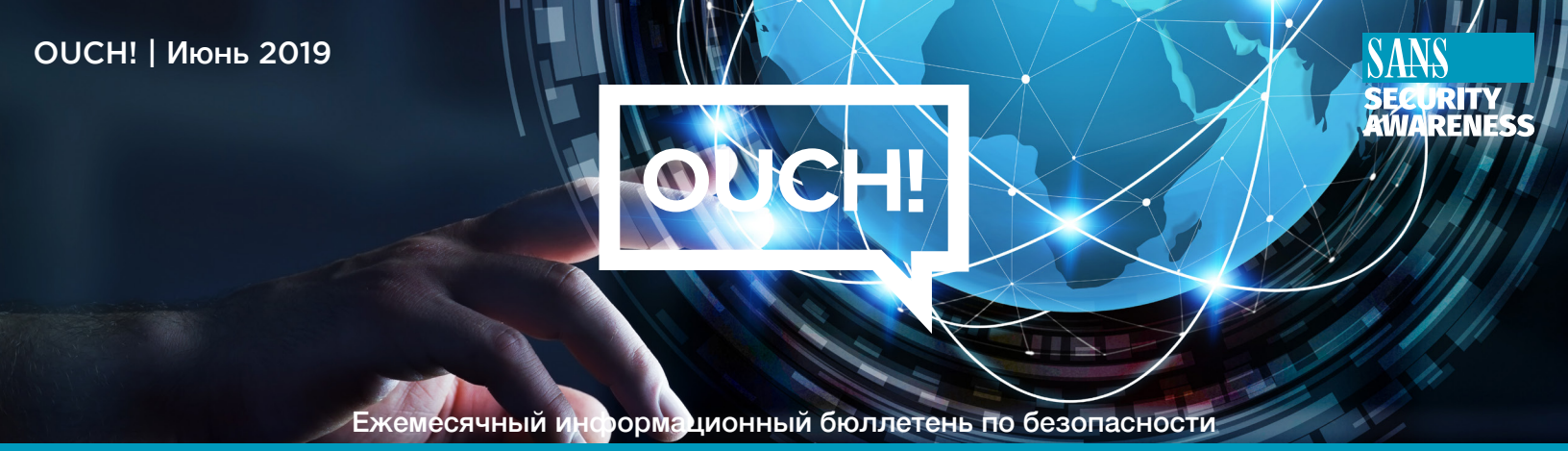

Ежемесячный информационный бюллетень по безопасности

Темная паутина «Dark Web»

Обзор

Возможно, вы слышали термин «Dark Web» Темная паутина, используемый людьми или в средствах массовой информации, и задавались вопросом «что такое Темная паутина?» или «что делать с этим?». Сегодня мы объясняем, что такое Темная паутина.

Что это?

Темная паутина состоит из систем в Интернете, предназначенных для безопасного и анонимного обмена информацией. Темная паутина - это не что-то вроде Facebook, где его управляет одна организация. Вместо этого Темная паутина - это разновидность различных систем и сетей, управляемых разными людьми, которые используются для самых разных целей. Эти системы по-прежнему подключены к Интернету и являются их частью, однако, как правило, вы не найдете их с помощью обычных поисковых систем. Вам также потребуется специальное программное обеспечение на вашем компьютере, чтобы найти или получить к ним доступ. Одним из примеров является проект Tor. Чтобы получить доступ к Темной паутине, скачайте и установите Tor Browser. Когда вы подключаетесь к веб-серверам с помощью браузера Tor, ваш зашифрованный трафик проходит через другие компьютеры, также использующие Tor. При переходе через эти компьютеры IP-адрес источника меняется, и это означает, что когда вы заходите на веб-сайт, ваша онлайн-активность анонимна. Другие примеры Темной паутины включают Zeronet, Freenet и I2P.

Кто это использует?

Киберпреступники - большие пользователи Темной паутины. Они используют веб-сайты и форумы в Темной паутине, чтобы разрешить их преступную деятельность, такую как покупка наркотиков или продажа гигабайтов - все анонимно и безопасно. Например, когда киберпреступник взламывает банк или интернет-магазин, они крадут столько информации, сколько могут, а затем продают эту информацию другим киберпреступникам на сайтах в Темной паутине.

Есть также законное использование Темной паутины. Например, люди в странах, где распространена цензура, могут использовать сети Темной паутины для обмена информацией и просмотра того, что еще происходит в мире, при этом защищая свою конфиденциальность и оставаясь анонимными. Журналисты, информаторы и люди, предпочитающие конфиденциальность, могут использовать Темную паутину для повышения своей анонимности и обхода цензуры.

Кроме того, такие люди могут использовать такие технологии, как Tor Browser, не только для доступа к Темной паутине, но и для анонимного просмотра обычного Интернета.

Итак, что нужно делать?

Если у вас нет особых причин для доступа к Темной паутине, мы предостерегаем вас от этого. Некоторые сайты Темной паутине используются в незаконных целях, многие сайты будут использовать ваш компьютер в одноранговой сети для достижения своих целей, а в некоторых случаях ваш компьютер может даже быть зондирован или атакован. Некоторые компании предлагают услуги по мониторингу, чтобы сообщить вам, если ваше имя или другая информация была украдена киберпреступниками и найдена в Темной паутине. Фактическая стоимость этих услуг сомнительна. Лучший способ защитить себя - предположить, что часть вашей информации уже находится в Темной паутине, которую используют киберпреступники. В следствии . . .

⚠

- **С подозрением относитесь к любым телефонным звонкам или электронным письмам, притворяющимися официальными организациями и вынуждающими вас принять меры, например оплатить штраф. Преступники могут даже использовать информацию, которую они нашли о вас, для создания персонализированной атаки.**
- **Контролируйте свою кредитную карту и банковские выписки. Возможно, даже настроить ежедневные оповещения о любых транзакциях, которые происходят. Таким образом, вы можете определить, происходит ли какое-либо финансовое мошенничество. Если вы обнаружите что-либо подозрительное, немедленно сообщите об этом в свою компанию-эмитент кредитной карты или в банк.**
- **Заморозить свой кредитный отчет. Это не влияет на то, как вы можете использовать свою кредитную карту, и является одним из наиболее эффективных шагов, которые вы можете предпринять, чтобы защитить себя от кражи личных данных.**

Приглашенный

Мика Хоффман *(@WebBreacher) является главным исследователем в Spotlight Infosec LLC, сертифицированным инструктором SANS Institute и автором курсов SANS OSINT. Мика увлечен кибер-аналитикой и открытым исходным кодом в своих проектах, учебных курсах и стиле преподавания.*

Ресурсы

Персональные атаки:	https://www.sans.org/u/RfW
Социальный инжиниринг:	https://www.sans.org/u/Rg1
Кража личных данных:	https://www.identitytheft.gov
Заморозить кредитный отчет:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Tor Browser:	https://www.torproject.org/
SANS OSINT Course:	https://sans.org/sec487

Редакция журнала: Уолт Скривенс, Фил Хоффман, Алан Ваггонер, Шерил Конлиie