Det mørke nettet

Oversikt

Du har kanskje hørt om "det mørke nettet" i media eller i prat med andre og lurt på "*hva er det mørke nettet?*" Eller "*skal jeg gjøre noe med det?*". Her skal vi forklare hva det mørke nettet er og hva det betyr for deg.

Hva er det?

Det mørke nettet består av systemer på internett designet for å kommunisere eller for å dele informasjon sikkert og anonymt. Det finnes ikke ett enkelt "mørkt nett". Det kan heller ikke sammenlignes med noe som Facebook som drives av ett selskap. Det mørke nettet er en samling av ulike systemer og nettverk styrt av mange forskjellige personer og brukt for en rekke ulike formål. Systemene er koblet til og er en del av internett, men man finner dem ikke med normale søkemotorer. Du trenger ofte spesifikk programvare for å finne og aksessere dem. Et eksempel er Tor Project. For å aksessere det mørke nettet laster du ned og installerer nettleseren Tor Browser. Når du kobler deg til webservere med Tor, sendes trafikken din kryptert igjennom andre datamaskiner og servere som også bruker Tor. Etterhvert som den hopper gjennom disse maskinene blir IP-adressen til kilden endret, det vil si at nettaktiviteten din blir anonymisert. Zeronet, Freenet og I2p er noen andre eksempler på mørke nett.

Hvem bruker det?

Cyberkriminelle bruker ofte det mørke nettet. De bruker drifter nettsteder og forum på det mørke nettet for å drive med kriminelle aktiviteter som kjøp og salg av narkotika, og salg av gigabyte med hacket data - alt anonymt og sikkert. For eksempel, når cyberkriminelle hacker seg inn i en bank eller nettbutikk stjeler de så mye informasjon de kan, og så selger de den til andre cyberkriminelle på nettsteder i det mørke nettet.

Det er også legitime grunner til å bruke det mørke nettet. For eksempel, personer i land hvor det er mye sensur bruker det mørke nettet til å dele informasjon og se hva som skjer i verden, alt mens de beskytter personvernet sitt og forblir anonyme. Journalister, whistleblowers (varslere), og personvernfokuserte folk bruker det mørke nettet for å øke anonymiteten sin og forbigå sensurering. De kan også bruke verktøy som Tor Browser til mer enn å besøke nettsider i det mørke nettet, de kan også bruke det normale internettet anonymt.

Hva burde jeg gjøre?

Med mindre du har en spesifikk grunn til å besøke det mørke nettet, anbefaler vi at du lar være. Noen nettsteder i det mørke nettet blir brukt for ulovlige formål, og i noen tilfeller kan maskinen din bli undersøkt for sårbarheter og forsøkt angrepet. Noen firmaer tilbyr overvåkningsløsninger for å la deg vite om ditt navn og annen informasjon har blitt stjålet av cyberkriminelle og er tilgjengelig i det mørke nettet. Den faktiske verdien av disse tjenestene er tvilsom. Den beste måten å sikre seg er å anta at informasjonen din allerede er tilgjengelig i det mørke nettet og blir brukt av cyberkriminelle. Derfor:

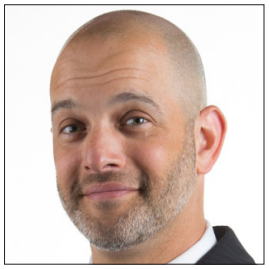
- **Vær på vakt ved telefonoppringninger eller e-poster fra folk som later som de tilhører offentlige organisasjoner og presser deg til å gjøre noe, for eksempel som å betale en regning. Kriminelle kan bruke informasjonen de har funnet til å utføre personaliserte angrep.**
- **Følg med på transaksjonene til kredittkortet ditt, og kontoutskriften for bankkortet ditt. Vurder å sette opp daglig varsling dersom det er en mulighet. På denne måten kan du oppdage om du blir utsatt for økonomisk svindel. Om du oppdager det, kontakt banken eller kredittkort-firmaet umiddelbart.**
- **Få på plass frivillig kredittsperre. Det påvirker ikke kredittkort eller lån du allerede har, og er en av de mest effektive tiltakene for å beskytte mot ID-tyveri. Dersom du skulle trenge å ta opp lån eller ordne nytt kredittkort, kan du enkelt heve kredittsperren.**

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Gjesteredaktør

Micah Hoffman *(@WebBreacher) er hovedforsker på Spotlight Infosec LLC, en sertifisert instruktør ved SANS-instituttet og forfatter av SANS OSINT-kurset. Micahs lidenskap for cyber og open source intelligence kan sees gjennom prosjektene hans, kursmateriellet, og undervisningsstilen hans.*



Ressurser

Persontilpasset svindel:	https://www.sans.org/u/RfW
Sosial manipulering:	https://www.sans.org/u/Rg1
ID-tyveri:	https://nettvett.no/id-tyveri/
Kredittsperre:	https://www.datatilsynet.no/regelverk-og-verktoy/verktoy/sporsmal-svar/kredittopplysning/hvordan-sette-sperre/
Tor Browser:	https://www.torproject.org/
SANS OSINT kurs:	https://www.sans.org/course/open-source-intelligence-gathering

OUCH! utgis av SANS Security Awareness, og er distribuert under Creative Commons BY-NC-BD 4.0 lisensen. Du står fritt til å distribuere dette nyhetsbrevet, eller bruke det i ditt eget bevissthetsprogram, så lenge du ikke gjør endringer på nyhetsbrevet. For oversettelser og mer informasjon, ta kontakt med oss på www.sans.org/security-awareness/ouch-newsletter. Redaksjon: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Oversatt av: NorSIS