

SEQRITE | Quick Heal

UNMASKING GRASSCALL CAMPAIGN

The Hackers Behind **JOB RECRUITMENT CYBER SCAMS**





About Us



Dixit Panchal
Security Researcher
Seqrite Labs, Quick Heal
[@Dixit_404](#)



Soumen Burma
Senior Security Researcher
Seqrite Labs, Quick Heal
[@SOuMEn_B1](#)



Agenda

01 Overview of Campaign

02 Threat actor Behind the Scam

03 Infection Chain

04 Attack tactics & Approach

05 Analysis of Grasscall.exe

06 TTPs

07 Preventives Measures





Overview of Campaign

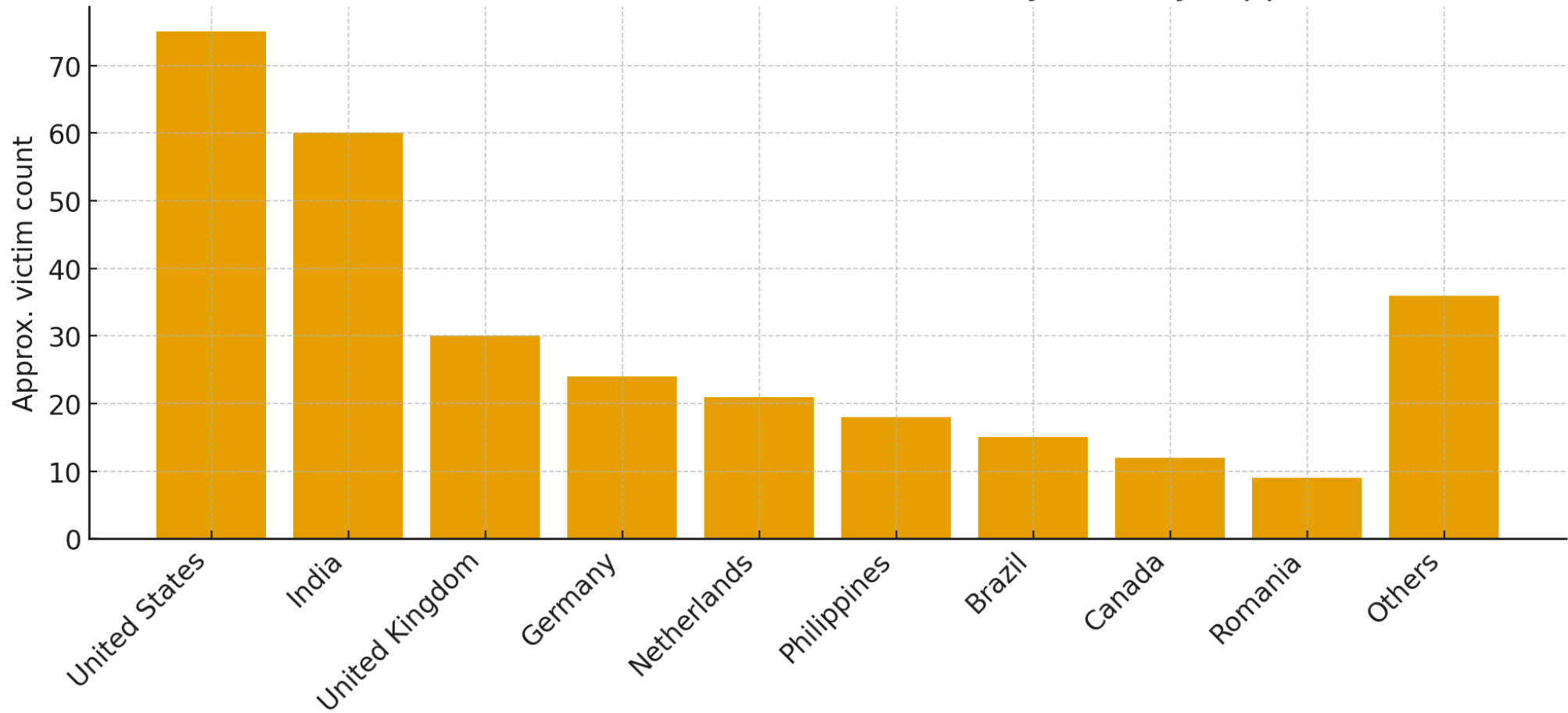


- The campaign was first observed in early **March 2025**. During ongoing monitoring of Telegram, Seqrite Labs identified the scam and its associated tactics
- It represents advanced attack techniques carried out by a well-known Russian-speaking cybercriminal organization known as "**Crazy Evil**" and its subgroup "Kevland"
- 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
- With this Hundreds of people have been impacted by the scam, with some reporting having their wallets drained in the attacks



Targeted Countries

Estimated number of GrassCall victims by country (approx)





- **Cryptocurrency & Web3:** Professionals in the blockchain and cryptocurrency industries are the primary targets
- **Freelancers & Remote Workers:** Individuals seeking remote job opportunities are also at risk
- **Job Seekers:** Especially those unfamiliar with advanced cybersecurity practices



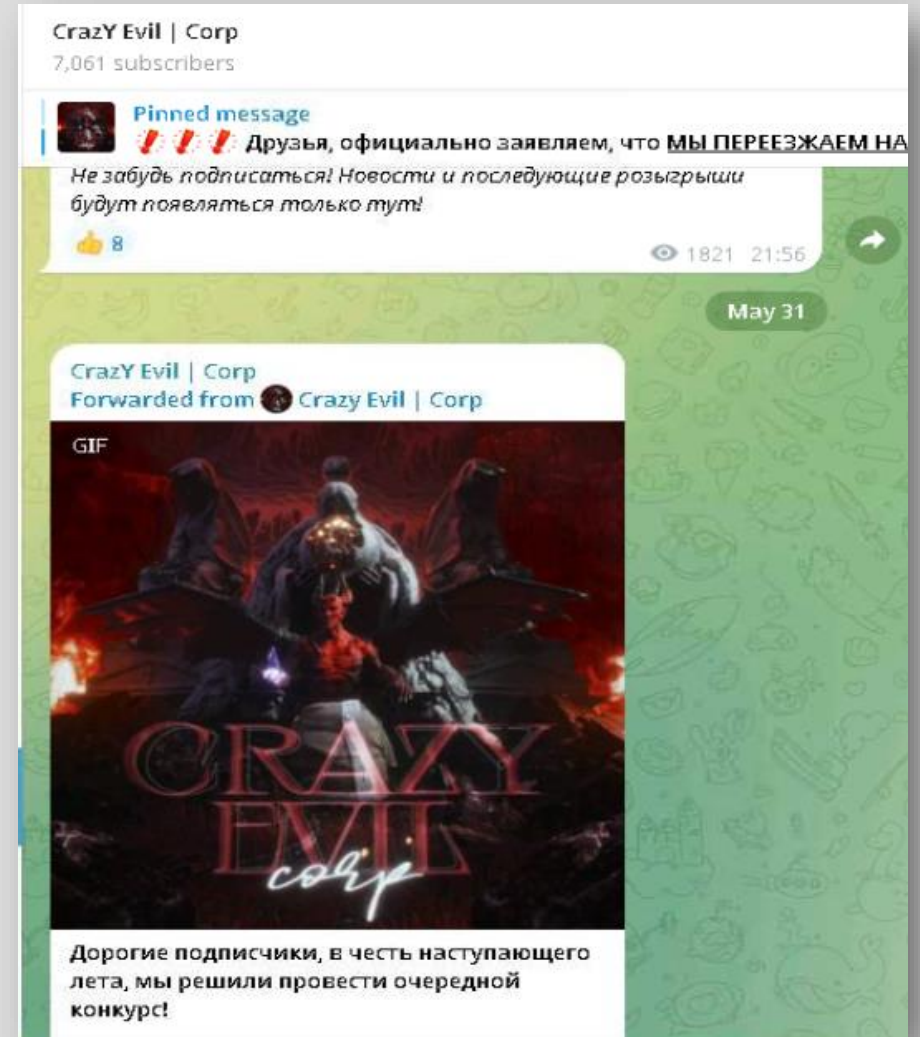
```
elif _operation == "MIRROR_X":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add back the deselected mirror
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is active
#mirror_ob.select = 0
name = bpy.context.selected_objects[0]
#bpy.data.objects[name].select = 0
```

Unveiling the Threat actor Behind the Scam

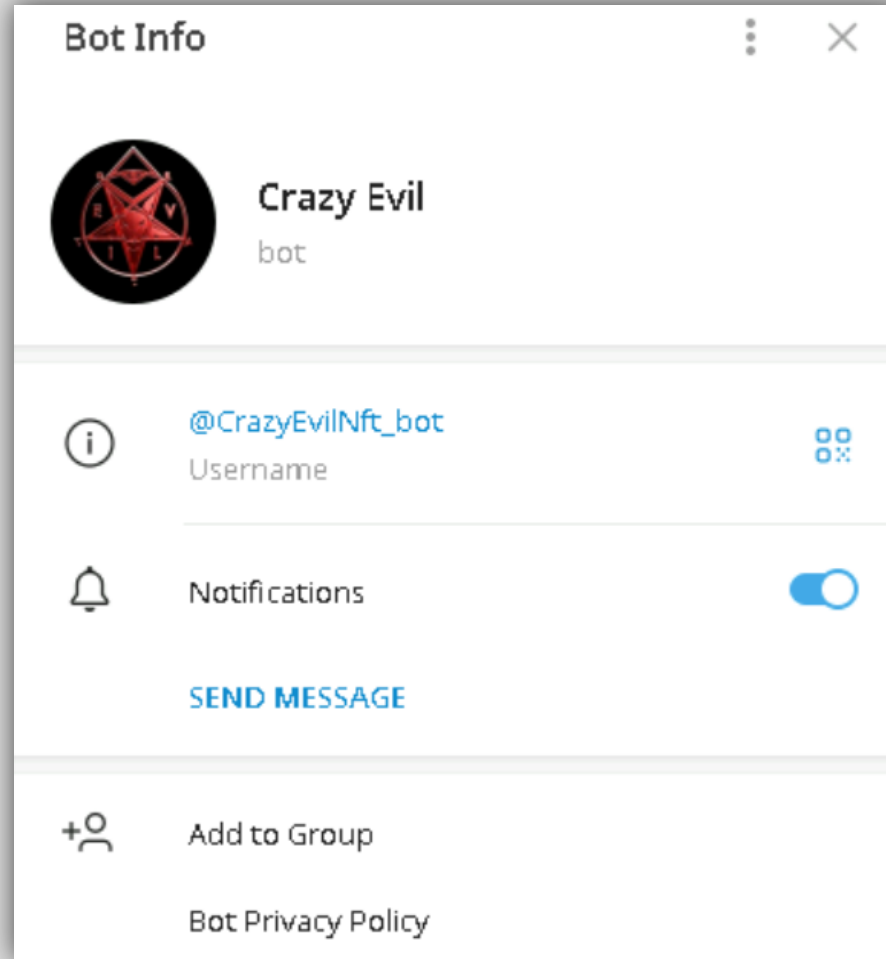
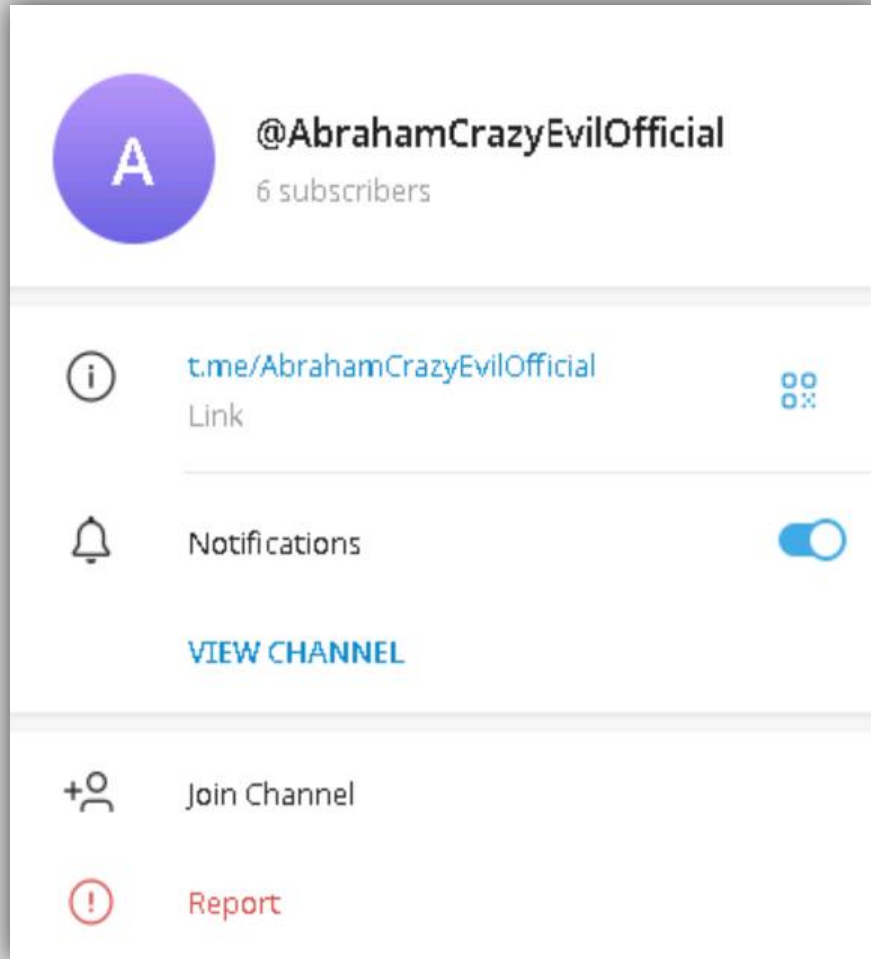


- "Crazy Evil" is a Russian-speaking cybercriminal organization that emerged in 2021
- The group specializes in:
 - Identity fraud
 - Cryptocurrency theft
 - Deployment of information-stealing malware
- Their operations involve sophisticated social engineering tactics
- They frequently employ "traffers"—social engineering experts who redirect legitimate traffic to malicious phishing pages





- o Telegram profile for Abraham — the alleged leader of Crazy Evil





- 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)**: Organization’s central hub, with a membership of over ~3,000 at
- **“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”**: 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.



Crazy Evil | Corp” (@CrazyEvilCorp)



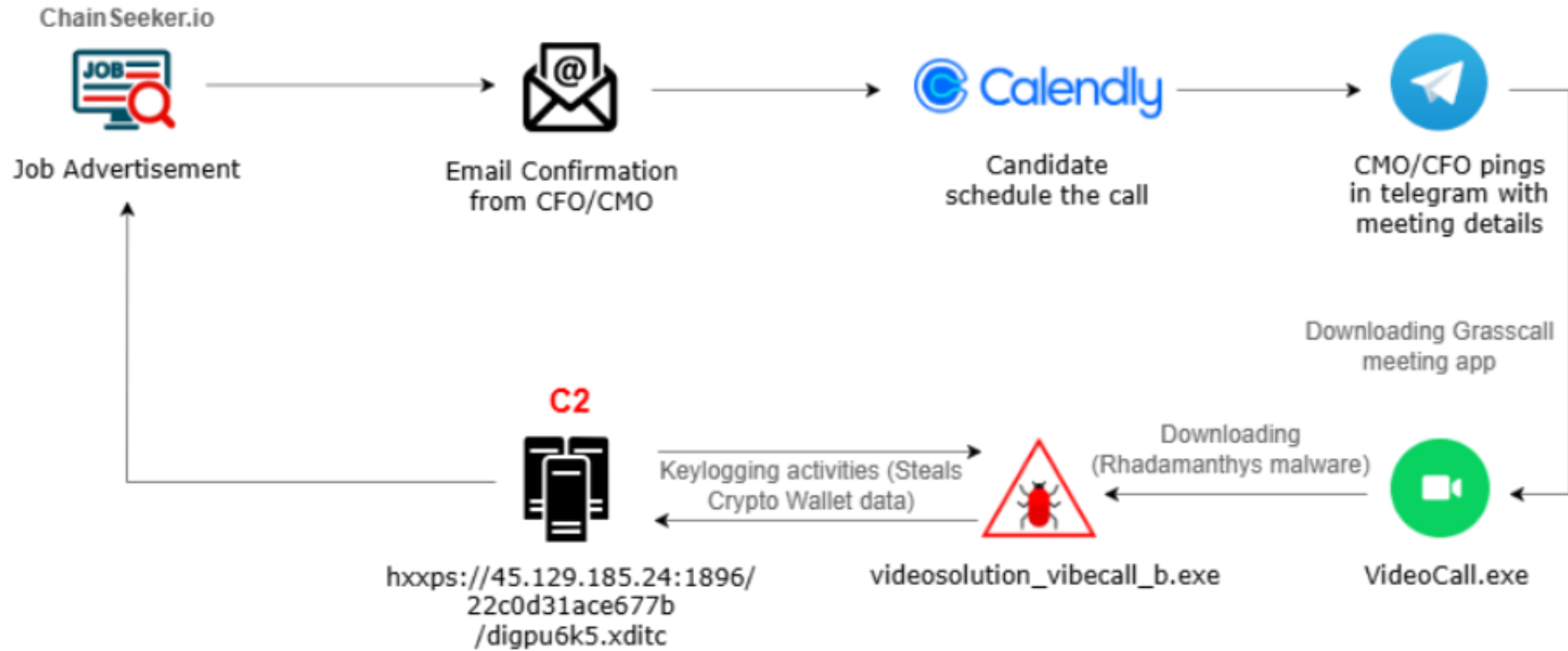
Info | Crazy Evil

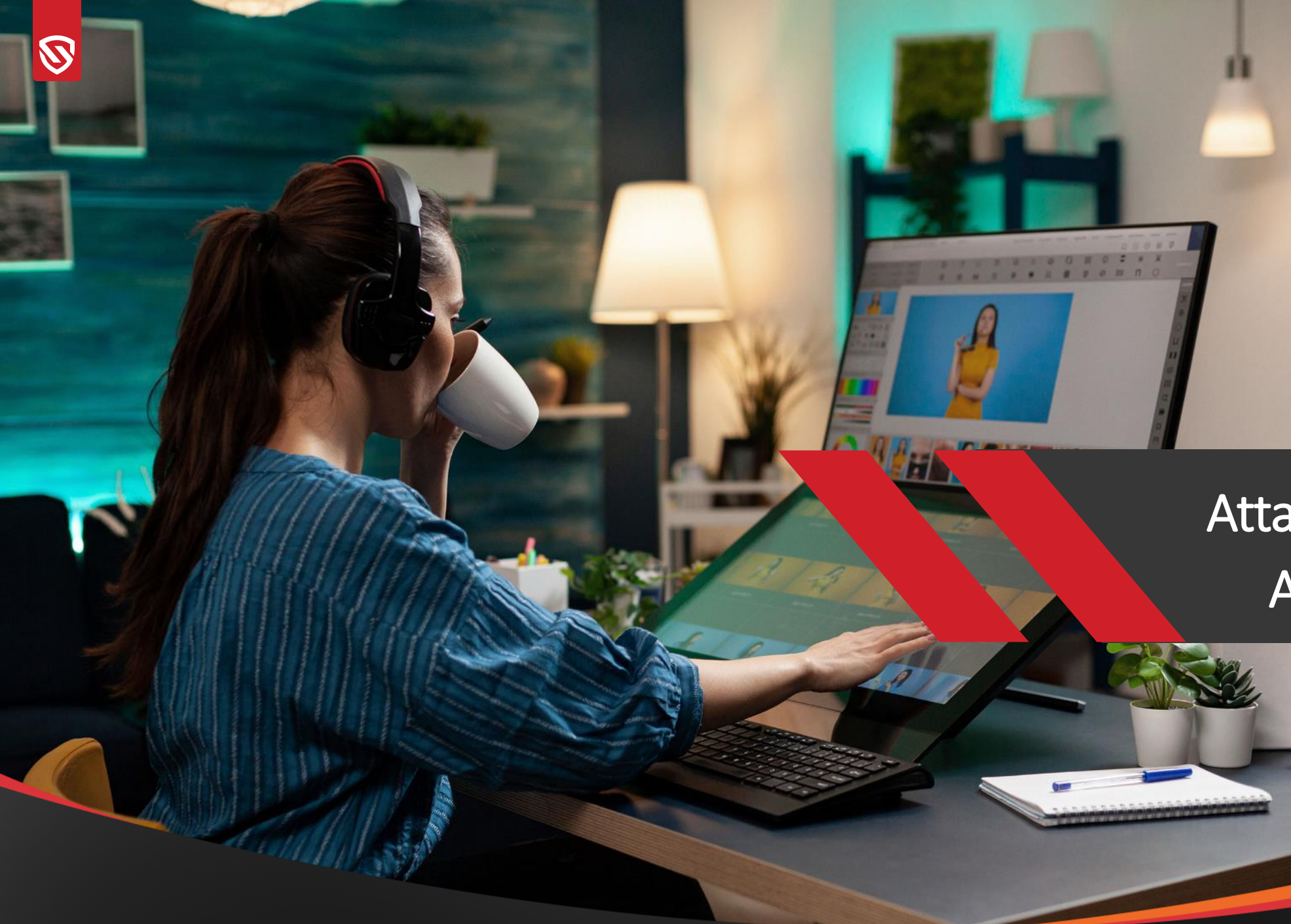


Global Chat | Crazy Evil



Infection Chain

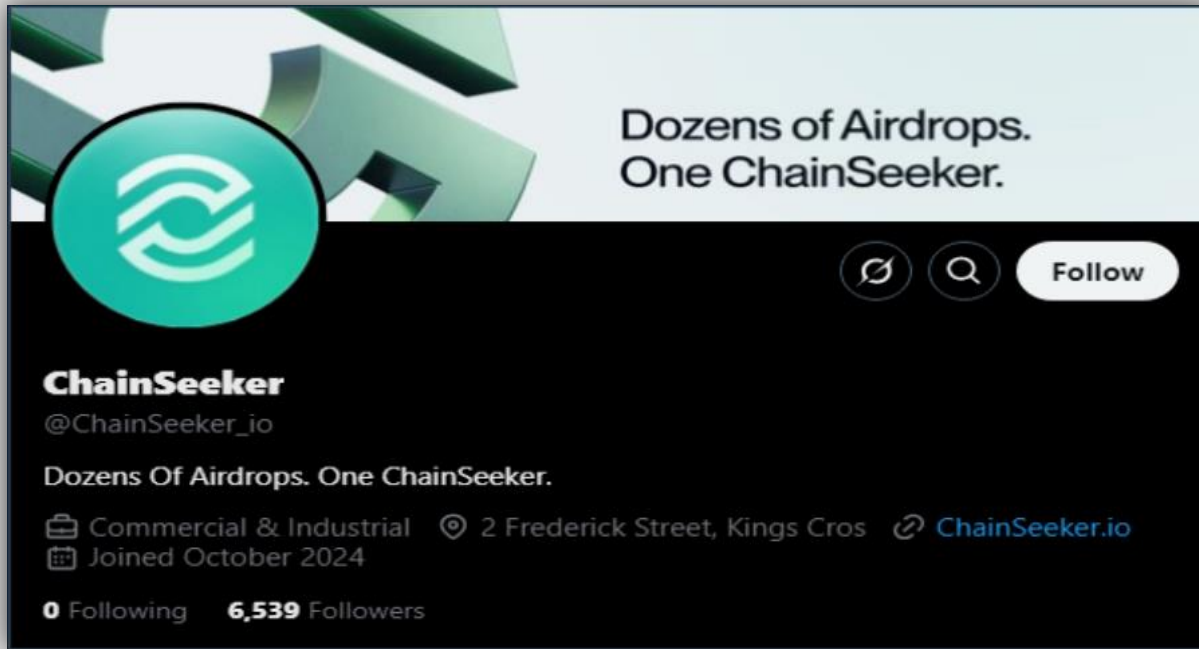




Attack Tactics & Approach



o Impersonating a Fake Company – Over Twitter



The attackers set up a fabricated business, such as "ChainSeeker.io," featuring a professional website and active social media accounts on platforms like LinkedIn and X (previously Twitter).



- Job Advertisement over social media platform

The screenshot shows a LinkedIn job advertisement for a Business Development Manager at Chain Seeker. The job is located in the United States (Remote) with a salary range of \$80K/yr - \$150K/yr. The applicant has applied 1 day ago. The advertisement includes a feedback section asking if the results are helpful and a link to see jobs where the applicant is a top applicant. The job details are highlighted to match the applicant's preferences and skills.

Jobs in Worldwide
1 result

Business Development Manager
Chain Seeker
United States (Remote)
\$80K/yr - \$150K/yr
Applied

Are these results helpful?
Your feedback helps us improve search results.

See jobs where you're a top applicant

Chain Seeker

Business Development Manager
United States · 1 week ago · Over 100 applicants

We highlight job details that match your preferences and skills. Click below to view and edit them.

\$80K/yr - \$150K/yr Remote Contract 0 of 10 skills match


Applied 1 day ago See application >

- They publish high-quality job advertisements on reputable job boards like LinkedIn, Well-found, and Crypto Jobs List to attract unsuspecting applicants



○ Mail received after applying to the Job posted also ping from CMO/CFO

interview invitation Inbox x

 **cfo@chainseeker.io** cfo@chainseeker.io <cfo@chainseeker.io>
to me ▾

21:01 (1 hour ago) ☆ 😊 ↶ ⋮

Dear [REDACTED]

Please use our Calendly to select a time that is convenient for you.

<https://calendly.com/chro-chainseeker/new-meeting?month=2025-02&date=2025-02-28>

Isabel Olmedo
CFO ChainSeeker

We'd like to invite you to the next stage of the interview process at Chain Seeker.

Please use this Calendly link to schedule a time that works best for you: <https://calendly.com/chro-chainseeker/new-meeting?month=2025-02&date=2025-02-28>

If it's not convenient for you to attend the interview on the specified date, please let me know

Calendly
New Meeting - Adriano Cattaneo

21:41



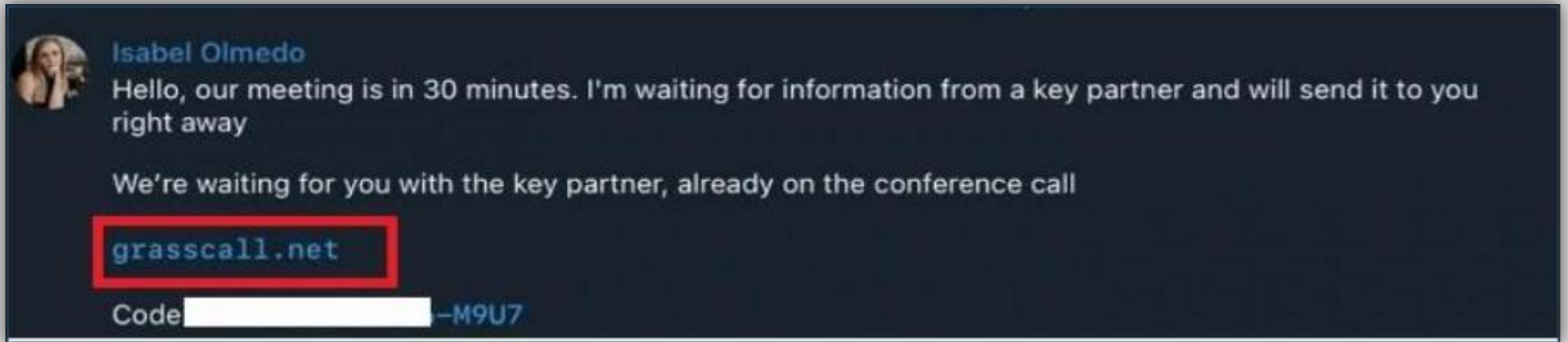
- After candidates schedule their call within the chosen time frame, the CMO or CFO will reach out to them beforehand to provide additional details

The screenshot shows a calendar event window with the following details:

- Title:** New Meeting with Adriano Cattaneo (highlighted with a red box)
- Date & Time:** Friday, 28 February - 3:30 - 4:00am
- Location:** grasscall
- Guests:** 1 guest, 1 maybe
- Event Name:** New Meeting
- Date & Time:** 03:30am - 04:00am (India Standard Time) on Friday, February 28, 2025
- Location:** grasscall (highlighted with a red box)
- Options:** Need to make changes to this event?
Cancel: <https://calendly.com/cancellations/dd9c6379-6fe7-451b-a767-Oe093857477a>
Reschedule: <https://calendly.com/reschedulings/dd9c6379-6fe7-451b-a767-Oe093857477a>



- Before the call, their CFO/CMO contacting the candidate to join the call with shared passcode



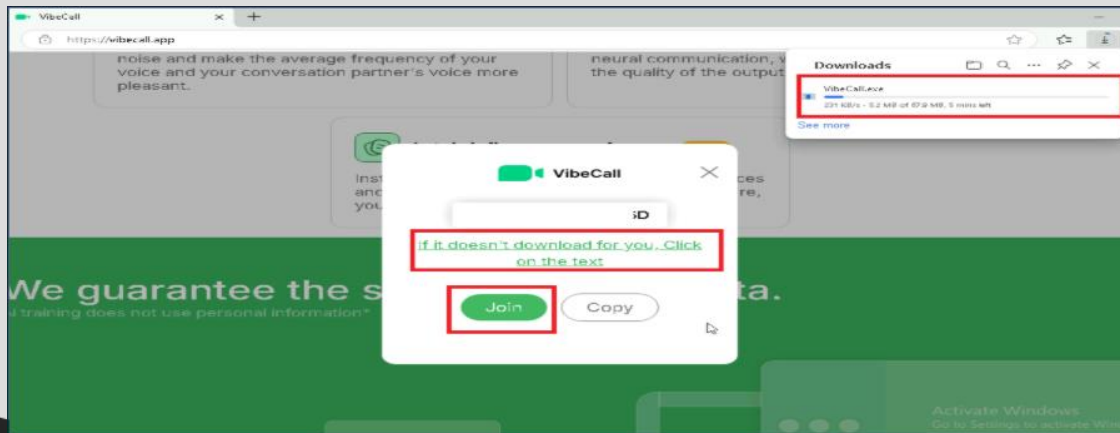
- Malicious Software Deployment: The fake CMO directs candidates to download a video conferencing application named "GrassCall" from a specific website (e.g., "grasscall[.]net")



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



- During the campaign they have also rebranded it as https://vibecall[.]app/





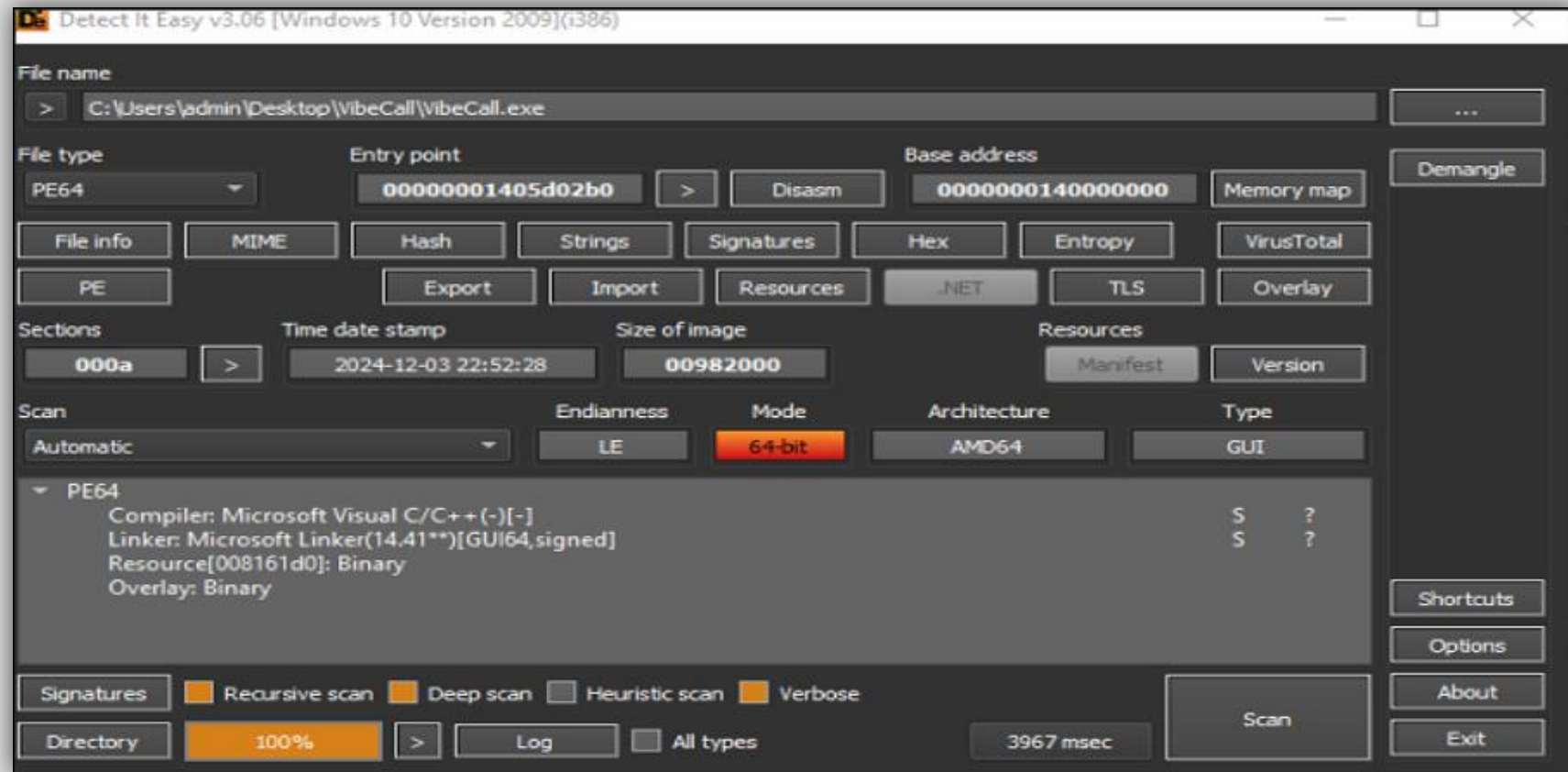
- **Windows Users:** Installing "GrassCall.exe" triggers the deployment of a Remote Access Trojan (RAT) combined with an information-stealing program like Rhadamanthys. These malicious tools enable attackers to maintain ongoing access, log keystrokes, and extract sensitive data, including cryptocurrency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



Technical Analysis of GrassCall.exe / VibeCall.exe

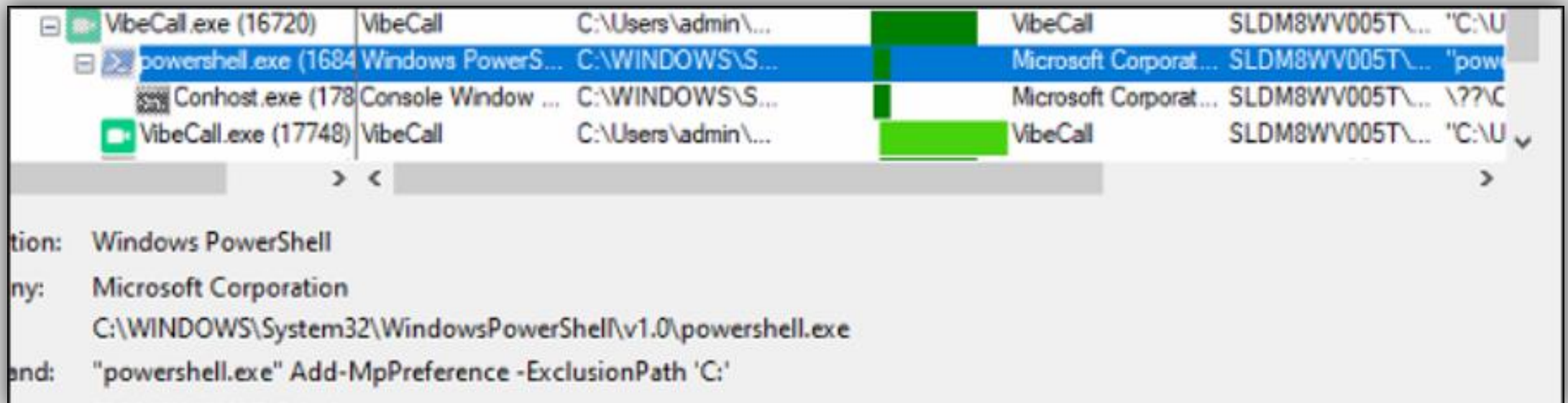


- VibeCall.exe is a 64-bit executable file that acts as an installer
- Upon execution, it attempts to install and deploy the Rhadamanthys malware





- 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





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

http://rustaisolutionnorisk.com/downloads/contry_solution_vibecall_e.exe
4b371777c2c638c97b818057ba4b0a2de246479776eaaacebccf41f467bb93c3

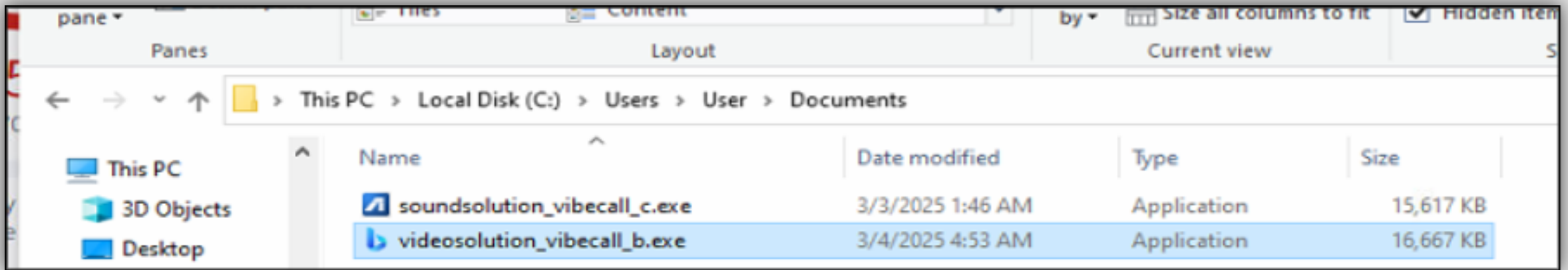
http://rustaisolutionnorisk.com/downloads/aisolution_vibecall_a.exe
f2e8f1f72abbc42f96c5599b8f27f620d91ae1680aa14b4f0bbf3daabd7bee30

http://rustaisolutionnorisk.com/downloads/soundsolution_vibecall_c.exe
d23f79f9b7e1872d4671a18aa85b810c0cec2e0f5ce07c2cf99ed39f8936c8fb

http://rustaisolutionnorisk.com/downloads/videosolution_vibecall_b.exe
386b61ccdd4b785c835a064179d5fa58dc0d5fe34970a04487968e1ee0189ce6



- It drops the downloaded samples in *C:/Users/user/Documents* folder and tries to execute it



- It drops the second layer of Payload which is called Rhadamanthys malware



Rhadamanthys malware Analysis

The screenshot shows the Detect It Easy v3.06 interface. The file path is C:\Users\User\Documents\videosolution_vibecall_b.exe. The file type is PE32, with an entry point at 004089f0 and a base address at 00400000. The file size is 0005, and the time date stamp is 2025-02-24 04:01:55. The architecture is I386, and the type is GUI. The linker is Microsoft Linker(14.42**)[GUI32,signed]. The resource is Binary, and the overlay is Binary. The interface includes various analysis buttons like File info, MIME, Hash, Strings, Signatures, Hex, Entropy, VirusTotal, PE, Export, Import, Resources, .NET, TLS, Overlay, Manifest, and Version. The bottom section shows scan options: Recursive scan (checked), Deep scan (checked), Heuristic scan (unchecked), and Verbose (checked). The scan progress is 100% and the scan time is 1940 msec.



- It checks for processes associated with debugging, reverse engineering, sandboxing etc. It may enumerate running processes and if names match known debugger/analysis tools, it may abort or modify its behaviour.
- We can see APIs like IsDebuggerPresent and IsProcessorFeaturePresent(0x17) + **__fastfail** which is used for **Anti-Debugging**

```
__fastcall __usercall sub_408E60@eax(int a1@ebx, int a2@edi, int a3@esi)
{
    int v4; // edx
    int v5; // ecx
    unsigned int v6; // kr00_4
    int vars0; // [esp+324h] [ebp+0h]
    int retaddr; // [esp+328h] [ebp+4h]

    if ( IsProcessorFeaturePresent(0x17u) )
        __fastfail(2u);
    dword_429730 = 0;
    dword_42972C = v5;
    dword_429728 = v4;
    dword_429724 = a1;
    dword_429720 = a3;
    dword_42971C = a2;
    word_429748 = __SS__;
    word_42973C = __CS__;
    word_429718 = __DS__;
    word_429714 = __ES__;
    word_429710 = __FS__;
    word_42970C = __GS__;
    v6 = __readeflags();
    dword_429740 = v6;
    dword_429734 = vars0;

```

```

{
    v7 = IsDebuggerPresent();
    if ( v7 )
        goto LABEL_23;
}
sub_4108A0(a1 - 5, v20, 4, &v13, v19, 0x104u);
if ( v4 )
{
    v7 = v4(v4, a2, v20, v13, v19, L"Run-Time Check Failure #%- %s", v15, v6);
}
else
{
    v8 = WideCharToMultiByte(0xFDE9u, 0, v20, -1, MultiByteStr, 778, 0, 0);
    v9 = WideCharToMultiByte(0xFDE9u, 0, v19, -1, v18, 778, 0, 0);
    v10 = "Unknown Module Name";
    if ( v9 )
        v10 = v18;
    v11 = "Unknown Filename";
    if ( v8 )
        v11 = MultiByteStr;
    v7 = v14(a2, v11, v13, v10, "Run-Time Check Failure #%- %s", v15, lpMultiByteStr);
}
if ( v7 == 1 )
LABEL_23:
    __debugbreak();
return v7;

```



- Breaking on VirtualAlloc and monitoring the first 4 bytes at the EAX-returned address revealed executable code.
 - Upon unpacking we found the 2nd payload of Rhadamanthys malware.

The screenshot shows a debugger window with assembly code on the right and a memory dump on the left. The assembly code includes instructions like `movzx eax, byte ptr ds:[ecx+eax]`, `mov dword ptr ss:[ebp+10], eax`, `add eax, dword ptr ss:[ebp-14]`, `mov cl, byte ptr ss:[ebp-10]`, `mov byte ptr ds:[eax], cl`, `mov eax, dword ptr ss:[ebp-14]`, `inc eax`, `mov dword ptr ss:[ebp-14], eax`, `mov eax, dword ptr ss:[ebp-14]`, `cmp eax, dword ptr ss:[ebp+18]`, `jb 148923C`, `jmp 1489258`, `mov eax, dword ptr ss:[ebp-C]`, `add eax, dword ptr ss:[ebp-8]`, `mov cl, byte ptr ss:[ebp-10]`, `mov byte ptr ds:[eax], cl`, `mov eax, dword ptr ss:[ebp-8]`, `inc eax`, `mov dword ptr ss:[ebp-8], eax`, `mov eax, dword ptr ss:[ebp-8]`, `and eax, FFF`, `mov dword ptr ss:[ebp-8], eax`, `jmp 14891FC`, `jmp 14890FC`, `push 8000`, `push 0`, `push dword ptr ss:[ebp-C]`, `mov eax, dword ptr ss:[ebp+8]`, and `call dword ptr ds:[eax+4]`. The memory dump shows a table with columns for Address, Hex, and ASCII. The ASCII column contains the text "MZ.....yy.. is program cannot be run in DOS mode. \$..... IA-(.'0)IA-(.'0) AAB-(.'0).2H(.'0) .40(.'0).4+(.'0)".

Address	Hex	ASCII
01450000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....yy..
01450010	B8 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00@.....
01450020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01450030	00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00i..
01450040	0E 1F BA 0E 00 84 09 CD 21 B8 01 4C CD 21 54 68	..*...!..Li!Th
01450050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program cannot
01450060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
01450070	6D 6F 64 65 2E 00 0A 24 00 00 00 00 00 00 00 00	mode. \$. ..
01450080	CD D8 9A 7A 89 89 F4 29 89 89 F4 29 89 89 F4 29	IA-(.'0).\$.....
01450090	C2 C1 F7 28 82 89 F4 29 C2 C1 F1 28 06 B9 F4 29	IA-(.'0)IA-(.'0)
014500A0	C2 C1 F0 28 90 89 F4 29 9C C6 F1 28 AF B9 F4 29	AAB-(.'0).2H(.'0)
014500B0	9C C6 F0 28 98 89 F4 29 9C C6 F7 28 9D B9 F4 29	.40(.'0).4+(.'0)



- The second payload contained a configuration file that attempts to establish a connection to a command-and-control (C2) server. The connection is directed to the URL: `hxxps://45.129.185.24:1896/22c0d31ace677b/digpu6k5.xditc`

The screenshot shows a debugger window with assembly code on the left and a hex dump on the right. The assembly code includes instructions like `lea eax, dword ptr ss:[ebp-4]`, `push ebx`, `push eax`, `push dword ptr ss:[ebp+C]`, `call 14810A0`, `add dword ptr ss:[ebp+10], ebx`, `add dword ptr ss:[ebp+14], ebx`, `add esp, C`, `sub esi, ebx`, `dec edi`, `jne 1487305`, `pop esi`, `pop ebx`, `pop edi`, and `leave`. The hex dump shows the payload data, including the URL `https://45.129.185.24:1896/22c0d31ace677b/digpu6k5.xditc`. A red annotation in the hex dump reads "return to 014872E0 from 014872E8".



Current Infra State

- The current state of C2 involves resolving an IP address linked to a .work domain, allowing them to target job seekers and professionals by leveraging social engineering tactics.

<input type="checkbox"/>	45.129.185.24	PTR	43843.ip-ptr.tech
	AS 211529		
<input type="checkbox"/>	45.129.185.24	A	mail.betheew.work
	AS 211529		
<input type="checkbox"/>	45.129.185.24	A	betheew.work
	AS 211529		
<input type="checkbox"/>	45.129.185.24	A	mail.idoloegfi.work
	AS 211529		
<input type="checkbox"/>	45.129.185.24	A	idoloegfi.work
	AS 211529		



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



- **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 antivirus 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.



Thank You
Simplifying Cybersecurity