Введение

Четвертого января 2025 года последовало обращение о хищении активов (Exit Scam) в размере **300$** при проведении сделки через посредника. Субъект выступил в роли «гаранта» сделки, однако после получения финансовых средств присвоил их, прервав выполнение обязательств. Принимая во внимание мошеннический характер действий, основной целью расследования стала полная деанонимизация субъекта для формирования доказательной базы.

Задача

Преодоление созданной субъектом анонимности и установление его физической личности (деанонимизация) для последующего формирования доказательной базы и передачи материалов заказчику.

Цели

- Установление персональных данных: Получение верифицированных ФИО и точной даты рождения.
- Физическая привязка: Установление контактных номеров телефонов и региона проживания субъекта.
- Верификация через Pivot-анализ: Подтверждение связи между Telegram-аккаунтом мошенника и его профилями в социальных сетях и банковских сервисах.

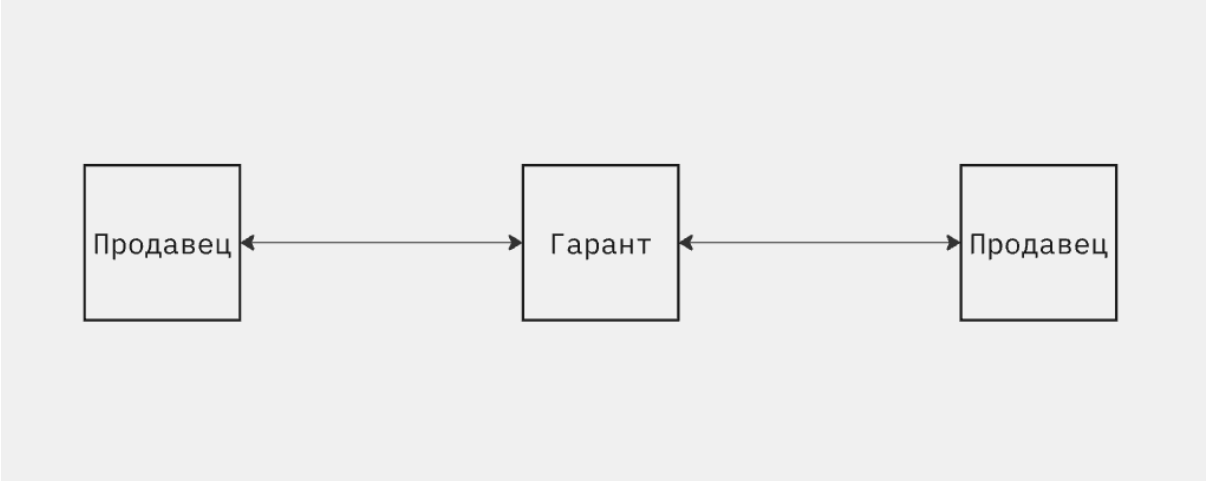
Группа расследования

@ownstates
Исследователь

@praganodox
Исследователь

Анализ мошеннической схемы («Левый гарант»):

В ходе аудита инцидента была восстановлена механика взаимодействия сторон. Субъект использовал классическую, но технически подготовленную модель «левого гаранта»:



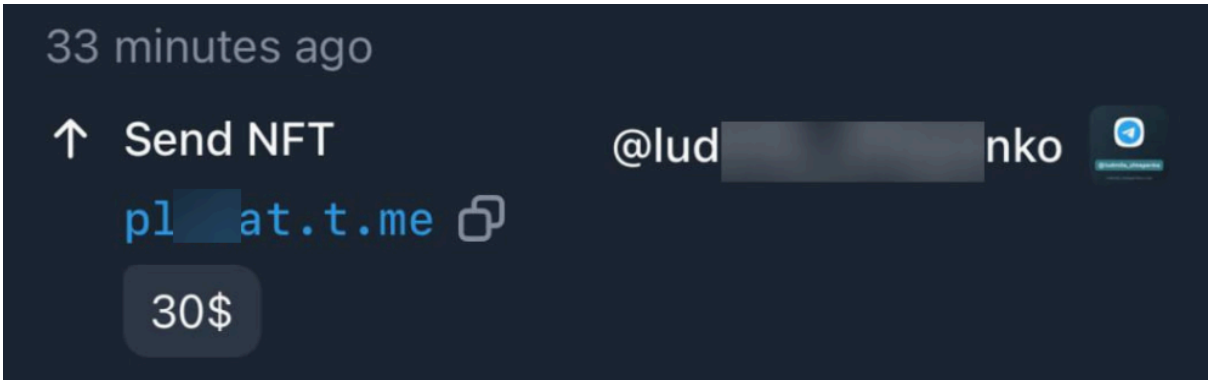
1. **Инициация:** Сторона-продавец и сторона-покупатель привлекают третью сторону (субъекта) для обеспечения безопасности транзакции.
2. **Алгоритм сделки:** По регламенту гарант должен депонировать товар от продавца и денежные средства от покупателя, осуществляя обмен только после подтверждения выполнения условий обеими сторонами.
3. **Эксплуатация доверия:** Получив оплату в размере **300$**, субъект не произвел передачу товара/выплату средств, заблокировал коммуникацию и скрыл следы активности, присвоив всю сумму сделки.

Ход расследования

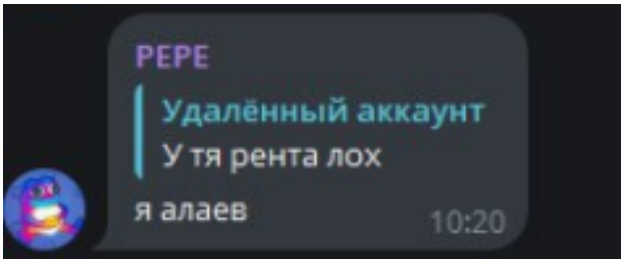
Одной из ключевых преград на начальном этапе стало использование субъектом **Anonymous Telegram Numbers (коллекционные номера +888).** Для обычного

OSINT-специалиста это тупик: номер не привязан к SIM-карте, что вызывает трудности для классического «пробива» по номерам телефона через способы, вроде HLR-запросов.

Однако, с точки зрения **Threat Intelligence**, использование номера +888 не скрывает объект, а, напротив, **открывает окно анализа через блокчейн TON.** Мы деанонимизировали цепочку владения NFT-номером через TonViewer. Был проведен аудит кошелька-холдера, который вывел нас на историю продажи юзернеймов. Это позволило нам связать анонимную «личность» мошенника с конкретными финансовыми следами и выявить его технический аккаунт @pl..at.



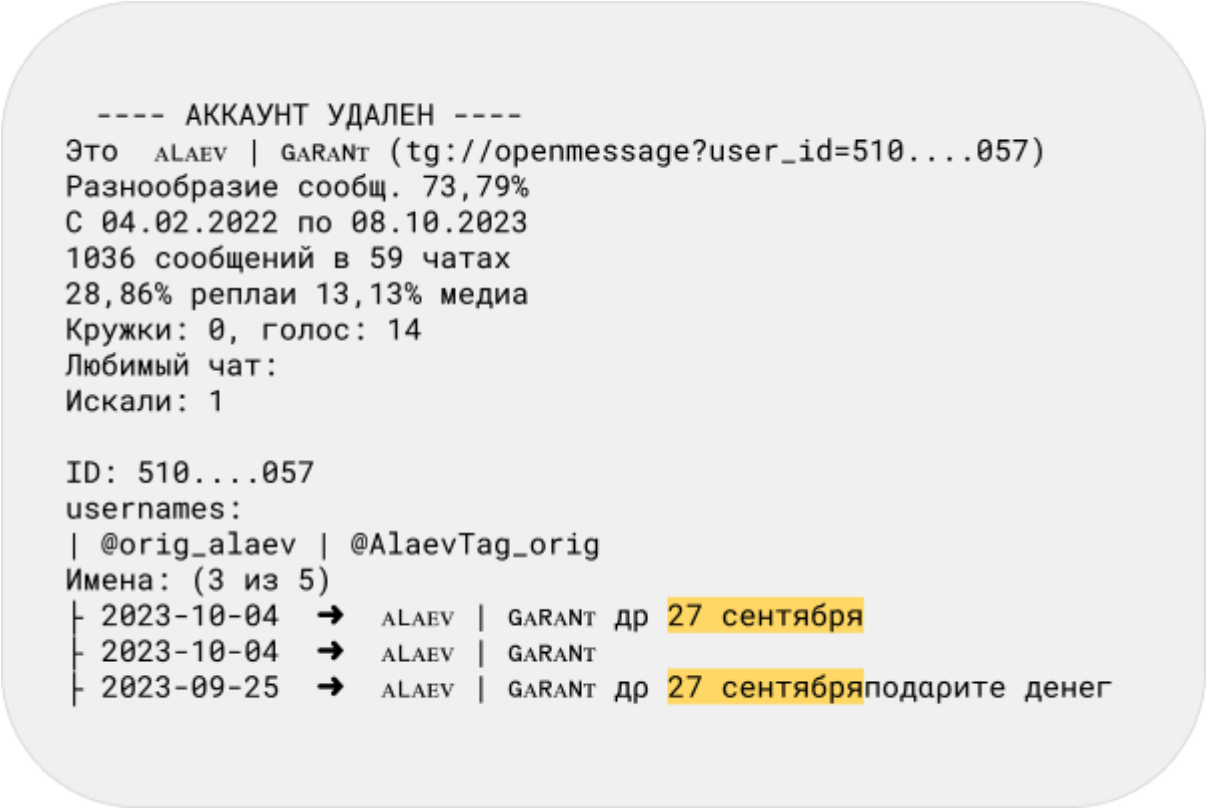
Поскольку субъект пытался мимикрировать под «чистый» аккаунт, мы применили анализ сообщений в публичных чатах с помощью мониторингового сервиса «Telelog», что позволило достать нам один из alias’ов фигуранта расследования:



Логичным следующим шагом стало применение доркинга. Вместо стандартного поиска по русскоязычным запросам, потребовалось перевести поиск в плоскость

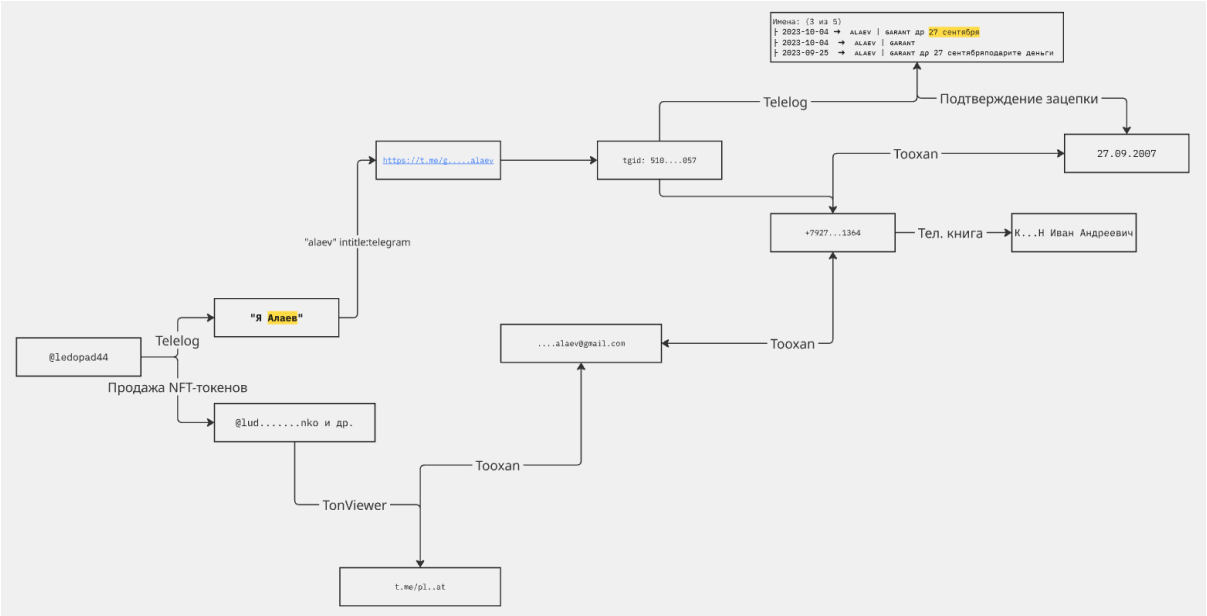
транслитерации. Использование латинского написания alias’а и связанных идентификаторов для обхода ограничений локальных поисковиков.

Использование дорка в транслите: "alaev" intitle:telegram позволило, найти заархивированный сервисом TgramSearch канал, где фигурировал технический юзернейм «....alaev». На момент проведения расследования на него был зарегистрирован канал, это означало, что юзернейм был изъят другим пользователем. Чтобы установить технический идентификатор (UID) аккаунта понадобилось вновь использовать тот же мониторинговый сервис, который использовался для анализа публичных сообщений субъекта:



Помимо мониторингового сервиса, был использован инструмент «Tooxan», который на основе UID аккаунта позволил получить номер телефона +7927....1364. Проведение ресерча на основе утечек по найденному идентификатору позволило нам установить полное ФИО

(К....Н Иван Андреевич), а также подтвердило указанный субъектом в профиле день рождения. Помимо подтверждения мы получили год рождения (2007), который указывал, что на момент проведения сделки он являлся несовершеннолетним.



Реализация целей и итоговые выводы

На основе проведенного OSINT-расследования можно констатировать успешное выполнение всех поставленных целей. Личность правонарушителя деанонимизирована в полном объеме. Вечером **восьмого января 2025 года** консолидированный отчет и визуализация связей были переданы заказчику для инициации дальнейших мероприятий по возврату средств и пресечению незаконной деятельности фигуранта.

Данный документ носит информационный и образовательный характер. Все данные получены из открытых источников (OSINT). Автор не несет

ответственности за дальнейшее использование данной информации третьими лицами.