Хактивизм, DDoS и борьба за суверенитет

SOLAR

В эпоху стремительной цифровизации бизнеса вопросы кибербезопасности выходят на первый план, особенно в свете активности хактивистов.

Артем Избаенков

Директор продукта Solar Space ГК "Солар"

Консультант ООН по информационной безопасности

Член РОЦИТ

Член правления АРСИБ

Проблема хакерских атак нового уровня

Кто такие Хактивисты?

«Ты можешь не интересоваться хактивистами, но они уже интересуются твоим сервером»

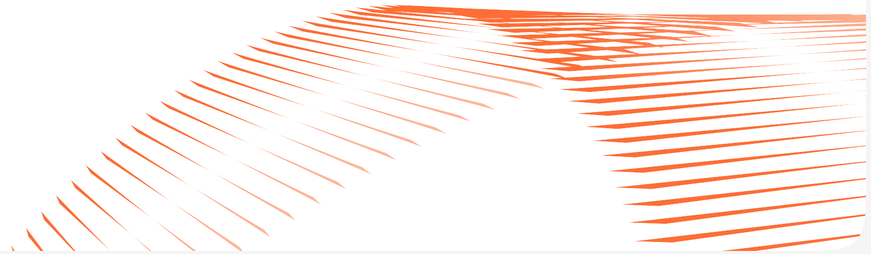
Хактивисты (от английского "hacktivists" — "hack" и "activists") — это люди или группы, использующие методы хакерского взлома для достижения политических или социально значимых целей. В отличие от традиционных хакеров, которые могут быть мотивированы материальной выгодой, хактивисты преследуют идеологические цели, стремясь привлечь внимание к различным вопросам, вызвать изменения или протестовать против тех или иных действий правительств, корпораций или других организаций.

Как атакуют?

Действуя в рамках своих политических или социально значимых взглядов, хактивисты могут выполняют кибератаки, такие как атаки типа DDoS (распределенные атаки отказа в обслуживании), взломы веб-сайтов, утечки данных и другие формы цифрового саботажа.

Активизация Хактивистов

Одна из самых известных новых группировок хактивистов на текущий момент — это ИТ Армия Украины. Эта группа, сформировавшаяся в условиях текущего политической ситуации СВО, занимается различными киберактивностями противоправительственных структур и компаний, поддерживающих противоположные взгляды. Их действия включают кибератаки на сервисы, направленные на дестабилизацию и привлечение международного внимания к событиям и проблемам, с которыми сталкивается Россия.



Основные угрозы Хактивистов

«Остаться онлайн — это уже не про аптайм, это про выживание»

1 . DDoS-атаки (Distributed Denial of Service):

- Цель этих атак — перегрузка серверов и сетей большим количеством запросов, что приводит к недоступности услуг для легитимных пользователей.
- DDoS-атака может сильно повлиять на репутацию МФО и привести к финансовым потерям из-за простоя систем и услуг.

2 . Автоматизированные атаки ботами:

- Credential Stuffing: Злоумышленники используют автоматизированные инструменты (боты) для массового подбора паролей с использованием украденных учётных данных.
- Скрэйпинг данных: Боты могут собирать конфиденциальные данные или контактные данные клиентов с веб-ресурсов МФО.
- Автоматические заявки на кредиты: Боты могут подавать массовые заявки на кредиты с мошенническими целями, перегружая систему обработки заявок и создавая дополнительные риски.

3 . Атаки на структуру веб-приложения:

- Внедрение вредоносного кода через пользовательский ввод для получения несанкционированного.
- Внедрение вредоносных скриптов на веб-страницы, которые могут украсть данные пользователя или выполнить нежелательные действия от его имени.

Основные угрозы Хактивистов

4. Фишинг, Спам и Малварь через электронную почту:

- Распространение поддельных электронных писем с целью кражи учётных данных или других конфиденциальных данных.
- Распространение вредоносного ПО через вложения в электронных письмах или ссылки на вредоносные сайты.
- Нежелательные письма, которые могут содержать рекламные материалы, фишинговые ссылки или вредоносное ПО.

5. Социальная инженерия:

- Манипулирование сотрудниками организации
  для получения доступа к конфиденциальной информации.

6. Неизвестные или неуправляемые активы:

- Системы и сервисы, которые могут быть незарегистрированными
  или неправильно сконфигурированными и, следовательно, уязвимыми для атак.
- Использование несанкционированных программного обеспечения и сервисов,
  которые остаются вне контроля службы безопасности организации.

7. Уязвимости в третьих сторонах:

- Поставщики и партнеры, чьи системы
  могут быть скомпрометированы и
  использованы для атак на МФО.

Блокировки и конец привычного интернета?

Что делать без Cloudflare, Let’s Encrypt, Google?

- Мы привыкли к глобальным и простым сервисам как к «базовой инфраструктуре» интернета.

Риски:

  - Cloudflare → прекращение защиты сайтов от DDoS.
  - Let’s Encrypt → невозможность бесплатно выпускать SSL-сертификаты.
  - Google Services → падение аналитики, рекламы, API и карт.
- Потеря доступа = массовая нестабильность работы компаний.
- Опасность для бизнеса: зависимость от внешних решений, которые могут быть отключены в любой момент.

Суверенный интернет и локальная инфраструктура

Суверенитет: вызовы и необходимость

- Суверенный интернет ≠ изоляция, а устойчивость и независимость.

Основные элементы:

- Национальная система сертификации и шифрования.
- Локальные CDN и анти-DDoS.
- Отечественные DNS и системы маршрутизации.

Компании должны:

- Дублировать критичные сервисы внутри страны.
- Инвестировать в собственные периметры безопасности.
- Планировать отказоустойчивость «без глобальных игроков».

Новый подход к защите: от Enterprise к SMB

Доступная защита для всех

- Традиционно киберзащита → для крупных корпораций.
- Но SMB (малый и средний бизнес) = наиболее уязвимая часть рынка.
- Принципы новой модели:
  - Free-тарифы: базовая защита доступна каждому.
  - Прозрачные условия: никаких скрытых платежей и сложных договоров.
  - Локальная поддержка: эксперты, говорящие на языке клиента.
  - Соответствие нормам РФ: встраивание в национальное регулирование.
- Solar Space делает защиту «массовым сервисом», а не элитарным продуктом.

Так что же делать ???

Призыв к объединению усилий

Единая платформа для защиты суверенитета

- Киберзащита невозможна в одиночку:
  - Разработчики → создают технологии.
  - Интеграторы → внедряют их в компании.
  - Государство → задаёт правила игры и обеспечивает поддержку.
  - Экспертное сообщество → формирует культуру безопасности.
- Необходима единая платформа, которая станет ядром:
  - Объединение анти-DDoS, WAF, DNSSEC, сертификации.
  - Локальная альтернатива Cloudflare и другим глобальным сервисам.
  - Сервисы, доступные как крупным корпорациям, так и SMB.
- Solar Space позиционирует себя как фундамент для такой экосистемы.

SOLAR

“Многие говорят, что Мир изменить нельзя, а мы с командой SolarSpace его меняем”

Артем Избаенков

Директор продукта Solar Space ГК “Солар”

Консультант ООН по информационной безопасности

Член правления АРСИБ

Член РОЦИТ