
SEQRITE
Quick Heal
UNMASKING
GRASSCALL
CAMPAIGN
The Hackers Behind JOB RECRUITMENT CYBER SCAMS
vb 2025
BERLIN
24-26 Sept 2025

About Us

Dixit Panchal
Security Researcher
Seqrite Labs, Quick Heal
@Dixit_404

Soumen Burma
Senior Security Researcher
Seqrite Labs, Quick Heal
@SOuMEn_B1

Agenda

SECRITE | Quick Heal

01 Overview of Campaign

02 Threat actor Behind the Scam

03 Infection Chain

04 Attack tactics & Approach

05 Analysis of Grasscall.exe

06 TTPs

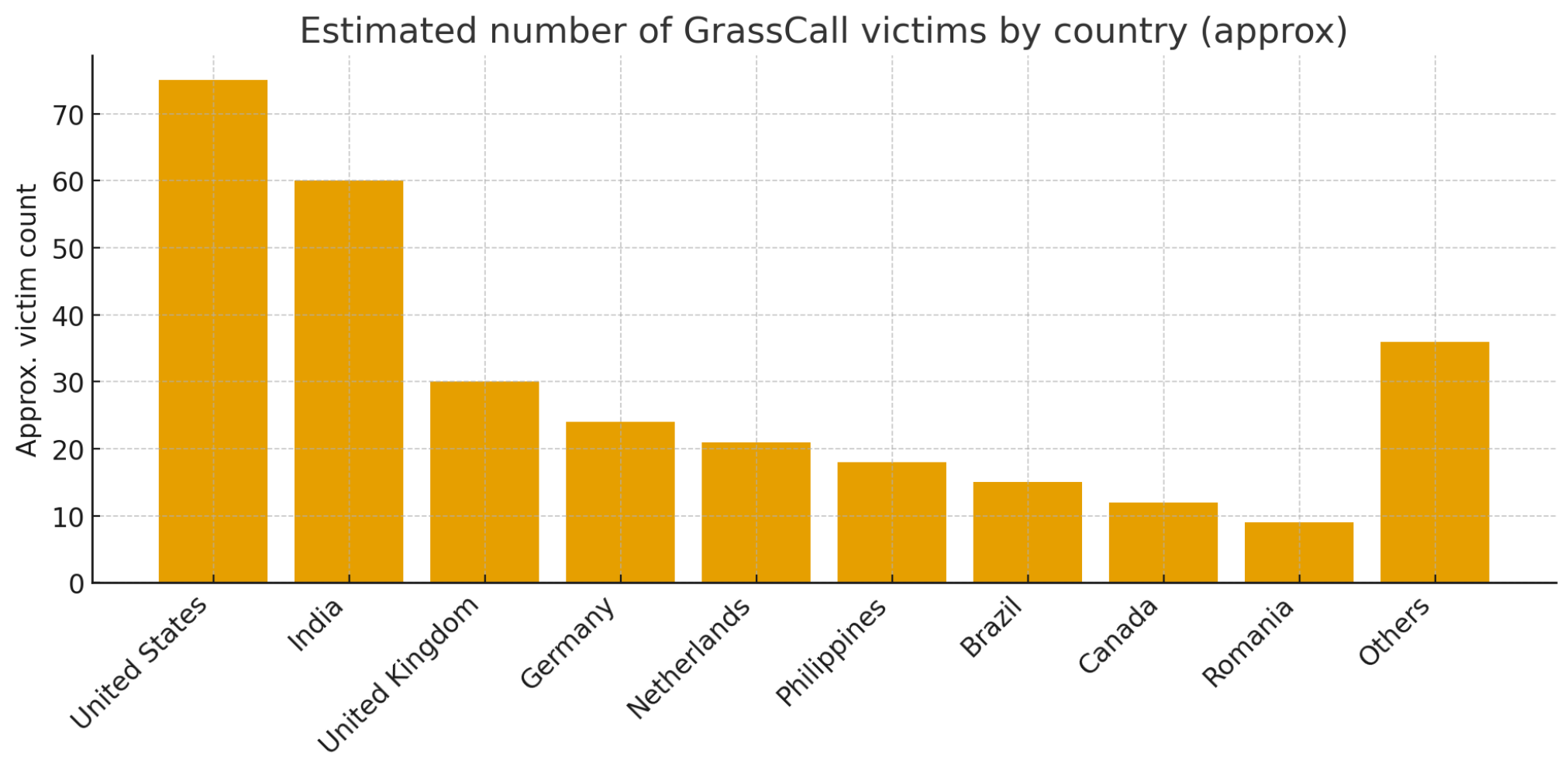
07 Preventives Measures

3

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



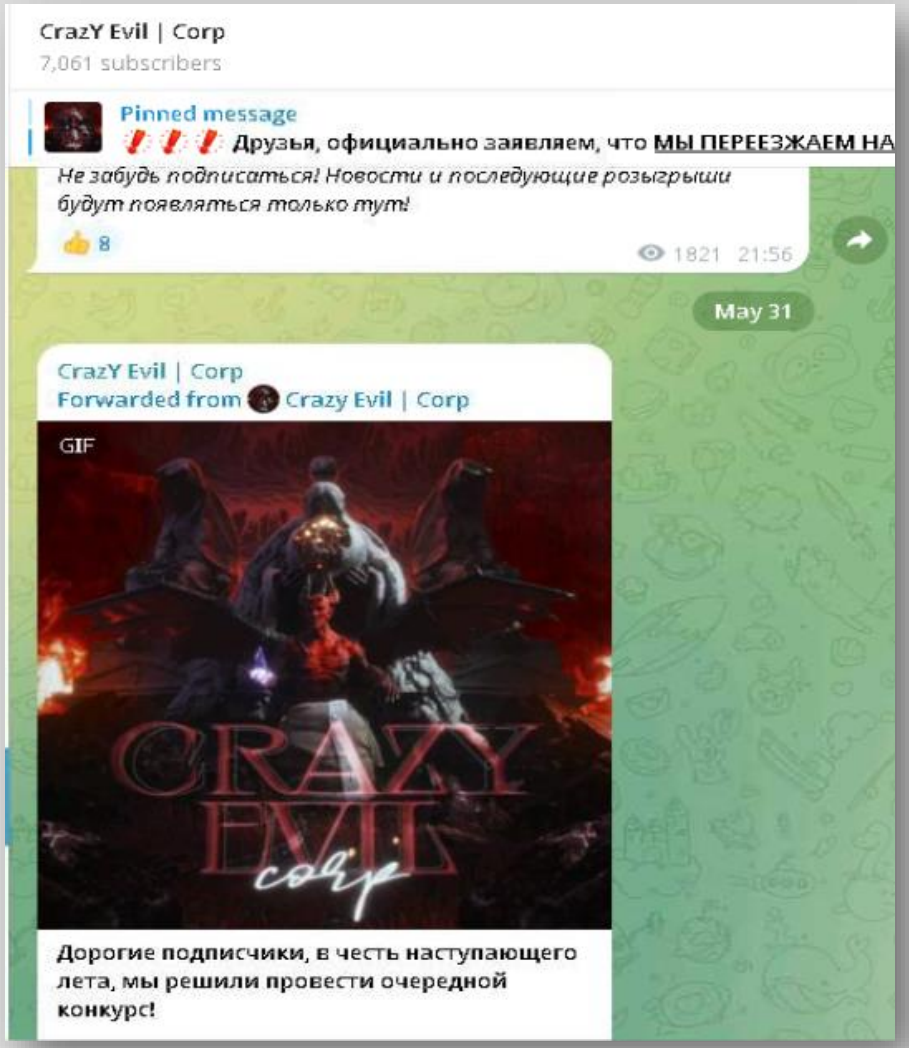
Targeted Sector

- **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

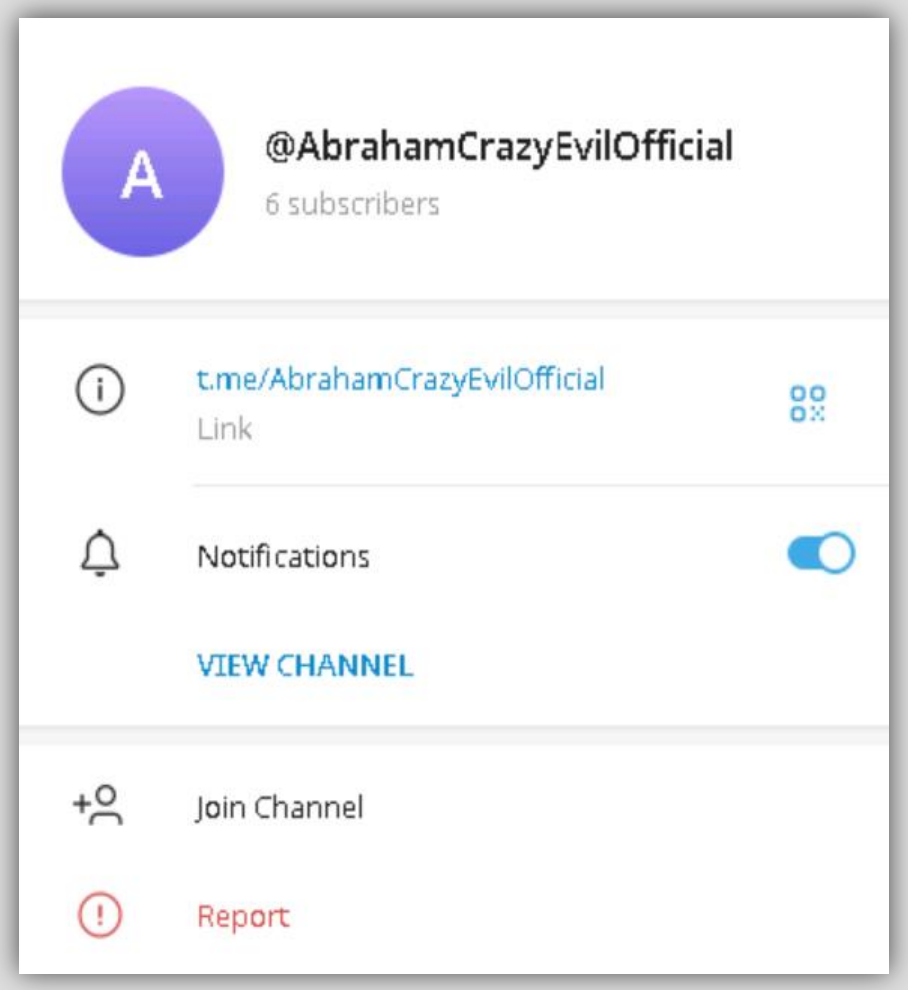
SEQRITE | Quick Heal

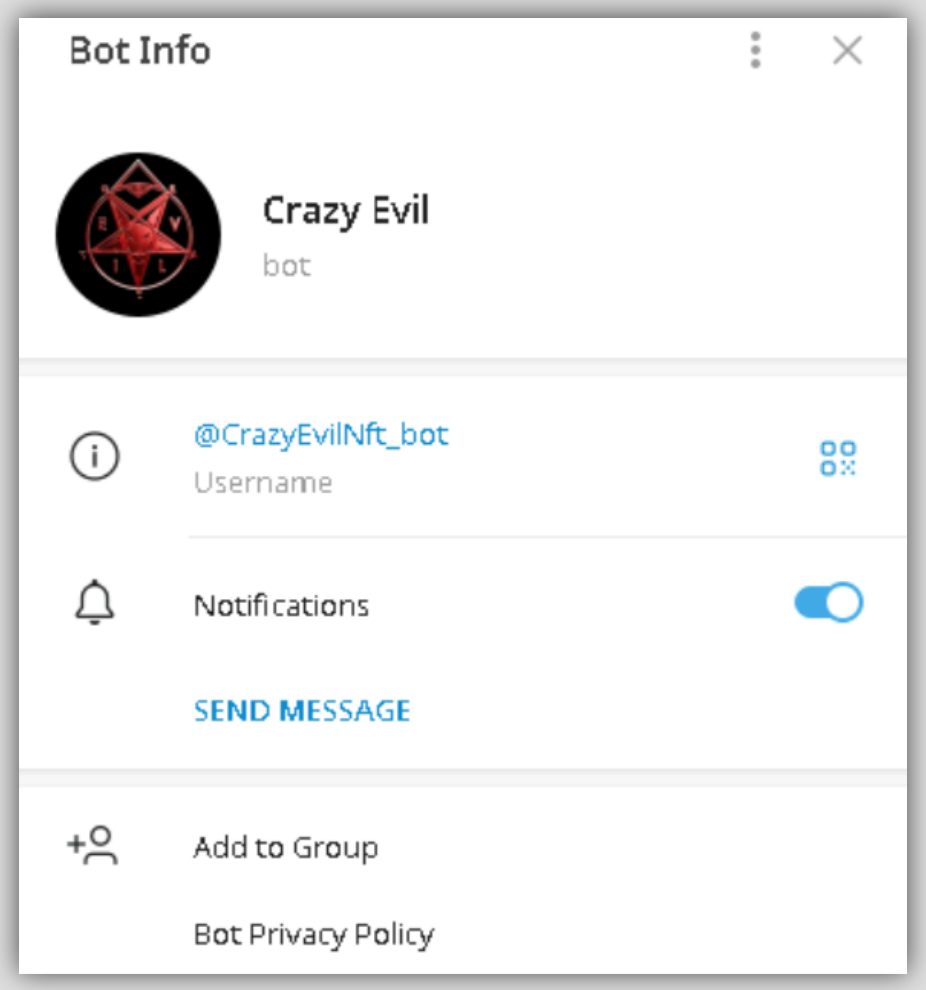
Unveiling the Threat actor Behind the Scam

- "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



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

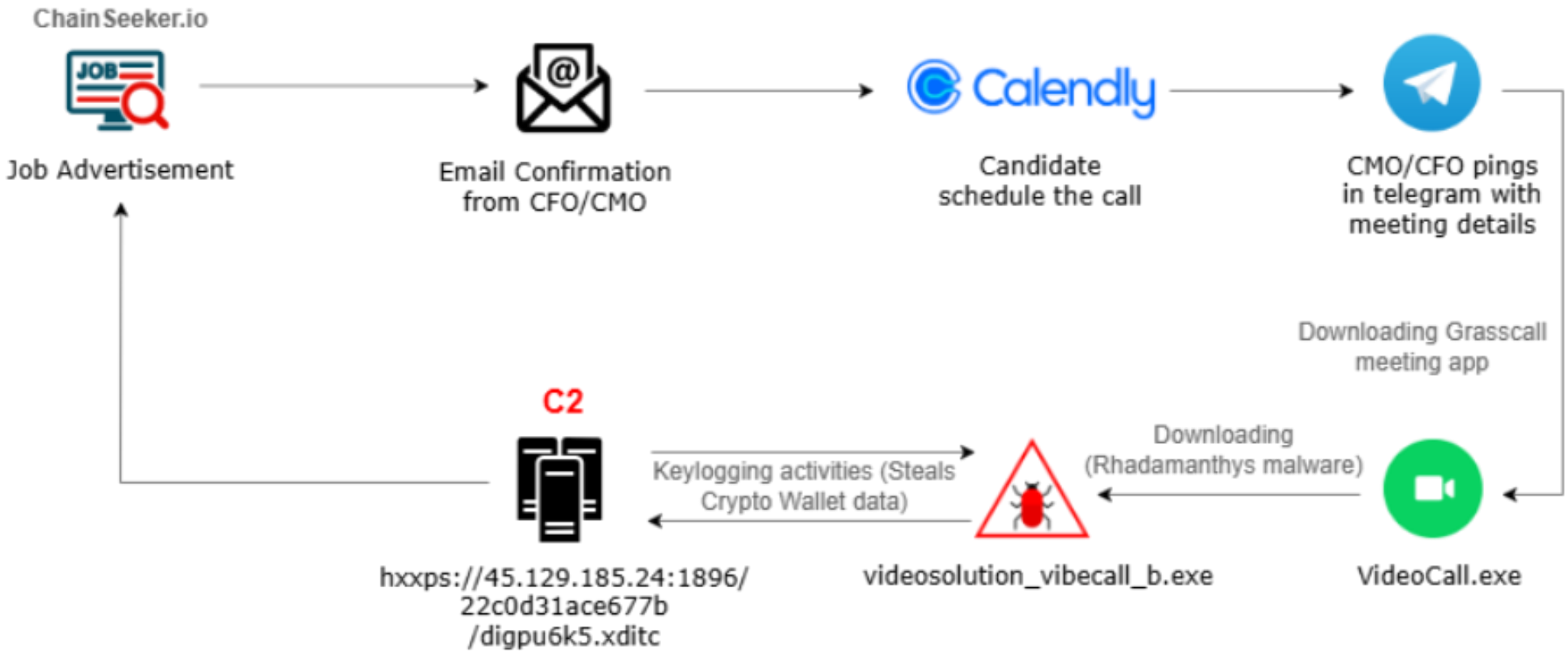


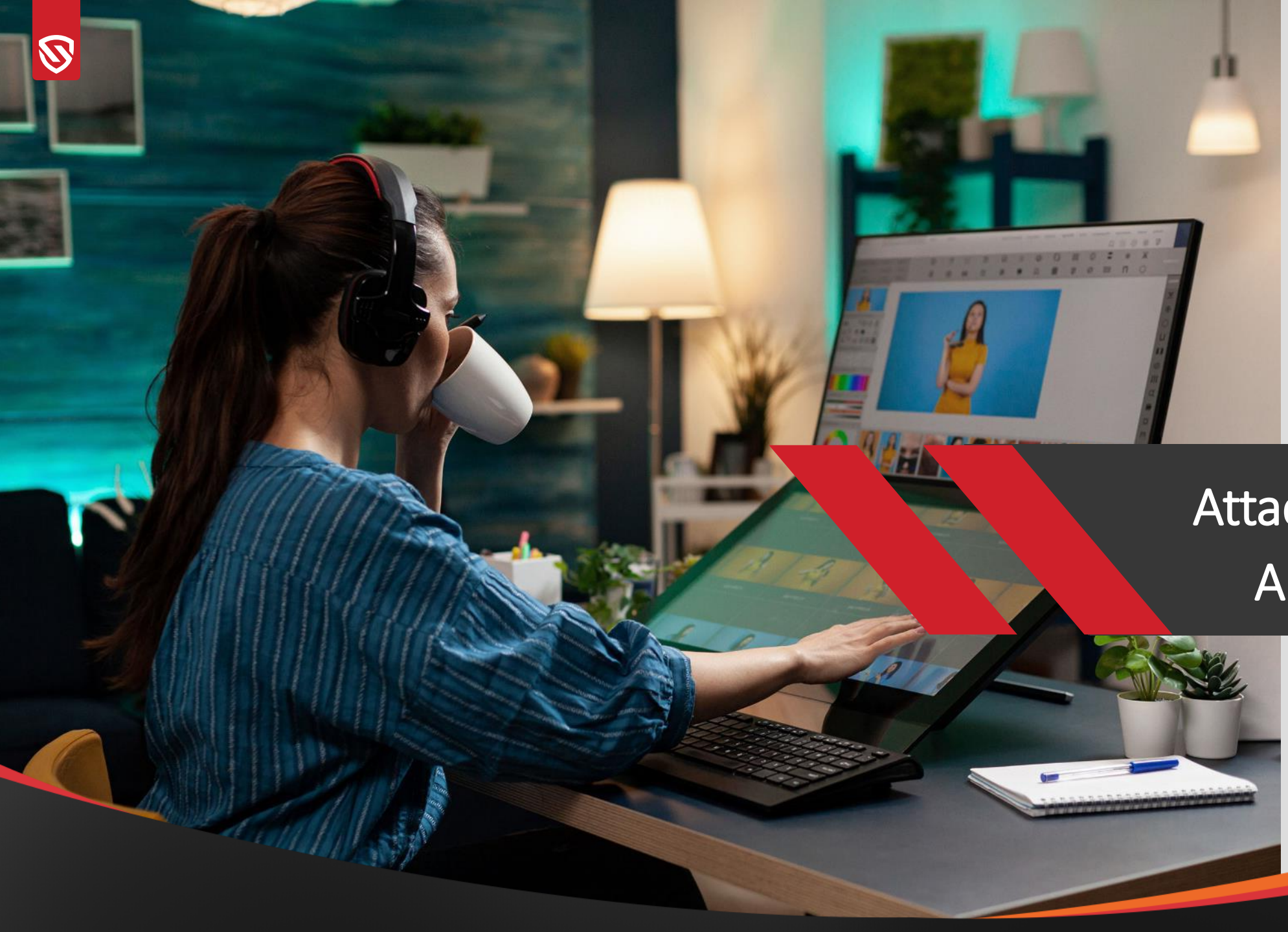


- Beyond its main Telegram channels, Crazy Evil also manages two primary information-focused channels and a private discussion group for its traffers:

  - **“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.

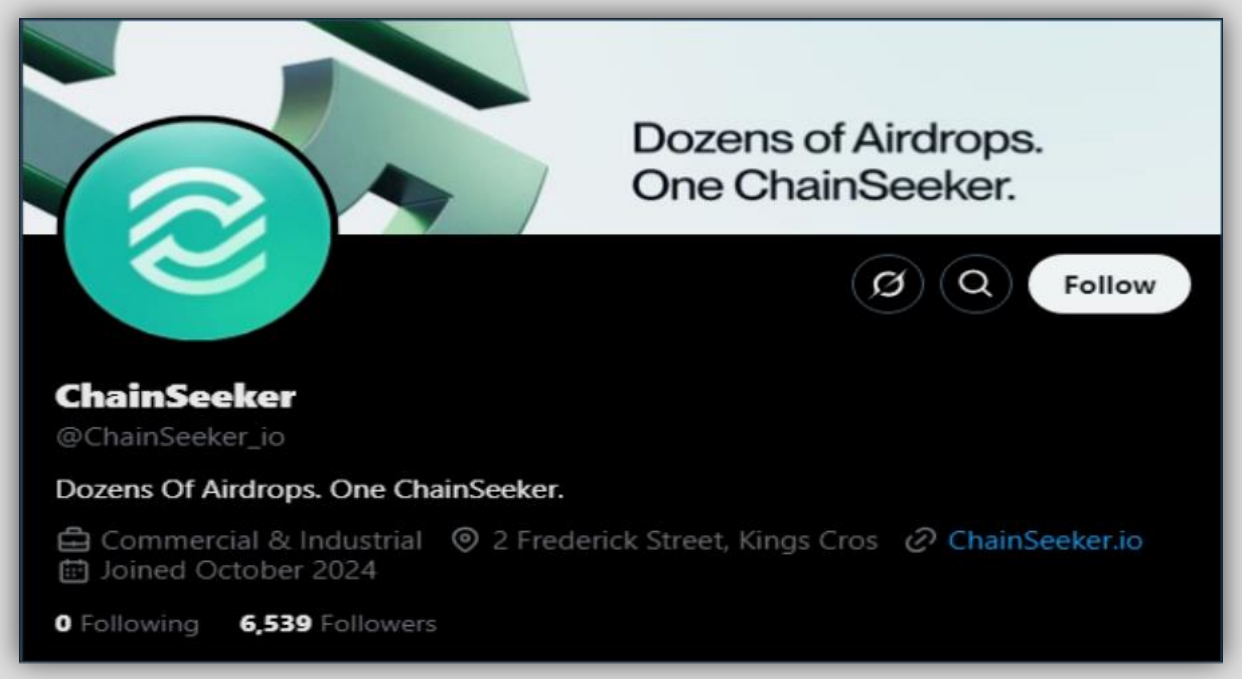
Infection Chain


ChainSeeker.io
JOB
Job Advertisement
Email Confirmation from CFO/CMO
Calendly
Candidate schedule the call
CMO/CFO pings in telegram with meeting details
Downloading Grasscall meeting app
VideoCall.exe
Downloading (Rhadamanthys malware)
videosolution_vibecall_b.exe
Keylogging activities (Steals Crypto Wallet data)
C2
hxxps://45.129.185.24:1896/22c0d31ace677b/digpu6k5.xditc



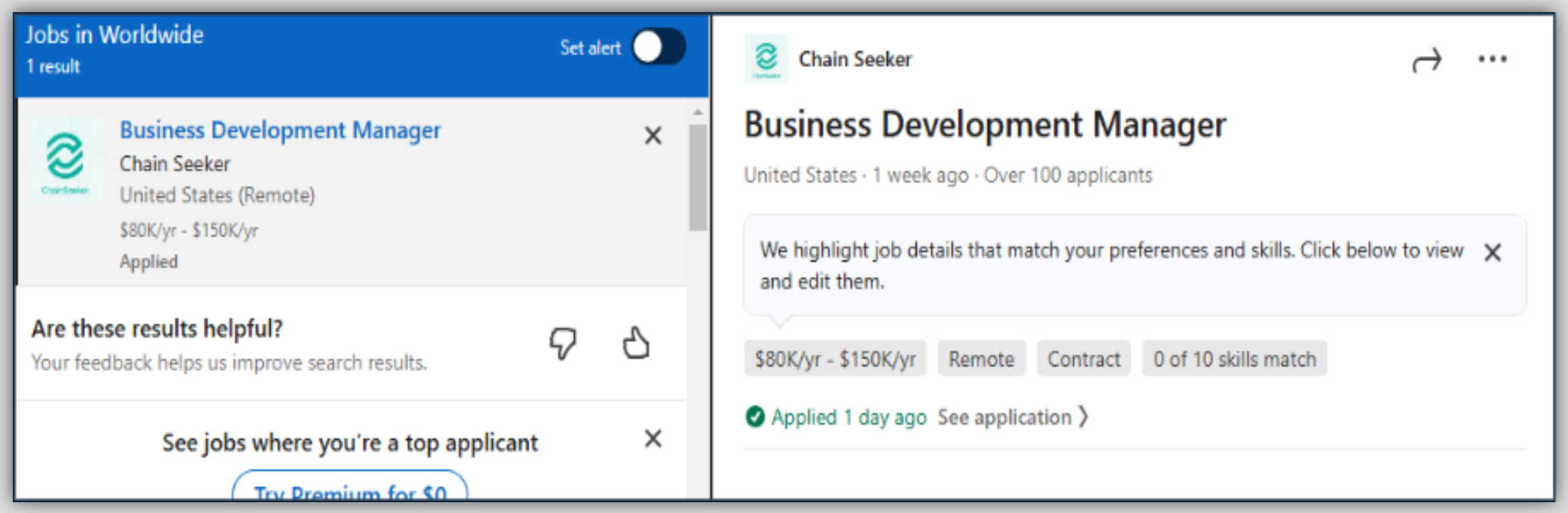
Attack Tactics & Approach

○ Impersonating a Fake Company – Over Twitter



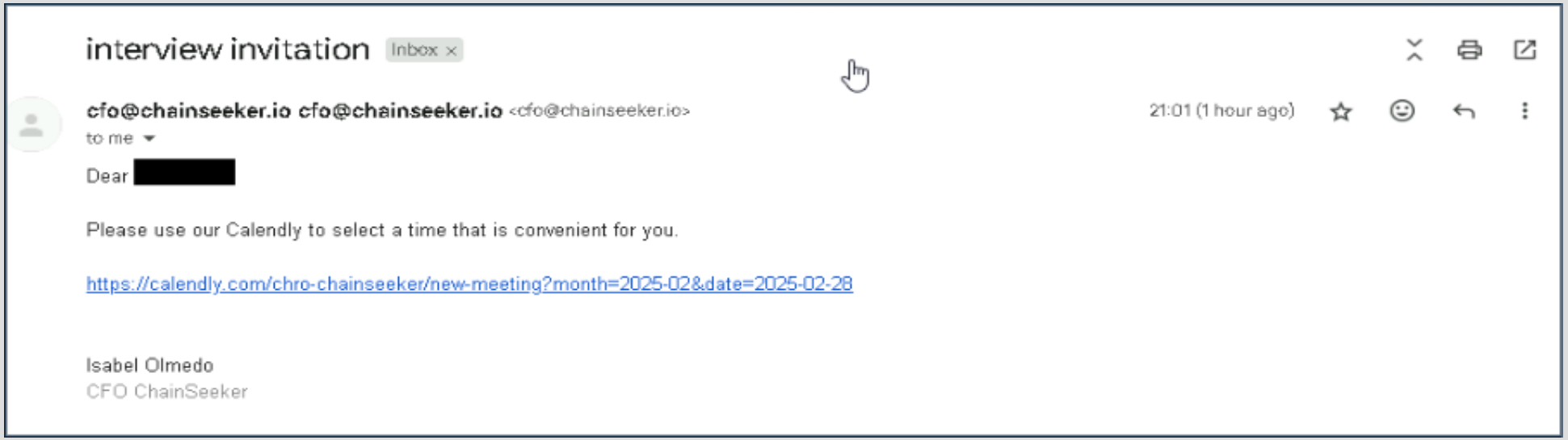
The attackers set up a fabricated business, such as **"ChainSeeker.io,"** featuring a professional website and active social media accounts on platforms like LinkedIn and X (previously Twitter).

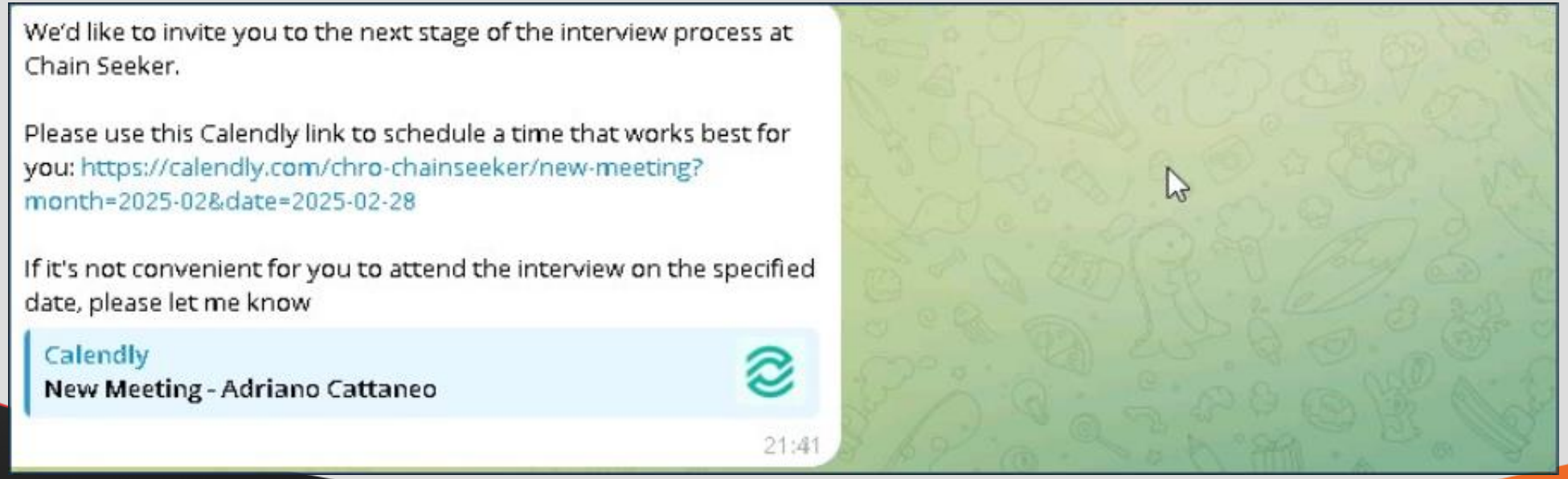
- Job Advertisement over social media platform



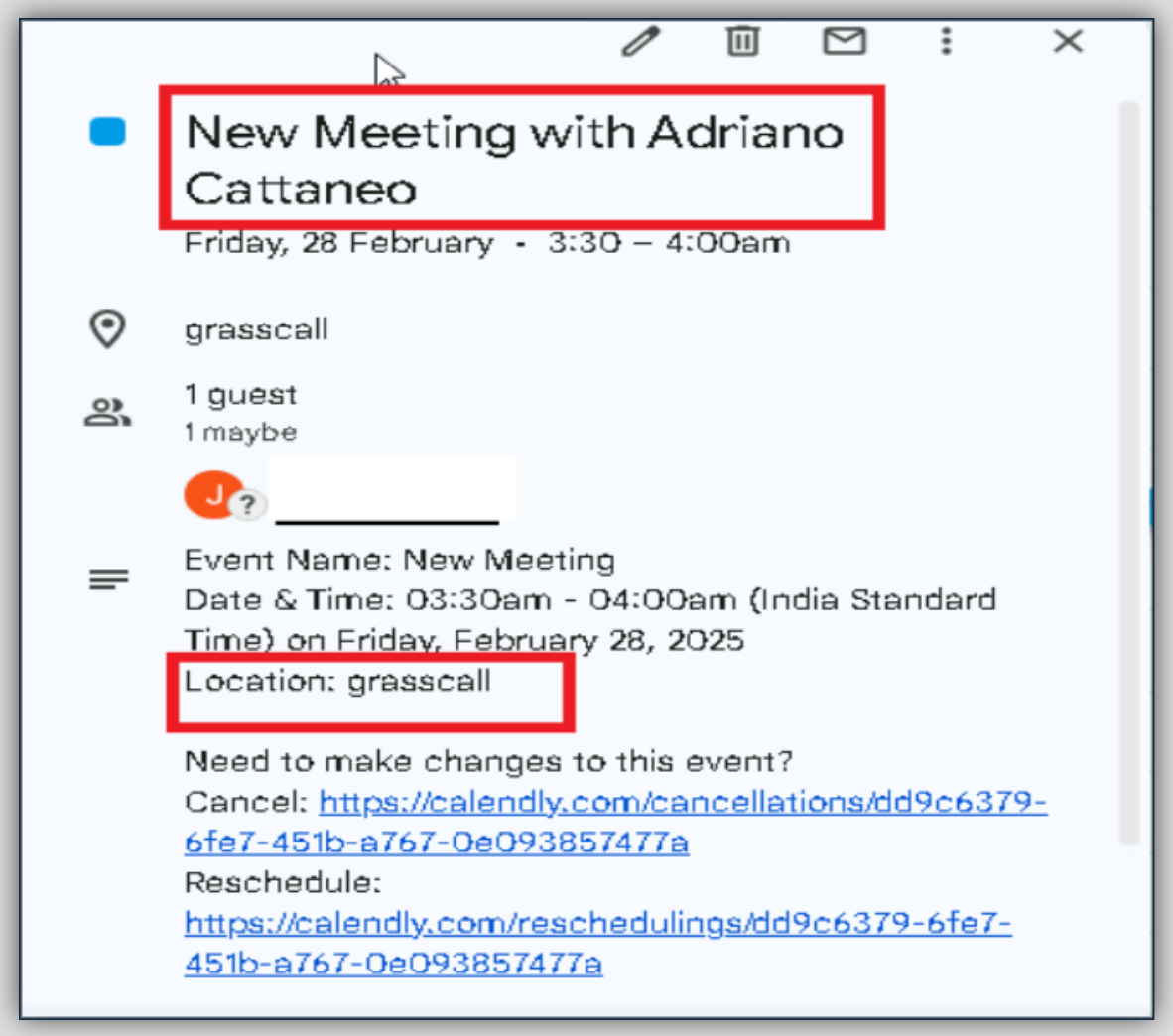
- They publish high-quality job advertisements on reputable job boards like LinkedIn, Well-found, and Crypto Jobs List to attract unsuspecting applicants

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

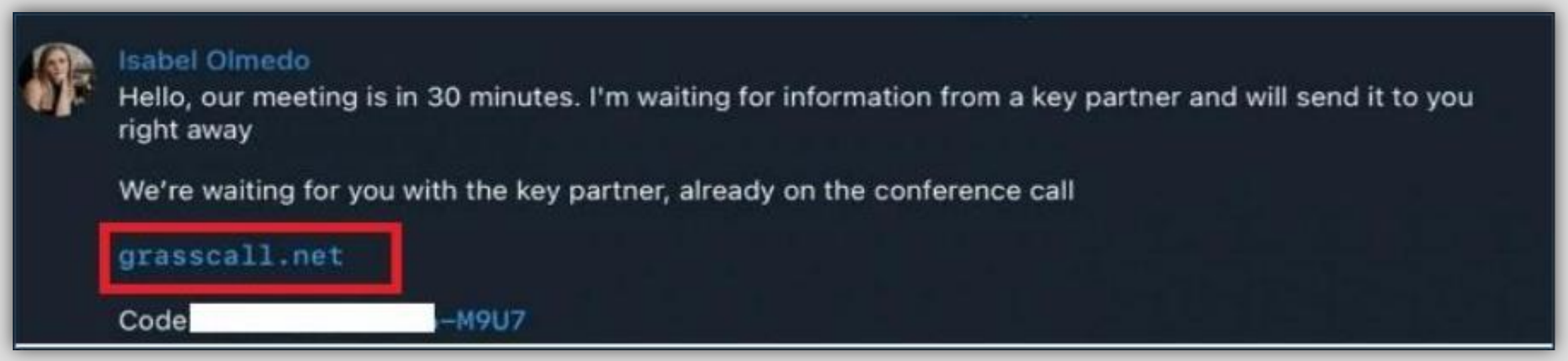




- After candidates schedule their call within the chosen time frame, the CMO or CFO will reach out to them beforehand to provide additional details



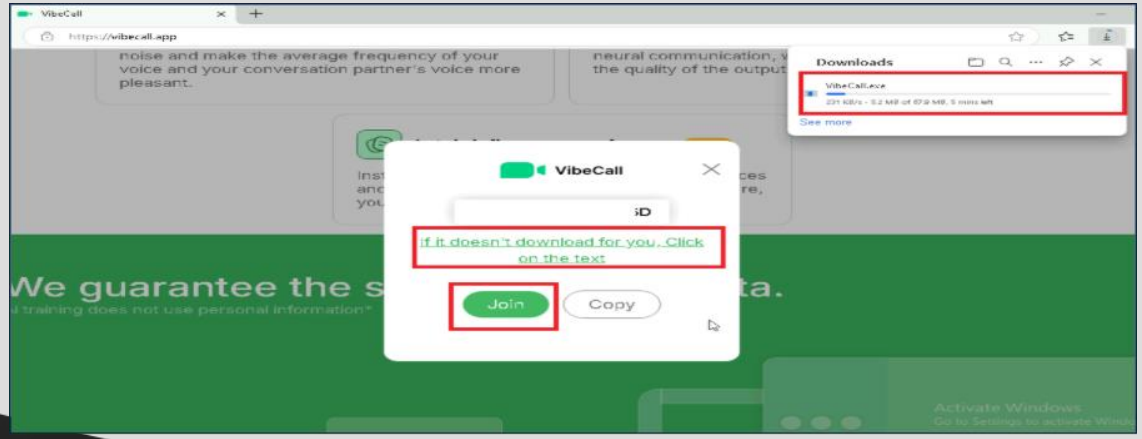
- Before the call, their CFO/CMO contacting the candidate to join the call with shared passcode



- 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/



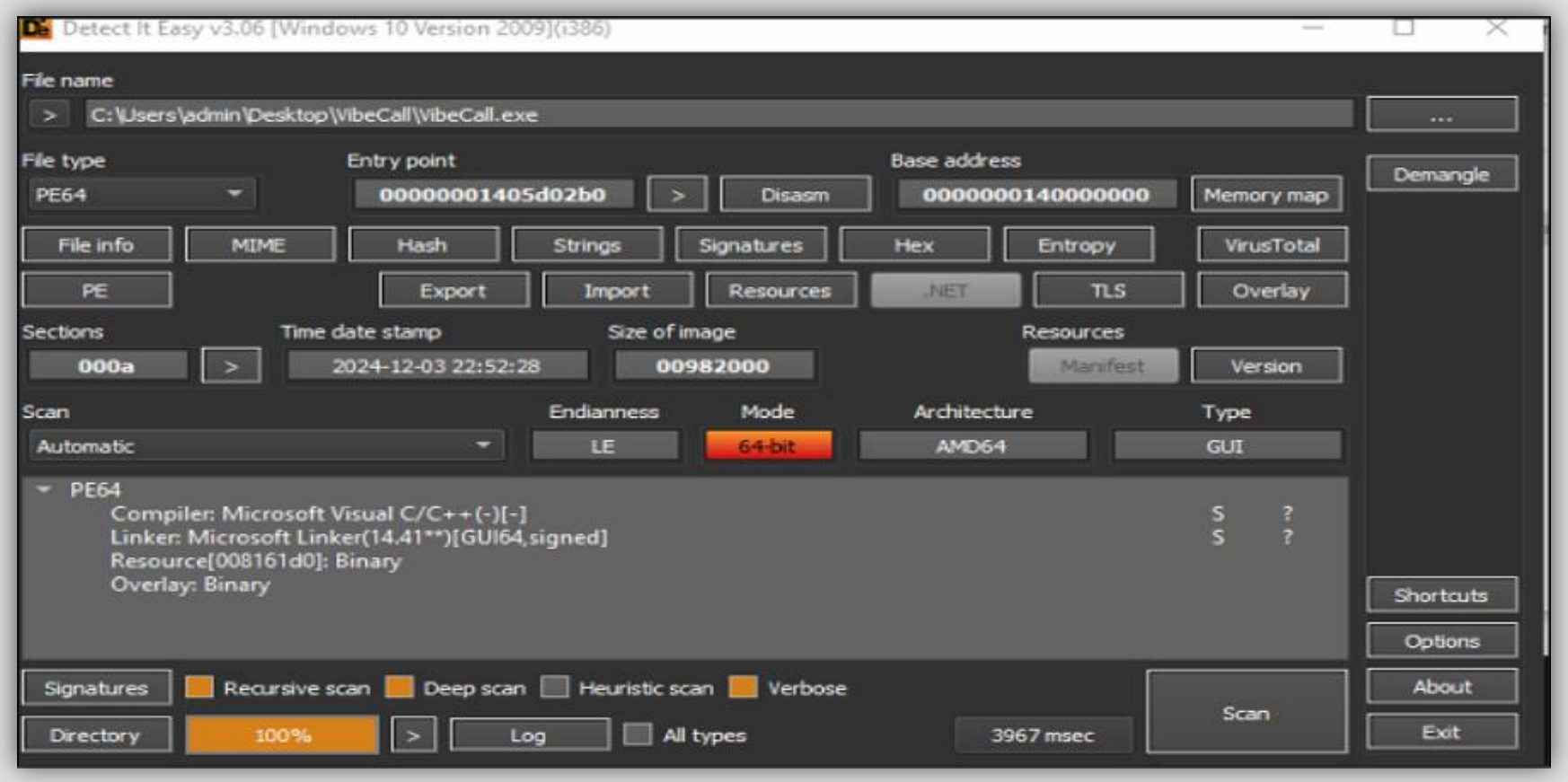
- **Windows Users:** Installing "GrassCall.exe" triggers the deployment of a Remote Access Trojan (RAT) combined with an information-stealing program like Rhadamanthys. These malicious tools enable attackers to maintain ongoing access, log keystrokes, and extract sensitive data, including cryptocurrency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

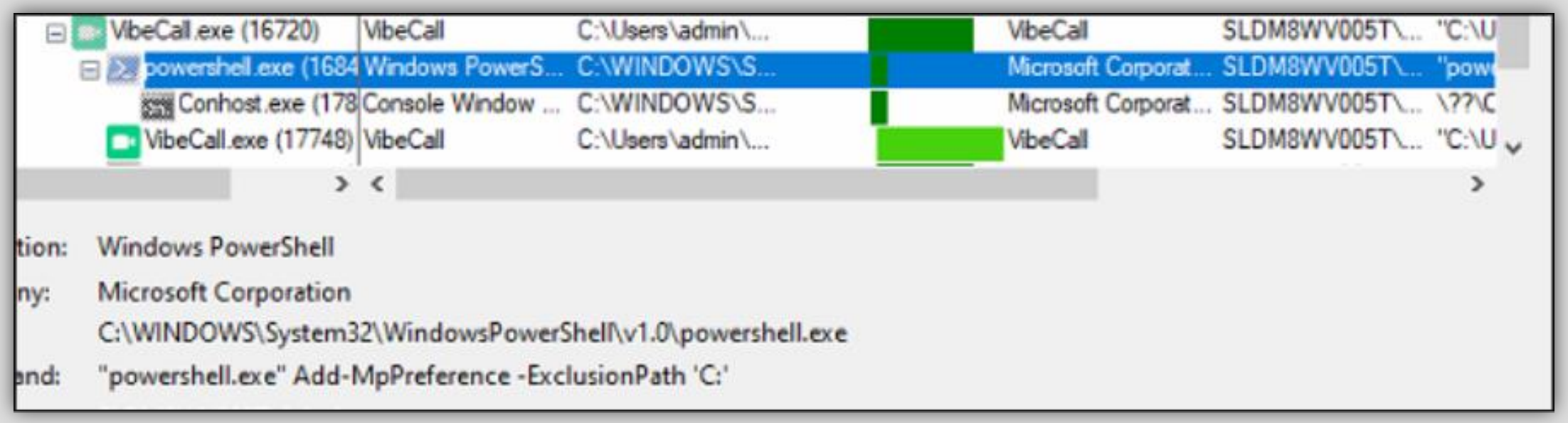
SECRITE | Quick Heal

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

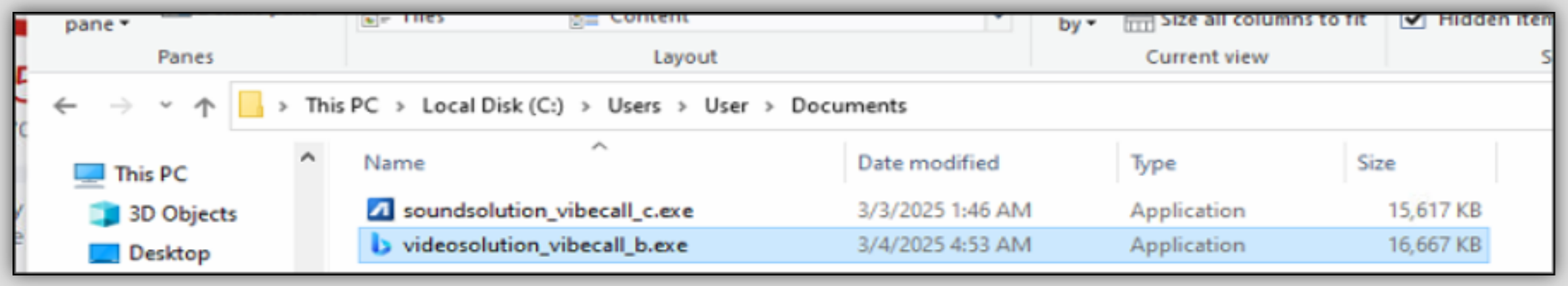
http://rustaisolutionnorisk.com/downloads/contry_solution_vibecall_e.exe
4b371777c2c638c97b818057ba4b0a2de246479776eaaacebccf41f467bb93c3

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

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

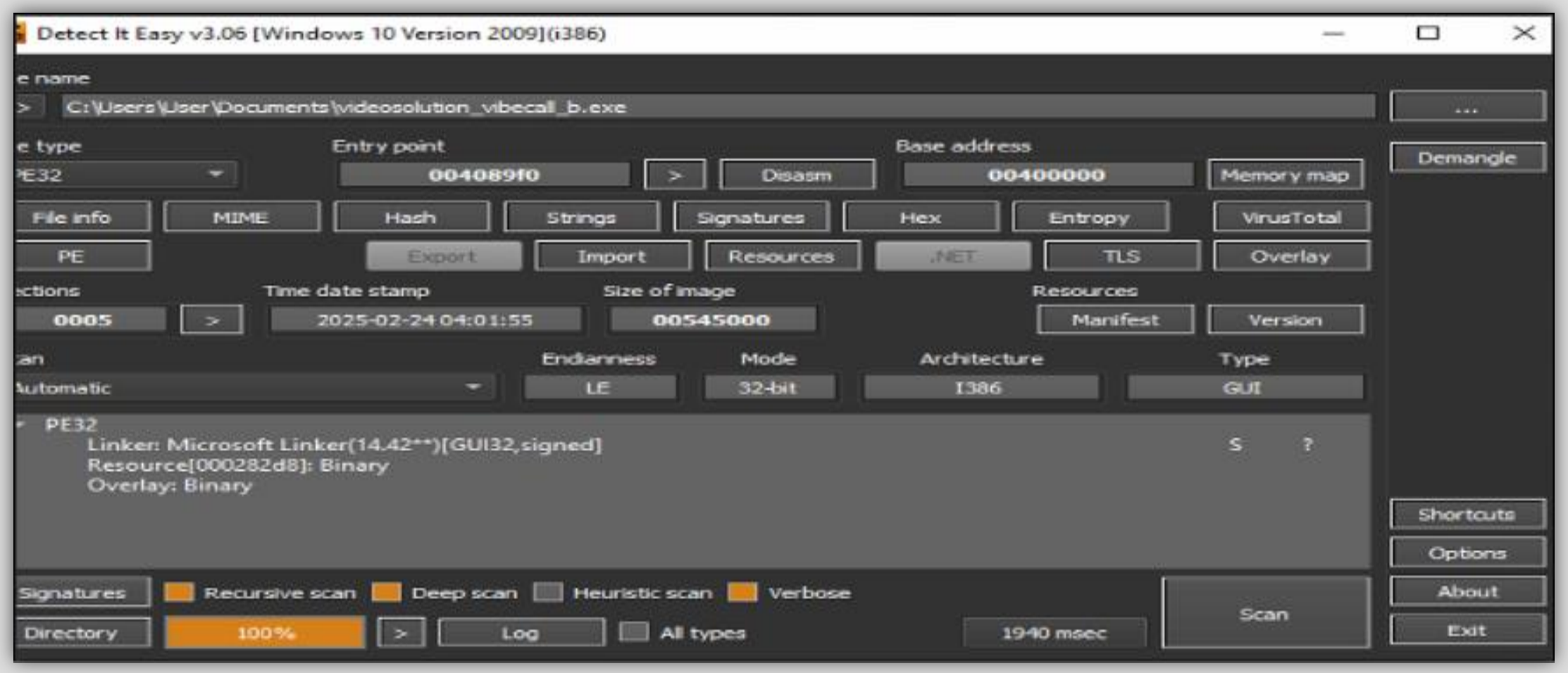
http://rustaisolutionnorisk.com/downloads/videosolution_vibecall_b.exe
386b61ccdd4b785c835a064179d5fa58dc0d5fe34970a04487968e1ee0189ce6

- 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



Anti-Debugging techniques

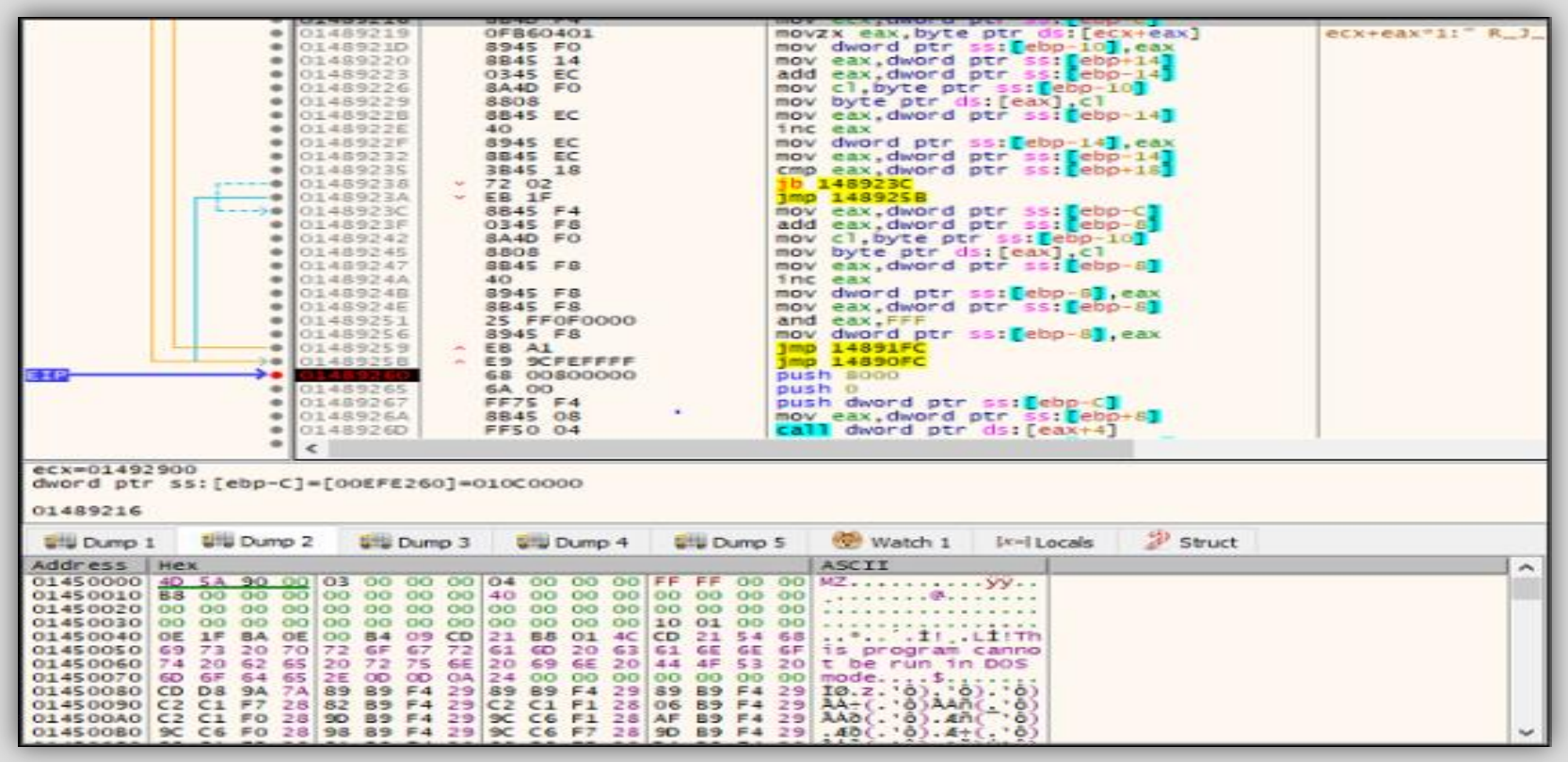
- It checks for processes associated with debugging, reverse engineering, sandboxing etc. It may enumerate running processes and if names match known debugger/analysis tools, it may abort or modify its behaviour.

- We can see APIs like IsDebuggerPresent and IsProcessorFeaturePresent(0x17) + __fastfail **which is used for Anti-Dubugging**

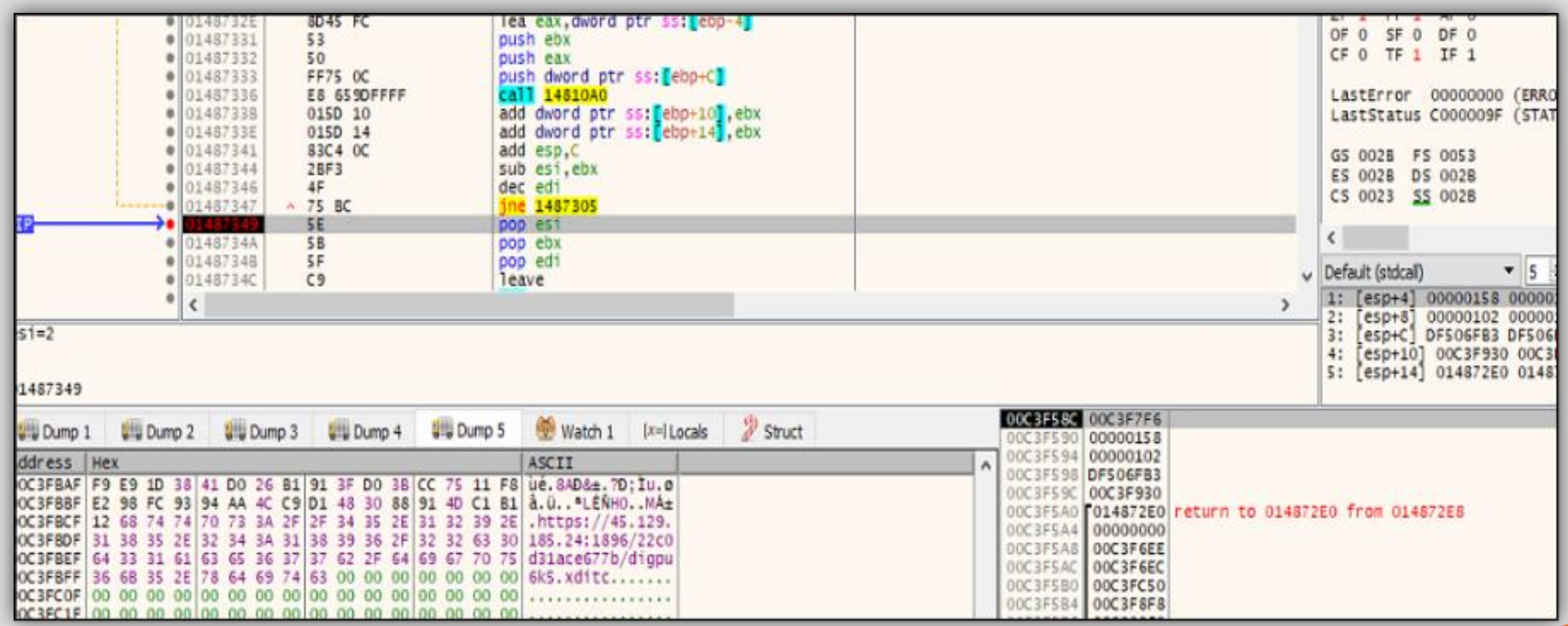
```
BOOL __usercall sub_408E60@<eax>(int a1@<ebx>, int a2@<edi>, int a3@<esi
{
  int v4; // edx
  int v5; // ecx
  unsigned int v6; // kr00_4
  int vars0; // [esp+324h] [ebp+0h]
  int retaddr; // [esp+328h] [ebp+4h]

  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_41D8A0(a1 - 5, v20, 4, &v13, v19, 0x104u);
  if ( v4 )
  {
    v7 = v4(v4, a2, v20, v13, v19, L"Run-Time Check Failure #%d - %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 #%d - %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 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



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.

☐	45.129.185.24 AS 211529	PTR	43843.ip-ptr.tech
☐	45.129.185.24 AS 211529	A	mail.betheew.work
☐	45.129.185.24 AS 211529	A	betheew.work
☐	45.129.185.24 AS 211529	A	mail.idoloegfi.work
☐	45.129.185.24 AS 211529	A	idoloegfi.work

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