ТОМСКИЙ ПОЛИТЕХ

tpu.ru

Кибербезопасность

В условиях информационных спецопераций

30.11.2022

Александр Фадеев

Проректор по цифровизации

ТОМСКИЙ ПОЛИТЕХ

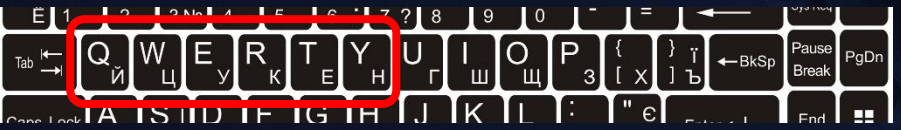
СОДЕРЖАНИЕ

Пароли

В случае подбора вашего пароля, злоумышленник от вашего имени сможет рассылать и выводить на печать экстремистские материалы, подписывать документы, получать доступ к корпоративной информации и внутренним ресурсам сети. При этом вся ответственность останется за вами!

Почему нельзя использовать простые пароли?

- Простые комбинации типа «qwerty» и «12345678», все слова из английского и русского словаря, все даты за последние 100 лет перебираются роботами-взломщиками за доли секунды



Самый надежный пароль:
Двухфакторная авторизация через СМС

Когда категорически необходимо поменять пароль?

- если ваш пароль состоит из даты (рождения), или одного слова, или последовательности на клавиатуре (типа, «qwerty»)
- если вы хоть раз сохраняли пароль на облачном сервисе (диске, заметках)
- если вы хоть раз пересылали пароль по сети (электронная почта, мессенджер, СМС)
- если вы хоть раз передавали пароль хоть кому-либо
- если вы хоть раз оставляли пароль на видном месте (на мониторе, под стеклом стола и т.д.)
- если вы использовали пароль на разных сайтах
- если вы сохраняли пароли в браузерах
- если вы вводили пароль на сенсорной клавиатуре

Облачные сервисы

Все, что размещено на облаке – вам не принадлежит

Чему угроза:

- Файлы на облачных хранилищах: DropBox, GoogleDrive, AppStore, OneDrive, …
- Электронная почта на иностранных серверах
- Переписка в мессенджерах
- Веб-приложения (общие документы, доски, сайты, заметки, …)

В чем угроза:

- Чтение, анализ, поиск по словам
  - **(в файлах, письмах, сообщениях)**
- Распространение личной информации
- Рассылка от вашего имени
- Авторизация на третьих сервисах
- Блокировка, недоступность

Что делать:

- Сделать копию всех документов на локальный компьютер, на доверенное облако, на съемный носитель.
- Удалить файлы, документы, письма с облаков
- Перейти на российские электронную почту, видеоконференцсвязь, общие документы

СЕРВИСЫ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Лицензия на программное обеспечение может стать недействительной

Производитель ПО знает всё о 100% копий своего ПО

… даже о пиратских копиях …

… и управляет ими …

В чем угроза:

Отзыв лицензий для проприетарного (коммерческого) программного обеспечения, ПО перестает работать, возможна блокировка компьютера/смартфона

Что делать:

1. Сделать копии всех важных данных на съемные носители
2. Сделать копии инсталляций программ, операционных систем, ключей
3. Временно отключить все обновления, заблокировать сайты производителей ПО
4. Перейти на отечественное ПО
5. Перейти на свободно распространяемое ПО с открытым (!) кодом
6. Сделать копию адресной книги смартфона

Сервисы и программное обеспечение

Лицензия на программное обеспечение может стать недействительной

https://habr.com/ru/news/t/655381

В чем угроза:

Отзыв лицензий для проприетарного (коммерческого) программного обеспечения, ПО перестает работать, возможна блокировка компьютера/смартфона

Что делать:

1. Сделать копии всех важных данных на съемные носители
2. Сделать копии инсталляций программ, операционных систем, ключей
3. Временно отключить все обновления, заблокировать сайты производителей ПО
4. Перейти на отечественное ПО
5. Перейти на свободно распространяемое ПО с открытым (!) кодом
6. Сделать копию адресной книги смартфона

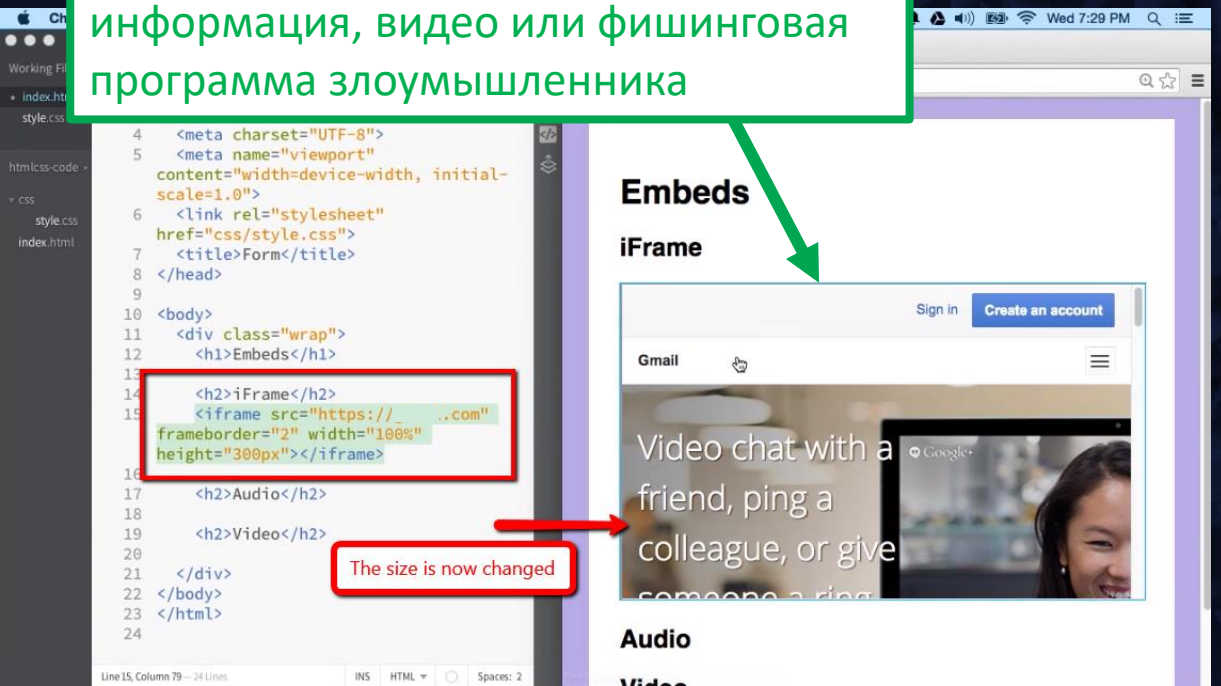
https://freeanalogs.ru

https://alternativeto.net

Сайты

«iFRAME-закладки» и скрипты чужих сайтов
HTTPS:// - защита соединения с сайтом

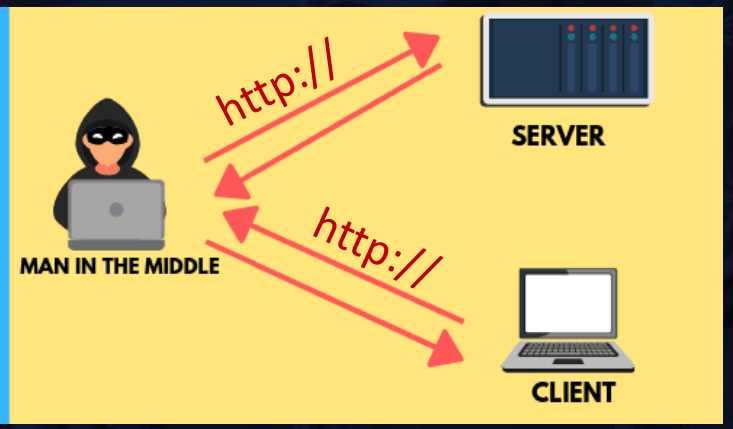
Вместо видеоплеера с сервера может быть загружена экстремистская информация, видео или фишинговая программа злоумышленника



Удалить: метрики, статистику, блоки рекламы, iFrame, Capcha, все java-скрипты сторонних систем

Без SSL злоумышленник может осуществить:

- Подмену информации
- Перехват и просмотр информации



VPN и прокси

Любой посредник – шпион

VPN и Прокси позволяют отправлять ваши запросы от имени другого компьютера в другой стране

В чем угроза:

- Все передаваемые данные через посредника – могут просматриваться, подменяться, удаляться:
  - **Пароли, переписка, данные банковских карт, просмотренная информация и т.д.**

Базовые принципы личной кибербезопасности

Будьте бдительны!

Электронная почта

- Не открывайте электронные письма от неизвестных отправителей.
- Не нажимайте на ссылки, картинки и кнопочки в электронных письмах
- Никогда не запускайте программы, присланные по электронной почте

Оплата картой

https://vash.bank.ru/...

- Платите только на сайтах проверенных банков, с реальным адресом
- Платите только картой с ограниченным балансом
- Используйте одноразовые коды для подтверждения каждого платежа
- Не сохраняйте данные банковской карты

В Интернете

Download on the App Store | Get it on Google play | Download on the Windows Store

- Устанавливайте программы только с официальных маркетов и сайтов производителей
- Не скачивайте файлы, расширения и программы, на неизвестных сайтах
- Не запускайте неизвестные программы
- Установите разработанный в России антивирус
  - Браузер, поисковик, офис…

Сеть учреждения

1. DDoS атаки: Огромное количество безобидных запросов. Парализуют ваши серверы.
    1. Отключать зоны-источники атак на время (договор с провайдером, два провайдера)
2. Поиск уязвимостей на компьютерах сети: Подключение к компьютеру, внедрение вредоносного кода, **включение компьютера в хакерские сети**
    1. Блокировка всех портов – точек подключения к компьютеру
    2. Удаление всех программ, позволяющих подключиться (Radmin, Torrent, p2p…)
    3. Удаление любых серверов с персональных компьютеров (сайты, ftp…)
    4. Удаление нелицензионных и взломанных программ
    5. Перенос компьютеров в сети с «серыми IP-адресами» 10.x.x.x, 172.16-31.x.x, 192.168.x.x
    6. **Отключить неиспользуемые службы, сервисы, устройства, пользователей. Инвентаризация. Ведение журнала инцидентов.**
3. Поиск уязвимостей на сетевом и офисном оборудовании (принтеры, роутеры)
4. Установка вредоносного ПО под предлогом «супер-антивируса»: Обычный компьютер превращается в агента сети компьютерных атак. Использовать легальный антивирус.
5. Полное отключение интернета учреждения, региона, страны
    1. Переход на отечественные DNS-системы

ТОМСКИЙ ПОЛИТЕХ

tpu.ru

Кибератаки
на веб-сайты ТПУ

Июнь, июль 2022 г.

Кибератаки на веб-сайты университетов РФ

- Начало кибератак – 20.06.2022 г. (начало приемной кампании)
- Вид атаки: отказ в обслуживании (DDoS):
  - Количество запросов к одному серверу так велико, что сервер не успевает их обрабатывать и становится недоступен
- Атакованные серверы ТПУ:
  - tpu.ru
  - abiturient.tpu.ru
  - apply.tpu.ru
- Около 500 университетов России атакуется одновременно
- Количество запросов – 35000–50000 запросов в секунду (rps)
- Журнал регистрации запросов сервера apply.tpu.ru протоколировал со скоростью 7 Гб/час

Характер кибератак

7000 атакующих компьютеров 20.06.2022 г. ➢ Блокировка по IP-адресам

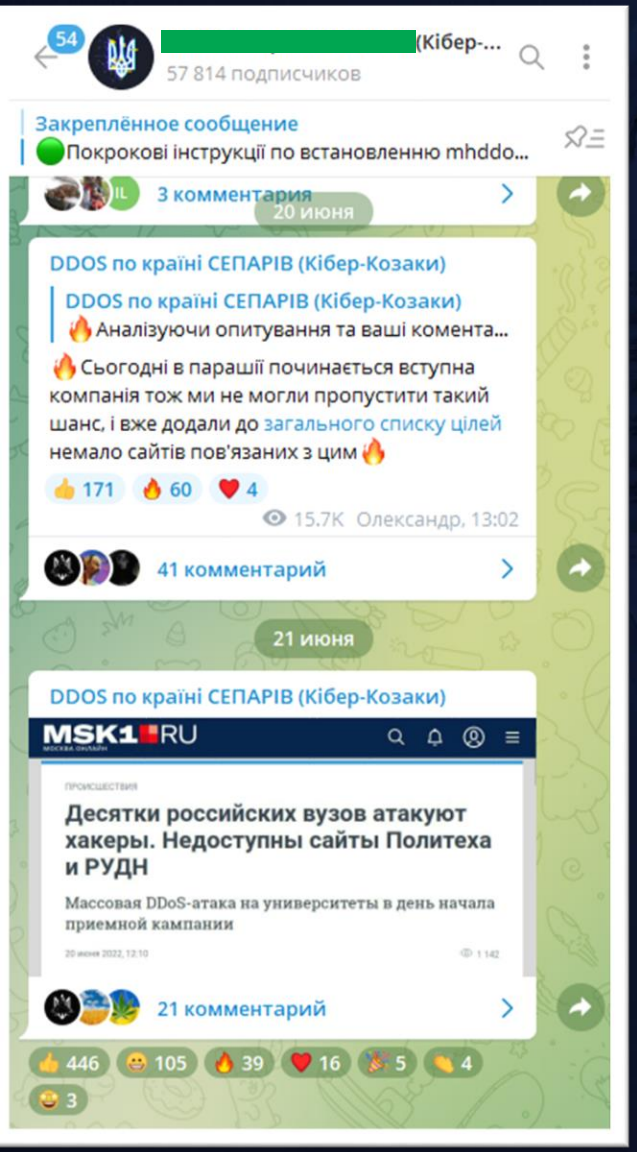
36 000 атакующих компьютеров 21.06.2022 г. ➢ Блокировка по IP-адресам не возможна

120 000 атакующих компьютеров 22.06.2022 г. ➢ Блокировка по IP-адресам не возможна

Требуются промышленные телекоммуникационные мощности

- Частая смена IP-адреса
- Использование арендованных серверов на облачных вычислительных мощностях
- Использование смартфонов и ПК в сетях с динамической IP-адресацией
- Использование прокси-серверов

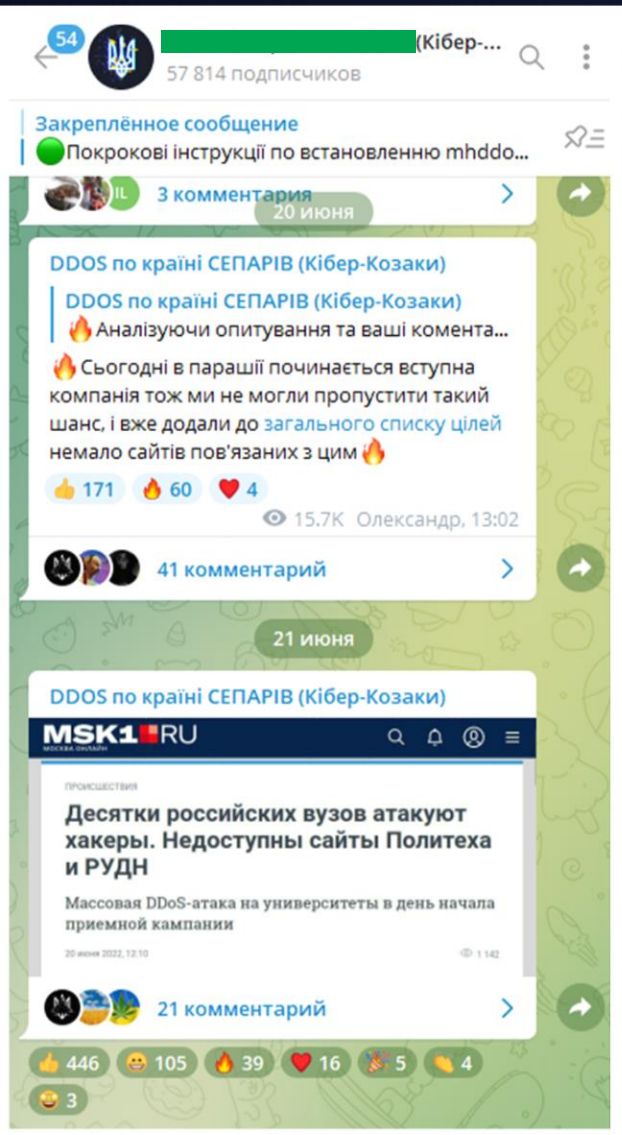
Организация кибератак

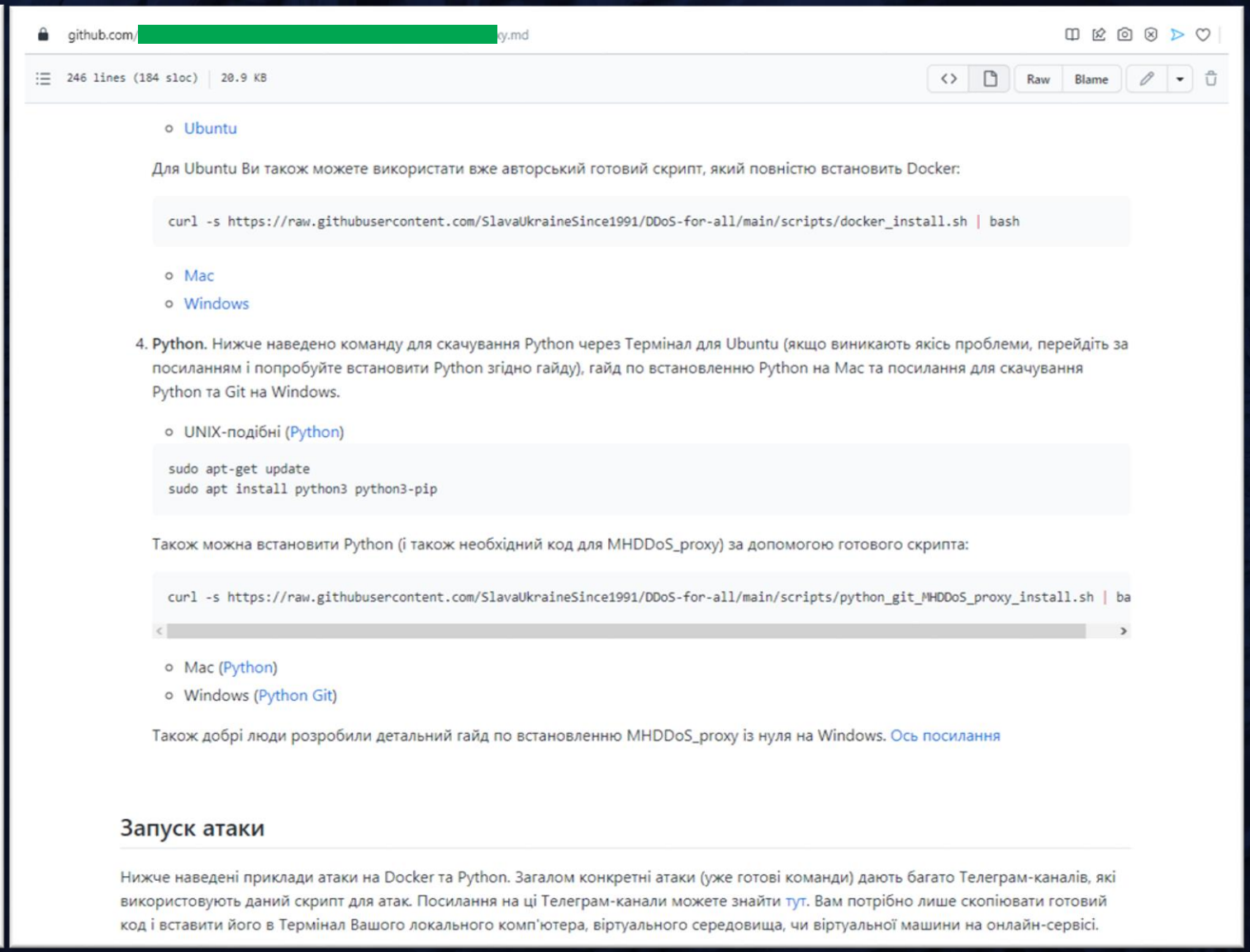


Телеграм-чат:

- призывает вступить в ряды террористической организации (кибер-армия)
- Выдает инструкции по установке и настройке программ для кибератак
- Поощряет и восхваляет террористические и экстремистские успешные деяния

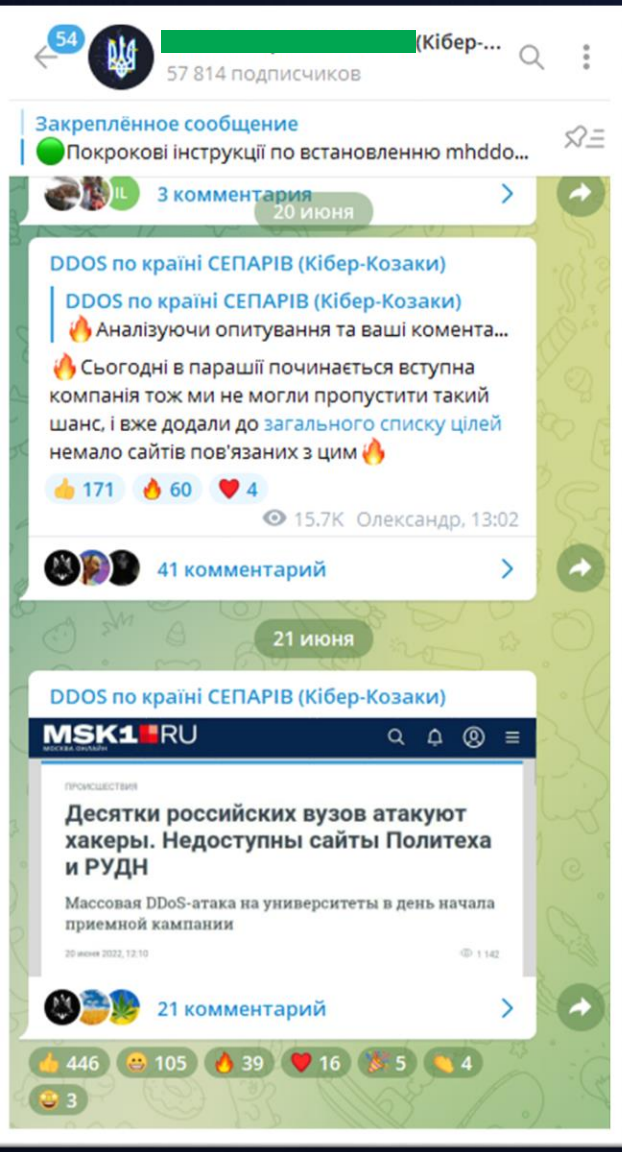
Организация кибератак

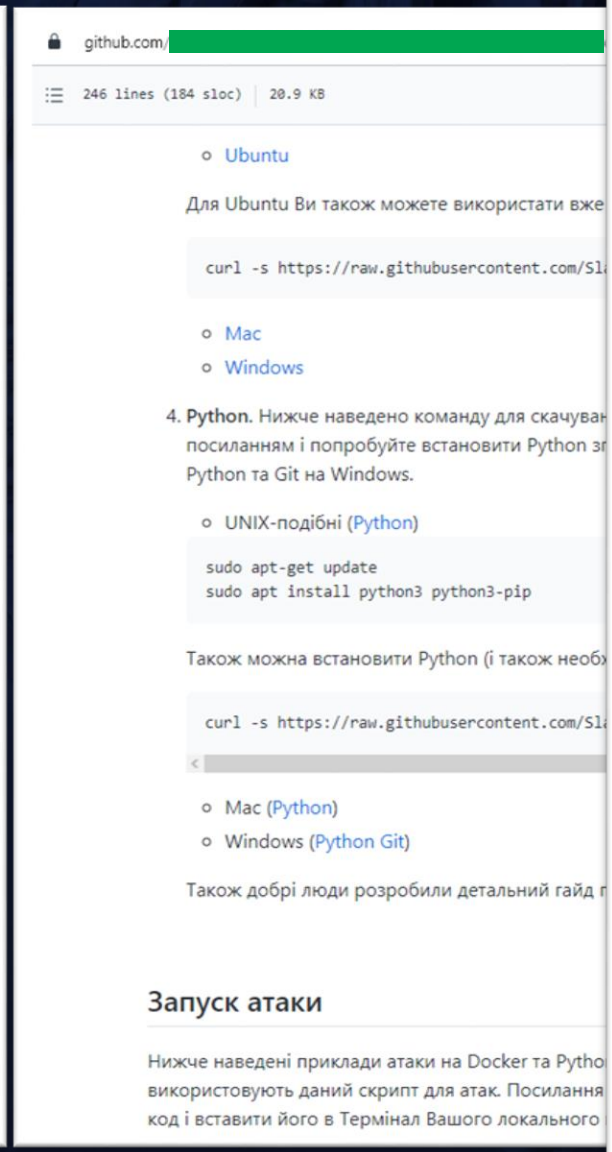


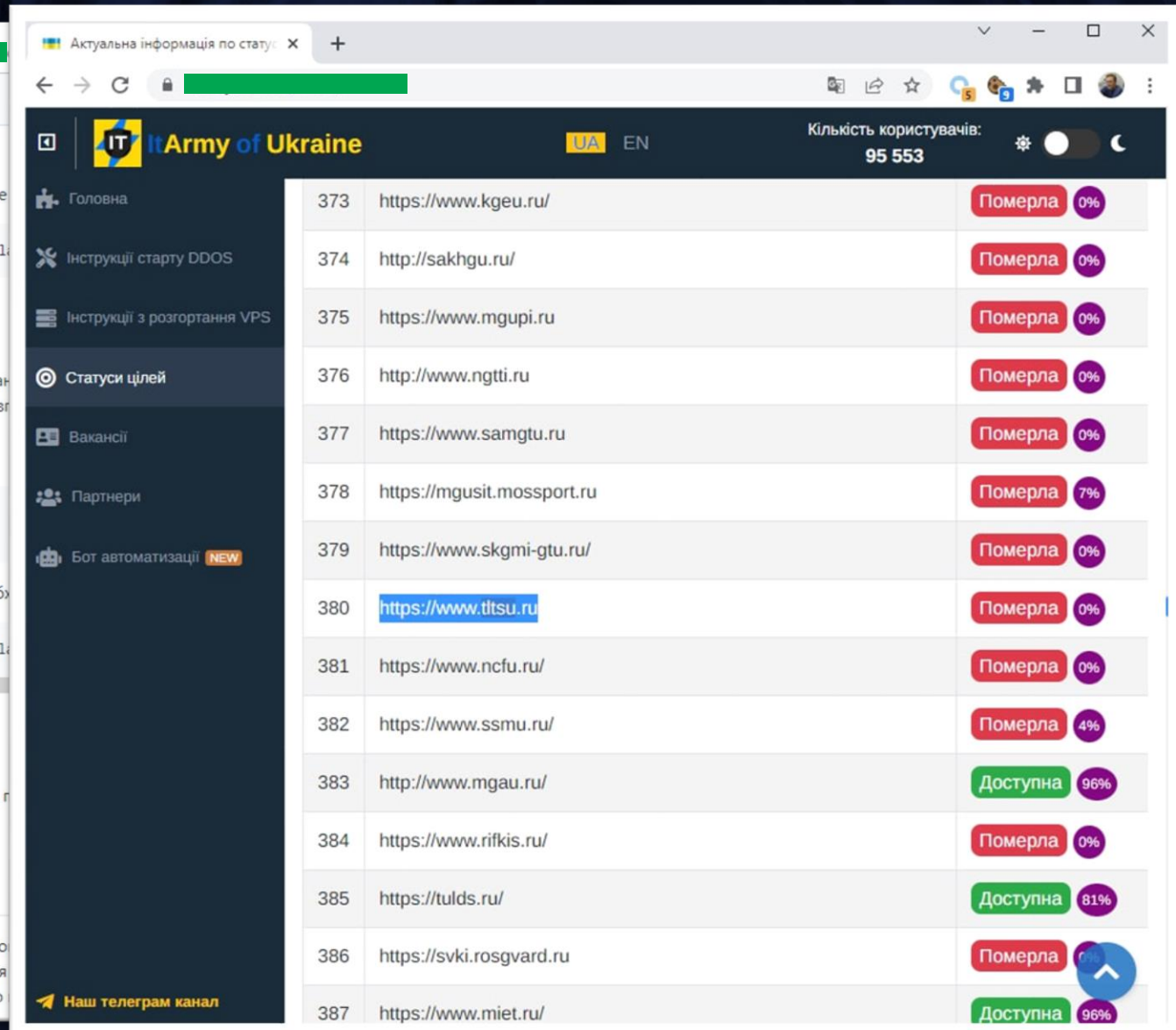


Веб-сайт с инструкциями и исходными кодами программного обеспечения, организующего кибератаки для любого типа компьютеров, серверов, смартфонов

Организация кибератак







ТОМСКИЙ ПОЛИТЕХ

Спасибо за внимание

Фадеев Александр Сергеевич

Проректор по цифровизации


Г. Томск, проспект Ленина, 30


+79234579515


fas@tpu.ru