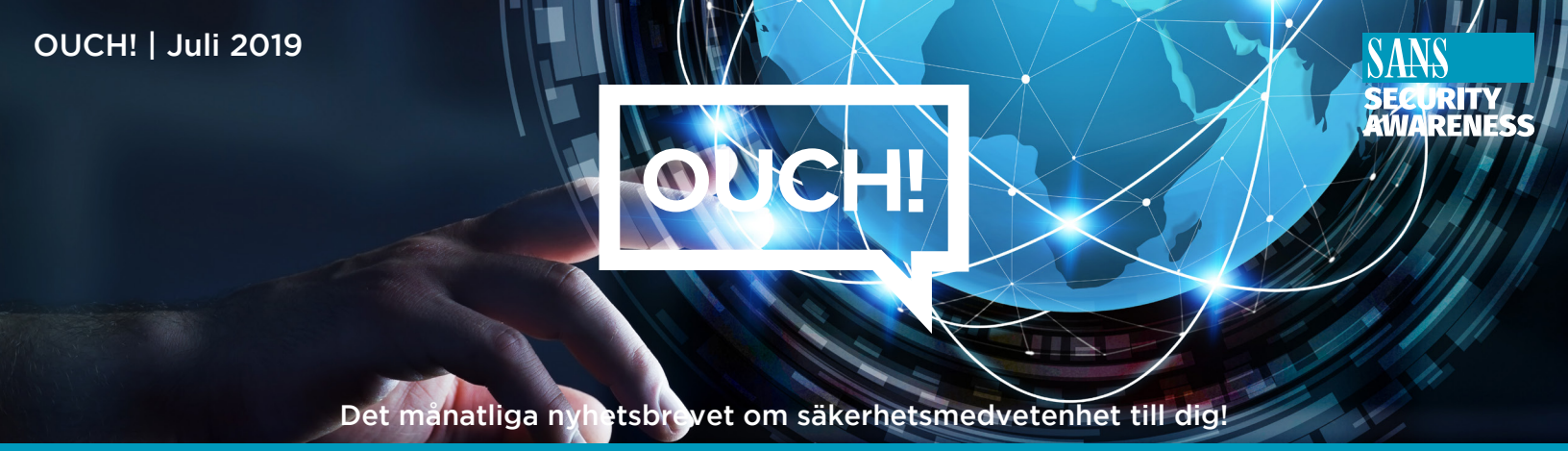

Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Dark Web

Inledning

Du har säkert hört talas om uttrycket “Dark Web” när det används av personer i din närhet eller när det förekommer i media och undrat “*vad är egentligen Dark Web?*” eller “*borde jag göra något åt det?*”. Idag ska vi förklara vad Dark Web är för något och vad det betyder för dig.

Vad är det?

Dark Web består av system på Internet designade för att kommunicera eller dela information säkert och anonymt. Det finns inte ett “Dark Web”, det är inte som Facebook som hanteras av en enstaka organisation. Istället är Dark Web en samling av olika system och nätverk som hanteras av olika organisationer och personer som använder det till en mängd olika syften. Dessa system är fortfarande anslutna till och är en del av Internet men du kommer oftast inte hitta dom med dina vanliga sökmotorer. Du behöver ofta speciell mjukvara installerad på din dator för att hitta och få åtkomst till dom. Ett exempel är Tor-projektet. För att ansluta till Dark Web laddar du ner och installerar Tor Browser. När du ansluter till webbservrar med Tor Browser skickas din krypterade nätverkstrafik genom andra datorer som också använder Tor. När den hoppar via dessa datorer ändras IP-adressen som innebär att när du når webbsidan är din ursprungliga IP-adress maskerad. Andra exempel av Dark Webs inkluderar Zeronet, Freenet och I2P.

Vem använder det?

Cyberbrottslingar är storkonsumenter av Dark Web. Dom tillhandahåller webbsidor och forum på Dark Web för att tillhandahålla handelsplatser för deras kriminella aktiviteter så som drogförsäljning eller försäljning av data från intrång - på ett anonymt och säkert sätt. Till exempel när en cyberbrottsling hackar en bank eller en onlinebutik stjäl de så mycket information dom kan och därefter säljer information till andra cyberbrottslingar på dessa handelsplatser på Dark Web.

Det finns också legitima användarfall av Dark Web. Som exempel personer i länder där censur är förekommande kan nyttjandet av Dark Web bidra till att dela information och se vad som händer i världen utanför censuren samtidigt som deras integritet skyddas och förblir anonyma. Journalister, visselblåsare och integritetsfrämjande personer kan använda Dark Web för att öka

anonymitet och förbise censur. Det går självklart att nyttja teknologier som Tor Browser att inte enbart ha åtkomst till Dark Web utan även surfa anonymt på vanliga Internet.

Vad borde jag göra?

Om du inte har en specifik anledning för åtkomst till Dark Net varnar vi dig för det. Vissa webbsidor på Dark Web används för olagliga syften. Flertalet webbsidor avser att nyttja din dator i ett nätverk för att uppnå sina mål och vissa fall attackeras även din dator. Vissa företag erbjuder övervakningstjänster för att notifiera dig om information kopplat till dig eller ett varumärke har blivit stulet av cyberbrottslingar och hittat på Dark Web. Det verkliga värdet av dessa tjänster är tveksamma. Bästa sättet att skydda dig själv är att förutse att din information redan är på Dark Web och nyttjas av cyberbrottslingar. Som resultat av detta...

- **Var misstänksam när du tar emot telefonsamtal eller e-postmeddelanden från officiella organisationer som uppmanar dig att uträtta något skyndsamt, det kan t.ex. vara att betala böter eller liknande. Brottslingar använder ofta information de har hittat om dig för att skapa en personligt anpassad attack.**
- **Övervaka dina kort- och banktransaktioner. Du kanske till och med kan sätta upp larm när transaktioner genomförs. På så sätt kan du lätt uppmärksamma om du är utsatt för bedrägerier. Om du upptäcker det, kontakta genast din kortutgivare eller bank.**
- **Spärra eller lås ditt personnummer med en bedrägerispärr för kreditupplysning. Spärren påverkar inte hur du kan nyttja dina redan godkända krediter men skyddar dig mot försök att stjäla din identitet och ta nya krediter.**

Visolit är nordens ledande specialist på molntjänster. Visolit har för närvarande Europas största och mest moderna driftsplattform för SMB-marknaden. Vi levererar allt från komplett IT-drift till enklare IT-tjänster som anpassas och integreras utifrån kundens existerande behov och infrastruktur. Med våra tjänster får små och medelstora företag tillgång till IT med en kvalitet och säkerhet som normalt är undantaget stora internationella företag. www.visolit.se eller följ oss på LinkedIn https://www.linkedin.com/company/visolit

Gästredaktör

Micah Hoffman *(@WebBreacher) är huvudutredare hos Spotlight Infosec LLC, en certifierad SANS Institute instruktör och författaren till SANS OSINT-kurser. Micah's passion för cyber och open source intelligence framhävs i hans projekt, kursmaterial och lärarstil.*

Referenser

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