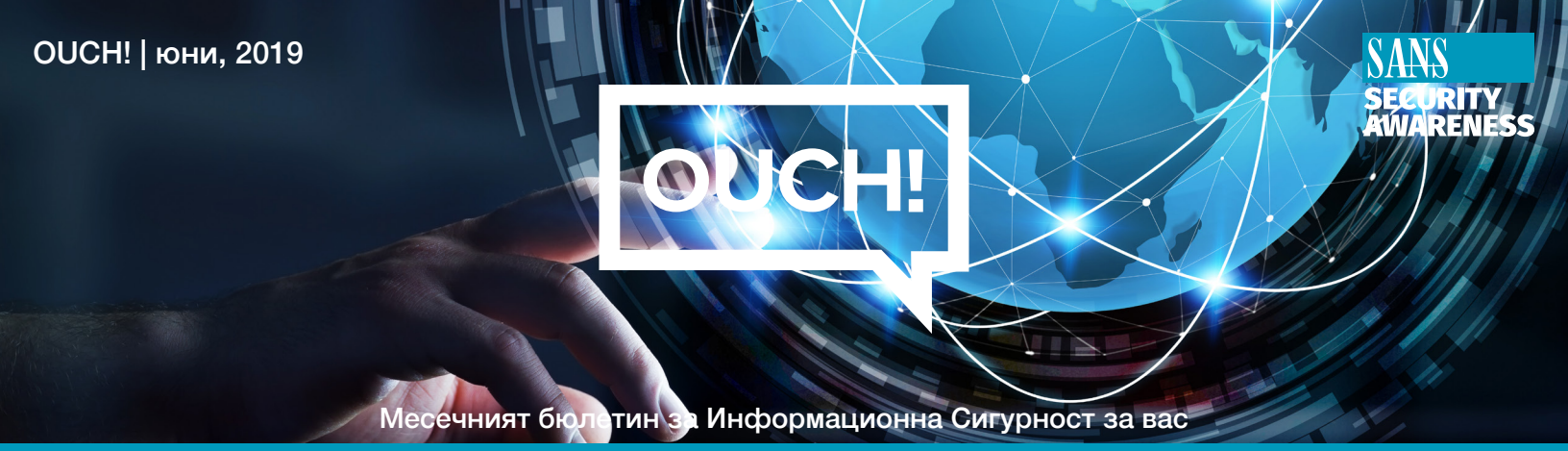
OUCH! | юни, 2019



Месечният бюлетин за Информационна Сигурност за вас

Dark Web

Преглед

Може би сте чували термина „dark web" („дарк уеб", в превод от английски „тъмна мрежа"), използван от други хора или в медиите, и сте се се питали „*Какво е dark web?*" или „*Трябва ли да правя нещо за него?*". Днес ние ще ви обясним какво е „dark web" и какво означава за вас.

Какво е това?

„Dark Web" се състои от системи в Интернет, предназначени за комуникация или споделяне на информация сигурно и анонимно. Няма един „Dark Web"; това не е нещо като Facebook, което се управлява от една организация. Вместо това „Dark Web" е колекция от различни системи и мрежи, управлявани от различни хора, използвани за различни цели. Тези системи са свързани с интернет и са част от интернет, но като цяло не ги намирате с нормалните си търсачки. Често се нуждаете от специален софтуер на компютъра си, за да ги намерите или получите достъп. Пример за това е проектът Tor. За да получите достъп до този „Dark Web", изтегляте и инсталирате браузъра Tor. Когато се свързвате към уеб сървъри с помощта на браузъра Tor, вашият криптиран трафик преминава през други компютри, които също използват Tor. Тъй като прескача през тези компютри, IP адресът на източника се променя, което означава, че когато стигнете до уеб сайта, вашата онлайн дейност е анонимна. Други примери за „Dark Web" са Zeronet, Freenet и I2P.

Кой го използва?

Кибер престъпниците са големи потребители на „Dark Web". Те поддържат уебсайтове и форуми в „Dark Web", за да извършват своите престъпни дейности, като закупуване на наркотици или продажба на гигабайтове хакнати данни - всичко анонимно и сигурно. Например, когато кибер престъпникът хакне банка или магазин за онлайн пазаруване, те откраднат толкова информация, колкото могат, след което продават тази информация на други кибер престъпници на сайтове в „Dark Web".

Има и законни употреби на „Dark Web". Например, хората в страни, където цензурата е широко разпространена, могат да използват „Dark Web" мрежи, за да споделят информация и да видят какво друго се случва в света, като същевременно предпазват своята неприкосновеност и остават анонимни. Журналистите, лицата, подаващи сигнали за нередности, и хората, имащи отношение към неприкосновеността на личния живот, могат да използват „Dark Web", за да засилят анонимността си и да заобикалят цензурата. Освен това такива хора могат да използват технологии като браузъра Tor не само за достъп до „Dark Web", но и за анонимно сърфиране в обикновения интернет.

Какво трябва да направя?

Освен ако нямате конкретна причина за достъп до „Dark Web", ние ви предупреждаваме да внимавате с него. Някои сайтове в „Dark Web" се използват за незаконни цели, много от сайтовете ще използват компютъра ви в партньорска мрежа, за да постигнат целите си, а в някои случаи компютърът ви може дори да бъде прегледан или атакуван. Някои компании предлагат услуги за наблюдение, за да ви уведомят дали вашето име или друга информация са били откраднати от кибер престъпници и намерени в „Dark Web". Действителната стойност на тези услуги е под въпрос. Най-добрият начин да се защитите е да приемете, че част от информацията ви вече е в „Dark Web", който се използва от кибер престъпниците. В резултат на това...

- **Бъдете подозрителни към всички телефонни обаждания или имейли, които се преструват, че са официални организации, и ви принуждават да предприемете действие, като например заплащане на глоба. Престъпниците дори могат да използват информацията, която са намерили за вас, за да създадат персонализирана атака.**
- **Наблюдавайте кредитната си карта и банковите си извлечения. Може би създайте и ежедневни предупреждения за всякакви транзакции, които се извършват. По този начин можете да засечете дали не се случва някаква финансова измама. Ако откриете такава, незабавно уведомете компанията от която е кредитната ви карта или банката.**
- **Поставете замразяване на кредитния си рейтинг. То не влияе върху това как можете да използвате кредитната си карта и е една от най-ефективните стъпки, които можете да предприемете, за да се предпазите от кражба на самоличност.**

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Гост-редактор

Мика Хофман *(@WebBreacher) е главният изследовател в Spotlight Infosec LLC, също сертифициран инструктор на институт SANS и автор на курсовете SANS OSINT. Страстта на Мика към кибер и отворено разузнаване си личат в неговите проекти, курсове и стил на преподаване.*

Ресурси

Персонализирани атаки:	https://www.sans.org/u/RfW
Социално инженерство:	https://www.sans.org/u/Rg1
Кражба на самоличност:	https://www.identitytheft.gov
Замразяване на кредитирането:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Браузърът Tor:	https://www.torproject.org/
Курсът SANS OSINT:	https://sans.org/sec487

 Редакторски колектив: Уолт Scrivens, Фил Хофман, Алън Уагонър, Черил Конли | Превод: Николай Дачев и Радослава Несторова