



NFT SCAM CASE

OSINT Investigation Successfully Closed

After two intensive weeks of work, our OSINT investigation has been officially closed.

Team size: 4 analysts Duration: 14 days (full-time effort) Primary objective: fully achieved

Both of the main targets (2/2) were successfully identified, located, and verified with a high degree of confidence. All key research questions assigned to this cycle were answered, primary digital footprints mapped, associated accounts and connections documented, geolocation elements confirmed where possible, and the most relevant findings consolidated into the final report.

No critical loose ends remain. The collected material is now ready for handover / further operational use.

Status: Done. Nowhere to go.

t.me/osint_xaynov

Введение

Поздней ночью 27 января 2026 года обычный пользователь Telegram получил сообщение, пересланное от бота, под предлогом, что ему купили NFT-подарок, и чтобы его получить нужно что-то подтвердить. Через несколько минут все его активы размещенные на аккаунте были переведены на подконтрольный злоумышленниками профиль.

В ответ на попытку вернуть украденное жертву пытались завербовать, предложив промышлять аналогичными схемами в составе закрытой группы: главным требованием было обмануть суммарно на 15 TON (~20\$).

Так начиналась каждая атака схемы проекта Loot Market — высокотехнологичного фишинга через *Telegram Web App*, маскирующегося под премиум-маркетплейс NFT-подарков и фейковыми подарками в разделе *Gifts* с имитацией профиля.

Схема работала нагло и эффективно: искусственная задержка 60 секунд после того, как данные от аккаунта были введены — ровно столько, сколько нужно «воркеру¹», чтобы войти в аккаунт жертвы по перехваченным данным; в качестве сервера использовался *ngrok-free.dev* с заголовком *ngrok-skip-browser-warning* для сокрытия реального IP.

Через схему прошло несколько сотен TON. Исполнители соревновались в таблице лидеров по прибыли главный разработчик (он же выплатчик) сидел в Праге и брал свой процент.

В ходе нашего OSINT-расследования мы смогли:

1. Выявить прямые связи между инфраструктурой и разработчиком:
 - Установили причастность конкретного лица к проекту;
2. Собрать компромат на деятельность организатора схемы:
 - Задокументировали факты мошеннической деятельности;
3. Установить и систематизировать причастных лиц:
 - идентифицировали участников и вынесли их в таблицу;
4. Вернуть активы и ликвидировать проект:
 - обеспечили полный возврат средств и ликвидацию инфраструктуры проекта с дальнейшим его удалением.

Цель

- Добиться полной ликвидации инфраструктуры и символического возврата активов пострадавшей стороне

Задачи

- Получить установочные данные ключевых аккаунтов и ролей
- Исследовать геолокацию и личность главного разработчика
- Выявить всю веб-инфраструктуру и логику фишинга
- Собрать доказательную базу для передачи в правоохранительные органы

Intelligence collective



@ownstates
Case Officer



@sositetv4ri
Technical Analyst



@osint_shaid
OSINT-Analyst



@OsintMikhaill
GEOINT-Analyst

[1] воркеры — участники мошеннических групп, которые занимаются непосредственным поиском жертв и их обманом в интернете.

Общая характеристика схемы и принцип работы Telegram Mini-App в Loot Market

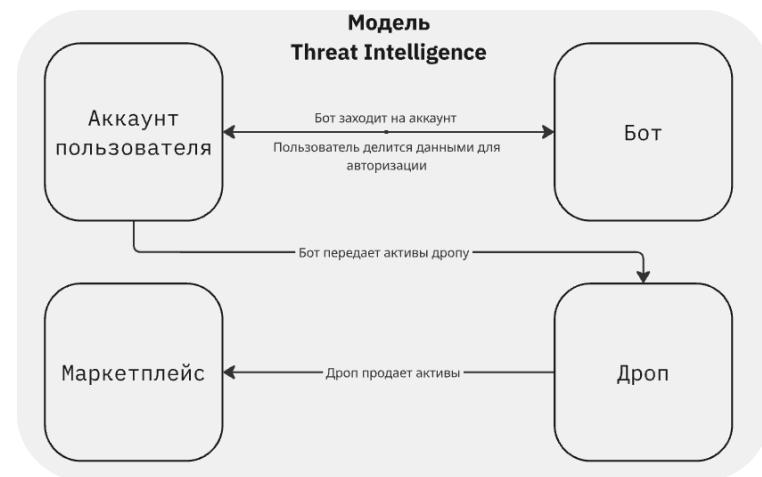
Telegram Mini-App (Telegram Web App, TWA) — это веб-приложение, которое запускается внутри Telegram по ссылке из бота или сообщения. Оно работает на базе обычного веб-технологий (HTML, JavaScript, CSS), но имеет прямой доступ к API Telegram через глобальный объект `Telegram.WebApp`. Это позволяет:

- получать данные пользователя (имя, аватар, ID) через `initDataUnsafe`
- запрашивать номер телефона через `requestContact`
- получать доступ к контактам, геолокации, файлам
- отправлять сообщения, платежи, запрашивать разрешения

В легитимных сценариях это используется для игр, магазинов, форм, мини-сервисов внутри Telegram без выхода из приложения. В схеме "Loot Market"² Mini-App был полностью перепрофилирован под фишинг.

Жертва получала сообщение от воркера, который пересыпал сообщение от бота Loot Market о "сделке" с подарком ("Сделка #RX72937 успешно открыта").

При клике по ссылке запускалось приложение, которое внешне выглядело как маркетплейс NFT-подарков: разделы Market, Gifts , Profile (баланс и настройки). При попытке вывода или пополнения Telegram Mini-App перебрасывает пользователя в окно чата с ботом, требуя поделиться номером телефона.



Процесс эксплуатации:

- Сбор идентификаторов сессии**
 - Извлечение `start_param` для привязки жертвы к ID злоумышленника в базе данных.
 - Получение `user_id` и метаданных через `tg.initDataUnsafe` для формирования уникального лога взлома.
- Эксфильтрация номера телефона**
 - Вызов системного окна Telegram через метод `tg.requestContact`.
 - Перехват объекта `contact` после подтверждения пользователем.
 - Передача номера телефона на C2-сервер (команда `send_phone`) для инициации попытки входа в аккаунт со стороны злоумышленника.
- Перехват авторизационного кода (OTP)**
 - Ожидание ввода кода, присланного официальным сервисным аккаунтом Telegram.
 - Чтение значения из `tgCodeInput` и немедленная отправка на сервер через `check_code`.
 - В этот момент сервер злоумышленника в реальном времени подставляет этот код в активную сессию авторизации.
- Захват облачного пароля (2FA)**
 - Анализ ответа сервера: если на аккаунте стоит двухфакторная аутентификация, скрипт динамически отображает поле для ввода пароля.
 - Перехват текстового пароля и его отправка (команда `check_password`), что завершает процесс получения полного доступа к аккаунту.
- Механика удержания и сокрытия (Time-jacking)**
 - Активация функции `runFinalLoadingSequence` — принудительная задержка на 60 секунд.
 - Назначение: пока пользователь видит полосу загрузки «транзакции», злоумышленник успевает завершить вход, сбросить другие сессии и установить свои настройки безопасности.
 - Туннелирование трафика через `ngrok` с параметром `ngrok-skip-browser-warning` для обхода систем защиты и сокрытия IP-адреса управляющего сервера.

[2] <https://xaynov.github.io/Sterilized-version-of-Loot-Market/> (Стерилизованная версия сайта)

Исходные данные, первичная оценка цифровых следов и построение гипотез

Параметр	Описание
Фишинговый Mini-App	На основе Telegram-бота
Аккаунт первичного контакта с жертвой	Аккаунт для переговоров по похищению активов и первичного контакта
Аккаунт получателя похищенных активов	Аккаунт, на который передавались похищенные активы (NFT и TON)
Аккаунт вербовщика (первый)	Первый аккаунт, осуществлявший вербовку в группу
Аккаунт вербовщика (второй / разработчик)	Второй аккаунт вербовки, одновременно основной разработчик схемы

Работа по кейсу началась с фиксации базового набора идентификаторов, которые послужили отправной точкой для всего дальнейшего анализа. На начальном этапе в нашем распоряжении оказались ключевые узлы сети: фишинговый Mini-App на базе бота, а также цепочка связанных аккаунтов, выполнявших разные роли — от «лица» для первичного контакта с жертвой до конечного хаба для аккумулирования похищенных активов. Кроме того, были зафиксированы профили вербовщика, действующего с двух разных аккаунтов, который занимался масштабированием мошеннической схемы.

Понимая специфику мошенников, версия о случайных людях была отброшена сразу: все аккаунты, мелькавшие в схеме, являлись либо «отработанным материалом» после взлома, либо купленным на теневых форумах «мясом». Ключевым направлением в таком случае стал удар не по аккаунтам, а по фундаменту — технической инфраструктуре, на которой держался фишинговый Mini-App (домены, IP-адреса и хостинг-провайдеры). Это был единственный способ вытащить наружу реальное устройство Loot Market и понять, как именно проект живет в тени, обищаю кошельки пользователей под прикрытием аккаунтов-однодневок. Сфокусировавшись на архитектуре можно было вскрыть всю цепочку обслуживания вредоносного софта и выставить на свет тех, кто стоит за кнопками управления, а не просто исполняет команды «в поле».

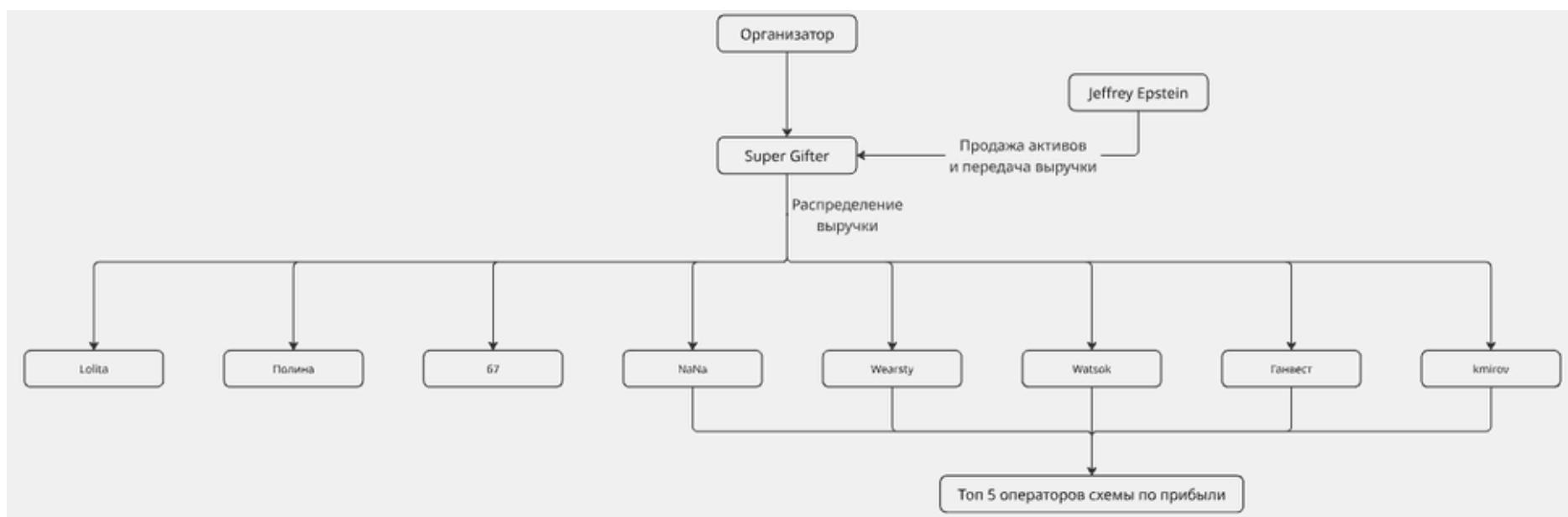
Полученные идентификаторы были зафиксированы как исходная точка для анализа. Установлено, что схема имеет чёткую последовательность: первичный контакт → перевод активов → вербовка → участие в группе. Первичная обработка позволила выделить, что аккаунты выполняют вспомогательную роль, а основная доказательная база находится в инфраструктуре Mini-App. Именно поиск домена и хостинга стал приоритетным направлением, поскольку только там можно найти следы авторства, логику хищения и организаторов схемы.

При детальном изучении того, как развивались события, стало ясно: вся цепочка действий была выстроена под одного конкретного клиента и носила разовый характер. Схема отработала классически: от первого «привета» до кражи активов. Но финальный аккорд с предложением «вступить в команду», поступивший от администратора, — это не признак того, что они строят огромную сеть воркеров. Скорее всего, это был ситуативный ход, чтобы либо успокоить жертву, либо выжать из ситуации максимум, превратив пострадавшего в соучастника. В исходных данных нет ничего, что указывало бы на системный рекрутинг, поэтому мы рассматриваем этот эпизод как частный финал обработки конкретного человека.



Фигуранты схемы

Переход от изучения технических параметров Mini-App к анализу лиц, стоящих за его эксплуатацией, позволил выстроить иерархическую модель управления проектом: было установлено отсутствие сложной многоуровневой иерархии, что характерно для локальных фишинговых проектов. Основная масса зафиксированных субъектов относится к категории рядовых исполнителей (воркеров), чьи функции максимально унифицированы. В рамках рассматриваемого инцидента именно эта группа обеспечивает весь цикл операционной работы: от поиска цели и установления первичного контакта до технического сопровождения жертвы внутри интерфейса приложения. Для этой категории участников не предусмотрено разделения труда — один и тот же субъект отвечает и за социальную инженерию, и за контроль перехода по фишинговой ссылке. Такая децентрализация исполнителей позволяет организаторам минимизировать риски и оперативно заменять скомпрометированные профили, не затрагивая при этом общую работоспособность системы.



Особое внимание стоит уделить механике распределения похищенных активов, которая исключает прямой доступ рядовых исполнителей к результатам их деятельности. Воркеры, обеспечивающие приток целей, не имеют технической возможности самостоятельно получать или удерживать «подарки» и иные виртуальные ценности. Система настроена таким образом, что все активы в момент хищения автоматически транзитируются на единый аккаунт дропа³. Этот субъект выполняет функцию централизованного хаба: он аккумулирует похищенное, осуществляет его последующую реализацию на маркетплейсах и конвертацию в ликвидные средства. Такая архитектура лишает исполнителей финансовой автономности и полностью замыкает их на организаторе проекта.

В этой цепочке дроп выступает в роли связующего звена между техническим софтом и реальными деньгами. После продажи активов вся выручка передается организатору, который лично контролирует «касси» и распределяет доли между воркерами в соответствии с их эффективностью. Подобная модель финансовой логистики подтверждает, что рядовые участники схемы — это лишь низкооплачиваемый операционный персонал, работающий в условиях жесткого контроля сверху. Для расследования это означает, что отслеживание мелких транзакций воркеров малоэффективно, так как основной финансовый поток и, соответственно, наиболее значимые цифровые следы сосредоточены в руках организатора и его доверенного дропа. Именно на пересечении их интересов — управлении сервером и движении средств — локализована точка, в которой анонимность схемы дает сбой.

Согласно сведениям, полученным от дропа, экономика схемы строится на распределении выручки в пропорции 60% в пользу воркера и 40% организатору. Несмотря на высокий процент вознаграждения, воркер получает выплату только после реализации актива дропом и одобрения транзакции организатором. Такая модель «выплаты по факту» является рычагом давления на персонал и удерживает исполнителей внутри системы. Для расследования этот расклад подтверждает, что организатор — не просто технарь, а операционный директор, управляющий «кассой». Однако необходимость регулярных выплат и администрирования сервера создает уязвимые точки.

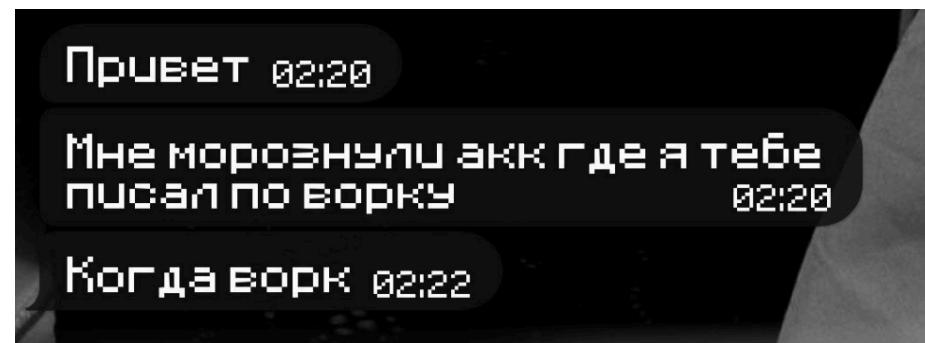
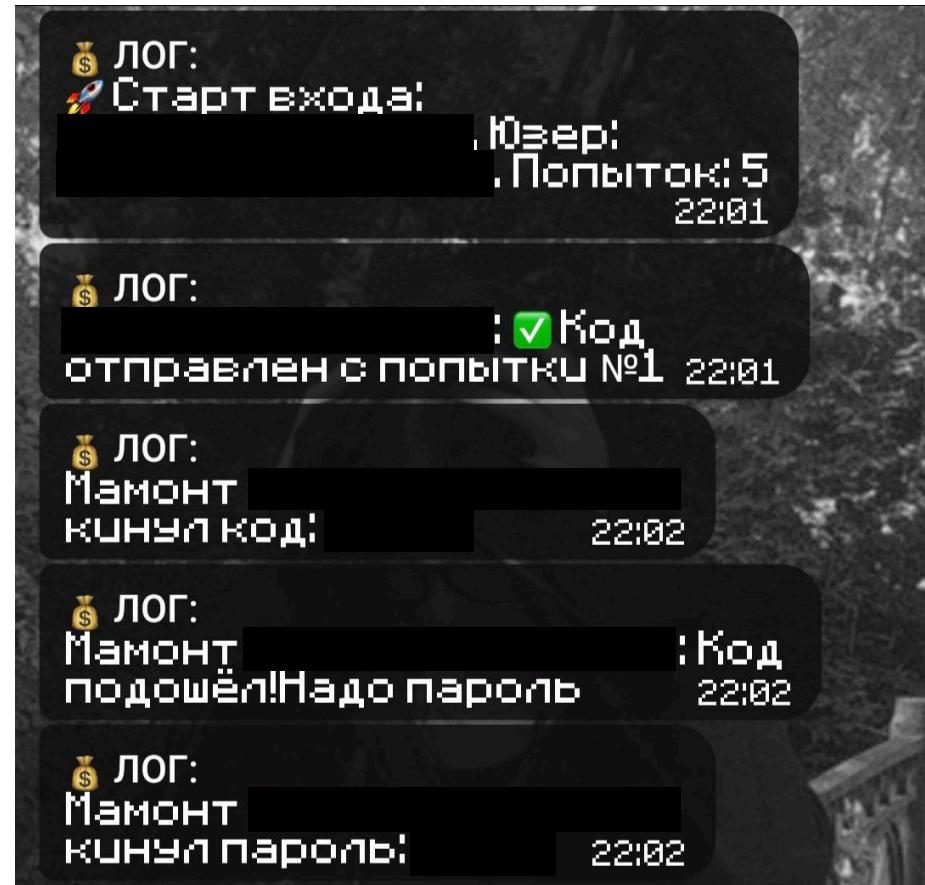
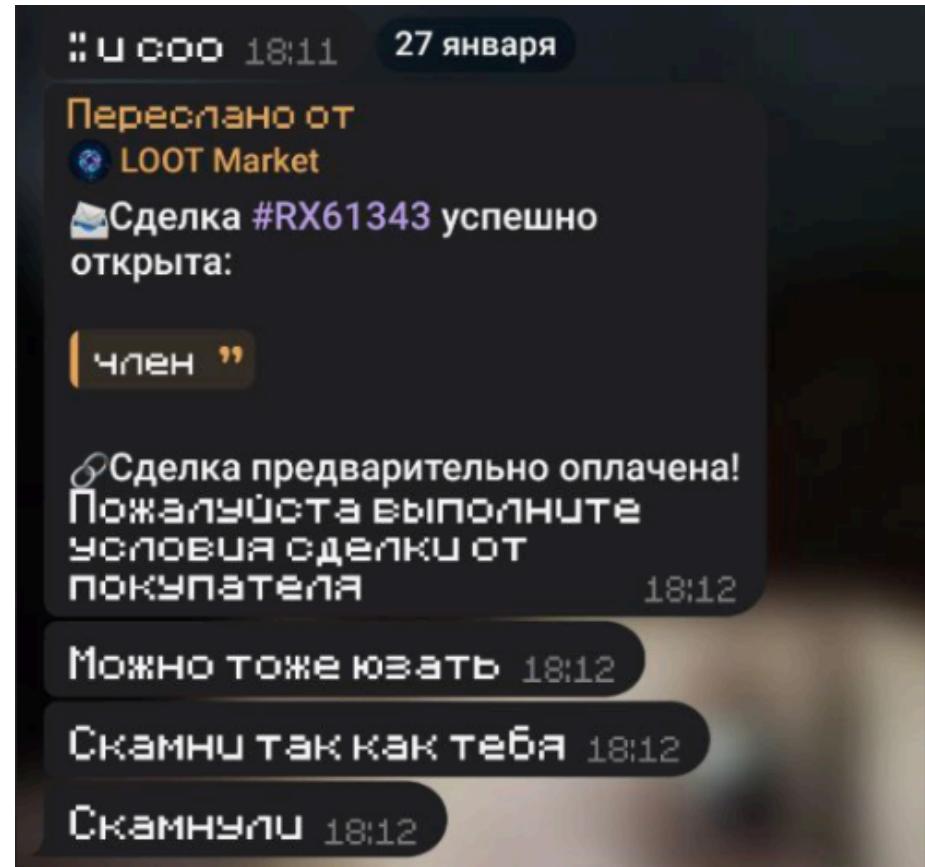
[3] Дроп — это подставное лицо, которое используется как посредник для «отмывания» украденных денег или товаров. В нашем случае, помимо отмывания дроп использовался для осуществления продажи активов и передачи выручки организатору, который в его случае распределял ее для воркеров, оставляя процент себе.

Мероприятие социальной инженерии

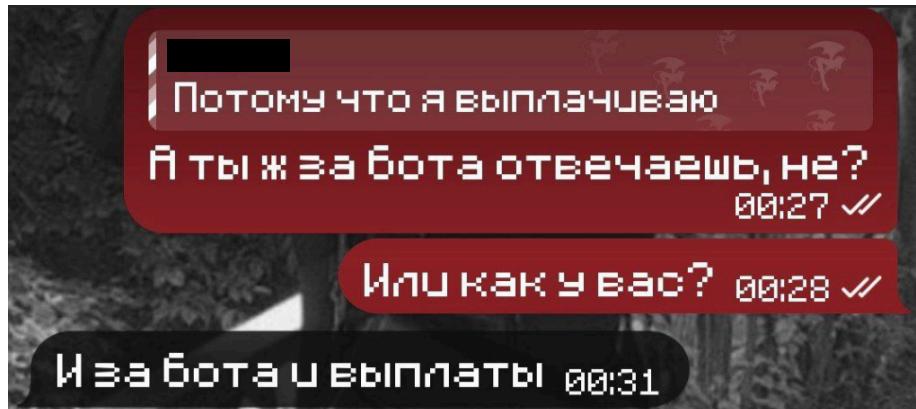
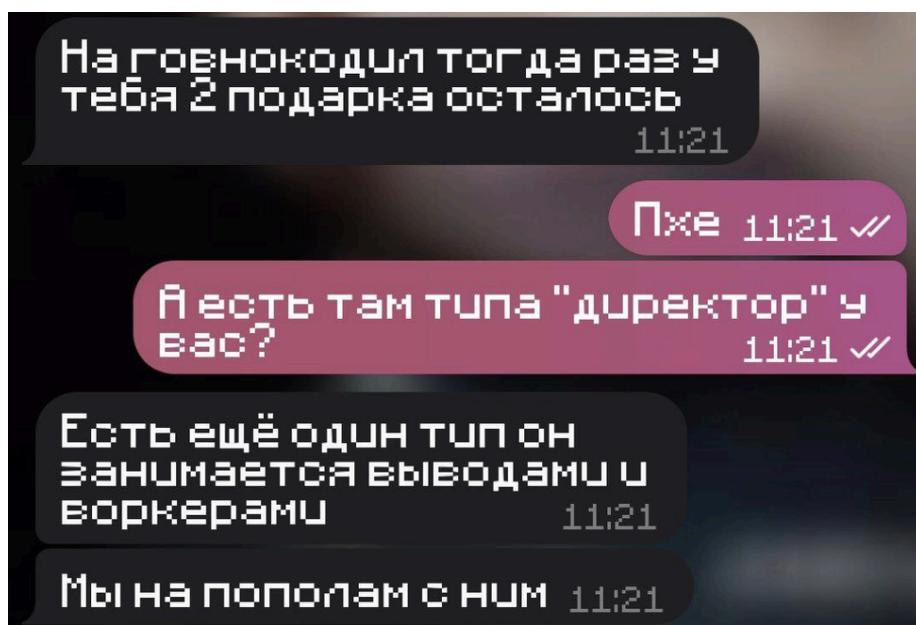
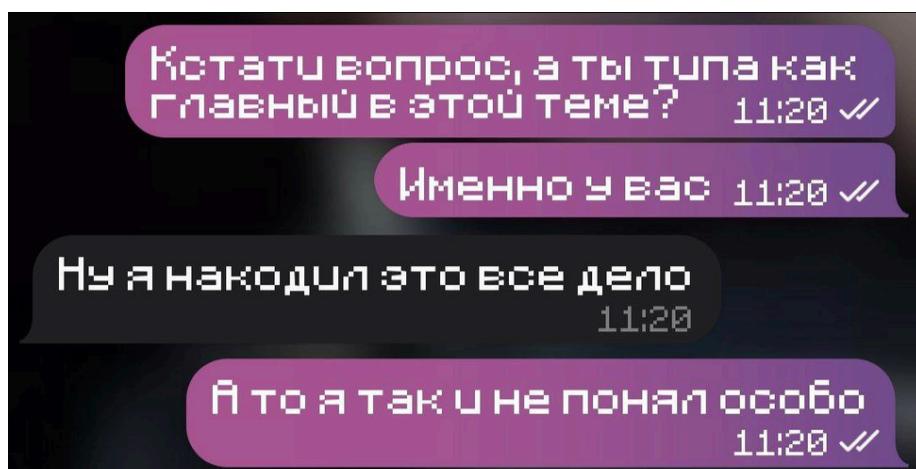
Ключевой этап идентификации субъектов стал возможен благодаря избыточной открытости администратора в процессе попытки вовлечения пострадавшего в деятельность группы. Для демонстрации «профессионализма» и доходности схемы организатор лично раскрыл внутреннюю механику работы системы, фактически проведя технический аудит собственного продукта для потенциального «сотрудника». В частности, был детально продемонстрирован функционал управления ботом, позволяющий в ручном режиме инициировать отправку кастомных push-уведомлений. Эти сообщения, имитирующие системные алерты об «открытии сделки» или «зачислении средств», являются ядром психологического давления на жертву, создавая ложное ощущение безопасности внутри фишингового интерфейса.

Помимо демонстрации интерфейса, организатор допустил передачу прямых выгрузок из системных журналов (выдачи бота), содержащих актуальные логи действий других пользователей в реальном времени. Эти данные позволили не только зафиксировать структуру базы данных и формат обработки транзакций на бэкенде, но и подтвердить масштаб активности системы. Анализ предоставленных скриншотов и текстовых фрагментов логов выявил характерные технические маркеры, которые позже использовались для сопоставления с инфраструктурой на внешнем хостинге.

Существенным продвижением расследования стало прямое взаимодействие с организатором через отдельный аккаунт, использовавшийся для координации рабочих процессов и уточнения готовности к работе (контрольные вопросы в стиле «когда ворк»). Важно учитывать, что данный профиль никак не позиционировался как личный или основной. В условиях профессионально выстроенных схем использование «рабочих» аккаунтов для связи является стандартным методом сегментации рисков. По этой причине появление нового идентификатора рассматривалось лишь как гипотетическое расширение структуры, а сам профиль мог оказаться покупным реквизитом для оперативной связи.



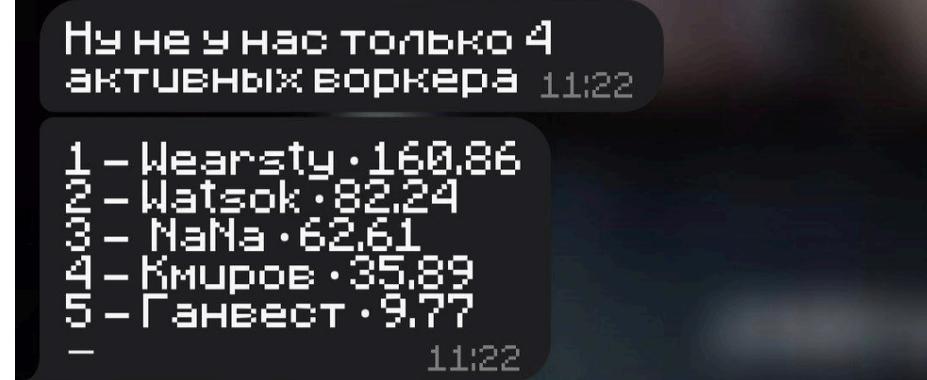
Продолжение мероприятия социальной инженерии



В качестве финального подтверждения своей власти над проектом и масштабов его деятельности, организатор предоставил список «Топ-5 воркеров». Этот перечень не только раскрыл наиболее активных исполнителей внутри системы, но и окончательно подтвердил наличие у субъекта прав суперпользователя с доступом к полной статистике доходности каждого участника. Демонстрация внутреннего рейтинга эффективности стала неопровергаемым доказательством того, что субъект обладает абсолютным доступом к базе данных и финансовой аналитике проекта. Таким образом, совокупность полученных данных в ходе продолжения СИ-мероприятий позволила установить, что организатор полностью замыкает на себе все критические циклы: от разработки и поддержки серверной части до личного распределения прибыли и контроля за эффективностью воркеров.

Следующим этапом оперативной разработки стала детализация внутренней структуры управления проектом через продолжение контролируемого диалога. Основной задачей было разграничение зон ответственности между техническим персоналом и финансовыми распорядителями. В ходе уточнения иерархии субъект изначально позиционировал себя исключительно как разработчика. Данное признание закрепило за ним статус автора и владельца программного кода Mini-App, подтверждая его прямую связь с архитектурой фишингового скрипта. Однако в процессе дальнейшего общения организатор допустил критическое противоречие в своих показаниях касательно обработки платежей.

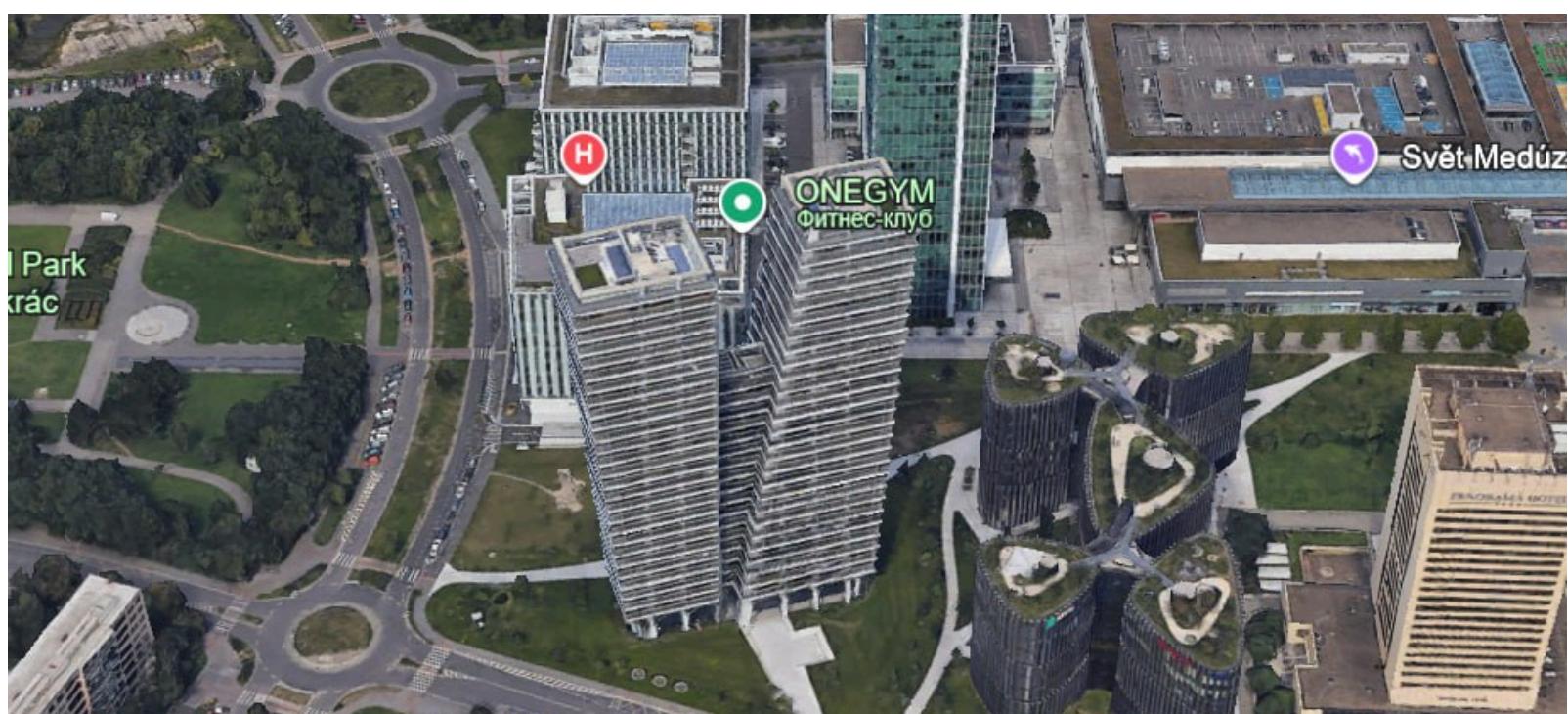
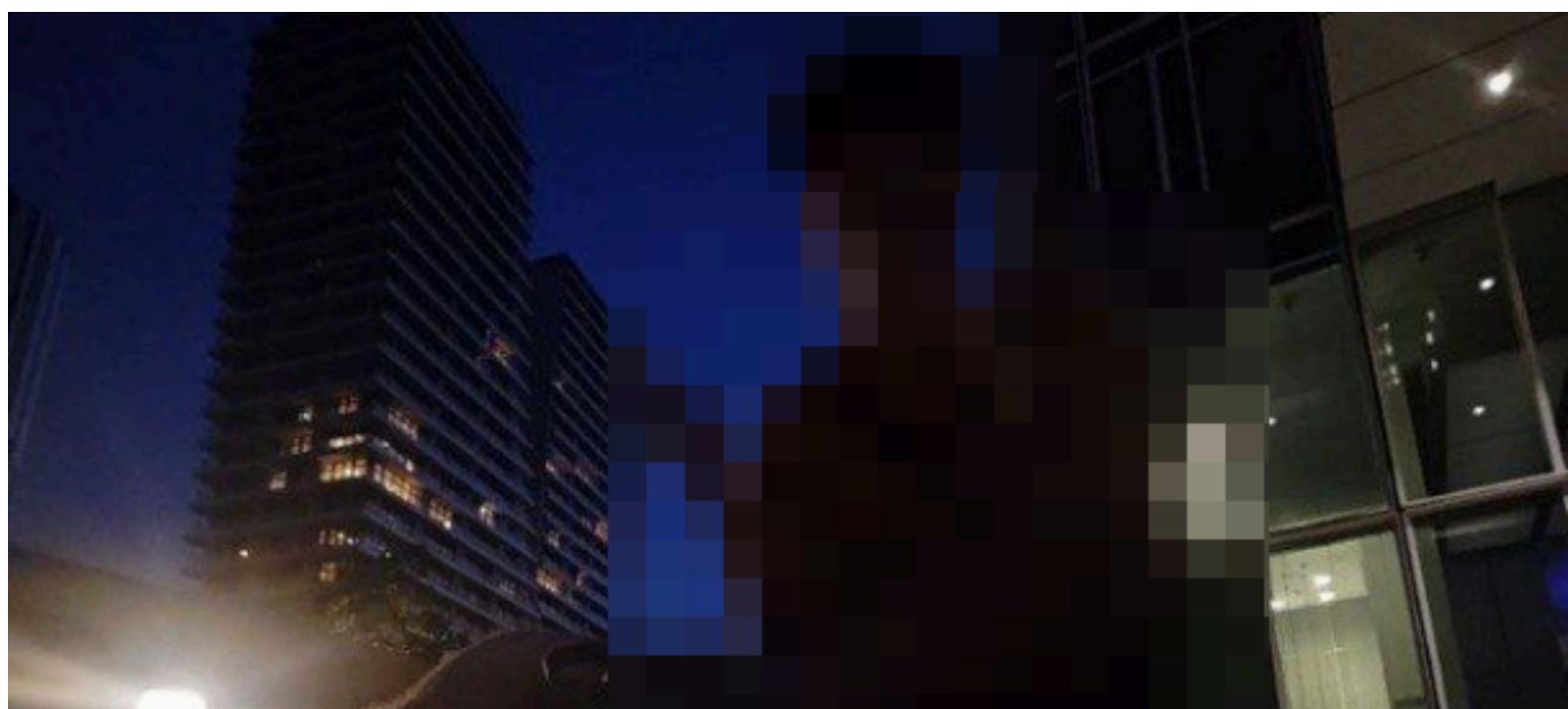
Первоначально субъект утверждал, что вопросами выплат и распределения средств занимается его партнер (дроп), дистанцируясь от прямого контакта с финансами. Тем не менее, спустя короткий промежуток времени, стремясь продемонстрировать полный контроль над процессами и гарантировать своевременность вознаграждения, он изменил позицию и подтвердил, что выплатами занимается также лично.



Анализ инфраструктуры

Технический этап расследования был сосредоточен на деконструкции архитектуры Mini-App. Поскольку Telegram Web App (TWA) по своей сути является встроенным браузером, было логично предположить наличие прямой ссылки на управляющий сервер в исходном коде. Запуск приложения через Telegram Web позволил с помощью стандартного инспектора браузера извлечь содержимое *iframe*. В нем был обнаружен URL-адрес, указывающий на размещение сервера в сети одной из чешских школ (на ресурсах для лабораторных работ).

Для верификации этих данных был проведен анализ визуальных артефактов в профиле субъекта. На одной из фотографий был запечатлен городской фон, в котором посредством GEOINT идентифицировали архитектурные объекты Праги. Совпадение локации серверной инфраструктуры и физического присутствия автора подтвердило, что проект развернут на базе учебного заведения, к которому субъект имеет прямой доступ.



Дополнительным подтверждением связи послужил анализ параметров самого URL. При попытке очистки адреса от технических параметров открывалась страница, где никнейм организатора был жестко прописан в коде (hardcoded). Данный идентификатор полностью совпадал с аккаунтом, с которого субъект выходил на связь, что окончательно закрепило его роль в структуре проекта.

Осознав, что инфраструктура обнаружена, организатор предпринял попытку экстренного переноса данных. В панике все ресурсы были перемещены на GitHub Pages. Однако с точки зрения Threat Intelligence этот шаг лишь открыл новый вектор для исследования: использование GitHub позволило изучить исходный код приложения, понять внутреннюю логику его работы и методы обработки данных. Более того, учетная запись на GitHub содержала тот же уникальный никнейм, что и в предыдущих случаях. Таким образом, попытка скрыть следы привела к еще большей утечке информации, предоставив полный доступ к технической базе проекта и подтвердив личность автора на еще одной платформе.

Верификация группового состава и структуры

На определенном этапе у нас возникли сомнения в реальности существования целой команды, так как субъект мог просто пытаться набить себе цену. Чтобы исключить вероятность очередного обмана, мы прямо запросили гарантии и подтверждение того, что он действует не один. Пытаясь доказать серьезность своей позиции, организатор предоставил скриншот закрытого чата, в котором четко отображалось наличие восьми участников.

Этот скриншот окончательно закрыл вопрос о формате деятельности. Стало ясно, что мы имеем дело не с одиночкой, а с организованной группой, координирующей свои действия внутри закрытого сообщества. Для самого субъекта этот шаг стал критическим проколом: стремясь подтвердить свои слова, он фактически задокументировал групповой характер правонарушения. В сочетании с использованием школьного сервера это превратило ситуацию из мелкого инцидента в полноценный коллективный кейс, масштабы которого теперь были подтверждены им самим. Попытка убедить нас в своей значимости лишь добавила конкретики к обвинению, раскрыв внутреннюю структуру управления и реальный размер его «ячейки».

Предоставленный скриншот группы и данные рейтинга позволили начать поиск внутри мониторингового сервиса. Основная зацепка заключалась в использовании админских префиксов — специальных подписей, которые появляются у администраторов группы. Поиск по этим признакам в сервисе позволил идентифицировать аккаунты «Super Gifter» и «kmirov».

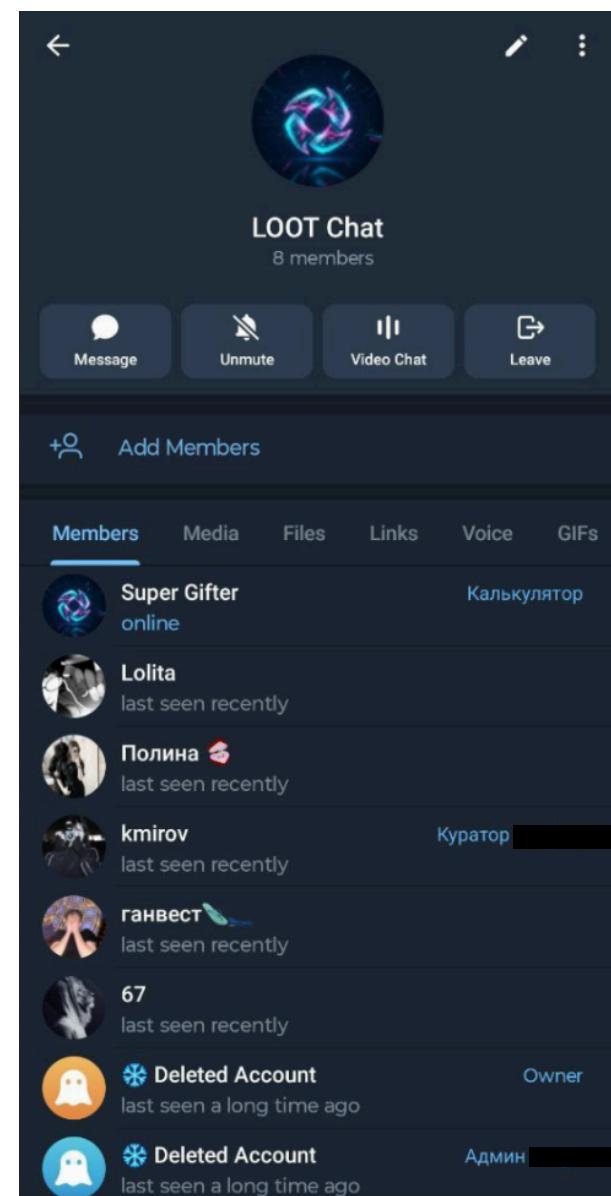
Через аккаунт самого организатора в том же сервисе был найден чат, в котором напрямую фигурировал один из воркеров «NaNa». Дальнейшая цепочка выстроилась через анализ подарков в профиле kmirov'a — так был обнаружен след еще одного воркера «Watsok», чей аккаунт на тот момент уже был удален. Из всего списка участников не найденным остался только один человек.

В итоге попытка дать гарантии существования команды привела к раскрытию почти всей структуры. Вместо анонимных участников на руках оказались связанные профили и история их взаимодействий. Это подтвердило полную прозрачность группы и позволило восстановить связи между организатором и его исполнителями, включая тех, кто попытался скрыться, удалив свои страницы.

Наличие скриншота с составом участников и данных мониторинга о связях между ними окончательно закрепило статус происходящего. Это больше нельзя было списать на личную неосторожность или разовый эксперимент одного человека. Факт наличия восьми участников, иерархии с админскими префиксами и четко распределенного заработка внутри «Топ-5» позволил квалифицировать деятельность как полноценную организованную группу.

Для организатора это стало самым тяжелым пунктом обвинения. Одно дело — отвечать перед администрацией школы за нецелевое использование сервера в одиночку, и совсем другое — выступать создателем структуры, координирующей действия группы лиц для систематического совершения правонарушений. Тот факт, что в цепочке связей всплыли даже удаленные аккаунты, лишил его возможности заявить о распаде группы или прекращении деятельности. Весь собранный материал теперь представлял собой готовую схему работы ОПГ, где школьные ресурсы использовались как техническая база для коллективной наживы.

Этот фактор стал критическим рычагом давления. Учитывая, что субъект является русскоговорящим в Чехии, возникло обоснованное предположение о его статусе беженца из Украины. В контексте юридического разбирательства это в корне меняло последствия: любое официальное заявление в полицию или администрацию школы могло запустить процесс, итогом которого стала бы не только потеря учебного места, но и аннулирование права на пребывание в стране с последующей депортацией.



Кульминация

Наличие доказательств по деятельности организованной группы в сочетании с эксплуатацией школьных ресурсов создавало состав правонарушения, несовместимый со статусом временной защиты. Для организатора ситуация из плоскости «проблем с учебой» перешла в плоскость угрозы принудительного выдворения. Перспектива потерять возможность находиться в Европе из-за участия в фишинговой сети стала весомым аргументом, лишающим его пространства для маневра и дальнейших попыток обмана. Каждое звено в цепочке — от использования школьного домена до списка воркеров — теперь работало как прямое основание для пересмотра его законного нахождения в Чехии.

Когда все фрагменты мозаики — от чешского сервера до списка воркеров и финансового рейтинга сошлись в единую картину, взаимодействие перешло в стадию прямого урегулирования. Субъекту была предъявлена аргументированная досудебная претензия. Все действия со стороны пострадавших были квалифицированы как законная защита своих прав и интересов в ответ на использование инфраструктуры школы для обеспечения деятельности организованной группы.

Основной удар пришелся на понимание юридических и административных последствий. Ему прямо обозначили, что использование инфраструктуры школы для работы организованной группы — это прямой путь к немедленному отчислению. Однако более весомым аргументом стал риск депортации. Учитывая вероятный статус беженца, участие в систематическом мошенничестве и эксплуатации государственных ресурсов Чехии превращало его пребывание в стране в вопрос времени до первого официального обращения в полицию.

После предъявления всех фактов и обозначения перспектив депортации, субъекту был выставлен список жестких условий. Требования включали немедленное прекращение работы платформы, удаление всех ресурсов и чатов с соучастниками, а также полный возврат активов пострадавшей стороне. Особое внимание было уделено верификации процесса: организатор должен был предоставить видеофиксацию каждого шага по ликвидации инфраструктуры.

Процесс возврата имущества столкнулся с технической сложностью: один из активов уже был продан конечному пользователю. В этой ситуации субъекту пришлось выкупать его обратно за свой счет. В итоге все активы были возвращены, хотя в одном случае возврат был осуществлен путем передачи идентичного подарка той же стоимости.

Alex K.

📁 Screenshoty	2/15/2026 2:19 AM	File folder		
📄 Protokol_Loot_Market.pdf	2/15/2026 3:04 AM	WPS PDF Docume...	471 KB	
xlsx Prvky vizualizace dat.xlsx	2/15/2026 2:23 AM	XLSX Worksheet	10 KB	
Seznam spolupracatelů a jejich rozdělení...	2/15/2026 2:26 AM	XLS Worksheet	24 KB	
ultimate-nft-marketplace-main.zip	2/10/2026 10:23 PM	ZIP File	322 KB	
jpg Vizualizace dat.jpg	2/15/2026 2:22 AM	JPG File	93 KB	
txt Všechny archivované stránky.txt	2/15/2026 3:04 AM	Text Document	1 KB	

, читай внимательно и один раз.

Папка на скриншоте — это твой приговор и уголовное дело. У меня на руках полная доказательная база твоих махинаций с Loot Market, использования хостинга SPŠEAG (V Úžlabině) и репозиториев GitHub. Это прямой состав преступлений по статьям § 209 (Podvod) и § 230 (Neoprávněný přístup) УК Чехии. Мне все равно, 14 тебе, или 16. Если тебе есть 15, то ты отвечаешь за свои деяния как взрослый преступник. Если тебе нет 15, то за твои действия немедленно и в полном объеме ответят твои родители.

Заявления в Policie ČR и администрацию школы уже составлены. Для тебя, как для обладателя Dočasná ochrana, запуск этого механизма означает автоматическую проверку легитимности твоего пребывания в ОАМП MV ČR. Результат предсказуем: аннулирование статуса, депортация и пожизненный запрет на въезд в Шенгенскую зону. Ты потеряешь всё из-за двух NFT. Я не собираюсь с тобой торговаться или слушать оправдания. У тебя есть последний шанс закрыть вопрос в рамках «деятельного раскаяния» до того, как государственная машина придет за тобой прямо в колледж.

Мои условия (срок — до конца сегодняшнего дня
1. Возврат обоих NFT на аккаунт [REDACTED]).
2. Полная ликвидация всей инфраструктуры (GitHub, боты, чаты соучастников) с предоставлением видеодоказательства удаления.

Если до полуночи понедельника условия не будут выполнены, документы уходят в официальный оборот. Обратного пути не будет. После подачи заявления я не смогу и не стану его отзывать.
Время пошло. Решай, стоит ли этот мусор твоей жизни в Европе.

AK

Продолжение кульминации

Этот скриншот фиксирует стадию признания вины и начала возврата похищенного имущества. В переписке организатор прямо подтверждает свою осведомленность о составе украденных активов, задавая вопрос о том, что именно подлежит возврату. Его попытка договориться о передаче «подобных» предметов по той же цене указывает на то, что оригинальные активы на этот момент уже были выведены или распределены внутри его группы.

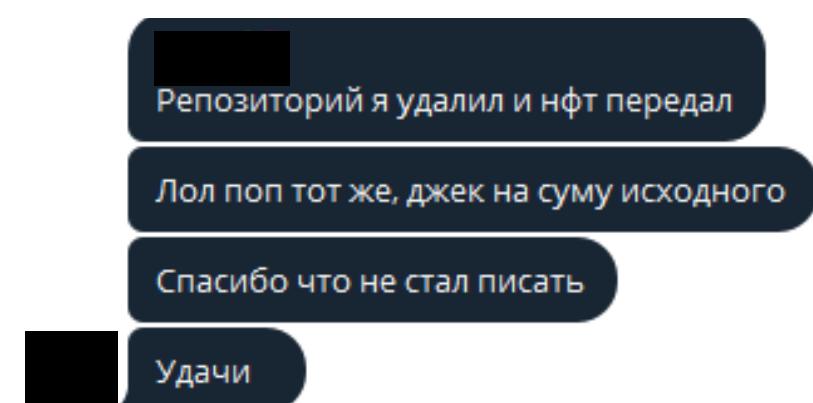
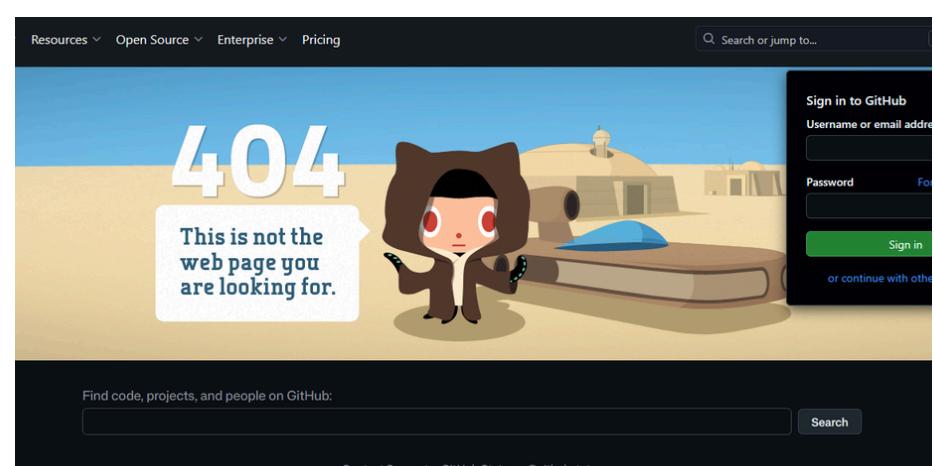
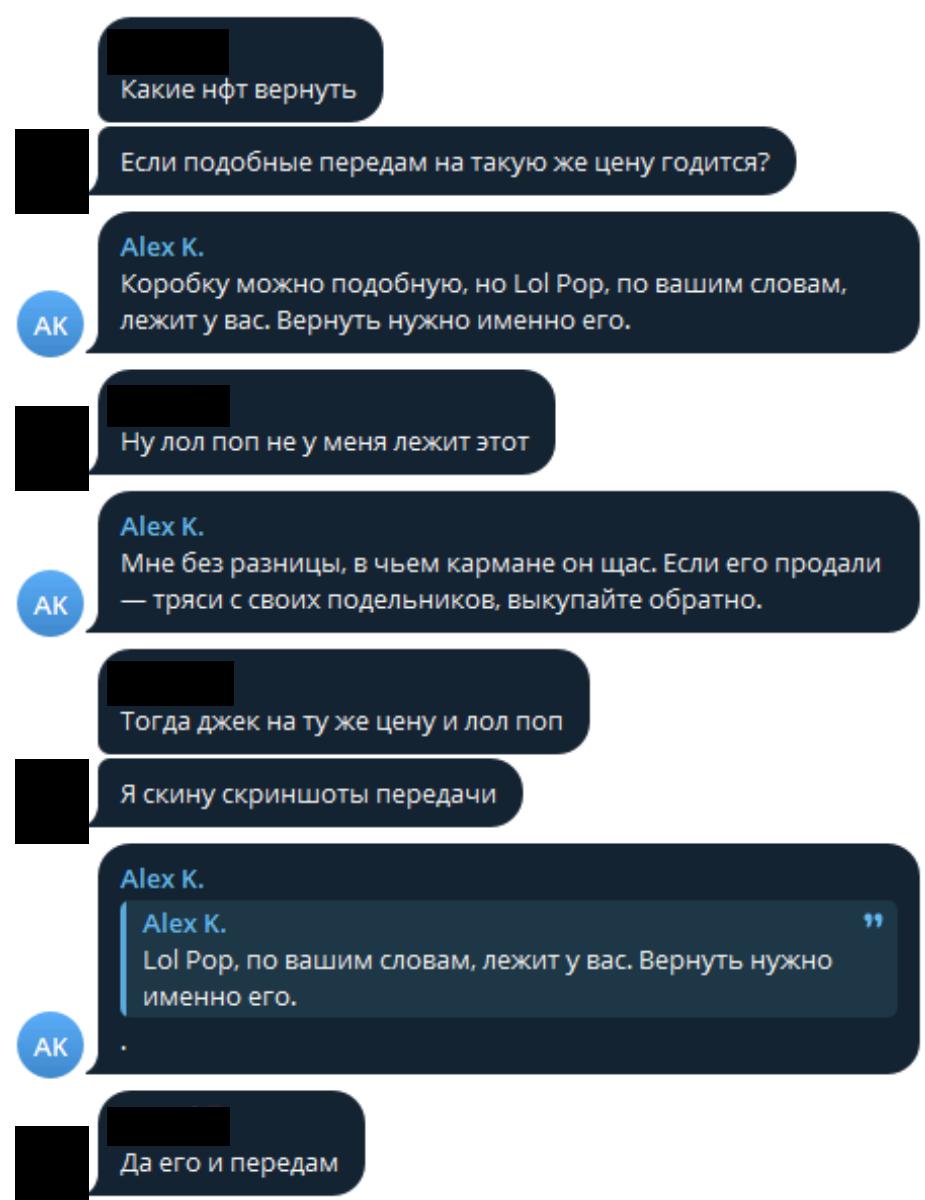
Особое внимание стоит обратить на эпизод с «Lol Pop». Изначально субъект заявляет, что актива у него нет, однако после требования выкупить его у подельников или найти любым другим способом, он соглашается на возврат оригинала. Это подтверждает, что организатор полностью контролирует действия своих воркеров и имеет возможность принудительно изымать у них полученную добычу.

Диалог доказывает, что субъект осознал бесперспективность дальнейшего обмана. Скриншот служит подтверждением того, что под угрозой депортации и отчисления организатор перешел к полной ликвидации последствий своих действий, включая выкуп активов за собственный счет. Это финальный документ, закрепляющий добровольный возврат имущества в рамках досудебного урегулирования.

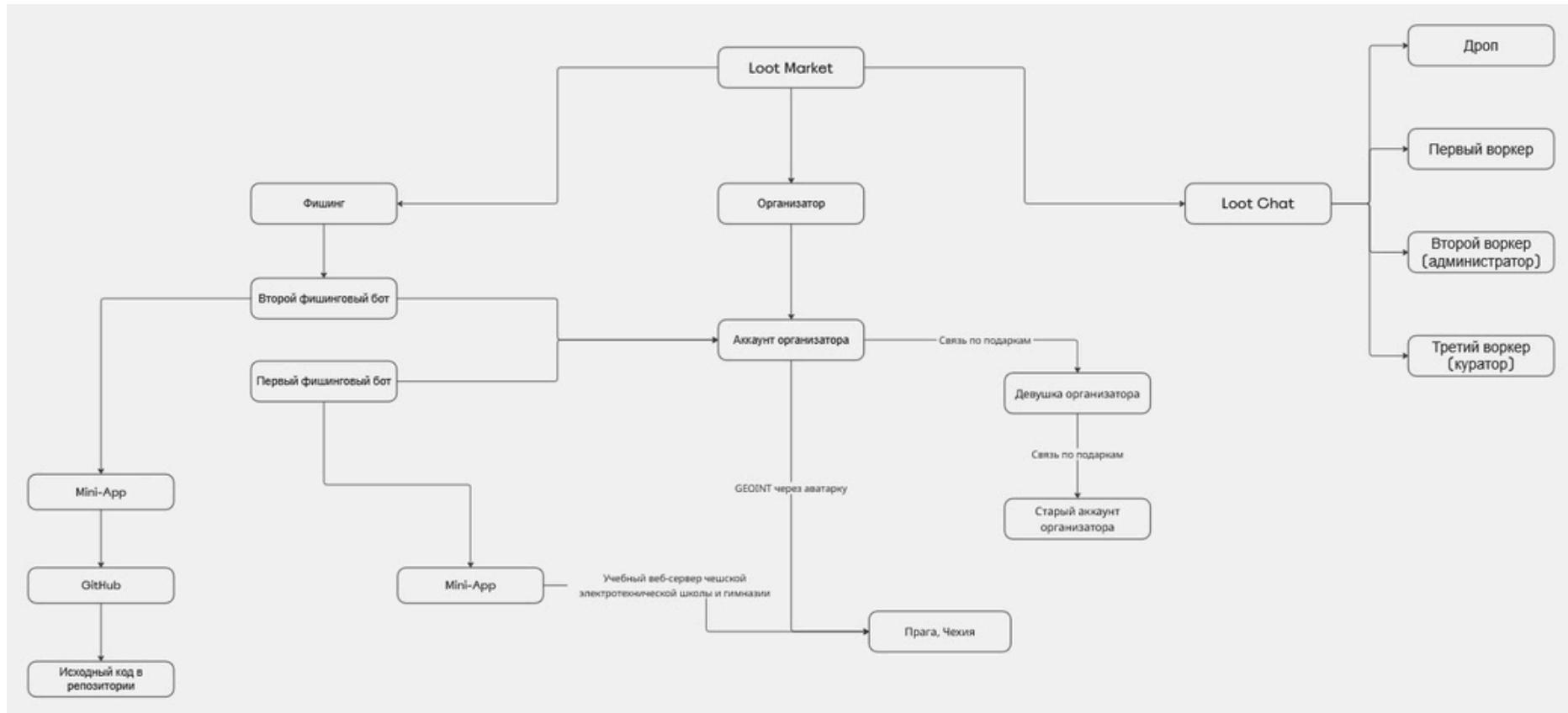
После завершения процедуры возврата активов организатор приступил к полной ликвидации технической инфраструктуры проекта. Финальным этапом стало удаление репозитория на GitHub, где размещался исходный код платформы.

Этот шаг подтверждает выполнение одного из ключевых условий досудебной претензии — полное прекращение существования проекта. Скриншот страницы репозитория, выдающий ошибку **404**, служит документальным подтверждением того, что программная база больше не доступна для использования или копирования. Удаление кода вместе с ранее зафиксированной очисткой баз данных и закрытием чатов воркеров означает окончательный демонтаж всей сети.

Завершающим штрихом в коммуникации стало официальное заявление организатора о полном выполнении всех условий. После того как последние транзакции по возврату активов были подтверждены, а технические ресурсы стерты, субъект в личной переписке констатировал, что «все вернул» и проект полностью ликвидирован. Это заявление подвело черту под процессом досудебного урегулирования.



Вывод



Инцидент с эксплуатацией школьных серверных мощностей для развертывания фишинговой платформы завершился полным демонтажем выявленной структуры. Ключевым фактором успеха стала детальная идентификация всех звеньев цепи: от технической базы на чешском домене до персональных данных участников организованной группы. Предъявление обоснованной досудебной претензии позволило перевести конфликт из цифровой плоскости в правовую, где риски депортации и отчисления стали для организатора решающим аргументом.

Результатом предпринятых действий стало не только полное возмещение материального ущерба и возврат активов пострадавшему, но и превентивное уничтожение всей инфраструктуры проекта. Видеофиксация удаления репозитория, баз данных и роспуска рабочих чатов гарантирует, что созданная сеть перестала функционировать. Случай подтвердил, что даже технически продуманные схемы, использующие государственные ресурсы, оставляют достаточный цифровой след для их полной деанонимизации и законного подавления.

Итог дела — признание организатором своей вины и его добровольное содействие в ликвидации последствий, что позволило разрешить ситуацию без привлечения полиции Чехии, сохранив при этом права пострадавшей стороны.