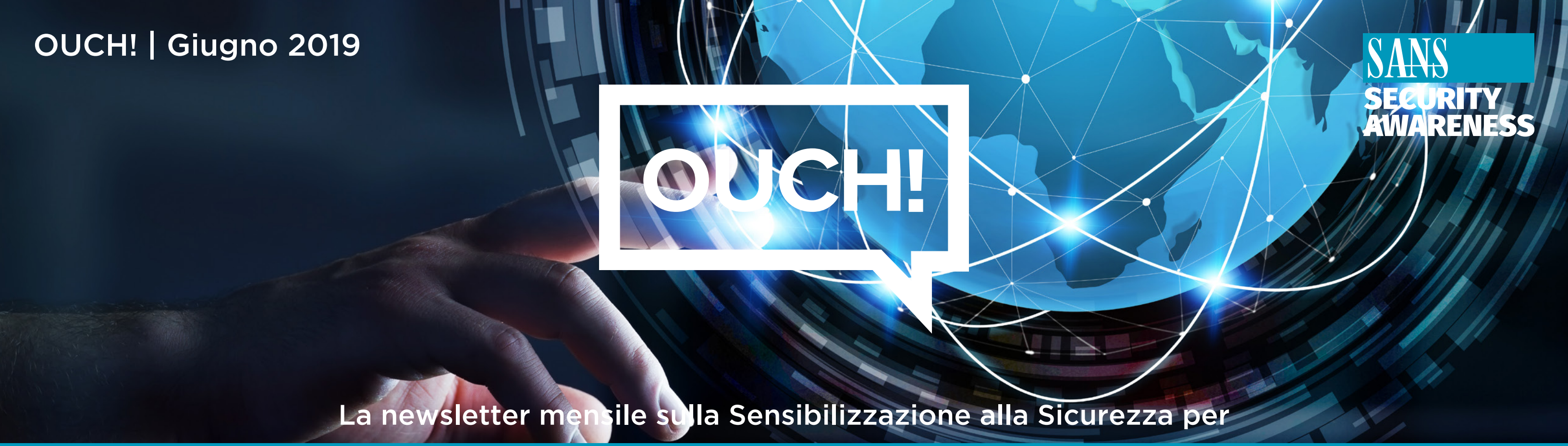


Dark Web

In sintesi

Ti sarà capitato di sentire il termine "Dark Web" da altre persone o nei notiziari e ti sarai chiesto cosa significhi o se sia necessario fare qualcosa in proposito. Oggi ti spieghiamo cosa è il Dark Web e in che modo ti riguarda.

Di cosa si tratta?

Il Dark Web è costituito da sistemi in Internet pensati per comunicare o condividere informazioni in maniera sicura ed anonima. Non esiste un singolo "Dark Web"; non è qualcosa come Facebook che viene gestito da una sola organizzazione. Invece il Dark Web è un insieme di diversi sistemi e reti gestiti da molte persone per una varietà di scopi. Questi sistemi sono connessi ad Internet e ne fanno parte, ma in generale non è possibile trovarli attraverso i normali motori di ricerca. Spesso avrai bisogno di applicazioni specifiche sul tuo computer per trovarli o accedervi. Un esempio è il progetto Tor. Per accedere a questa parte del Dark Web, devi scaricare ed installare il browser Tor. Quando ti connetti a dei server web usando il browser Tor, il tuo traffico criptato viaggia attraverso altri computer che usano Tor. Ad ogni passaggio tra questi computer, l'indirizzo IP di origine viene cambiato. In questo modo non sarà possibile tracciare la tua attività online. Altri esempi di Dark Web includono Zeronet, Freenet e I2P.

Chi lo usa?

I criminali informatici sono tra i principali utenti del Dark Web. Essi gestiscono siti e forum nel Dark web per facilitare le loro attività illegali, ad esempio l'acquisto di droga o la vendita di gigabyte di dati rubati. Il tutto in maniera sicura ed anonima. Ad esempio, quando un criminale informatico riesce a violare il sito di una banca o negozio online, ruberà quante più informazioni possibile per poi venderle ad altri criminali attraverso siti nel Dark Web.

Ci sono anche usi legittimi del Dark Web. Ad esempio, le persone che si trovano in paesi dove esiste una forte censura possono utilizzare il Dark Web per condividere informazioni e sapere cosa succede nel mondo, rimanendo anonimi e proteggendo la propria privacy. Giornalisti, informatori e persone attente alla privacy possono usare il Dark Web per aggirare la censura e rimanere anonimi. Inoltre è possibile usare tecnologie come quella del browser Tor non solo per accedere al Dark Web, ma anche per navigare in modo anonimo sui normali siti di Internet.

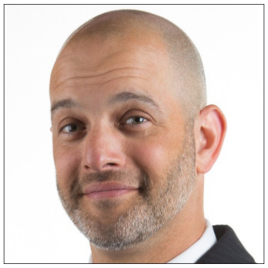
Cosa dovrei fare?

Se non hai una ragione precisa per accedere al Dark Web, ti consigliamo di non farlo. Alcuni siti del Dark Web vengono usati per scopi illegali. Molti di questi siti useranno il tuo computer come parte di una rete peer per raggiungere i loro scopi, e in alcuni casi il tuo computer potrebbe anche essere analizzato o attaccato. Alcune società offrono servizi di monitoraggio per farti sapere se il tuo nome o altre informazioni sono state rubate da criminali informatici e trovate nel Dark Web. Il valore effettivo di questi servizi è discutibile. Il miglior modo per proteggerti è quello di presumere che alcuni dei tuoi dati personali si trovino già nel Dark Web e che vengano usati dai criminali informatici. Di conseguenza . . .

- **Sospetta sempre di ogni chiamata telefonica o email dove qualcuno pretende di essere un'organizzazione ufficiale e ti sollecita a fare qualcosa, come pagare una multa. I criminali potrebbero anche utilizzare le informazioni che hanno trovato su di te per creare un attacco personalizzato.**
- **Controlla i resoconti della tua carta di credito e della banca. Potresti anche impostare avvisi giornalieri per ogni transazione effettuata. In questo modo puoi verificare se sei vittima di qualche frode finanziaria. Se noti qualcosa di strano, segnalalo immediatamente alla tua banca o istituto di credito.**
- **In caso di attività sospette blocca la tua carta di credito. Così eviterai che eventuali operazioni non autorizzate possano danneggiare il tuo merito creditizio.**

Guest Editor

Micah Hoffman *(@WebBreacher) è Investigatore Capo alla Spotlight Infosec LLC, un Istruttore Certificato al SANS Institute ed autore per i corsi SANS OSINT. La passione di Micah per l'informatica e per l'intelligenza open source si manifesta nei suoi progetti, nei corsi e nel suo stile d'insegnamento.*



Risorse

Attacchi personalizzati:	https://www.sans.org/u/RfW
Ingegneria sociale:	https://www.sans.org/u/Rg1
Furto d'identità:	https://www.identitytheft.gov
Merito creditizio:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Tor Browser:	https://www.torproject.org/
Corso SANS OSINT:	https://sans.org/sec487