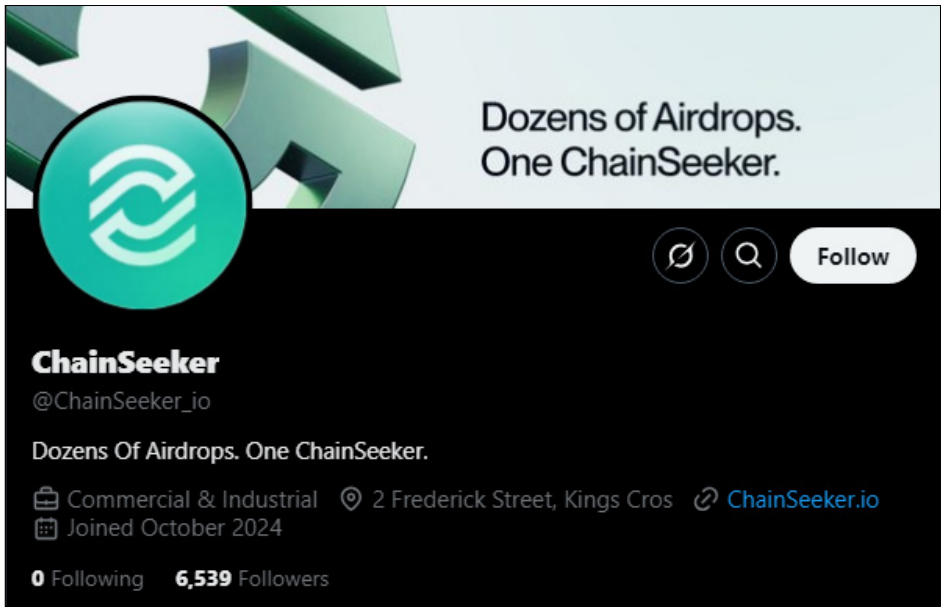


Figure 4: Fake company profile on X (Twitter).

Next, the attackers publish job advertisements on reputable job boards such as *LinkedIn*, *Well-found* and *Crypto Jobs List*, to attract unsuspecting applicants.

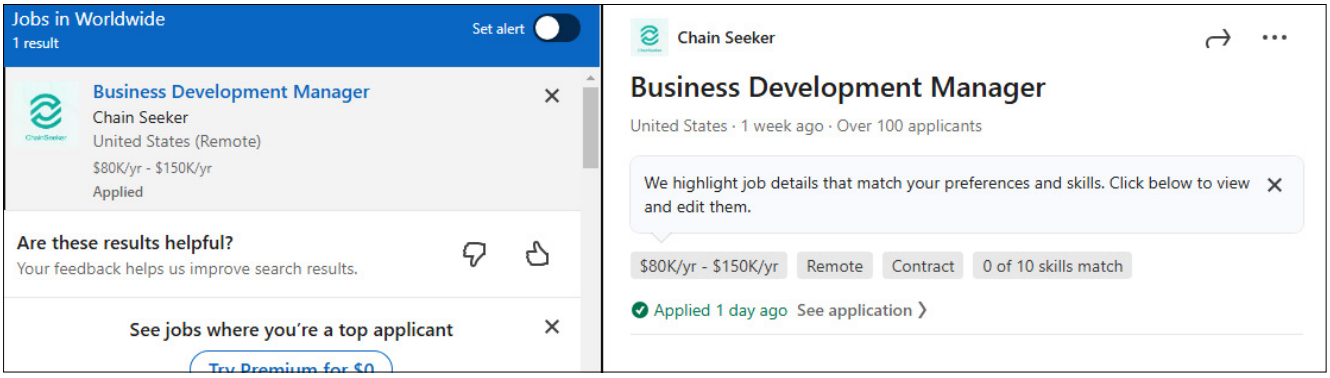
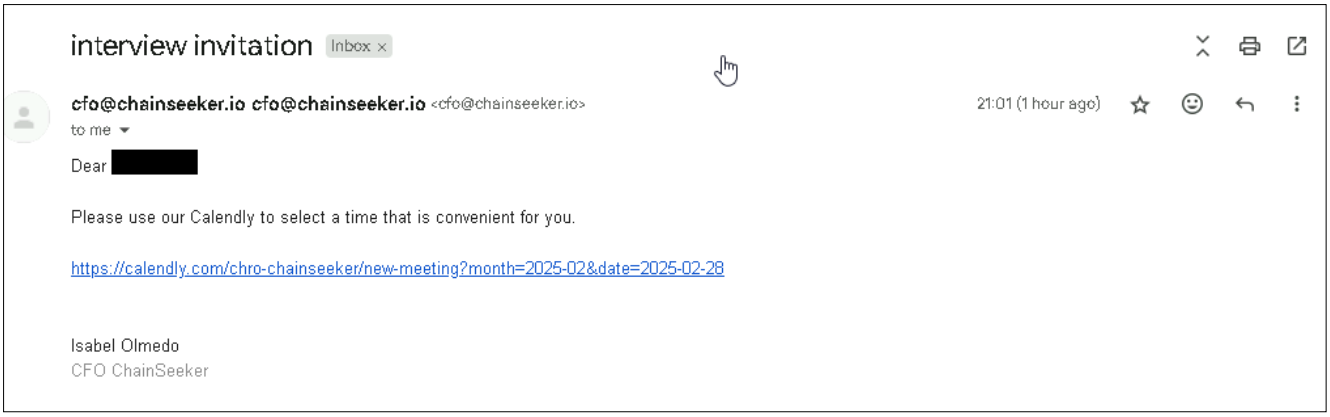


Figure 5: Job advertisement on LinkedIn.

When an interested candidate responds to the job postings on social media, they receive an email inviting them to interview with senior company officials, such as the Chief Marketing Officer (CMO) or Chief Finance officer (CFO). The conversation then transitions to *Telegram*, where the impersonated CMO/CFO provides further directions.



.Figure 6: Email to schedule interview call.

The conversation transitions to Telegram, where candidates are invited to schedule a call using *Calendly*, allowing them to select a suitable time slot.

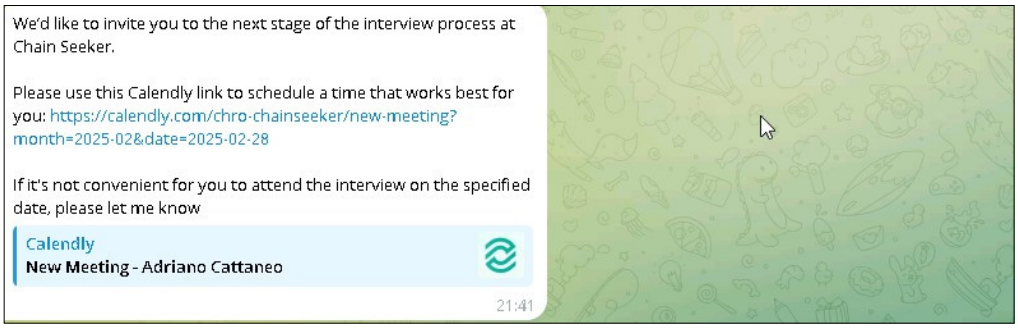


Figure 7: Telegram ping from impersonated CFO.

Once the candidate has scheduled their call within the chosen time frame, they receive confirmation of the call.

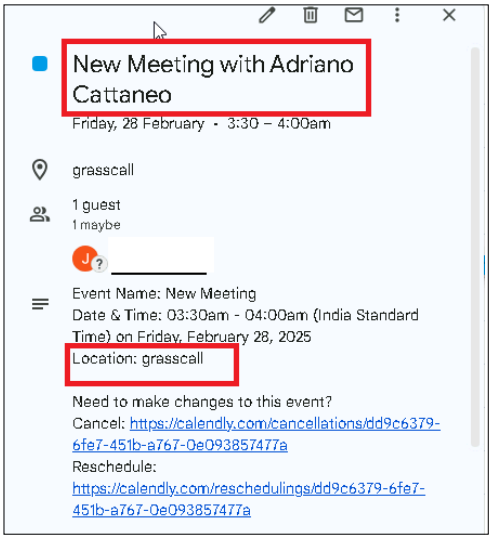


Figure 8: Details of scheduled call.

Just before the call, the CFO/CMO contacts the candidate again, directing them to join the call via a video conferencing application named 'GrassCall', and providing a link to download the application from a specific website (e.g. grasscall[.]net), as well as an access passcode.

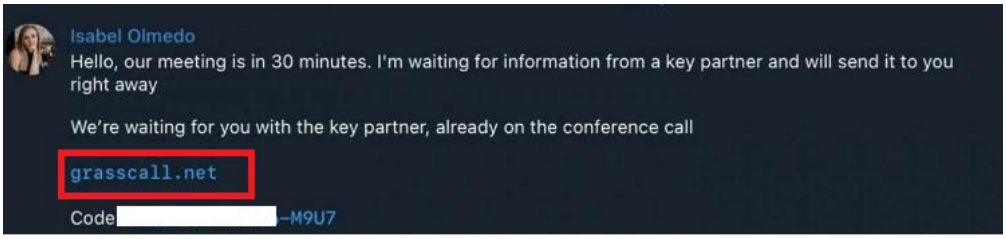


Figure 9: CFO directs the candidate to browse GrassCall[.]net.

Access to the download requires the code provided during the *Telegram* conversation. The website detects the visitor's operating system and offers the corresponding malicious client.

Figure 10: GrassCall.net.

In our ongoing research, we have identified that adversary has recently rebranded their platform 'VibeCall' (https://vibecall[.]app/).

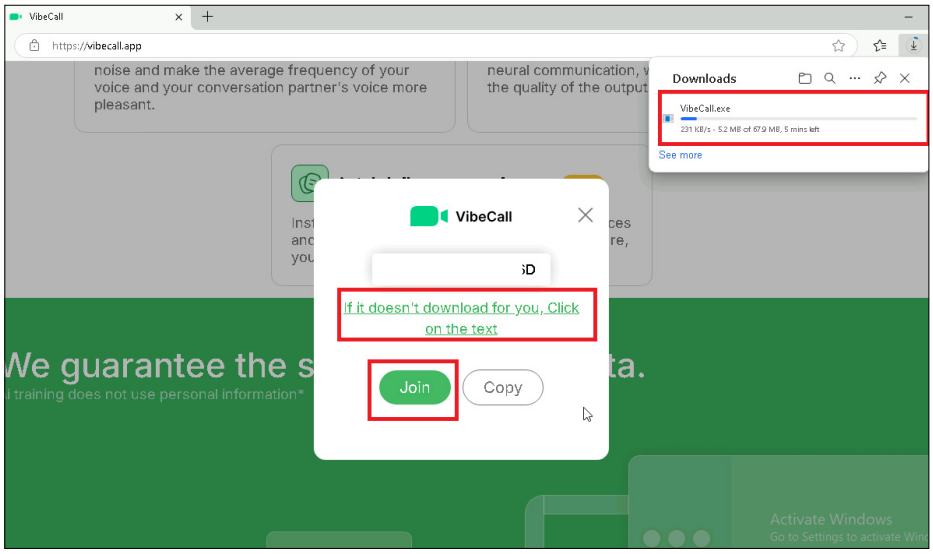


Figure 11: VibeCall[.]app.

Here, once the candidate enters their passcode to join the meeting VibeCall.exe will be downloaded, based on OS.

On *Windows* machines, installing GrassCall.exe (or VibeCall.exe) triggers the deployment of a Remote Access Trojan (RAT) combined with an information-stealing program like Rhadamanthys. These malicious tools enable attackers to maintain ongoing access, log keystrokes, and extract sensitive data, including cryptocurrency wallet credentials.

On *macOS* devices, installing GrassCall_v.6.10.dmg results in the activation of the Atomic macOS Stealer (AMOS), a tool specifically designed to harvest confidential data from *macOS* devices.

We have identified several platforms and tactics being utilized by the attackers. These methods are continuously evolving as they adapt their strategies to better target their audience.

Figure 12 shows the attackers utilizing fake organization 'Hyper Foundation' (hyperliquid[.]xyz) and targeting job seekers with the fake offer of a remote position.

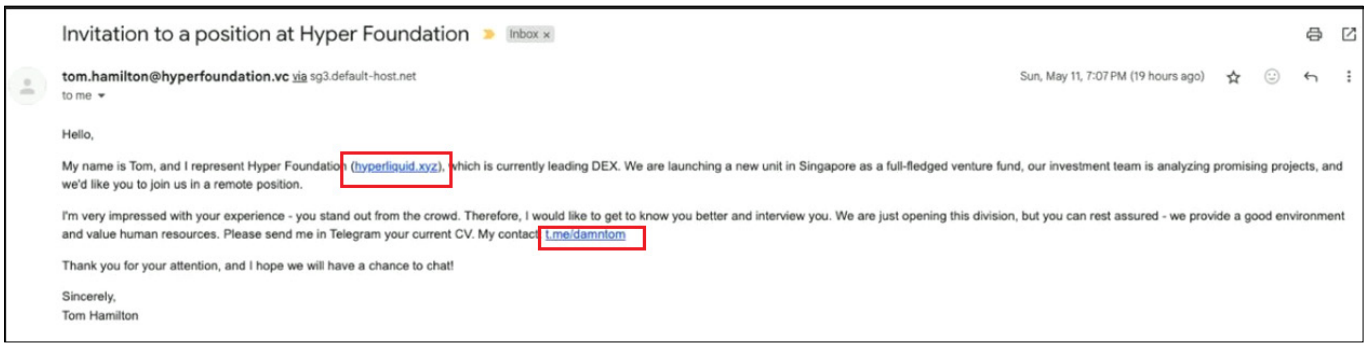


Figure 12: Email invitation to a position at Hyper Foundation.

TECHNICAL ANALYSIS OF GRASSCALL.EXE/ VIBECALL.EXE

VibeCall.exe is a 64-bit executable file that acts as an installer but is malicious in nature. Upon execution, it attempts to install and deploy the Rhadamanthys malware. Rhadamanthys is a sophisticated information-stealing trojan designed to harvest sensitive data, including login credentials, financial information, and system details.

Upon execution, it runs the Add-MpPreference command to add an exclusion path in *Microsoft Defender*. Specifically, it excludes the entire C: drive, causing *Defender* to completely bypass all files and folders on C: during its scans. This effectively disables *Defender*'s ability to detect or respond to any malicious activity occurring within the excluded drive.

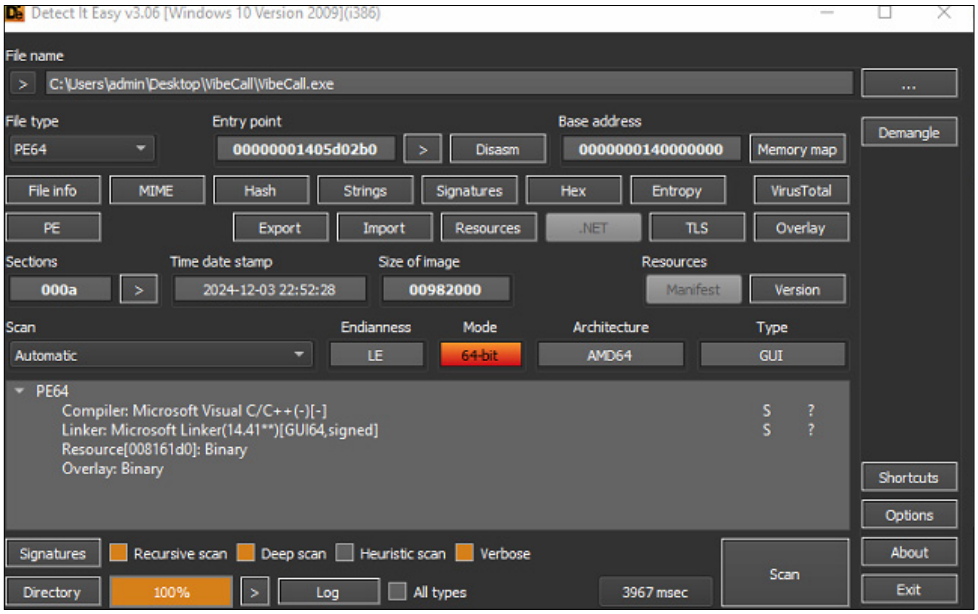


Figure 13: Win64 installer VibeCall.exe.

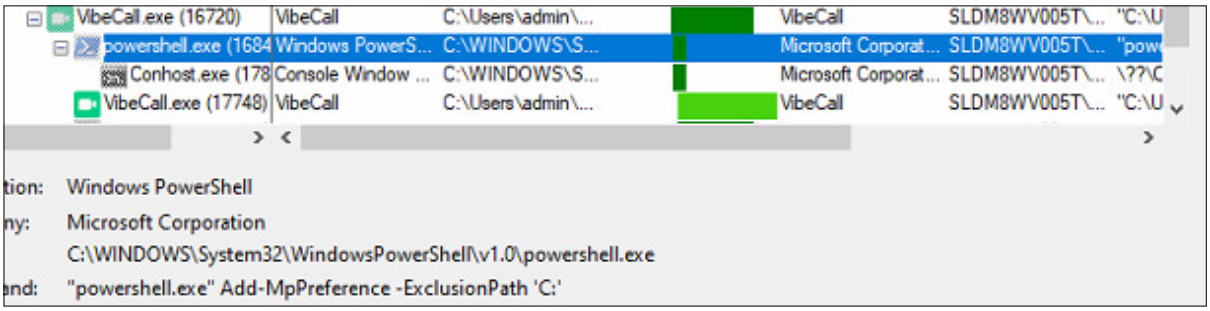


Figure 14: Add-MpPreference command via PowerShell.

It tries to download multiple Rhadamanthys malware samples and tries to execute it.

- http://rustaisolutionnorisk[.]com/downloads/contry_solution_vibecall_e.exe
  4b371777c2c638c97b818057ba4b0a2de246479776eaaacebccf41f467bb93c3
- http://rustaisolutionnorisk[.]com/downloads/aisolution_vibecall_a.exe
  f2e8f1f72abbc42f96c5599b8f27f620d91ae1680aa14b4f0bbf3daabd7bee30
- http://rustaisolutionnorisk[.]com/downloads/soundsolution_vibecall_c.exe
  d23f79f9b7e1872d4671a18aa85b810c0cec2e0f5ce07c2cf99ed39f8936c8fb
- http://rustaisolutionnorisk[.]com/downloads/videosolution_vibecall_b.exe
  386b61ccdd4b785c835a064179d5fa58dc0d5fe34970a04487968e1ee0189ce6

It drops the downloaded sample in the C:/Users/user/Documents folder and tries to execute it.

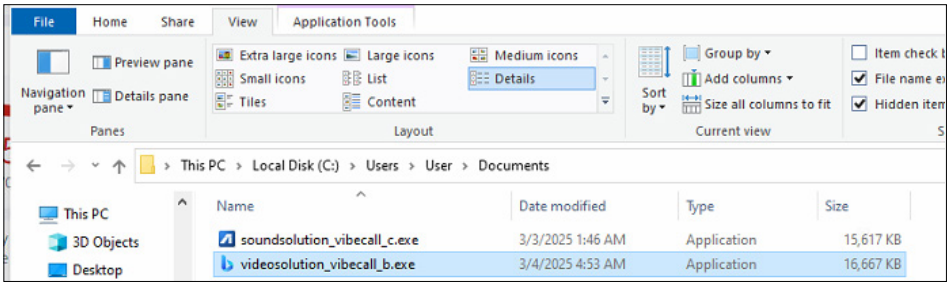


Figure 15: Downloading videosolution_vibecall_b.exe.

ANALYSIS OF RHADAMANTHYS MALWARE

Upon analysis of one of the Rhadamanthys samples (videosolution_vibecall_b.exe) we found that it is a 32-bit packed sample that contains shellcode.

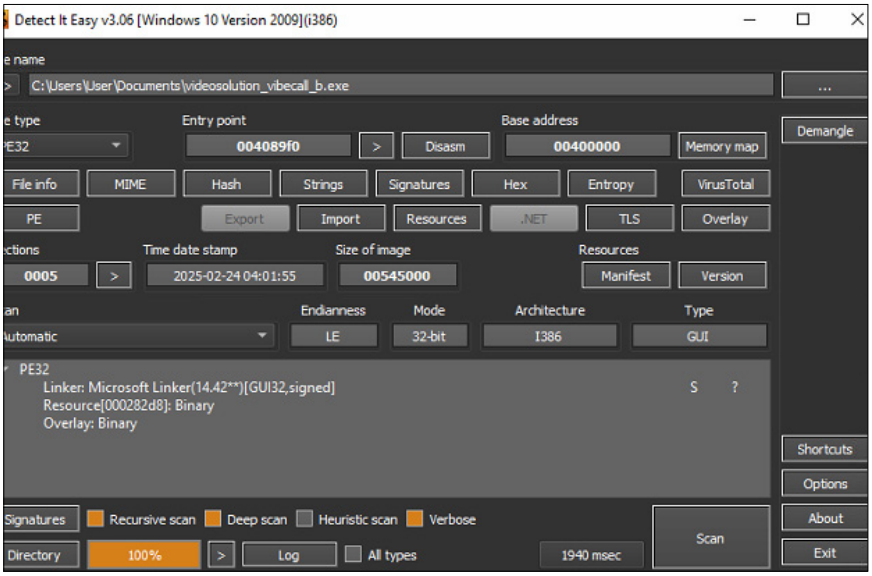


Figure 16: Ideosolution_vibecall_b.exe (Rhadamanthys stealer).

Upon unpacking we found the second payload of Rhadamanthys malware, as shown in Figure 17.

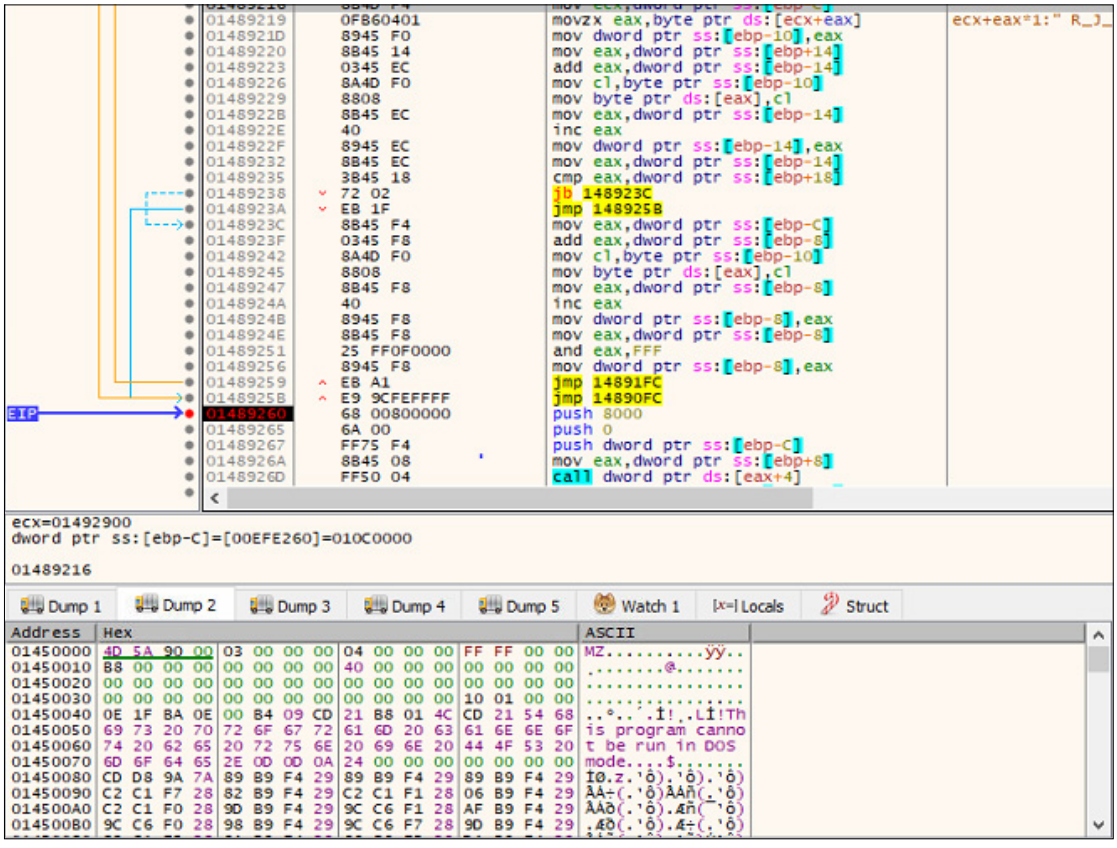


Figure 17: Unpacking second payload (sha256: 0160c14c3d84dcc5802a329a4d4bedcabd23b3a7761c1cd95d16bd0b7a7bb8eb).

The second payload contained a configuration file that attempts to establish a connection to a command-and-control server. The connection is directed to the URL:

hxxps://45.129.185.24:1896/22c0d31ace677b/digpu6k5.xditc

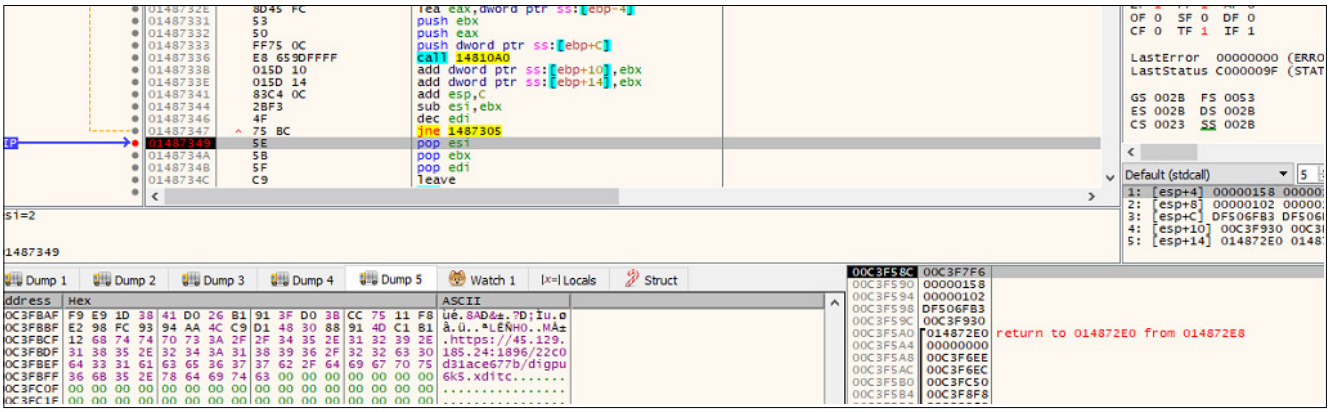


Figure 18: C2C config.

TTPs

Tactics	Techniques	ATT&CK code
Initial Access	Spear phishing Attachment	T1566.001
	Spear phishing Link	T1566.002
	Drive-by Compromise	T1189
Execution	User Execution – Malicious File	T1204.002
Defence 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
	Automated Exfiltration	T1020

PREVENTATIVE MEASURES

The following measures are recommended to prevent falling victim to a GrassCall or similar attack.

- Verify job opportunities: always confirm the authenticity of job opportunities and the companies offering them. Use official and verified channels to validate any recruitment-related communications.
- Exercise caution with downloads: avoid installing software from unknown or unverified sources, particularly when requested as part of unsolicited interactions.
- Install reliable security tools: utilize reputable anti-virus and anti-malware software to safeguard your system against threats.
- Conduct regular system checks: perform frequent scans on your device to detect and remove malware or other potentially harmful files.

IOCs

File name	Hash
VibeCall.exe	b63367bd7da5aad9afef5e7531cac4561c8a671fd2270ade14640cf03849bf52
videosolution_vibecall_b.exe	386b61ccdd4b785c835a064179d5fa58dc0d5fe34970a04487968e1ee0189ce6
contry_solution_vibecall_e.exe	4b371777c2c638c97b818057ba4b0a2de246479776eaaacebccf41f467bb93c3
aisolution_vibecall_a.exe	f2e8f1f72abbc42f96c5599b8f27f620d91ae1680aa14b4f0bbf3daabd7bee30