Biuletyn Bezpieczeństwa Komputerowego

Dark Web

Wstęp

Być może słyszałeś określenie „Dark Web" używane w mediach lub rozmowach i zastanawiałeś się czym ten „Dark Web" jest? W tym wydaniu biuletynu, pokrótce spróbujemy przybliżyć Ci definicję Dark Web i wyjaśnimy czym on jest.

Co to jest?

Sieć Dark Web to szereg internetowych usług przeznaczonych do bezpiecznej i anonimowej komunikacji lub udostępniania informacji. Nie ma czegoś takiego jak pojedynczy Dark Web, tzn. nie prowadzi go jedna organizacja tak jak w przypadku np. serwisu Facebook. Dark Web jest zbiorem systemów i sieci zarządzanych przez różne osoby i wykorzystywanych do najrozmaitszych celów. Systemy te są połączone z internetem i są jego częścią, jednak na ogół nie można ich znaleźć przy użyciu zwykłych wyszukiwarek internetowych. Zazwyczaj aby uzyskać do nich dostęp potrzebne będzie specjalne oprogramowanie. Jednym z takich przykładów jest Projekt Tor. Aby uzyskać dostęp do stron Dark Web, należy pobrać i zainstalować przeglądarkę internetową Tor Browser. Kiedy łączysz się z serwerami internetowymi przy pomocy Tor Browser, cały generowany przez Ciebie ruch przechodzi po zaszyfrowaniu przez inne komputery, które również korzystają z sieci Tor. Każde przejście pomiędzy komputerami zmienia adres IP komputera, z którego przychodzi połączenie, a tym samym wejście na dowolną stronę internetową jest anonimowe. Innymi przykładami programów służących do łączenia się z siecią Dark Web są Zeronet, Freenet lub I2P.

Kto tego używa?

Największymi użytkownikami sieci Dark Web są cyberprzestępcy. Wykorzystują anonimowość Dark Web do prowadzenia stron i forów umożliwiających prowadzenie działalności przestępczej takiej jak handel narkotykami czy sprzedaż baz danych pochodzących z włamań. Na przykład, cyberprzestępca wkradając się do banku lub sklepu internetowego, może pozyskać informacje o klientach, które następnie sprzeda innym cyberprzestępcom za pośrednictwem forum w Dark Web.

Dark Web nie jest wykorzystywany jedynie w celach przestępczych. Ludzie w krajach, w których panuje cenzura, mogą korzystać z sieci Dark Web aby omijać cenzurę i pozyskiwać informację o zewnętrznym świecie, jednocześnie chroniąc swoją prywatność i zachowując anonimowość. Dziennikarze, sygnaliści oraz osoby chcące zachować swoją prywatność mogą korzystać z sieci Dark Web w celu ukrycia się przed ewentualną cenzurą. Ponadto przeglądarka Tor Browser nie służy jedynie do przeglądania stron sieci Dark Web, można jej użyć przy przeglądaniu zwykłych stron internetowych z zachowaniem anonimowości.

Co powinienem zrobić?

Jeśli nie masz konkretnego powodu, aby korzystać z Dark Web, nie rób tego. Wiele stron jest wykorzystywanych do nielegalnych celów, a Tor działa jak sieć peer-to-peer. Przez Twój komputer może być więc przesyłany ruch związany z nielegalną działalnością. Istnieją firmy komercyjne, które oferują usługi monitorowania, oraz informowania, czy Twoje dane osobowe zostały skradzione przez cyberprzestępców i opublikowane w Dark Web. Najlepiej jednak przyjąć, że niektóre nasze dane znajdują się już w sieci Dark Web i są wykorzystywane przez cyberprzestępców. W związku z tym...

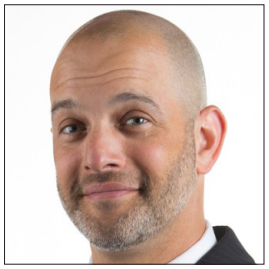
- **Bądź podejrzliwy w stosunku do wszelkich rozmów telefonicznych lub wiadomości e-mail udających oficjalne organizacje i nakłaniających Cię do podjęcia działań, chociażby takich jak zapłaty mandatu czy grzywny. Cyberprzestępcy mogą wykorzystywać znalezione informacje o Tobie do tworzenia spersonalizowanych ataków.**
- **Sprawdzaj wyciągi bankowe. Jeśli Twój bank daje taką możliwość, powinieneś włączyć powiadomienia o wszelkich transakcjach jakie miały miejsce. W ten sposób zauważysz nieautoryzowane transakcje płatnicze, a tym samym szybciej podejmiesz działania mające na celu powstrzymania oszustwa. Jeśli wykryjesz płatności, których nie robiłeś, natychmiast poinformuj o tej sytuacji bank lub firmę obsługującą Twoją kartę kredytową.**
- **Możesz skorzystać z usługi zastrzeżenia kredytowego aby nikt podszywając się pod Ciebie nie mógł zaciągać zobowiązań finansowych -- brać kredytów czy wyrabiać kart kredytowych.**

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK, powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.

WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redaktor wydania



Micah Hoffman *(@WebBreacher) jest głównym badaczem w Spotlight Infosec LLC, certyfikowanym instruktorem instytutu SANS oraz autorem kursów SANS OSINT. Pasja Micaha do cyberbezpieczeństwa oraz zbierania informacji z publicznych źródeł przejawia się w jego projektach, materiałach szkoleniowych oraz metodach nauczania.*

Źródła

Spersonalizowane ataki:	https://www.sans.org/u/RfW
Socjotechnika:	https://www.sans.org/u/Rg1
Identity Theft:	https://www.identitytheft.gov
Tor Browser:	https://www.torproject.org
Kurs SANS OSINT:	https://sans.org/sec487