

Ботоводство, накрутка, прослушка и медиа-войны: обзор практических кейсов и инструментов кибер-расследований

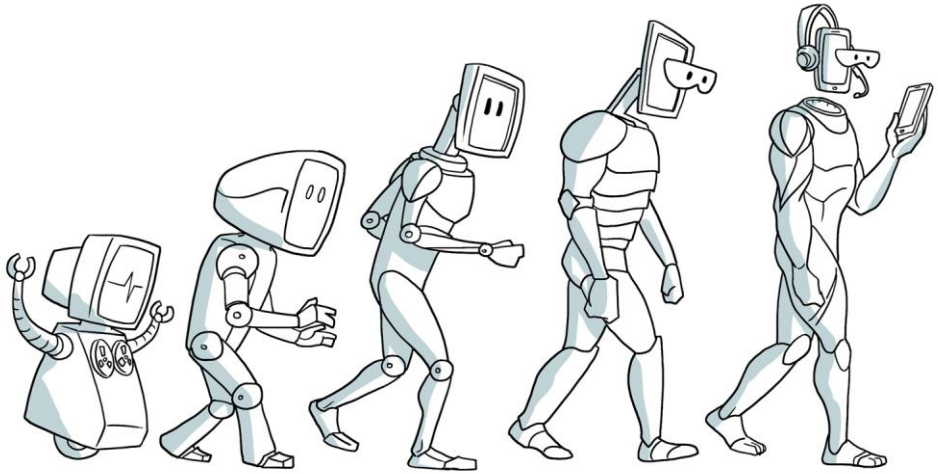
HackControl: Co-founder & CEO
Cyber Security Conference HackIT: Co-founder
В кибербезопасности более 10 лет
2 года в СБУ
Экс Советник Администрации Президента Украины
ProtectMaster: Co-founder & CEO
Специализация: защита веб-сервисов и расследование инцидентов

HackCtrl

Никита Кныш
hackcontrol.org

Типы социальных ботов

- Социальные боты в электронной коммерции. Боты-продажники.
- SEO боты, лайкатели, накрутчики и репостеры.
- CPA боты-многодневки.
- Политические социальные боты-тролли и лидеры мнений.



Их идентифицирующие признаки можно сформулировать, отвечая на вопросы:
кто, как и зачем использует ботов.

Никита Кныш
hackcontrol.org

Типы социальных ботов

- Социальные боты в электронной коммерции. Боты-продажники.

Идентифицирующий признак: стилизация под сервис своего владельца. Их, как правило, никто и не скрывает.



Никита Кныш
hackcontrol.org

Типы социальных ботов

- SEO боты, лайкатели, накрутчики и репостеры.

Идентифицирующий признак: огромное количество групп (подписок) и репостов при практически полном отсутствии личных публикаций.

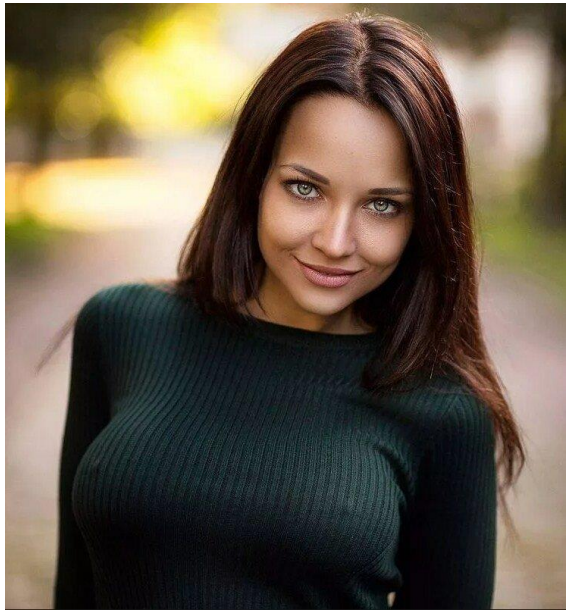


Никита Кныш
hackcontrol.org

Типы социальных ботов

- CPA боты-многодневки

Идентифицирующий признак: активная ссылка на сторонний сервис прямо в профиле или на стене пользователя с припиской "тут редко бываю, ищите меня (ссылка)".



Давай познакомимся?

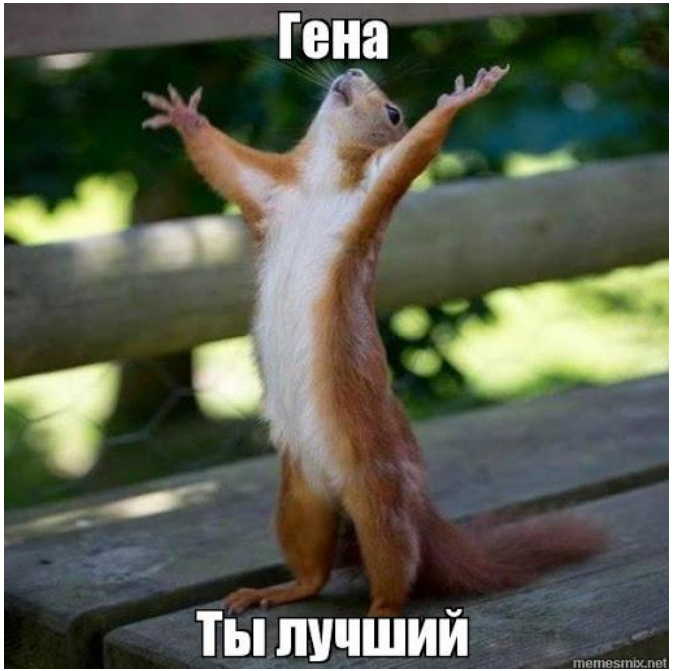
Никита Кныш
hackcontrol.org

Типы социальных ботов

- Политические социальные боты-тролли и лидеры мнений.

Идентифицирующий признак: явно не выражен, максимальное соответствие реальному аккаунту. Как правило, такие боты подключены к системам AI общения и даже могут односложно отвечать на ваши сообщения.

Из личного опыта: иногда владельцы таких ботов используют фотографии "под открытой лицензией" для "главарей" своих ботов, боясь жалоб за использование чужих фото. Иногда фото сгенерировано нейронными сетями, чтоб не воровать данные реальных людей.



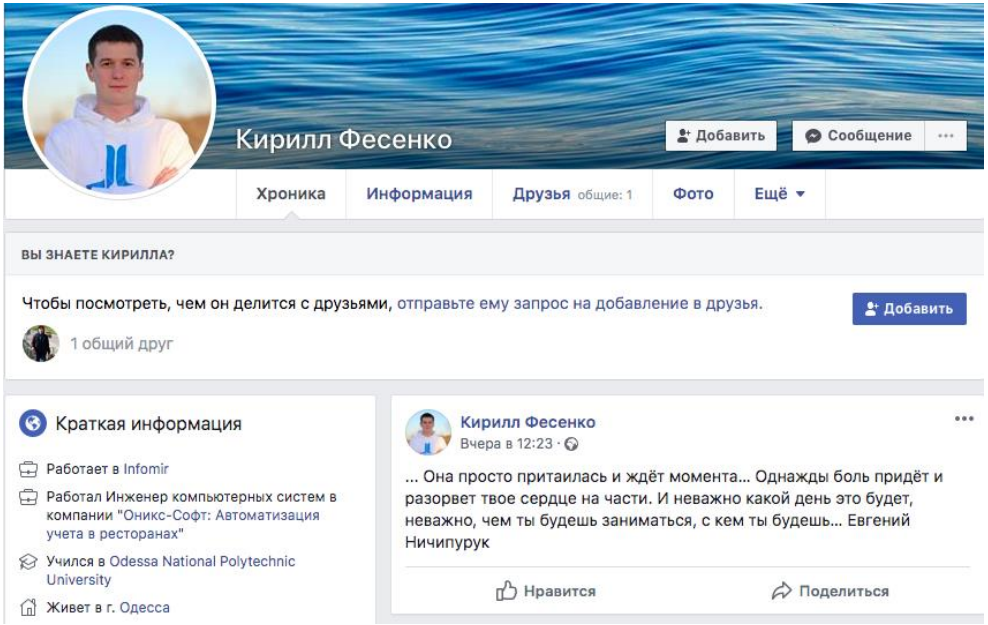
выбрано случайное имя, не ищите совпадений с реальными людьми

HackCtrl
Никита Кныш
hackcontrol.org

Определяем ботов “на глаз”

“День цитат, день пейзажей и день, когда они все провалились....

Выглядящая вполне живой, ФБ-страница парня по имени Кирилл Фесенко. Работает он якобы в украинской компании Infomir. Да вот только в фотоальбомах компании ни на одном фото его нет. В то же время с фотографиями Кирилла находится огромное количество фейковых страниц. На одной из фотографий, например, он в Петербурге, на другой – в городе Мозырь (Беларусь), на третьей – просто на корабле на фоне российского флага.



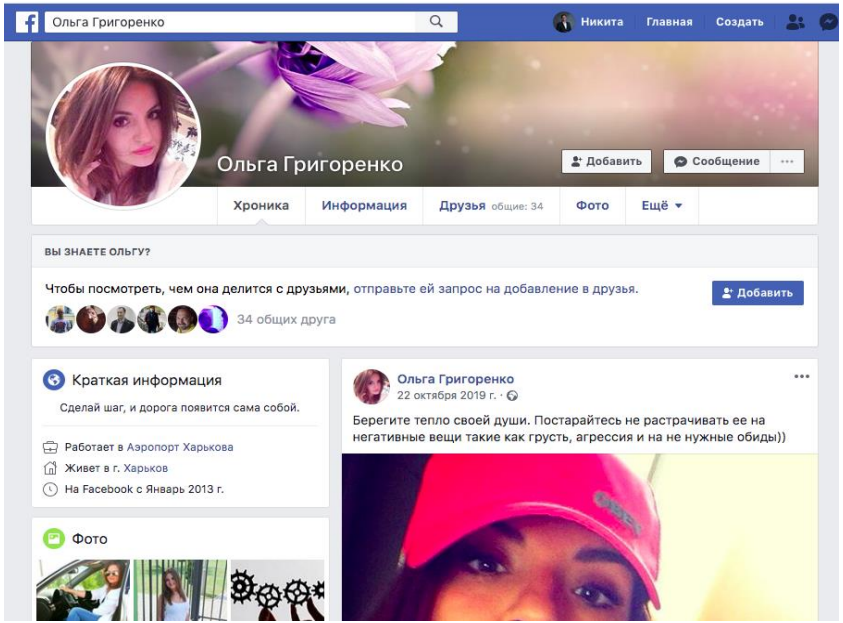
могут быть приведены примеры фото реальных людей, также, на глаз, 100% нельзя утверждать что страница - бот

Никита Кныш
hackcontrol.org

Определяем ботов “на глаз”

“День цитат, день пейзажей и день, когда они все провалились....

Второй пример – Ольга Григоренко (FB olga.grigorenko87), работающая якобы в Харьковском аэропорту. Дни цитат и пейзажей у них с вышеупомянутым Кириллом, естественно, совпадают. Еще интересно, что есть такая же страница у Оли в ВКонтакте (Ольга Григоренко из Харькова) – правда, её уже давно никто не ведет. Да только проблема в том, что оригинал – Анастасия Васильева (ВК id9696510) из города Лунинец (Беларусь)



могут быть приведены примеры фото реальных людей, также, на глаз, 100% нельзя утверждать что страница - бот

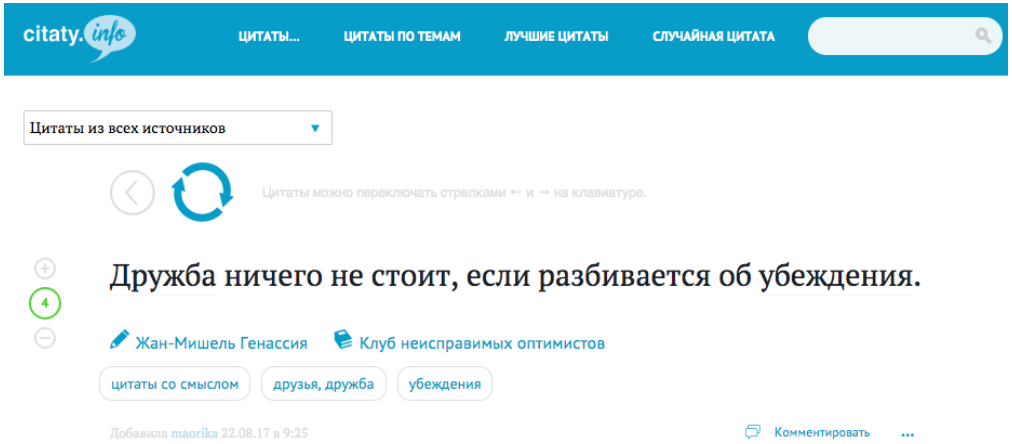
HackCtrl
Никита Кныш
hackcontrol.org

Определяем ботов “на глаз”

“День цитат, день пейзажей и день, когда они все провалились....

Откуда же все боты берут эти цитаты?

Domain Name: **CITATY.INFO**
Registry Domain ID: D15681447-LRMS
Updated Date: 2019-11-13T07:15:34Z
Creation Date: 2006-12-13T06:36:54Z
Registry Expiry Date: 2020-12-13T06:36:54Z
Registrant Country: CY
Name Server: DNS2.YANDEX.NET
Name Server: DNS1.YANDEX.NET

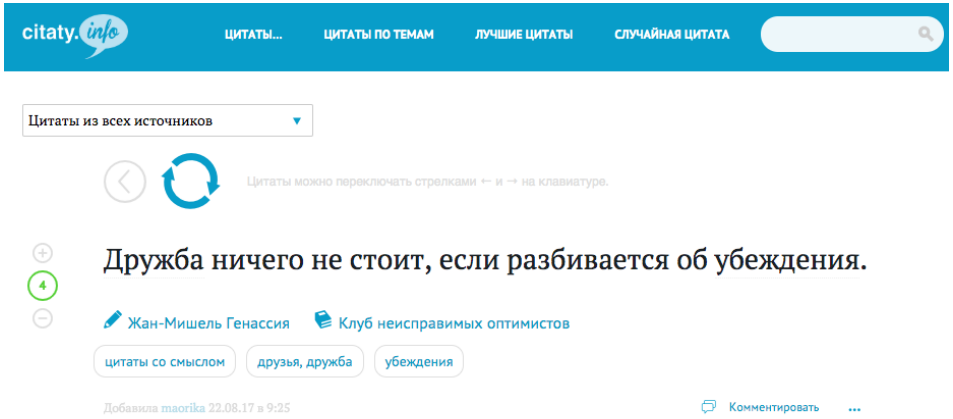


могут быть приведены примеры фото реальных людей, также, на глаз, 100% нельзя утверждать что страница - бот

HackCtrl
Никита Кныш
hackcontrol.org

Определяем ботов “на глаз”

“День цитат, день пейзажей и день, когда они все провалились....



Откуда же все боты берут эти цитаты?

www.citaty.info → 88.99.199.72

Registrant Email citaty.info@whoisprotectservice.net

Hetzner Online GmbH

Этого достаточно, чтобы связаться с владельцем и попробовать попросить у него логи запросов. Объяснив ситуацию еще и тем, что такие автоматические запросы от ботов просто повышают нагрузку на сайт, не принося никакой прибыли.

Таким образом, нам станет известен IP-адрес сервера, с которого боты парсят (добывают) цитаты. Узнав IP-адрес сервера, можно посмотреть, на кого он оформлен. И если нам повезет выйти на компанию разработчика ботов, дальше уже, как говорится, "дело техники"

HackCtrl
Никита Кныш
hackcontrol.org

Расследование не “на глаз”, а при помощи софта

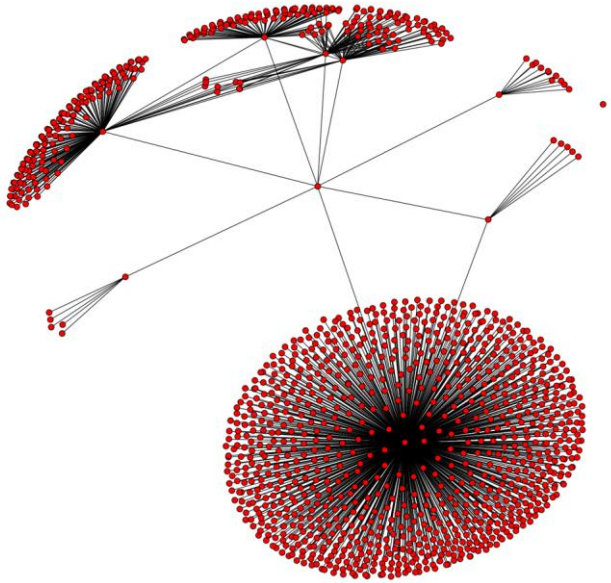


Сбор информации специализированным софтом

HackCtrl
Никита Кныш
hackcontrol.org

Графы для демонстрации связей

Расследование не “на глаз”, а при помощи софта



Анализ дружеских связей VK с помощью Python
https://habr.com/ru/post/243229/

HackCtrl
Никита Кныш
hackcontrol.org

ExifTool - анализ мета данных
Maltego - OSINT
DEFT - все в одном
CAINE (Computer Aided Investigative Environment)
nirsoft.net - любимый софт Украинских силовиков



Никита Кныш
hackcontrol.org

Существующие методы деанонимизация пользователей Telegram:

- Официальный запрос правоохранителей (на который, скорее всего, никто не ответит, если это не террористический канал, группа или пользователь)
- Социальная инженерия (забросить ссылку, трекер или выманить через другой ресурс)
- Идентификация пользователя путем полного перебора его номера
- Сетевой анализ трафика



https://tech.liga.net/technology/opinion/djoker-poka-kak-vychislit-vladeltsa-anonimnogo-telegram-kanala

HackCtrl
Никита Кныш
hackcontrol.org

Как поймать “медиа-киллеров” за *опу или поиск людей по цифровым следам

За что СБУ провело обыск в компании 1+1?

В отличии от медиа-киллеров, я вынужден сообщить, что в Украине никто не считается виновным, пока его вина не будет доказана в суде. Более того, цифровые доказательства могут быть подделаны так же как и обычные.



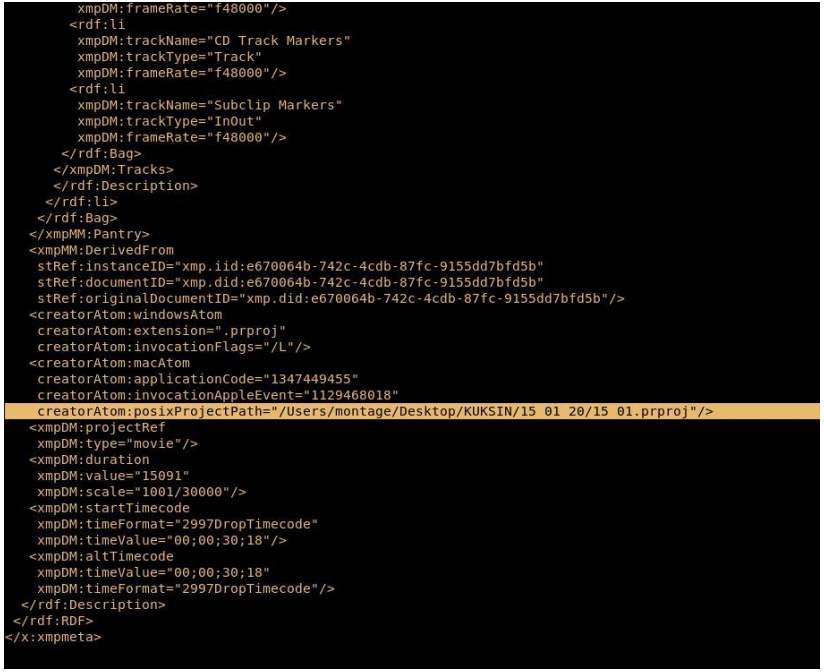
Никита Кныш
hackcontrol.org

Пленки Гончарука

Поиск людей по цифровым следам и конкурентная разведка.

/Users/montage/Descktop/Kuksin/15 01 20/15 01.prroj

В случае, если на компьютере журналиста Куксина найдут такой же файл, это будет являтся доказательством в деле о том, что **пленки Гончарука** монтировались именно на этом компьютере.





Что происходит вообще?

В зале есть юристы? Давайте подадим на кого-нибудь в суд, это же возмутительно!

снова Ждун, не мог придумать что-то поооригинальнее? Сейчас 2019, ало, гараж!

hackcontrol.org

Продукты HackControl



Smart Contract and BlockChain Audit



Company Security Audit



Secure Development and SDLC



Phishing Simulation and Social Engineering



Penetration Testing



Brand Protection and antiphishing



Что еще интересного? И где это все почитать?

Как "взламывают" Telegram с двухфакторной авторизацией:
https://www.epravda.com.ua/rus/columns/2019/03/16/646047/

Хакер не нужен. Как удалить нежелательные данные из интернета?
https://www.epravda.com.ua/rus/publications/2019/02/9/645080/

Какой мессенджер самый безопасный?
https://www.youtube.com/watch?v=58gTznSMPTk

Контакты компании:

https://t.me/hackcontrolua

HackCtrl hackcontrol.org

Мои контакты:

https://t.me/combonik

https://fb.com/knysh.nikita