De maandelijkse Security Awareness nieuwsbrief voor jou!

Dark Web

Overzicht

Misschien heb je de term “Dark Web” gehoord die door anderen of in de media wordt gebruikt en vroeg je je je af “*wat is het Dark Web?*” of “*moet ik er iets aan doen?*”. Vandaag leggen we uit wat het is en wat het voor jou betekent.

Wat is het?

Het Dark Web bestaat uit systemen op het internet die ontworpen zijn om veilig en anoniem te communiceren of informatie te delen. Er is niet één “Dark Web”; het is niet zoiets als Facebook waar het door één enkele organisatie wordt beheerd. In plaats daarvan is het Dark Web een verzameling van verschillende systemen en netwerken die door verschillende mensen worden beheerd en voor verschillende doeleinden worden gebruikt. Deze systemen zijn nog steeds verbonden met en maken deel uit van het internet, maar je zult ze over het algemeen niet vinden via de normale zoekmachines. Vaak heb je ook speciale software op de computer nodig om ze te vinden of te benaderen. Een voorbeeld is het Tor Project. Om toegang te krijgen tot dit donkere web, download en installeer je de Tor Browser. Wanneer je verbinding maakt met webservers met behulp van de Tor Browser, gaat je gecodeerde verkeer ook door andere computers met behulp van Tor. Als het door deze computers springt, verandert het bron-IP-adres, wat betekent dat wanneer je op de website komt, je online activiteit geanonimiseerd is. Andere voorbeelden van deze websites zijn Zeronet, Freenet en I2P.

Wie gebruikt het?

Cybercriminelen zijn grote gebruikers van het Dark Web. Ze onderhouden websites en forums in het Dark Web om hun criminele activiteiten mogelijk te maken, zoals het kopen van drugs of het verkopen van gigabytes aan gehackte gegevens - allemaal anoniem en veilig. Wanneer een cybercrimineel bijvoorbeeld een bank of een online winkel hackt, steelt hij zoveel mogelijk informatie en verkoopt die informatie vervolgens aan andere cybercriminelen op sites in het Dark Web.

Er zijn ook legitieme toepassingen van het Dark Web. Mensen in landen waar de censuur hoogtij viert, kunnen bijvoorbeeld gebruik maken van Dark Web-netwerken om informatie te delen en te zien wat er nog meer in de wereld gebeurt, terwijl hun privacy wordt beschermd en anoniem blijft. Journalisten, klokkenluiders en privacygerichte mensen kunnen het Dark Web gebruiken om hun anonimiteit te vergroten en censuur te omzeilen. Bovendien kunnen dergelijke personen technologieën zoals de Tor Browser niet alleen gebruiken om toegang te krijgen tot het Dark Web, maar ook om anoniem op het gewone internet te surfen.

Wat te doen?

Tenzij je een specifieke reden hebt om toegang te krijgen tot het Dark Web, waarschuwen we je ertegen. Sommige Dark Websites worden gebruikt voor illegale doeleinden, veel van de sites zullen je computer in een peer netwerk gebruiken om hun doelen te bereiken, en in sommige gevallen kan je computer zelfs worden onderzocht of aangevallen. Sommige bedrijven bieden monitoringdiensten aan om je te laten weten of je naam of andere informatie is gestolen door cybercriminelen en gevonden is op het Dark Web. De werkelijke waarde van deze diensten is twijfelachtig. De beste manier om jezelf te beschermen is te veronderstellen dat sommige van jouw informatie al in het donkere web wordt gebruikt door cybercriminelen. Dientengevolge.....

- **Wees wantrouwig ten aanzien van telefoontjes of e-mails die zich voordoen als een officiële organisatie en die je onder druk zetten om een actie te ondernemen, zoals het betalen van een boete. Criminelen kunnen zelfs informatie die ze over jou hebben gevonden gebruiken om een persoonlijke aanval te creëren.**
- **Controleer je creditcard en bankafschriften. Misschien zelfs dagelijks waarschuwingen instellen voor alle transacties die plaatsvinden. Op deze manier kan je ontdekken of er sprake is van financiële fraude. Als je het ontdekt, meld het dan direct aan je creditcardmaatschappij of bank.**
- **Zet een bevriezing op je kredietscore. Het heeft geen invloed op de manier waarop je je creditcard kunt gebruiken en is een van de meest effectieve maatregelen die je kunt nemen om jezelf te beschermen tegen identiteitsdiefstal.**

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft meer dan 4.200 medewerkers. In 2018 realiseerde Cegeka Groep een omzet van 512 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

Micah Hoffman *(@WebBreacher) is de Principal Investigator bij Spotlight Infosec LLC, een gecertificeerde SANS Institute Instructor en de auteur van de SANS OSINT cursussen. Micah's passie voor cyber- en open-source-informatie komt tot uiting in zijn projecten, cursusmateriaal en leerstijl.*

Bronnen

Personalized Attacks:	https://www.sans.org/u/RfW
Social Engineering:	https://www.sans.org/u/Rg1
Identity Theft:	https://www.identitytheft.gov
Credit Freeze:	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