2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

THE WOLF OF WALL STEAL: INSIDE CRYPTO TRAFFER GROUP OPERATIONS

Anna Pham

Huntress, USA

Joan Garcia

Universitat Politecnica de Valencia, Spain

cyberninja956@gmail.com
g0njxa@gmail.com

ABSTRACT

This paper presents a comprehensive analysis of cryptocurrency-targeted malware-as-a-service operations through examination of two traffer groups: CryptoLove and Wagmi. These Russian-speaking criminal enterprises demonstrate evolution in malware distribution, social engineering, and organizational structure, collectively generating over $5 million in documented cryptocurrency theft between 2022 and 2025. The research documents the switch from using basic .NET launchers to multi-stage delivery systems leveraging MSIX packaging, promotional code validation, and in-memory payload execution. Analysis reveals anti-analysis implementations, including virtualization detection, certificate abuse patterns, and adaptive evasion techniques. Both operations employed elaborate deception ecosystems featuring fake gaming platforms, business registrations, and Web3 applications targeting 24,527 documented victims across global social media platforms. The research covers the technical infrastructure, including HijackLoader deployment, stealer capabilities (Rhadamanthys, StealC, LummaC2 and AMOS), and certificate rotation that leverages certificate authorities. Findings demonstrate the development of cryptocurrency-focused cybercrime from opportunistic attacks into professional criminal operations with clear hierarchies and training programs, representing a significant threat to the growing cryptocurrency ecosystem.

INTRODUCTION

Crypto traffer groups emerged on Russian-speaking underground forums like Lolz Guru, BHF and XSS as cryptocurrency gained popularity. These ‘underground’ forums served as hacker incubators where individual cybercriminals could learn from each other and eventually form organized teams. The term ‘traffer’ comes from the Russian word ‘Трафер’, referring to criminals who specialize in redirecting internet traffic to malicious content. As cryptocurrency gained mainstream popularity, these forums developed escrow services utilizing cryptocurrency wallets, enabling criminals to conduct business safely with one another. Criminal transactions and communications moved beyond the forums themselves to *Telegram*, creating secure channels for coordinating operations and negotiating deals.

What started as loose collections of individual cybercriminals gradually evolved into structured criminal enterprises, with forum administrators recruiting ‘workers’ and providing training, tools and infrastructure. The forums became recruitment centres where established traffer teams would advertise for new members, offering everything from malware tools to step-by-step guides for conducting crypto scams.

Groups like CryptoLove [1] and Wagmi [2] demonstrate this evolution – CryptoLove was operating for over two years as a developing crypto scam operation, while Wagmi started as the ‘Triple Culture’ team in early 2023 before rebranding. CryptoLove alone logged over 22,000 unique IP addresses from November 2022 until the ‘scam exit’, with top earners like ‘MxDuke’ generating $55,000 from single operations. These organizations employ developers, mentors, profit handlers, and ground-level ‘workers’ in clearly defined roles with performance metrics and commission-based compensation structures ranging from 20-70% of stolen funds.

Both groups, CryptoLove and Wagmi, utilize these forums and *Telegram* channels to recruit new workers, having grown from small teams into large criminal organizations with structured training programs, multiple fake landing pages, and *Telegram* bots that automatically process stolen credentials and logs.

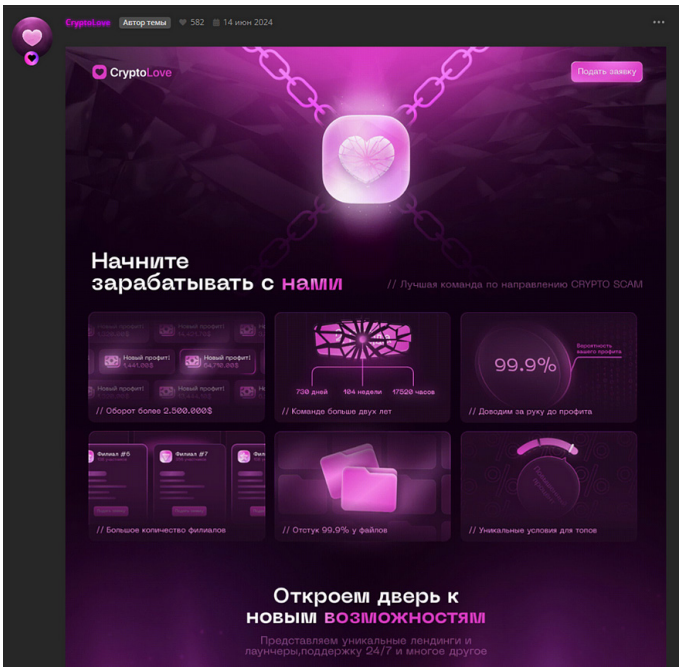


Figure 1: CryptoLove advertisement on hacking forum.

Figure 2: Wagmi advertisement on hacking forum.

Looking at the Russian underground forum screenshot in Figure 3, we can observe the contemporary landscape of traffer operations. The forum showcases a diverse array of illicit services, ranging from fake casinos and cryptocurrency scams to automated payout systems and arbitrage schemes. Notable postings include the Crazy Evil traffer group offering comprehensive cryptocurrency fraud tools, 'Elysium Project' promoting fake casino operations with 24/7 support, and multiple 'fake casino' listings promising high-percentage returns to attract victims. Each crypto traffer group offers specialized services and competes with other groups for market share in the cryptocurrency fraud ecosystem.

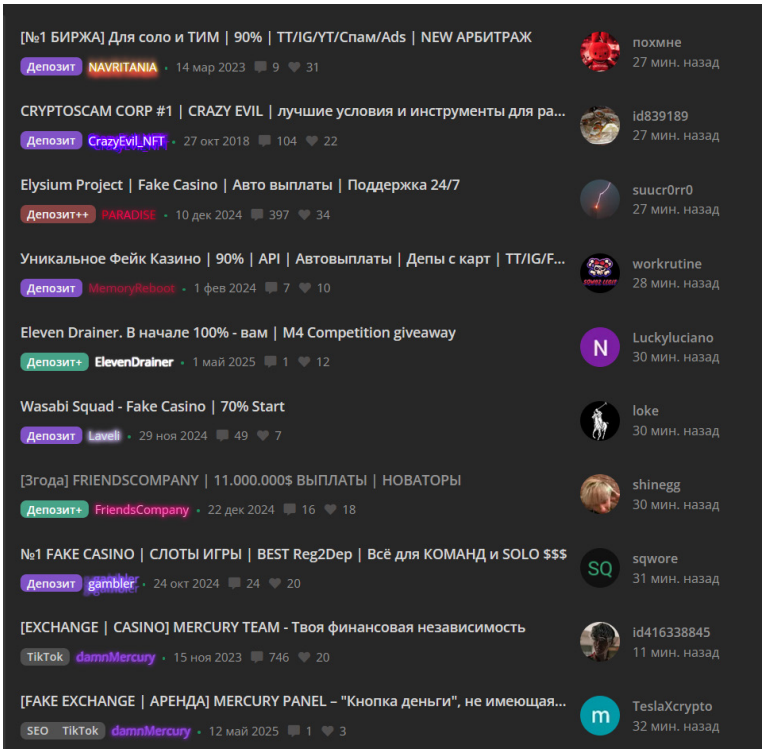


Figure 3: Forum postings from traffer teams.

Victimization

The Wagmi [3] and CryptoLove [4] victim maps shown in Figures 4 and 5 illustrate the global reach of this social-media-based crypto scam operation. Our analysis of 2,422 victim IP addresses of Wagmi and 22,105 IP victim addresses of CryptoLove reveals a widespread distribution across multiple continents, with the highest concentrations in the United States, Nigeria, India, the Philippines, Germany and Canada.

This geographic spread largely reflects where the scammers found their victims through social media platforms, rather than any sophisticated targeting strategy. The Wagmi operation relied heavily on copy-paste social engineering tactics deployed across *X* (*Twitter*), *Telegram*, and other platforms where crypto discussions are common. Victims were essentially those who responded to these scam messages and launched the malicious payloads, which are called 'launchers'.

The prominence of English-speaking countries and regions with large English-speaking populations makes sense given that the scam materials were primarily in English. Countries like Nigeria, India and the Philippines show up heavily not because of deliberate targeting, but because they have large online populations active in crypto spaces, making them naturally more likely to encounter and fall victim to these scams.

What the maps reveal is the global nature of social-media-based cryptocurrency fraud. The scammers cast a wide net across platforms, and victims emerged wherever that net happened to catch people with crypto knowledge and assets. The geographic distribution is more a reflection of global social media usage patterns and the prevalence of the English language than any strategic market analysis by the threat actors.

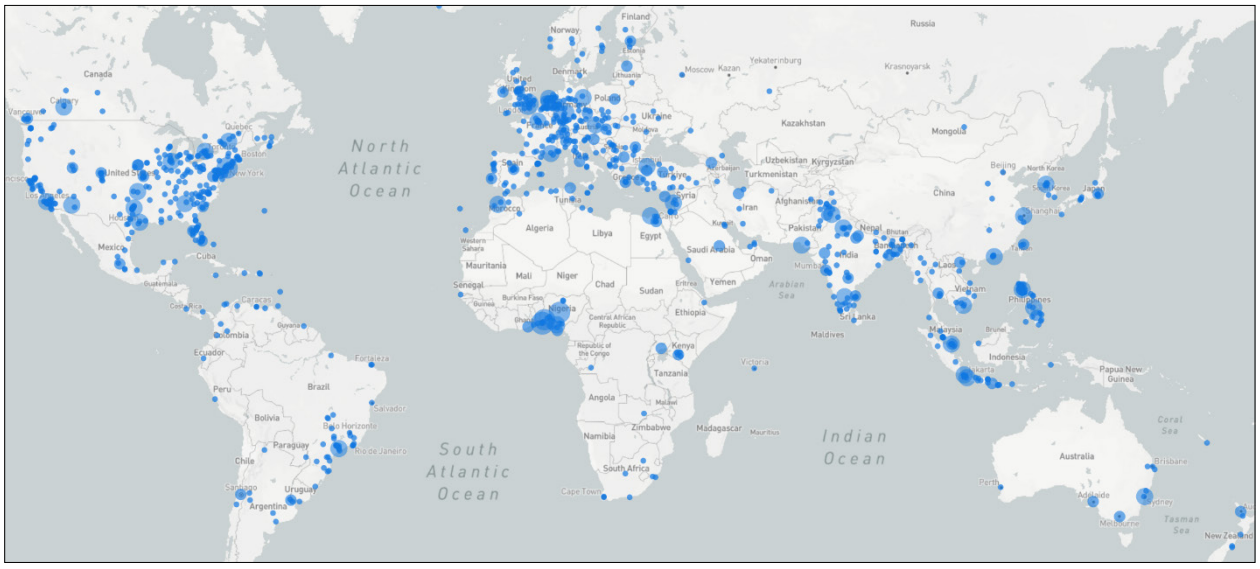


Figure 4: Wagmi victimization map.

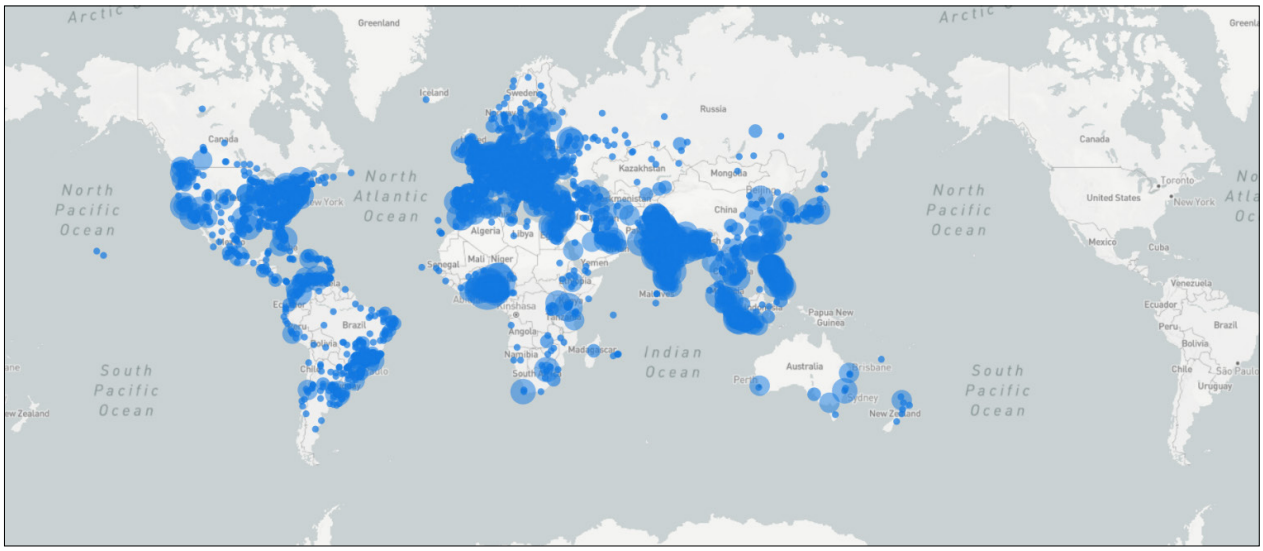


Figure 5: CryptoLove victimization map.

CryptoLove: a multi-million-dollar criminal enterprise

The CryptoLove traffer group represents a substantial cryptocurrency scam operation that has demonstrated considerable financial success, with a calculated total turnover exceeding $2.57 million across seven primary affiliate teams. This hierarchical criminal network has operated for over two years, systematically targeting cryptocurrency holders through elaborate social engineering campaigns disguised as legitimate gaming platforms, PDF readers and video conferencing software.

CryptoLove operated with clear business metrics, offering workers 50-65% payouts from stolen funds while maintaining operational security through geographic restrictions (avoiding Commonwealth of Independent States countries). Their affiliate structure mirrors that of legitimate marketing organizations, with teams such as PROFIT ($966,542 turnover), SCAMQUERTEO/YELLOW EMPIRE ($650,957) and Heaven Era 2.0 ($535,334) operating semi-independently while sharing common infrastructure and malware delivery mechanisms. The group's adaptability is evidenced by their quick adoption of emerging social platforms, such as *Bluesky*, following restrictions on *X* (*Twitter*) in Brazil, and their November 2024 launcher updates that moved to in-memory payload execution to evade detection – changes explicitly made in response to security research pressure.

The highest recorded single theft of $372,000 in Solana, resulting in a $186,328 payout to the worker, illustrates the significant financial impact on individual victims. This case study demonstrates how modern cybercriminal organizations have evolved beyond opportunistic attacks to become structured threats.

Wagmi: a $2.4 million cryptocurrency traffer operation

The Wagmi traffer group represents a substantial cryptocurrency scam operation that has demonstrated significant financial success, with documented earnings of at least $2.41 million between June 2023 and March 2025. Operating under the initial 'Triple Culture' branding before rebranding to Wagmi, this criminal network has maintained operations for over two years, systematically targeting Web3 community members and cryptocurrency holders through sophisticated social engineering campaigns. The organization's approach centres on impersonating legitimate mobile games and video conferencing software, creating convincing façades that have successfully deceived 2,422 documented victims across multiple platforms, including *Discord*, *X* (*Twitter*), and various NFT marketplaces.

The group allegedly has developed automated scraping tools to harvest cryptocurrency wallet addresses that are publicly posted on social media platforms, particularly targeting users involved in token airdrops and Web3 activities. Their operational methodology mirrors legitimate business practices, with clear hierarchical management under @DanbiWoo and @scarletexe, standardized worker manuals (albeit plagiarized from larger traffer groups like Crazy Evil). The organization's adaptability is evident in its rapid pivoting between different scam themes – from fake gaming platforms mimicking legitimate mobile games like *Takedown Legends* and *Tokyo Beast* to fraudulent meeting software impersonating *Zoom* and other conferencing tools.

The group's malware delivery infrastructure utilizes code-signed executables obtained through fraudulent means to bypass the User Account Control (UAC) prompt. The group deploys platform-specific malware, including LummaC2 and Rhadamanthys stealers for *Windows* systems via HijackLoader, and AMOS stealer for *macOS* environments.

CRIMINAL ENTERPRISE ORGANIZATION

CryptoLove has operated as a criminal group with a well-defined hierarchical structure for over two years. The organization has specialized roles and systematic operational procedures typical of organized cybercrime syndicates.

Organizational structure

The CryptoLove criminal group operates through a traditional hierarchical model with distinct operational layers. At the apex sits LanRock (@lanrock_dev), the primary developer responsible for the organization's technical infrastructure, including custom launchers, loaders, and administrative panels used across all affiliate operations.

The management layer consists of specialized support personnel who handle critical operational functions. Routine (@RoutineLove3) serves as the primary log handler, working 12-16 hours daily to process and parse stolen victim data. This role is complemented by general support staff including SS (@sssmmmnu) and Kupidon (@kup1donLove3), both of whom have been with the organization since 2022. Oscar (@magnificent_oscar) functions as the senior support manager and oversees the Mr. Beast affiliate team while managing money-laundering operations.

Individuals with specific technical and social engineering expertise manage specialized operations. Querteo (@yellowscam) leads the SCAMQUERTEO/YELLOW EMPIRE team and develops fraudulent landing pages, while Pink (@PinkorexxLove3) specializes in social engineering operations from her base in Israel. MxDuke (@mrxuyux) represents the organization's most successful operator, managing the Profit Team and is responsible for the most significant documented theft of approximately $372,000 in the Solana cryptocurrency.

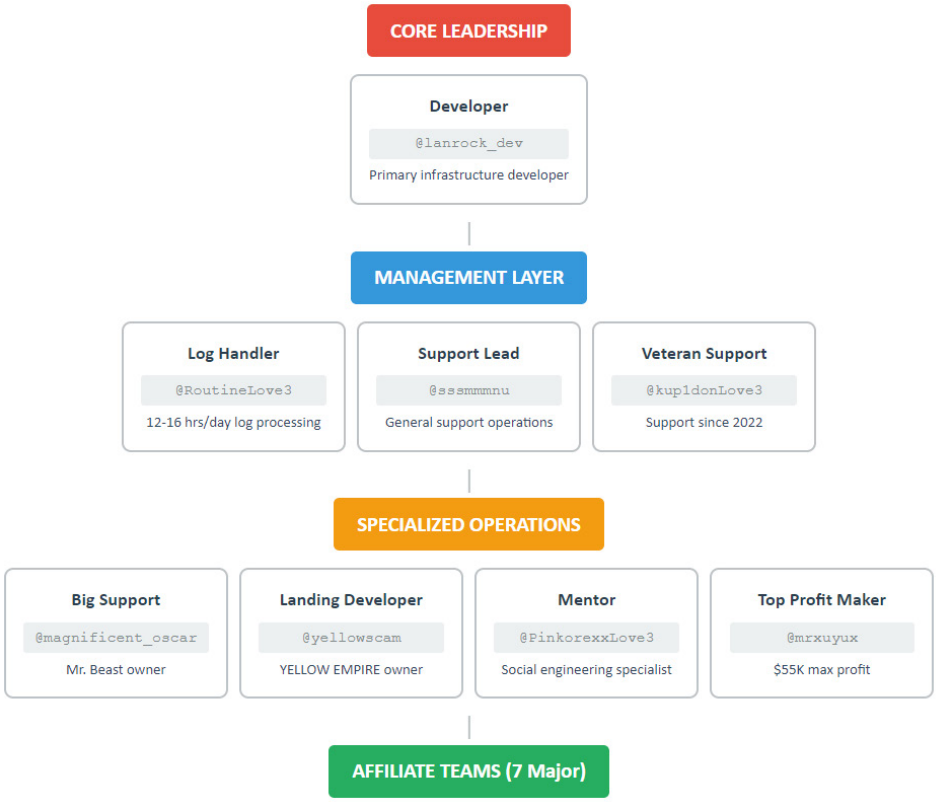


Figure 6: Diagram of CryptoLove organizational structure.

Affiliate team operations

The organization operated through seven major affiliate teams that functioned as semi-autonomous criminal units.

Affiliate team	Turnover	Specialization
PROFIT Team	$966,542	Gaming platforms, PDF readers
YELLOW EMPIRE	$650,957	PDF readers, meeting software
Heaven Era 2.0	$535,334	Gaming, meeting software
Wolves of Wall Street	$300,270	Gaming metaverse projects
ObmanVALUT	$77,404	Meeting software
Mr. Beast	$31,680	Gaming, PDF readers
CAPS LANDS	$10,774	Web3 software

The launchers

The CryptoLove launchers we analysed dropped Rhadamanthys and StealC for *Windows* and AMOS Stealer for *macOS*. During our analysis period, we successfully reported several Extended Validation (EV) certificates used to sign the malicious launchers, including certificates from Chengdu Yihui Weimeng Network Technology Co., Ltd, and Shenzhen Xinshitong Network Technology Co., Ltd.

The earliest observed CryptoLove distribution mechanism employed unbundled .NET executables with direct command-and-control communication. Upon execution, the primary launcher initiated system reconnaissance through the `sendstart()` method, establishing communication with infrastructure at `xilloolli[.]com/api.php`.

System profiling capabilities

The launcher implements comprehensive system profiling through two primary functions:

- Cryptocurrency wallet enumeration, where the launcher looks for 17 distinct cryptocurrency wallet browser extensions, including major platforms such as *MetaMask*, *Phantom Wallet*, *Binance Chain Wallet* and *Coinbase Wallet*. The enumeration process generates numerical identifiers corresponding to detected wallets, which are transmitted to the command infrastructure.

- Anti-virus detection mechanism – anti-virus identification occurs through Windows Management Instrumentation (WMI) queries targeting the `SecurityCenter2` namespace's `AntivirusProduct` class. Detected products receive numerical identifiers that are incorporated into the telemetry data structure.

Anti-analysis implementation

The `CheckEmulation()` method implements multiple environmental checks designed to detect analysis environments:

- Memory availability verification (minimum 4GB requirement)
- Current directory location assessment
- Executable filename length validation (maximum 11 characters)
- Hard-coded username and machine name blacklisting

Detection of analysis environments triggers a warning message: '`An attempt to launch a program using a virtual machine was detected. Update rejected (error code: D24VM09)`'.

Payload distribution architecture

The `PolicyGeneretic()` method orchestrates a three-stage payload delivery system through sequential task execution (`TaskLoad`, `TaskLoad2`, `TaskLoad3`). The system creates a '`microsoftgame`' directory under Program Files for payload storage and implements error reporting for each delivery attempt. The tasks execute sequentially with sleep intervals of 15 seconds and 20 seconds, respectively.

`TaskLoad` operates through the following sequence:

- Checks if the target file (e.g. `1.exe`) exists in the directory and deletes it if present to ensure the latest version download.
- Reports download attempts via the `download_first_bug()` method, with requests structured as: `hxxtp://xilloolli[.]com/api-debug.php?status=2&proc=[CPU_INFO]&av=[AV_ID].`
- Executes `1.exe` from the saved location and transmits success confirmation through the `sendopen1()` and `opened_first_bug()` methods, generating requests such as: `hxxp://xilloolli.com/api[.]php?status=4&wallets=1,5,7&av=1,3` and `hxxp://xilloolli.com/api-debug[.]php?status=3&proc=[CPU_INFO]&av=1,3`.
- Implements error handling with specific status codes: status=11 for execution failures, status=12 for fallback scenarios when files exist but cannot execute, and status=10 for download failures.

`TaskLoad2` and `TaskLoad3` follow similar operational patterns with different payloads and corresponding status codes, ensuring redundant delivery mechanisms for payloads.

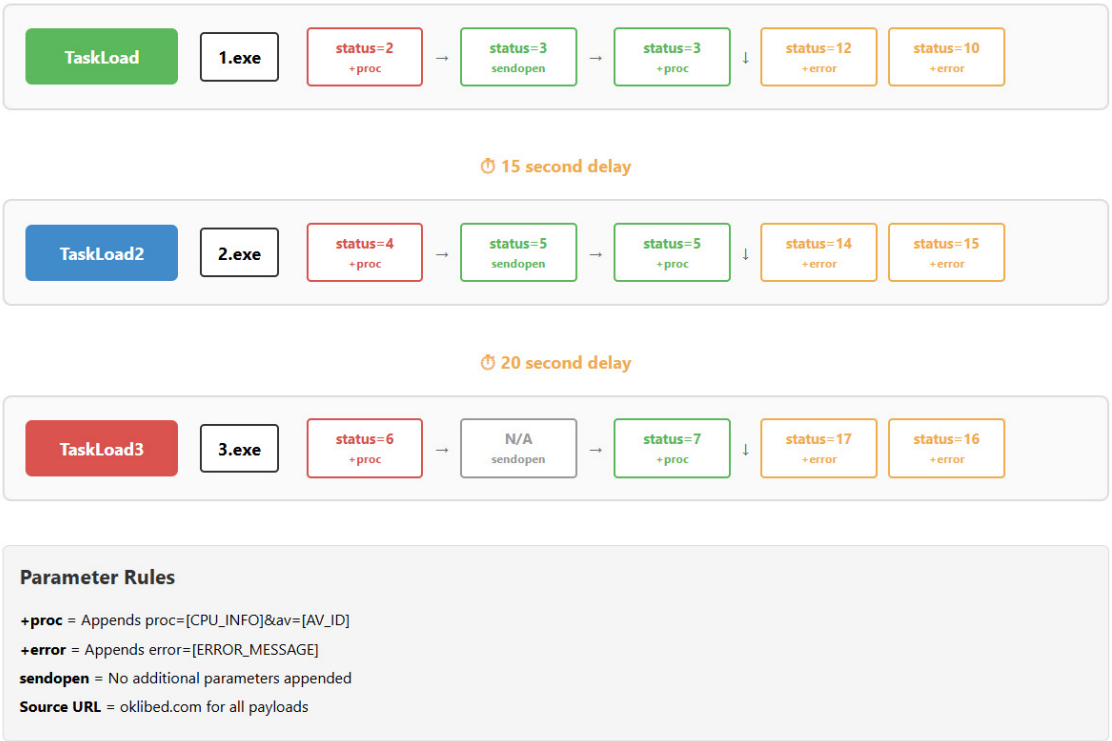


Figure 7: CryptoLove task execution flow.

MSIX implementation (October 2024)

October 2024 marked a significant architectural shift with the introduction of MSIX packaging for distribution. The MSIX container (hash: `9d4302876124b31deca3254bc0d0bfee`) encapsulated `TinyPatch.exe`, a .NET bundle containing runtime dependencies to reduce detection rates.

Unlike the previous launcher's comprehensive system profiling, this launcher variant implemented a simplified operational model. Similarly to the previous launcher, the `sendstart()` method initiates the main operation, while the `sendclick2()` method is triggered when the user clicks 'Cancel' during payload installation. Upon this action, a `POST` request is sent to the command-and-control (C2) server with the structure `?status=3&wallets=0&av=0`, indicating that the installation was cancelled (status=3), and no cryptocurrency wallets (wallets=0) or anti-virus programs (av=0) were found.

The core payload management occurs through the `DownloadManagement()` method, which operates as follows:

- Verifies if the target file (`1.exe`) exists in the specified temporary directory named 'LPC' and deletes it if present to ensure fresh payload downloads.
- Checks for the existence of the temporary directory and creates it if absent.
- Verifies that no running process named '1' corresponding to the `1.exe` payload exists.
- Initializes a WebClient to download data from the pre-configured URL and saves the payload in the 'LPC' directory as `1.exe`.

This launcher variant notably lacks the cryptocurrency wallet enumeration and anti-virus detection functionalities present in the September 2024 implementation. Additionally, it references '`gravitiumgame`', a landing page previously associated with the Heaven Era Team, suggesting potential operational connections or infrastructure reuse.

A secondary enhancement involved implementing .NET Reactor obfuscation while maintaining identical functional behaviour, demonstrating the threat actor's focus on evasion rather than capability expansion.

Promotional code system

The CryptoLove group initially released a major launcher update using the existing .NET framework, but removed the .NET Reactor obfuscation layer. Subsequently, they transitioned to DevelNext, an integrated development environment for PHP based on JPHP (Java-based PHP implementation). This shift represented a fundamental change in their development approach, moving away from traditional .NET implementations toward Java-based PHP payloads.

The enhanced system introduced a promotional code validation mechanism designed to restrict access and complicate analysis efforts. Code validation occurs through specific API endpoints, with launchers sending requests to `apikokoapi[.]com/add_code.php?method=get&code=code_entered`. The server responds with JSON structures indicating validation status: `{"available":true,"code":"XYZ","username":"#worker_handle"}`. Upon successful validation, the launcher retrieves the primary payload from `77.105.166[.]229/qicudt52b.dll`, while device registration and logging functions utilize separate infrastructure at `service-government[.]com/api.php`.

This mechanism serves multiple operational purposes: affiliate attribution tracking for accurate commission distribution, excluding analysis environments, and ensuring operational security through access control limitations.

Pe-Loader implementation and process hollowing

The initial November 2024 payload delivery mechanism leveraged `qicudt52b.dll`, a DLL loader based on the open-source Pe-Loader project [5], as evidenced by the PDB path: `C:\Users\Администратор\Documents\Pe-Loader-Sample-master\Release\Pe-Loader-Sample.pdb`. This loader implements process hollowing techniques for payload injection and retrieves final-stage malware from hard-coded URLs:

- `77.105.166[.]229/beast2` – LummaC2 stealer deployment
- `77.105.166[.]229/beast1` – StealC infostealer deployment

Figure 8 shows a snippet of the DLL loader.

Affiliate build identification system

Analysis revealed distinct build identifiers corresponding to specific affiliate operations, enabling attribution and commission tracking:

- ObmantVault: 'obman' build identifier
- Yellow Empire: 'yellow' build identifier
- Mr. Beast: 'beast' build identifier
- PROFIT Team: 'profitable' build identifier

```
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      }
```

Figure 8: Snippet of qicudt52b.dll.

Morpheme loader

The subsequent November evolution introduced the 'Morpheme' loader. This loader implements reflective loading methodologies to dynamically allocate, load and execute payloads entirely within the current process memory space, avoiding traditional file-based detection mechanisms.

Key technical implementations include:

- AsmJit library integration, which facilitates dynamic memory allocation and executable payload management within process boundaries.
- API encryption, which includes simple XOR encryption schemes and obscures *Windows* API calls from static analysis.
- Code obfuscation, which includes garbage function implementation, significantly increasing reverse engineering complexity and analysis time requirements.
- Capability of deploying LummaC2, StealC or Rhadamanthys stealers, based on operational requirements.

```
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;
```

Figure 9: InternetReadFile API obfuscated with XOR (Morphene32.exe).

Wagmi Windows infection chain

The Wagmi *Windows* infection chain begins with HijackLoader being injected into the `more.com` process, subsequently leading to `tcpvcon.exe` being executed and dropped in the `%TEMP%\21415` directory. This execution chain ends with the deployment of LummaC2 infostealer as the final payload. Analysis of captured LummaC2 configurations revealed user identification '`xMnLq7`' with build identifier '`SPL`' corresponding to Wagmi's Splare landing page operations, demonstrating systematic attribution tracking across the group's infrastructure.

HijackLoader anti-analysis implementation

HijackLoader implementation incorporates comprehensive virtualization detection mechanisms designed to evade analysis environments [6]. The `vm_calc_cpu_cycles()` function implements precise timing analysis by executing CPUID instructions within 100-iteration loops, utilizing RDTSC (Read Time-Stamp Counter) instructions to capture CPU timestamps before and after each CPUID execution. The timing differential analysis exploits the measurable overhead introduced by hypervisor instruction trapping and emulation, creating consistent timing signatures that distinguish between virtualized and bare-metal execution environments.

Intel's standardized hypervisor detection is implemented through the `vm_check_if_hypervisor_present()` function, which executes CPUID with EAX set to 1 and examines bit 31 of the ECX register. This bit serves as *Intel*'s designated hypervisor presence indicator [7], providing reliable detection of virtualized execution contexts. Additional hypervisor identification occurs through the `vm_cpuid_check()` function, which executes CPUID with EAX=0x40000000 (hypervisor leaf) to identify hypervisor-specific signatures.

Environmental validation extends beyond virtualization detection through the `mw_vm_additional_checks` function, which implements username and computer name validation. The system checks explicitly for numeric-only identifiers commonly used in automated analysis environments and verifies that the executable is not running from the user's desktop directory, a common characteristic of manual analysis scenarios.

```
14  v3 = 0;
15  v4 = (_DWORD *)vm_modules_check(a2, &v3, 0x4DAD7707);
16  if ( !v4 )
17    return 1;
18  v5 = v4;
19  if ( (*v4 & 1) != 0 && vm_calc_cpu_cycles((int)v5) )
20    return 0;
21  if ( (*v5 & 4) != 0 && (unsigned __int8)vm_check_if_hypervisor_present() )
22    return 0;
23  if ( (*v5 & 8) != 0 && vm_cpuid_check() )
24    return 0;
25  if ( (*v5 & 0x10) != 0 && mw_vm_GetTotalPhysicalMemory(a1, (int)v5) )
26    return 0;
27  if ( (*v5 & 0x20) != 0 && mw_GetNumberOfProcessors(a1, (int)v5) )
28    return 0;
29  if ( (*v5 & 0x40) != 0 )
30  {
31    nullsub_1(0, 216);
32    if ( mw_vm_additional_checks(a1, (int)v5) )
33      return 0;
34  }
35  return 1;
36}
```

Figure 10: Snippet of the anti-VM code.

HijackLoader implements *VMware* identification by searching for *VMware*'s I/O port magic signature (`0x564D5868` – '`VMXh`'), which allows the identification of *VMware*'s hypervisor communication channel. Upon detection, the system performs product-specific identification, distinguishing between *VMware Express*, *ESX*, *GSX*, *Workstation* and generic *VMware* implementations.

Secondary detection utilizes CPUID instruction with hypervisor leaf 0x40000000 to extract *VMware*'s vendor ID string through little-endian encoding analysis. The system checks for 'VMware' across three 32-bit values: `0x61774D56` corresponds to 'VMwa', `0x4D566572` represents 'reVM' and `0x65726177` indicates 'ware'

Beyond *VMware* detection, the implementation includes identification capabilities for *VirtualBox* and *Sandboxie* environments, ensuring comprehensive coverage of common analysis platforms.

```
12  mw_vmware_magic_signature = 0;
13  v2 = vm_check_vmware_((int)a1);
14  if ( mw_vmware_magic_signature == 0x564D5868 )// VMXh
15  {
16    v3 = v2 - 1;
17    if ( v3 )
18    {
19      v4 = v3 - 1;
20      if ( v4 )
21      {
22        v5 = v4 - 1;
23        if ( v5 )
24        {
25          if ( v5 != 1 )
26            return mw_vm_check_handler(a1, (__int32)&g_vmware_generic_str);
27          return mw_vm_check_handler(a1, (__int32)&g_vmware_workstation_str);
28        }
29        else
30        {
31          return mw_vm_check_handler(a1, (__int32)&g_vmware_gsx_str);
32        }
33      }
34      else
35      {
36        return mw_vm_check_handler(a1, (__int32)&g_vmware_esx_str);
37      }
38    }
39    else
40    {
41      return mw_vm_check_handler(a1, (__int32)&g_vmware_express_str);
42    }
43  }
44  else
45  {
46    if ( mw_vm_check_cpuid_hypervisor() )
47      return mw_vm_check_handler(a1, (__int32)&g_vmware_generic_str);
48    return mw_vm_not_detected_handler(a1);
49  }
50}
```

Figure 11: VMware detection function.

Recent evolution in Wagmi's evasion techniques includes Delphi-based packers containing anti-VM functionalities, demonstrating continued adaptation beyond the use of HijackLoader.

CODE-SIGNING CERTIFICATE ABUSE IN TRAFFER OPERATIONS

The abuse of legitimate code-signing certificates represents a critical component of modern malware distribution strategies, particularly within traffer operations targeting cryptocurrency assets.

Traffer groups acquire legitimate Extended Validation (EV) code-signing certificates through corporate entities, leveraging these credentials to bypass *Windows SmartScreen* protections, reduce User Account Control (UAC) prompts, and achieve significantly lower detection rates across security solutions. This approach exploits the inherent trust mechanisms built into operating systems, creating a false legitimacy that substantially increases the success rate of infections among targeted victims.

The Wagmi and CryptoLove operations consistently relied on *GlobalSign* and *Certum* certificates obtained through multiple entities across different geographic regions, including Vietnam, China and India. This diversification strategy suggests a sophisticated understanding of certificate authority validation processes and deliberate efforts to avoid detection patterns that might trigger enhanced scrutiny.

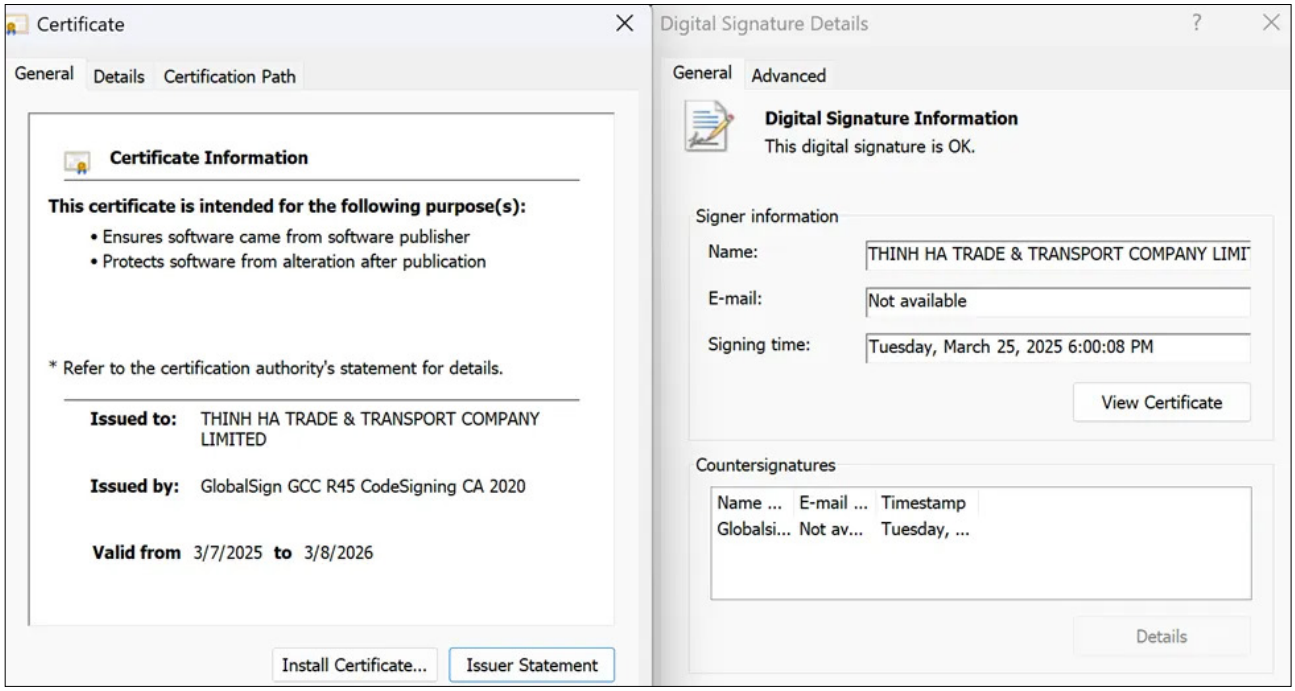


Figure 12: Payloads signed with EV certificates (1).

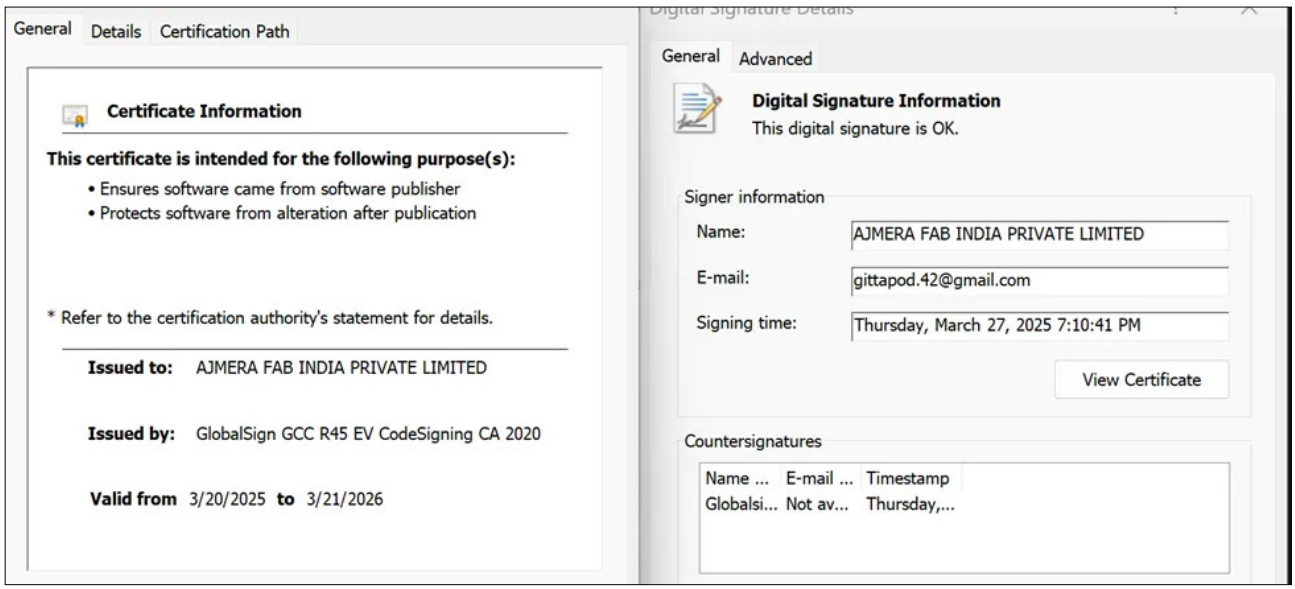


Figure 13: Payloads signed with EV certificates (2).

Operational impact of certificate revocation

Certificate revocation efforts have demonstrated measurable impact on traffer operations through multiple mechanisms. Revoked certificates trigger *SmartScreen* warnings for previously trusted executables, immediately reducing infection success rates and requiring operational adaptation. The financial costs associated with acquiring replacement certificates, combined with the operational overhead of re-signing and redistributing malware builds, impose significant resource burdens on threat actors.

Internal communications captured from Wagmi operations revealed explicit discussions regarding 'issues with the new EV certificate after revocation', indicating direct operational impact and forcing tactical adjustments. This evidence suggests that systematic certificate revocation campaigns represent an effective disruption methodology that should be prioritized by researchers.

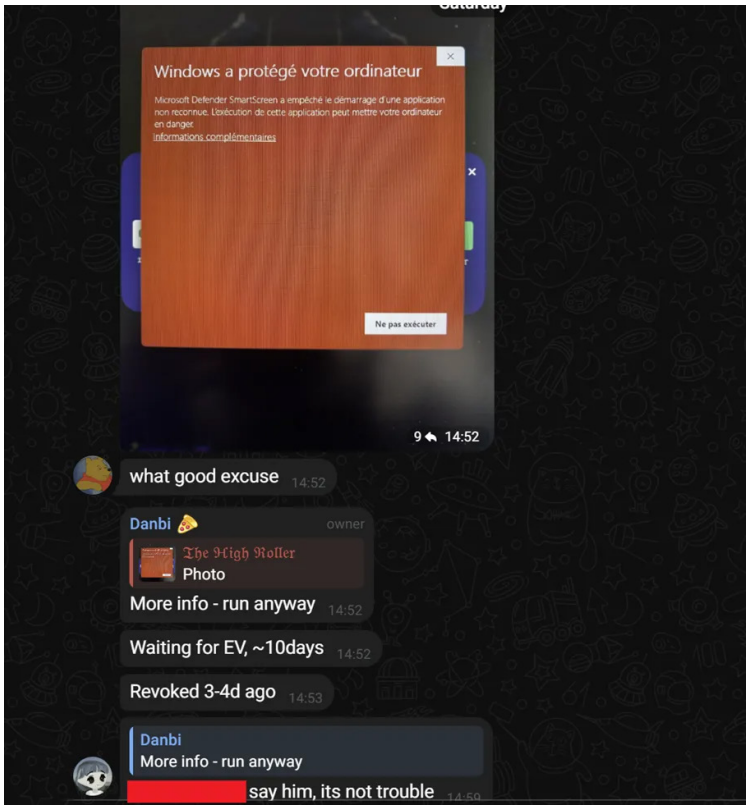


Figure 14: Dialog on the UAC prompt after EV certificate revocation (source: Telegram).

SOCIAL ENGINEERING AND VICTIM TARGETING

Mastering social engineering has become a crucial skill in the threat ecosystem, enabling individuals to successfully trick others into downloading and executing malware on their personal computers. Using fake identities and an apparently trustworthy engagement context, traffers will start a scam operation against victims previously identified as potential crypto holders. These potential victims are identified through the parsing of social media scraped data using automated tools and the exploitation of platforms related to cryptocurrencies, following the global trends and profiting from the emergence of new projects.

Victim identification and platform targeting strategies

It has been observed that CryptoLove and Wagmi traffers exploit platforms such as DappRadar – a platform that provides insights, analytics, and tracking services for decentralized applications (dApps) and blockchain-based projects – to find victims in their media channels like *Discord*, messaging the project's admins, holders, or users with *Nitro* subscriptions as they are considered potential high-balance money investors. By examining popularity and user base rankings, workers can be trend-conscious and start targeting crypto investors within their own Web3 communities, even using this information to impersonate legitimate dApps.

Despite the popularity among the traffer community of using traditional social media platforms such as *X* (*Twitter*), *Discord* or *Telegram* to engage in conversations with victims, CryptoLove and Wagmi workers have been aware of the

rapid growth of alternative social media platforms such as *Bluesky* – a service that has emerged as a significant counterpart in regions where *X* faces restrictions, attracting a substantial user base, including high-profile influencers who have migrated from *X*. Traffers have been observed adapting to the global trends and starting to target the users of *Bluesky*.

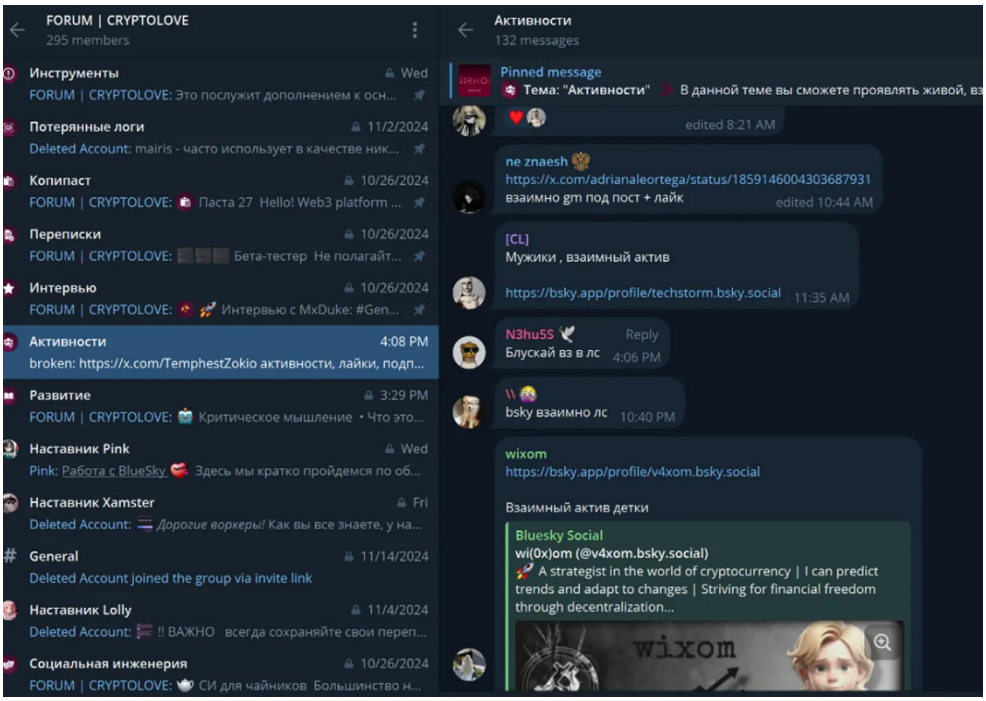


Figure 15: Workers sharing their X and Bluesky accounts and requesting engagement (source: Telegram).

Account acquisition

Traffer teams depend on authentic-looking, cryptocurrency-themed social media accounts to conduct successful scam operations. Establishing victim trust requires traffer team workers to present credible personas during the initial contact phases.

To achieve this credibility, workers systematically purchase pre-configured social media accounts through specialized services that are prevalent within the traffer ecosystem. These services include Aqua Twitter, Tiffany Store and Alpha Store, all operating as *Telegram*-based bots that facilitate rapid account acquisition across multiple social media networks, particularly *X* and *Discord*.

These marketplace services operate tiered pricing structures based on account authenticity and preparation levels:

- Entry-level pricing provides access to standard social media accounts with minimal preparation, suitable for workers operating on limited budgets or conducting high-volume, low-investment campaigns.
- Higher-tier services offer ‘ready-to-go’ *X* accounts specifically configured with cryptocurrency-focused content, follower networks, and posting history. These accounts, likely obtained through credential theft or account compromise, command premium pricing due to their immediate operational utility and enhanced credibility within crypto communities.
- The most expensive tier includes accounts with platform verification status (such as *X*’s blue checkmarks), which significantly enhance perceived legitimacy and enable access to expanded platform features, including direct messaging to users who otherwise restrict communications to verified accounts.

The *Telegram* bot-based infrastructure enables rapid account distribution and management, allowing workers to acquire multiple accounts across different platforms simultaneously. These automated systems manage inventory, process payments through cryptocurrency transactions, and deliver immediate account credentials upon purchase completion.

The marketplace channels feature detailed account listings with specifications including account age, follower counts, engagement metrics, and thematic focus, allowing workers to select accounts optimized for their specific operational requirements.

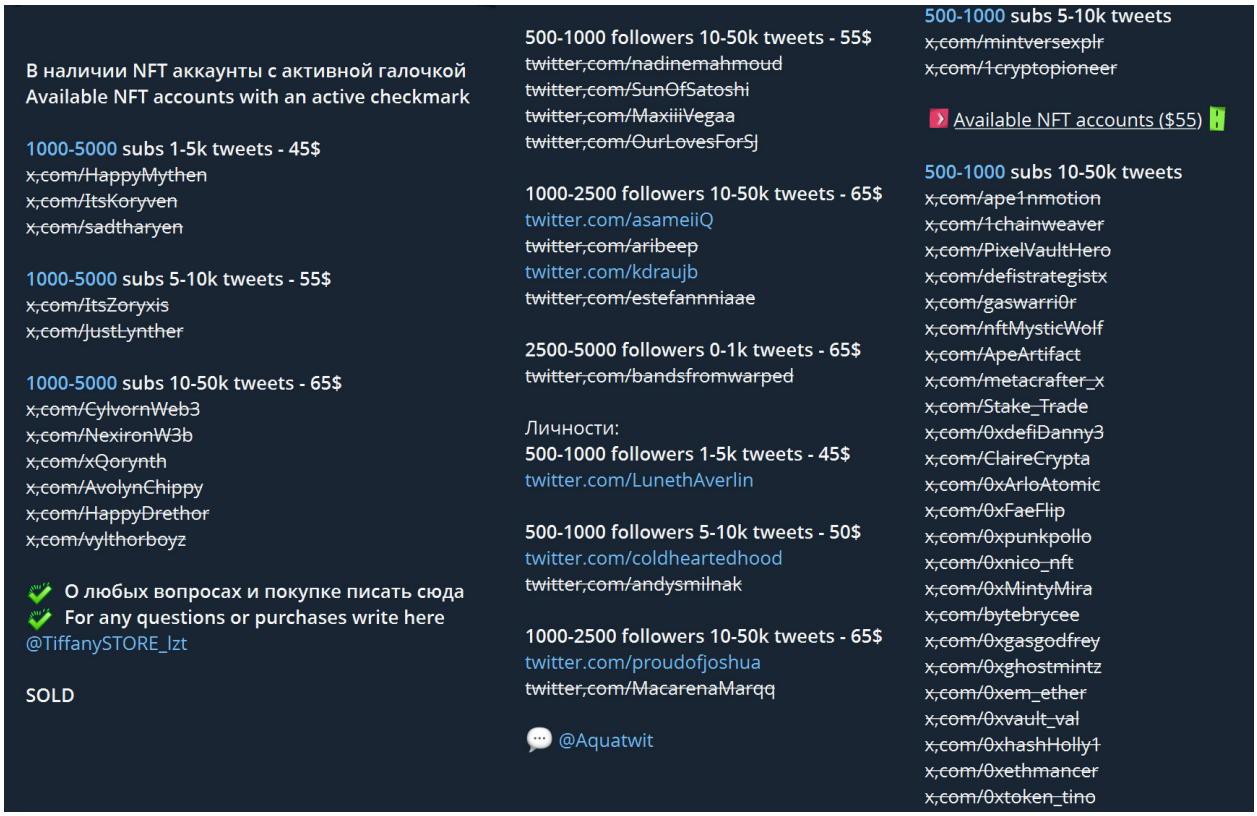


Figure 16: Active X accounts for sale (source: Telegram).

Victim selection

The primary objective of the traffer scam operations is to steal as much cryptocurrency as possible from the wallet information retrieved from victim logs. To ensure that workers are not wasting their time on victims who do not hold any cryptocurrency, they will select and profile the victims based on their appearance and the information available about them on the internet.

One of the first approaches to find potential victims is to check balances from wallets available on public profiles on *X*, based on the common Web3 usernames ending in '.eth'. The workers will parse accounts, check their balances in specific on-chain portfolio explorers such as Zapper or Debank, and decide if the individuals are worth taking the risk of engaging in a conversation.

Another common approach is to leverage NFT marketplaces such as *OpenSea*, *Magic Eden* and *Getgems* to select projects with a floor price (the lowest price at which a specific NFT can be purchased) of approximately $500 or more. Then, the worker will join the corresponding channels of the project, where they can easily identify holders and start targeting new potential victims, luring individuals to install malicious applications through social engineering.

DECEPTION METHODOLOGIES

Modern traffer operations employ diverse social engineering approaches that extend far beyond simple text-based communications, utilizing voice calls, fake video interviews, and emerging virtual environments to establish trust among victims and overcome increasingly sophisticated awareness among cryptocurrency users.

Voice-based social engineering

Voice calling operations, known as 'звонилки' in Russian traffer terminology, represent psychological manipulation techniques that exploit the increased trust humans place in voice communications compared to text-based interactions. These operations involve trained workers conducting professional-sounding phone conversations with potential victims, often presenting business opportunities such as freelance positions or technical consulting roles.

The effectiveness of voice-based approaches stems from several psychological factors: vocal authority creates perceived legitimacy, real-time conversation prevents victims from conducting verification research during the interaction, and the personal nature of phone calls triggers social compliance mechanisms.

'Video' interview

Traffer teams conduct fake video interviews through platforms like *Zoom*, *Google Meet*, and custom meeting software. These operations target victims through fake job recruitment campaigns or professional consulting opportunities within the cryptocurrency and blockchain space. Victims are instructed to navigate to malicious meeting links where they are prompted to download the launcher under the pretext of installing necessary 'meeting software' or 'collaboration tools' required to participate in the video conference.

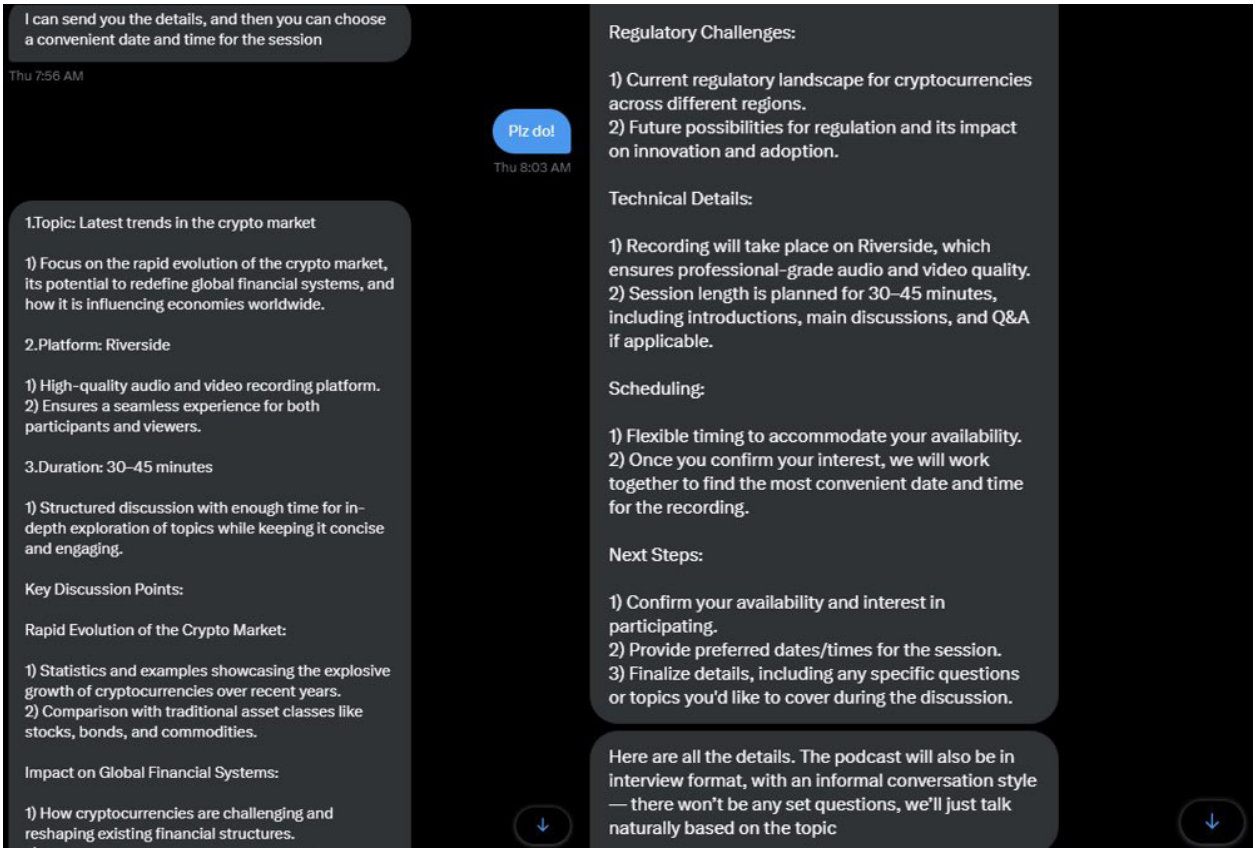


Figure 17: Example of traffer social engineering tactics used against community member @nft_dreww [8].

Metaverse and virtual gaming environment exploitation

Traffer groups create fake gaming platforms to lure victims into downloading malware. Projects like Argon 2.0/Genom, Dragonborn, Cosmo Whales and Dinoverse present themselves as legitimate blockchain games with virtual economies and metaverse features.

These platforms benefit from the growing intersection between gaming, NFTs and virtual worlds by offering 'beta access' to revolutionary new games featuring metaverse elements. Workers approach victims with exclusive opportunities to test next-generation blockchain games, participate in the development of virtual worlds, or gain early access to play-to-earn gaming economies.

Automated discovery tools

Manually parsing information on hundreds of potential victims could be a tedious job for workers in the CryptoLove and Wagmi gangs. That's why automation has become a solution to this problem, and traffers have been observed using automated discovery tools designed to scrape information about crypto holders and generate leads that will be used to target potential individuals under their scam operations. Users on social media platforms like *X*, especially within the Web3 community, often share their cryptocurrency wallet addresses publicly, such as when participating in token airdrops. However, this practice can inadvertently expose their asset holdings and create identifiable links to their wallets.

Despite the existence of specific services dedicated to this specific job, traffers created their own tools for this purpose, used at scale among the workers of the team. For example, Wagmi has been observed using its own 'wagmiscrapper', a tool maintained by the administration team that generates leads given to new workers to support their scam operations.

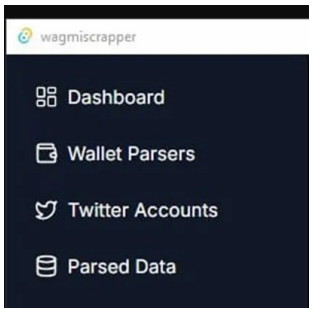


Figure 18: Wagmiscrapper tool to identify potential victims.

LANDING PAGE ECOSYSTEM AND DECEPTION TACTICS

Modern traffer operations leverage sophisticated landing page ecosystems designed to maximize victim engagement. Analysis of CryptoLove and Wagmi operations reveals systematic approaches to creating believable deception platforms that exploit psychological trust mechanisms and leverage legitimate business models to enhance credibility.

Multi-affiliate landing page architecture

CryptoLove was observed to operate through a distributed affiliate system where each affiliate maintained multiple landing pages targeting different victim demographics and interests. Major affiliates included SCAMQUERTEO (Yellow Empire), the PROFIT Team, the Wolves of Wall Street Team, the Heaven Era 2.0 Team, and smaller operations such as the Mr. Beast Team and the ObmanVALUT Team.

Each affiliate developed specialized landing pages optimized for specific social engineering approaches. Common themes included gaming platforms, PDF readers, video conferencing software, and Web3 applications. The diversity ensured broad target coverage while allowing affiliates to develop expertise in particular deception methodologies.

Gaming-themed deception platforms

Gaming-themed landing pages represent the most sophisticated category of deception platforms, often featuring complete game narratives, professional graphics, and legitimate-appearing business registrations. Notable examples include:

- The Argon 2.0/Genom project (Yellow Empire), which presented as a metaverse gaming platform with complete business registration as Genom LTD (later changed to Dragonborn LTD) through the UK's Companies House. The operation included professional NFT collections on *Rarible*, a comprehensive social media presence, and a functional fake token system that allowed workers to send fake BNB tokens to victim accounts, creating an investment psychological attachment.
- The Dragonborn project (Mr. Beast Team), which featured elaborate fake partnerships with major companies, including *Red Hat*, *HubGlobal* and *Vespertine Capital*. The platform falsely claimed management by *TelevisaUnivision* executive Steven Wolfe Pereira without authorization. The operation included a custom token ($DBT) available on *PancakeSwap*, a comprehensive administration panel (AdminDragon) for affiliate management, and corporate email services (@dragonborn.org) for professional communications.

Figure 19: Dragonborn fake partnership announcement with Red Hat.

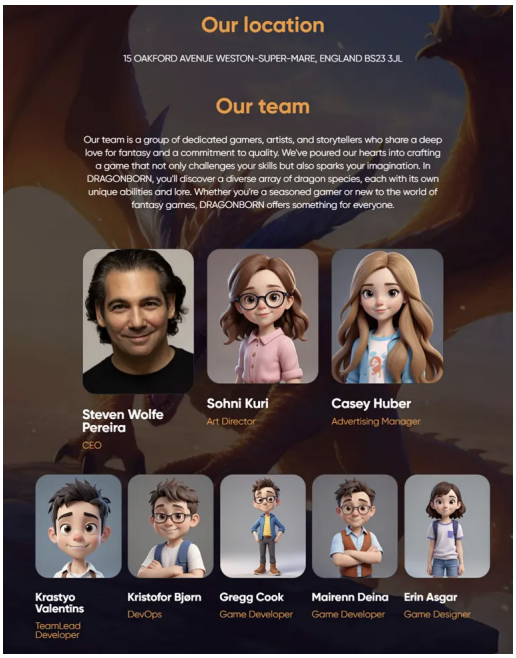


Figure 20: Dragonborn fake staff.

- The Cosmo Whales/Orbit projects (PROFIT Team), which registered as legitimate companies through Companies House with professional NFT collections on the *OKX* marketplace. The Orbit project leveraged content from gaming YouTuber 'MrZarokk' and presented fake gameplay footage as original content.

Professional meeting software impersonation

Video conferencing software impersonation represents a particularly effective deception vector, given the widespread adoption of remote work in recent years. CryptoLove affiliates created sophisticated *Zoom*, *Google Meet*, *WeChat* and custom meeting software impersonations.

The *Google Meet* landing pages implemented advanced psychological manipulation by requesting camera access and capturing victim photographs during the supposed meeting setup process.

Wagmi operations leverage similar tactics with their Splare application, described as 'video meeting software ideal for companies or people who value privacy'. The application closely mimics other traffer meeting software landing pages such as Vixcall/Voxium/Vorium observed in other teams.

PDF reader and document processing deception

Fake PDF reader applications serve dual purposes: direct malware delivery and sophisticated social engineering through document-based lures. Operations like VeriScroll (PROFIT Team) and Doculuma (Mr. Beast Team) created professional-looking document processing applications.

The social engineering methodology involves sending victims encrypted PDF files that display fake security warnings, requiring specific PDF readers to access them. Victims searching for the referenced software encounter the malicious landing pages, creating a natural discovery pathway that reduces suspicion compared to direct links.

Figure 21: Fake encrypted PDF document.

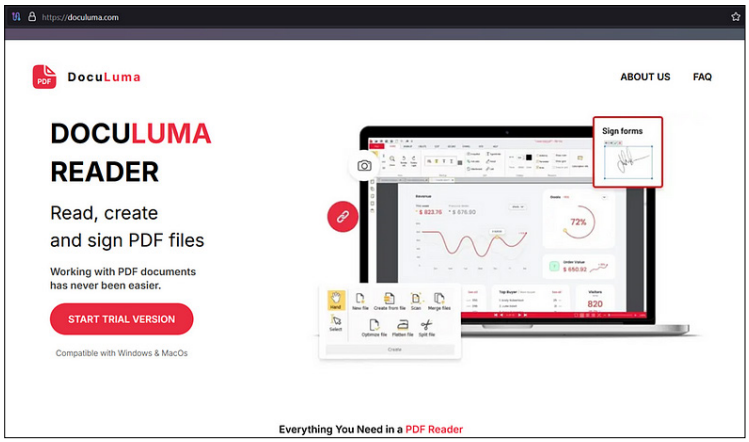


Figure 22: Fake PDF reader.

Web3 and cryptocurrency platform impersonation

Web3-themed deceptions exploit the complexity and rapid evolution of cryptocurrency platforms to create believable fake services. Examples include:

- Toffee Suite (Wolves of Wall Street), which presented as a comprehensive cryptocurrency research and aggregation platform featuring real-time project tracking, market analysis feeds, and professional interface design. The platform displays legitimate-looking cryptocurrency news, partnership announcements, project updates, and comprehensive listings of projects, including major DeFi protocols such as *1inch*, *Aave*, and others. Despite the sophisticated appearance of a fully functional crypto research tool with multiple sections for research feeds and market aggregation, the entire platform serves solely to deliver the malicious launcher through a 'Download app' button.

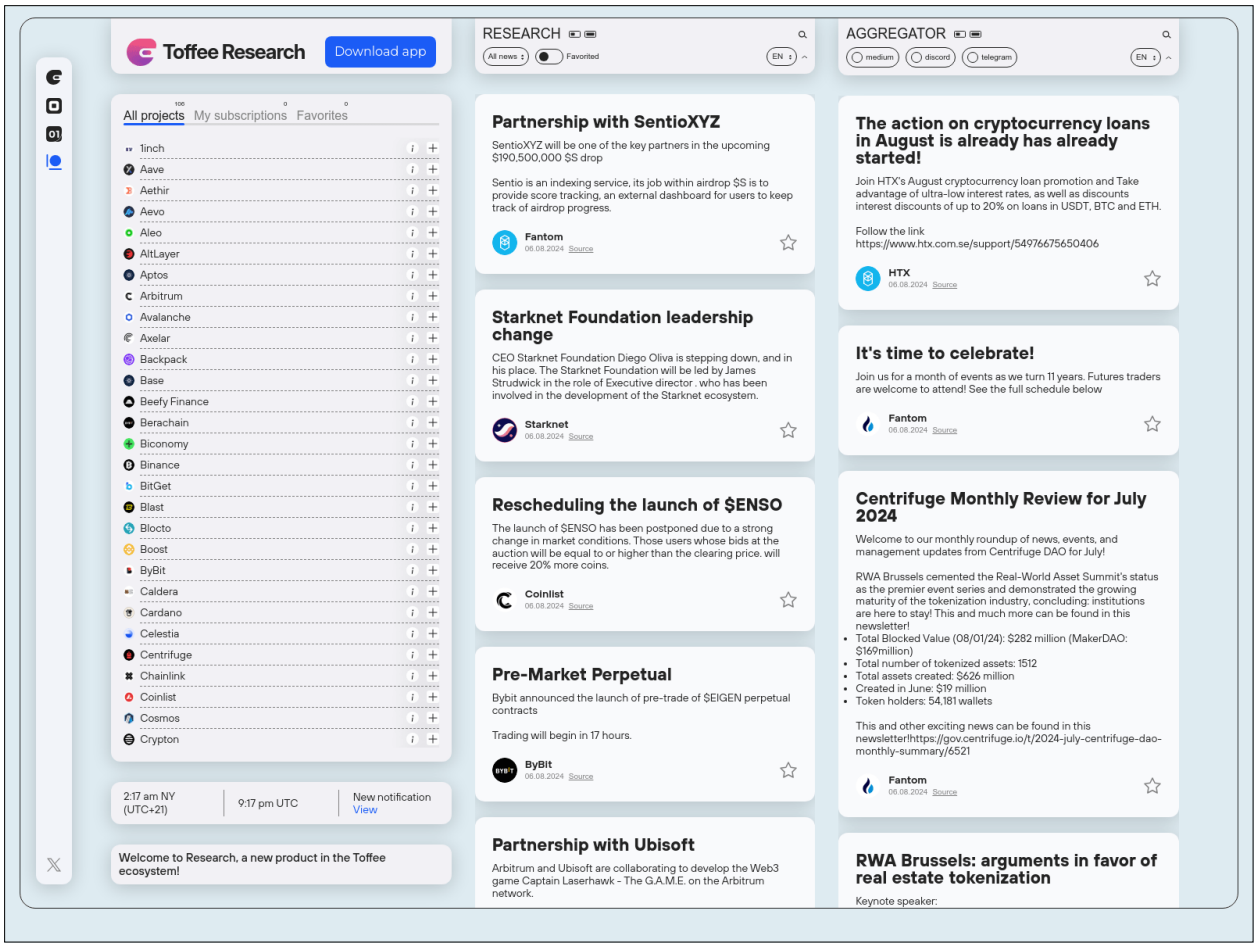


Figure 23: Landing page of Toffee project.

- Sleipnir DAO Browser (Wagmi) targeted Web3 users by creating elaborate fake decentralized applications. The Sleipnir platform included a detailed manifesto about internet democratization, criticizing centralized corporations and promoting user control over data and privacy. The operation features multiple branded Web3 products, including Sleipnir Browser, Sleipnir Secure, Sleipnir Wallet and Sleipnir Search. The platform claims to be a legitimate decentralized autonomous organization (DAO) built on the Polygon blockchain network with its own Sleipnir DAO Token.

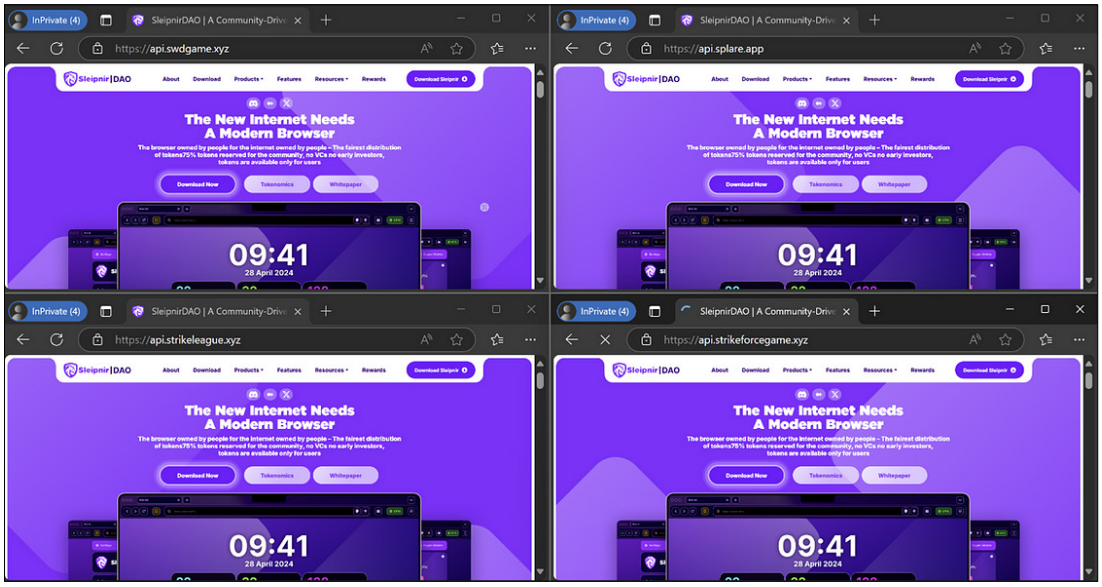
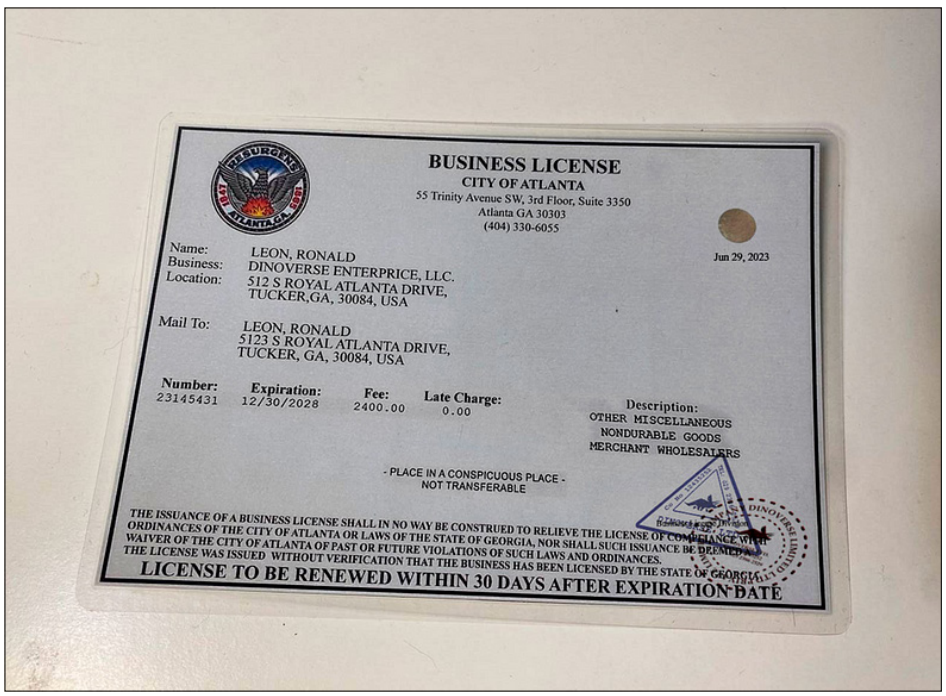


Figure 24: Sleipnir DAO Browser landing page.

Business registration and corporate identity theft

As mentioned previously, to enhance project credibility and overcome victim skepticism, traffer affiliates systematically create authentic business registrations across multiple jurisdictions. CryptoLove affiliates established fake corporate entities, claiming to be from the United States and the United Kingdom, and provided legal documentation that victims could verify through official government databases. CryptoLove affiliates registered multiple companies through the UK's Companies House, including Genom LTD (subsequently changed to Dragonborn LTD) and Cosmo Whales. Dinoverse claimed to establish registrations in both Georgia (UNI Enterprise, LLC) and Florida (Orionix LLC).


BUSINESS LICENSE
CITY OF ATLANTA
55 Trinity Avenue SW, 3rd Floor, Suite 3350
Atlanta GA 30303
(404) 330-6055

Jun 29, 2023

Name: LEON, RONALD
Business: DINOVERSE ENTERPRICE, LLC.
Location: 512 S ROYAL ATLANTA DRIVE, TUCKER,GA, 30084, USA

Mail To: LEON, RONALD
5123 S ROYAL ATLANTA DRIVE, TUCKER, GA, 30084, USA

Number: 23145431
Expiration: 12/30/2028
Fee: 2400.00
Late Charge: 0.00

Description:
OTHER MISCELLANEOUS NONDURABLE GOODS MERCHANT WHOLESALERS

- PLACE IN A CONSPICUOUS PLACE - NOT TRANSFERABLE

THE ISSUANCE OF A BUSINESS LICENSE SHALL IN NO WAY BE CONSTRUED TO RELIEVE THE LICENSE OF COMPLIANCE WITH ORDINANCES OF THE CITY OF ATLANTA OR LAWS OF THE STATE OF GEORGIA, NOR SHALL SUCH ISSUANCE BE DEEMED A WAIVER OF THE CITY OF ATLANTA OF PAST OR FUTURE VIOLATIONS OF SUCH LAWS AND ORDINANCES. THE LICENSE WAS ISSUED WITHOUT VERIFICATION THAT THE BUSINESS HAS BEEN LICENSED BY THE STATE OF GEORGIA

LICENSE TO BE RENEWED WITHIN 30 DAYS AFTER EXPIRATION DATE

Figure 25: Photo of the business licence provided to the workers.

CONCLUSION

The analysis of CryptoLove and Wagmi traffer operations reveals the evolution of cryptocurrency-targeted cybercrime into sophisticated criminal organizations that pose significant threats to the digital asset ecosystem. These criminal enterprises demonstrate remarkable adaptability, systematically responding to security research pressure through technical innovations, including promotional code systems, in-memory payload execution, and comprehensive anti-analysis implementations. Their combined documented theft of over $5 million across 24,527 victims illustrates both the scale and effectiveness of modern traffer methodologies.

The systematic abuse of legitimate code-signing certificates demonstrates evasion techniques designed to bypass *Windows SmartScreen* and UAC protections. At the same time, business registration fraud creates enhanced victim trust and operational legitimacy.

Rapid adaptation to emerging social media platforms, such as *Bluesky*, highlights the adaptive capabilities of these operations. The documented organizational structures, complete with hierarchical management and training programmes, mirror legitimate business enterprises while pursuing criminal objectives.

Security practitioners must recognize that traditional defensive measures are insufficient against these evolved threats. The rapid certificate rotation, promotional code access controls, and responsive technical adaptations demonstrate threat actors' ability to systematically counter detection and disruption efforts. Effective mitigation requires coordinated responses combining technical countermeasures, certificate authority collaboration, and international law enforcement cooperation.

The continued evolution of traffer operations suggests cryptocurrency-targeted threats will persist and intensify as digital asset adoption increases. Organizations and individuals within the cryptocurrency ecosystem require enhanced awareness of these sophisticated social engineering techniques and robust security practices to defend against increasingly professional criminal enterprises targeting digital assets through comprehensive deception campaigns and malware delivery systems.

REFERENCES

[1] TRAC Labs. Hearts Stolen, Wallets Emptied: Insights into CryptoLove Traffer's Team. TRAC Labs Blog. 27 November 2024. https://trac-labs.com/hearts-stolen-wallets-emptied-insights-into-cryptolove-traffers-team-3f65e84ccebe.

[2] TRAC Labs. The Wagmi Manual: Copy, Paste, and Profit. TRAC Labs Blog. 5 April 2025. https://trac-labs.com/the-wagmi-manual-copy-paste-and-profit-2803a15bf540.

[3] IPinfo. Wagmi Victim IP Address Distribution Map. IPinfo Tools. 2025. https://ipinfo.io/tools/map/08385d45-3a09-42db-a52b-2c68b7180324.

[4] IPinfo. CryptoLove Victim IP Address Distribution Map. IPinfo Tools. 2025. https://ipinfo.io/tools/summarize-ips/bee83f73-b853-406a-a740-993c60b511d6.

[5] Abhisek. Pe-Loader-Sample. GitHub Repository. https://github.com/abhisek/Pe-Loader-Sample/tree/master.

[6] Muhammed Irfan, V A. Analyzing New HijackLoader Evasion Tactics. Zscaler ThreatLabz. 31 March 2025. https://www.zscaler.com/blogs/security-research/analyzing-new-hijackloader-evasion-tactics.

[7] Microsoft. Feature Discovery. Microsoft Learn - Hyper-V on Windows Top-Level Functional Specification. 8 July 2022. https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/tlfs/feature-discovery.

[8] @nft_dreww. Post on X. 9 June 2025, 7:26 AM. https://x.com/nft_dreww/status/1932036600889770302.

APPENDIX

Indicator	Type	Description
`http://xilloolli.com/api.php`	URL	CryptoLove launcher C2
`http://xilloolli.com/api-debug.php`	URL	CryptoLove launcher C2
`https://cdn-gravitiumgame.xyz/launcher.exe`	URL	CryptoLove launcher C2
`oklibed.com`	URL	CryptoLove launcher C2
`723c731b3265cfe3960502219316bc13f4cd9929df507930a7e5010d4ada4e92`	SHA-256	CryptoLove loader
`a7edb703c4bd8a33434d18b72fd1e718608a9a99b8b30d35add27c609bd24c0e`	SHA-256	CryptoLove loader
`360a405b8eb0b6e748aafabf6db25e6b7137d2dce791d61c64f37f596df7bd6f`	SHA-256	CryptoLove loader
`a66b1738e5944d8117df8a6ac027a152de4759623e489422415b33cae25d8479`	SHA-256	CryptoLove launcher
`6b6648c129917fbd5769749952d6dc47623daec0eb509d585140307f9611e99b`	SHA-256	CryptoLove loader

Indicator	**Type**	**Description**
2b8625f76bade3b023cabb5b166cc9f768c3bf9185d94173465c85610a935d79	SHA-256	CryptoLove loader
10c3f8d1e213c640975f4e05b84c44eca992d9a04c55fe1b6e4656d4b1af5ba1	SHA-256	CryptoLove loader
7a866d41e2e5fbe3b8c2371d34094ed417c8de072db9f89b1c310f7eea701905	SHA-256	CryptoLove loader
10c3f8d1e213c640975f4e05b84c44eca992d9a04c55fe1b6e4656d4b1af5ba1	SHA-256	CryptoLove loader
154af50ab1f4b14e10b2532574c3856bbdadaabb042ade5bf39a7153cb9e89f8	SHA-256	Wagmi MacOS launcher
75ba94534ea1433f70c57de43b27b9dc1c9f310e004fa5c70ad3e6b79650328a	SHA-256	Wagmi MacOS launcher
9f4e52d4dfb7ebf09e0371a92280ad21519030f7032077cba125903454dd211d	SHA-256	Wagmi MacOS launcher
d516515e923875ae22b6325bba9e53f5fa531aa7c6c7a386fb380f3ae92b5009	SHA-256	Wagmi MacOS launcher
2005bd6b7613d7c6bc8ea6e179f498b05feb185237511eebce44a5d3d87662ec	SHA-256	Wagmi MacOS launcher
1ae7cdd81585233bfb3871385c67dd7fb43bfb2231ab2af5aded08d49c490f16	SHA-256	Wagmi MacOS launcher
38eff554ddee7664cd8b1c003ddf96f7ebe608acbe236b74e9045fd831a0c100	SHA-256	Wagmi Windows launcher
1d879fb13ed76a9892d8e9ea99aa6817cd1248d409956c1ab1b47c2f79c103bd	SHA-256	Wagmi Windows launcher
ecdd79c3228b8f354e6c0148c00038790bd8a874428dc9b3f57111e753d3565f	SHA-256	Wagmi Windows launcher
42735792cc7e76b7439751d4aa673d5bd61d100f8d4de42c9084db46e2a1dbf1	SHA-256	Wagmi Windows launcher
e0e0b3d2890053cbdf84d6c3177e267d8f767f4b2b6d6e5fb2de5860b0a09ee2	SHA-256	Wagmi Windows launcher
1a5bf23e14f7432202546093a0e025ddacebec0458ff21c137bd2cd69b9efde4	SHA-256	Wagmi Windows launcher