
Докс, кровь,
Minecraft

OSINT write-up: Докс, кровь, Minecraft

Описание кейса

Этот документ — пример райтапа[1]. Отличие райтапа от отчёта в том, что у райтапа вольная подача, я могу его писать в формате эссе. Очевидно, такой документ на работу не примут, но таким документом намного легче описывать кейсы малого масштаба, например этот.

Ночью 25-ого июня мне написал мой давний товарищ и попросил о консультации. После неудачной катки в доте ему написали два доксеренка и начали угрожать расправой, скинули запугивающее видео, как пример того, что случится с ним в будущем.

Если вы успели подумать, что этот райтап о помощи товарищу с проблемой доксеров — нет. Мне изначально было все равно, т.к. угрозы после игры не должны восприниматься всерьез, но сами угрозы мне показались довольно занимательными для анализа и поиска исходника.

Исходные данные

- Telegram-юзернеймы доксеров
  - @emojunkie
  - @tryagree
- Запугивающее видео
  - https://t.me/+2433b6VWsGE2OTIh (не для впечатлительных)

Цели расследования

- Доказать несостоятельность угроз
- Найти первоисточник видео

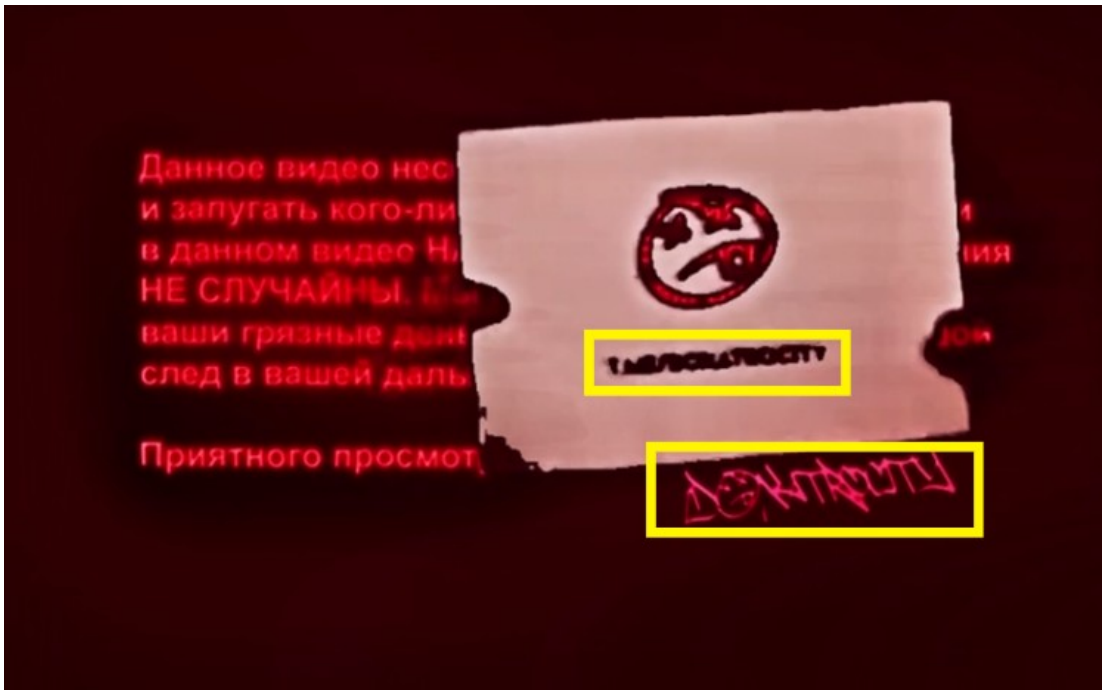
Первый этап: Изучение видео

Угрожающее видео разделено на несколько частей:

Интро	Парень в маске зайца идёт вдоль гаражей по улице
Дисклеймер	Содержит название оригинального проекта
Завязка	Парень с голым торсом стоит на коленях и держит в руках сигну с ссылкой на проект, за ним стоит другой парень с ножом — тот, что был в интро
Череда перебивок	1. “Помилование” 2. “Оно того стоило?” 3. “закрой рот и отдай все если я скажу”
Кульминация	Парень в маске зайца стоит в лифте, держит в руках брелок и предмет, облитый кровью, предположительно ухо
Аутро	Надпись “бежать некуда”

1 **Райтап** (от англ. write-up — “запись”, “отчет”) — это подробное пошаговое описание того, как было решено конкретное задание, взломана система или выполнена задача.

Первый этап анализа: расшифровка надписи на бумаге.



На бумаге видно, что сигна — ссылка на Telegram: t.me/**

Надписи на подписи дисклеймера и бумаге совпадают — это один и тот же текст. Методом подбора прийти к ссылке не получилось, я написал фигуранту @tryagree напрямую (помним, что кейс несерьёзный).

С его слов ссылка — его старый логин: doxatrocity. Такой канал действительно существовал, но сейчас остался только резерв: t.me/doxatroxity

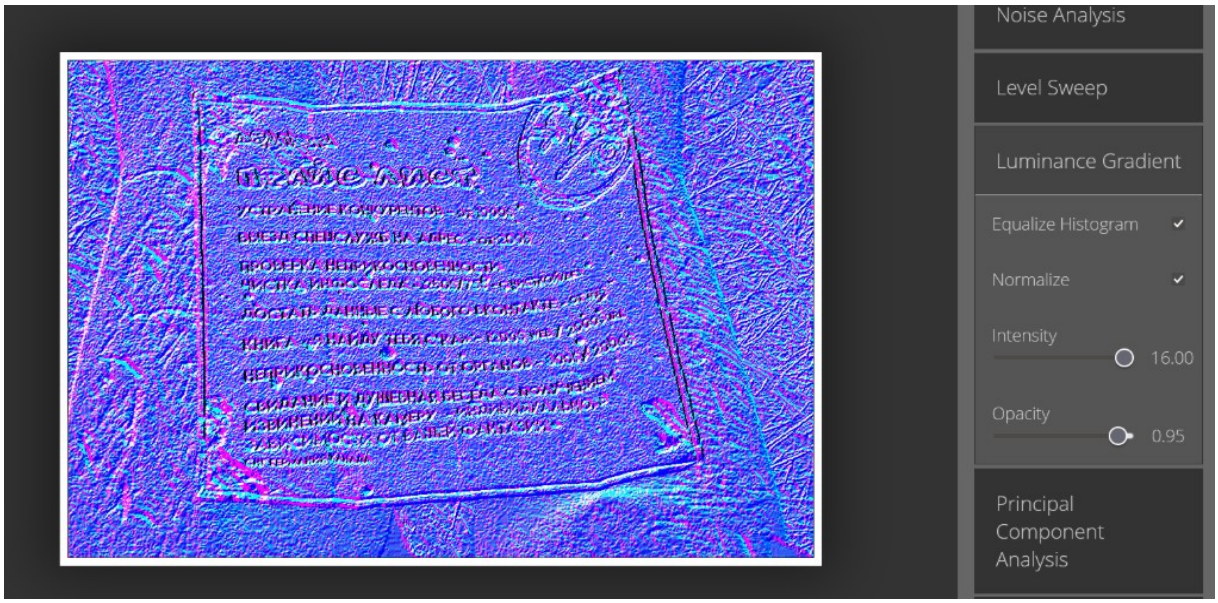
В ходе дальнейшего диалога с @tryagree я пришёл к выводу, что он не имеет никакого отношения к проекту Doxatrocity в силу возраста (самые старые упоминания Doxatrocity датируются 2022-ым годом) и когнитивных способностей, поэтому в дальнейшем райтапе о нём не будет никаких сведений, а вот проект Doxatrocity — по прежнему очень интересный искомый объект.

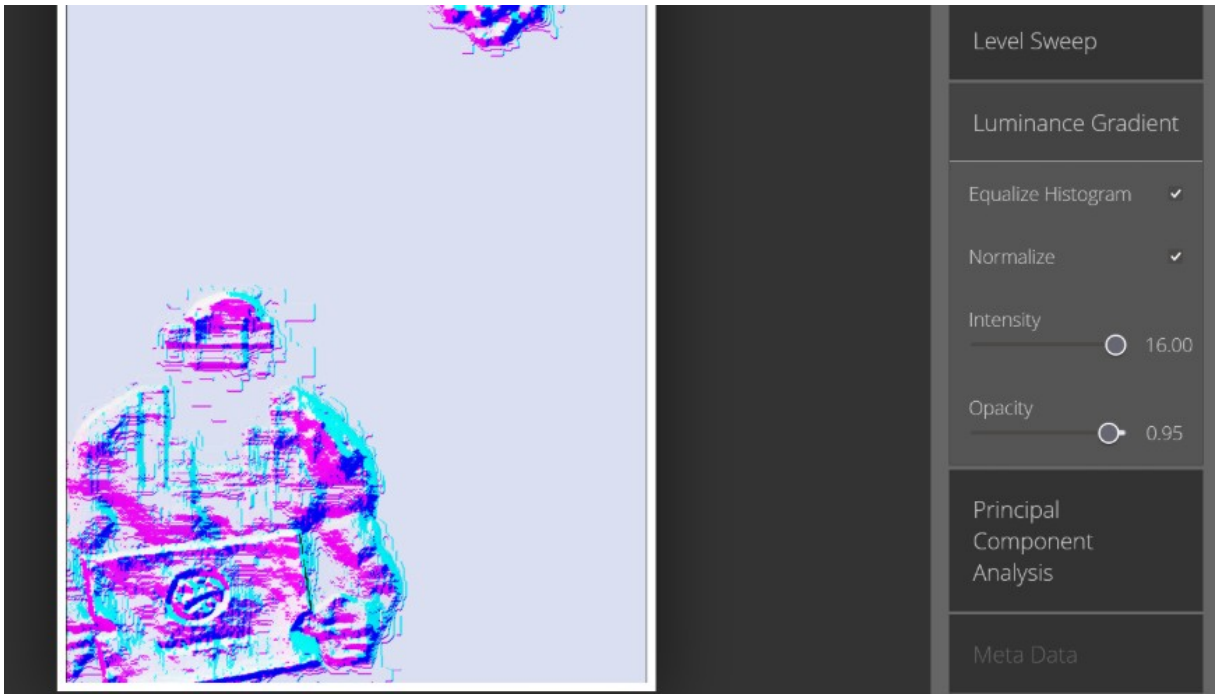
Канал представляет собой адаптер и прайс-лист на теневые услуги:

- Книга по “деанону” за огромные деньги
- Аудит безопасности
- “Крыша” от органов
- Силовые услуги

На превью прайс-листа стоит та же фотография, что была в видеоряде во время перебивок, слева сверху на листочке тот же логотип. Судя по контрастности надписи и следам крови на стикере справа сверху — это фотошоп (гипотеза). Автор им явно владеет.

Исходя из моей гипотезы о том, что все медиа — фейк, я посчитал уместным поёрзать ползунками в Forensically.





Очевидно, что я не гик форензики[2], и сами по себе эти ползунки мне мало что дадут, но для подтверждения гипотезы можно попробовать найти закономерность.

На двух медиафайлах есть листочек с текстом и картинками, напечатанными на принтере.

Покрутив ползунки Luminance Gradient, можно сделать вывод, что надпись на листочке в видео такая же контрастная, как остальные самые контрастные объекты, а на фото ещё контрастнее, чем всё остальное. Интереса ради можете провести следственный эксперимент: напечатать что-то на бумаге, сделать фото и также сравнить контрастность.

Для самой объективной экспертизы этого мало, но косвенно это подтверждает правдивость моей гипотезы. Напечатанное “что-то” не должно быть контрастнее остальных объектов.

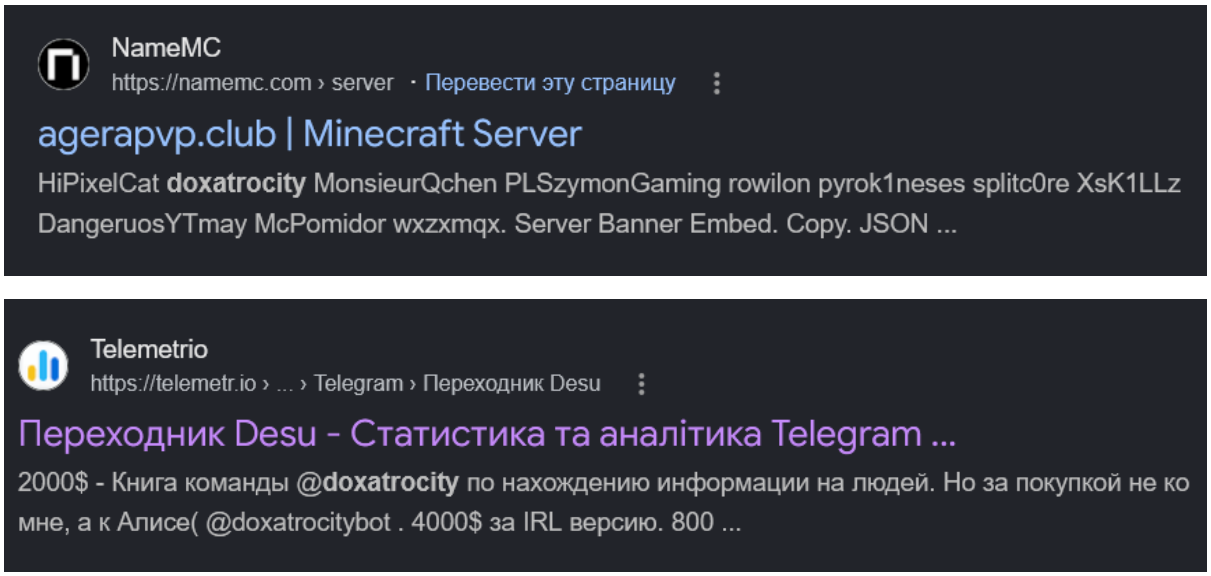
2 **Форензика** — цифровая криминалистика.

Второй этап: Бекграунд Doxatrocity

Кира @chronolocation рассказала мне о том, что знает этих ребят и когда-то давно сама занималась их поисками. Дала мне несколько ников, которые связаны с этим проектом: Кислит и Десу.

Хоть я и склонен ей верить, но даже для райтапа слов “она рассказала” — мало. Будем считать этот абзац за сведения, собранные путём HUMINT[3].

Чтобы подтвердить эти сведения, я использовал дорк[4] “doxatrocity”.



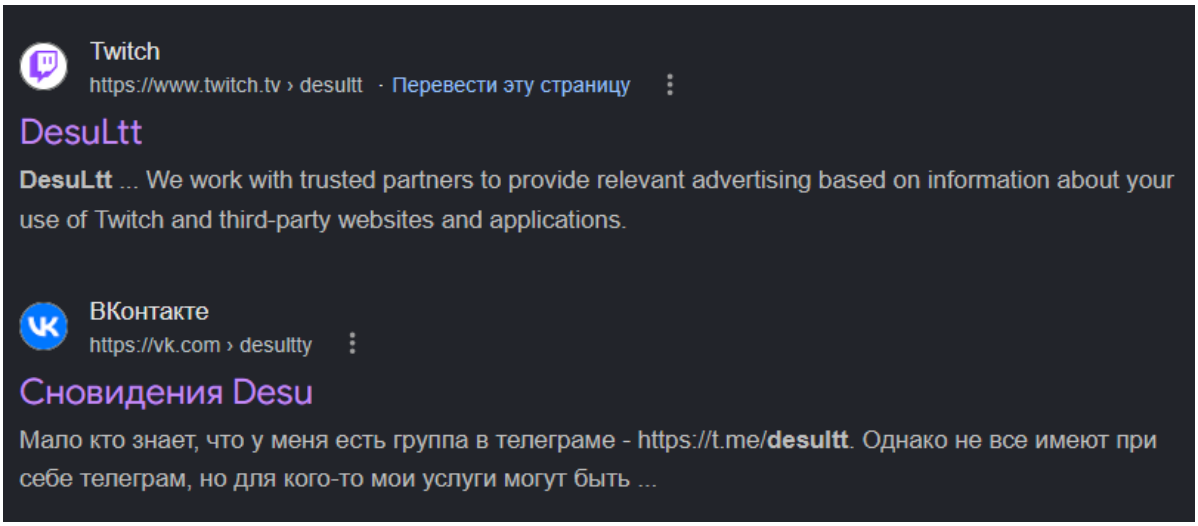
Результат дорка: несколько ссылок на сайты, связанные с Minecraft, и переходник Desu. Спасибо Кире за сведения.

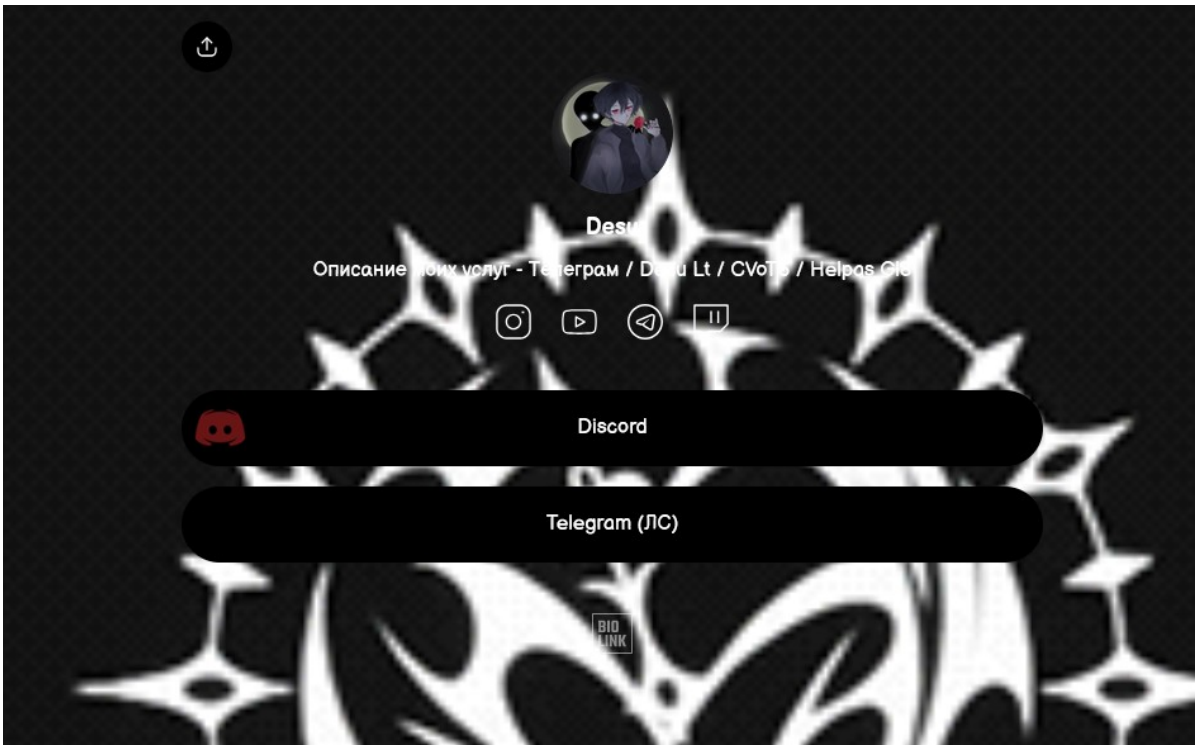
Просматривая записи в Telemetrio можно сделать вывод о том, что доксеры не меняются, и найти его логин desultt.

Взяв за основу для дорка логин “desultt”, можем найти следующие сведения:

Twitch	https://www.twitch.tv/desultt
Страница ВК	https://vk.com/desultty
Веб-био	https://bio.link/desultt

3 **HUMINT** — человеческая разведка.
4 **Дорк** — специфический поисковой запрос с использованием операторов поисковой системы.

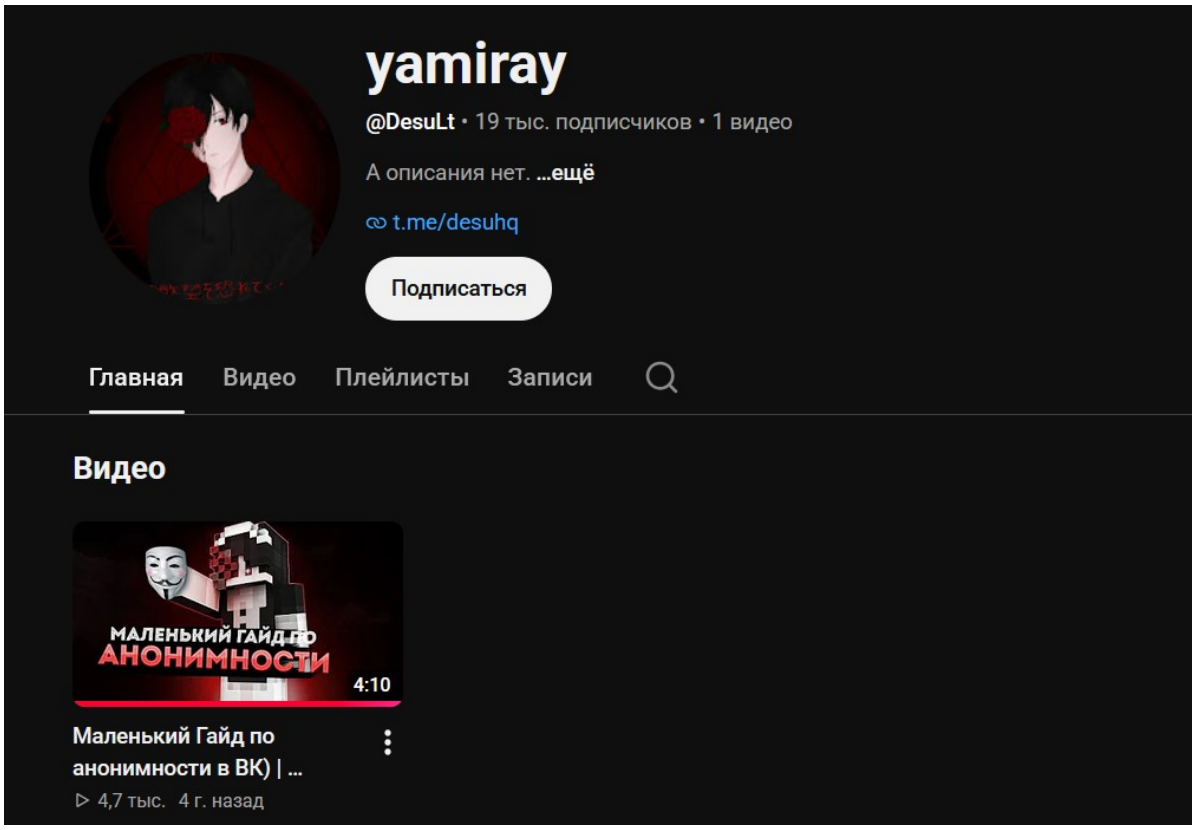




Веб-био содержит ссылки на профили:

Instagram	https://www.instagram.com/desuhazu
Youtube	https://www.youtube.com/channel/UCM4DZdilHfMOZMlWUkwgZEw
Telegram	• https://t.me/desulttt • https://t.me/likeyourdesu
Twitch	https://www.twitch.tv/yomiray
Discord	https://discord.com/users/915562417562468362

Его телега, дискорд и инста мало меня интересуют, цели задеанонить этого покемона у меня не стоит. Зато его ютуб — очень интересная зацепка.



На канале можно найти парочку новых ссылок, которые потенциально могли стать зацепками для деанона этого молодого человека, и одно видео.

Видео представляет собой геймплей Minecraft SkyWars и описание базовых профилактических мер для анонимности в сети с ноткой доксерского долб**бизма. Описание под видео является кладезем новых потенциальных зацепок.

На этом этапе, игнорируя ссылки и остальные потенциальные зацепки, возвращаясь к целям расследования и учитывая найденную информацию, можно полагать, что видео не является серьезной угрозой.

Имеющейся информации достаточно для того, чтобы перейти на новый этап расследования.

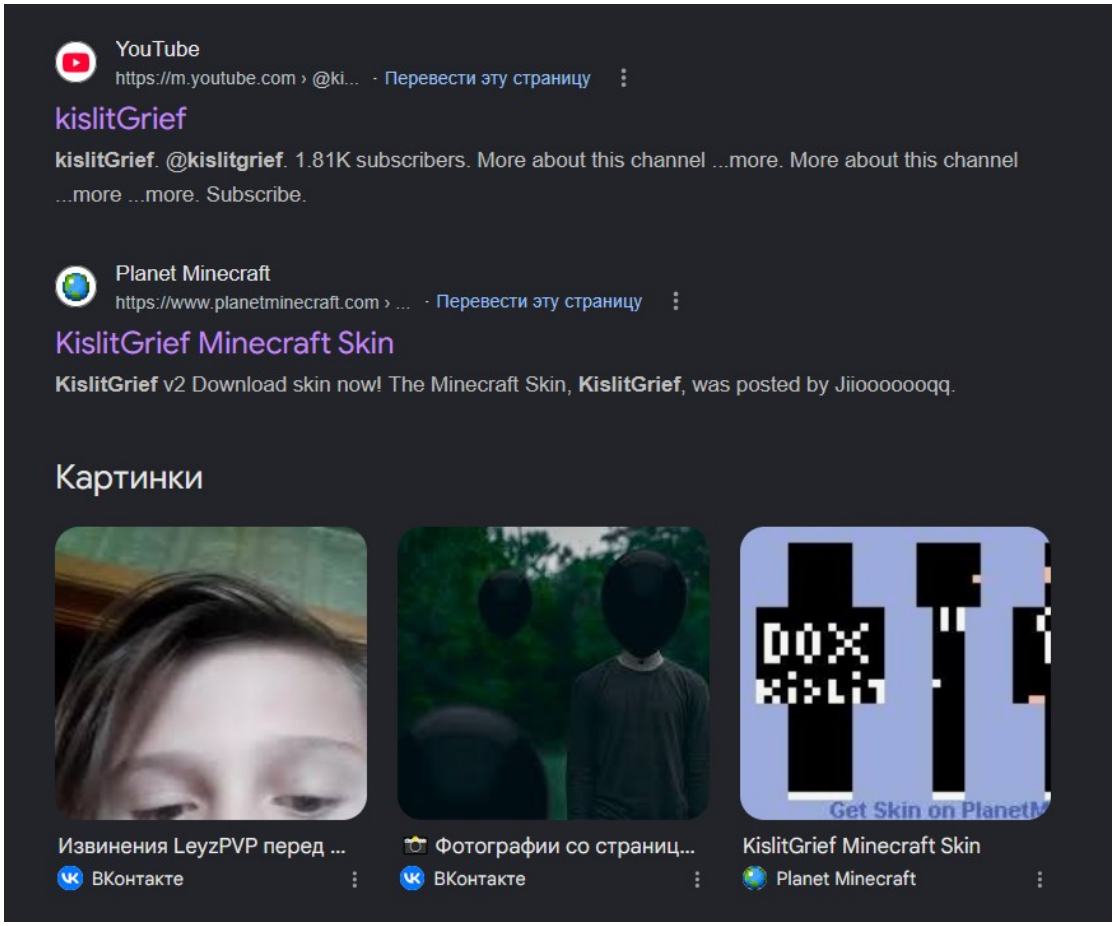
Третий этап: След Minecraft

Возвращаясь к HUMINT-сведениям Киры: Doxatrocity переходил из рук в руки. Упомянуто было два никнейма: Кислит и Десу. С Десу мы разобрались, кто же такой Кислит?

Логин, полученный от Киры: KislitGrief

По классике, этот логин становится основой для дорка: “KislitGrief”. Найденные сведения:

Youtube	https://www.youtube.com/@kislitgrief
Скин в Minecraft	https://www.planetminecraft.com/skin/kislitgrief-6853110/
Страница ВК	https://vk.com/kislitreviews
Извинения маленького майнкрафтера перед искомым	https://vk.com/video-199037894_456239017



Исходя из вышеуказанных сведений делаем вывод, что Кислит — еще один доксер-майнкрафтер.

Можно попытаться рыть дальше, установить какую-то связь между Кислит и Десу, чтобы подтвердить факт передачи Doxatrocity, задеанонить каждого из них, разобраться во внутренней кухне майнкрафтеров, но, думаю, что это уже лишнее, ибо цели расследования и без того давно выполнены.

Итоги расследования

Суммируя найденные сведения, я могу сделать вывод о том, что угрожающее видео — ИПСО, созданная с целью запугивания жертв “доксинга” лицами, причастными к проекту Doxatrocity.

Основатель проекта Doxatrocity — Десу — обычный майнкрафтер, который открыл для себя тему доксинга в 2021 году и подумал, что дорвался до власти. Его деятельность в интернете разделилась на дихотомию развлекательного майнкрафт-контента и пафосного, таинственного, злого и страшного доксинга.

Ведомый желанием казаться, а не быть, Десу основывает проект Doxatrocity в 2022 году, насыщенный устрашающими примочками, которые он создаёт благодаря своему опыту в фотошопе и рисовании (исходя из его постов в ВК за 2021): селфхарм-сигны, запугивающие посты, демонстративный прайс с чрезвычайно дорогими услугами и другие смешные атрибуты.

Одна из таких устрашающих примочек — это видео, которое он, вероятно, скидывал ребятам, с которыми ссорился на VimeWorld-е.

Видео настолько качественно исполняло свою функцию, что каждый, кому оно попадало в руки, брал его себе на вооружение. Именно поэтому его скидывают в качестве угроз после неудачной катки в доте даже сейчас, спустя 4 года.

Выводы

Не стоит верить всему, что вы видите или слышите в интернете, даже если увиденное или услышанное сильно вас впечатлило. Лучший друг социального инженера — эмоции.

Возьмите за основу обобщение и догму: доксеры — безобидные дети, неумеющие работать с информацией, а сводка ваших персональных данных не является компрометирующей.

Доксинг — одна из самых больших проблем интернета, катализатором влияния которой являются асоциальные подростки, но важно помнить, что доксинг влияет на качество жизни только того, кто им занимается. Жертва доксинга не станет жить хуже от того, что её персональные данные оказались в сети, т.к. они там были всегда.

Получая подобные угрозы в формате медиафайлов, попробуйте найти первоисточник или зацепиться за идентификаторы, указанные в этих медиафайлах. Вес угроз уменьшится до нуля, когда вы увидите, что за этим видео стоит майнкрафт-ютубер.

Учитесь OSINT-у и не занимайтесь ерундой в интернете.

Спасибо маме Кире @chronolocation за все исходные данные, идентификаторы искомых, описание устройства старого сообщества доксерят и их внутренней кухни, HUMINT-сведения для перекрёстной проверки, создание и дополнение категорий “Литература” и ”Форензика, крипторасследования, шифрование” в Личном Архиве и вообще всему, что она делает.