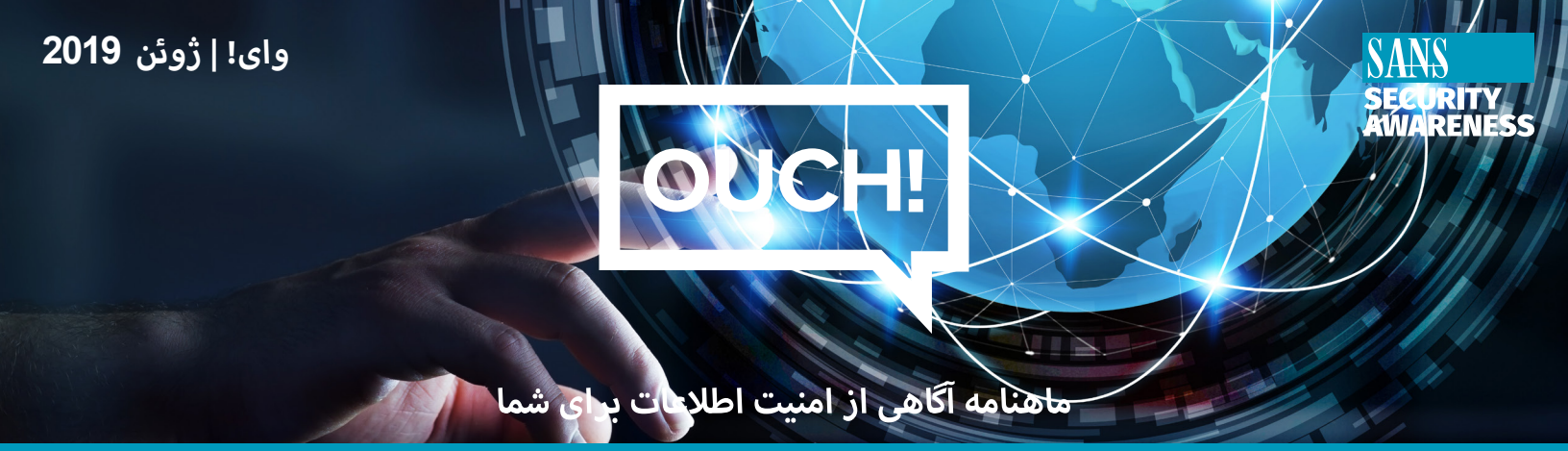
وای! | ژوئن 2019



اینترنت مخفی

مقدمه

ممکن است واژه «Dark Web» را که توسط دیگران یا در رسانه ها استفاده میشود را شنیده باشید و کنجکاو باشید که «اینترنت مخفی» چیست؟ یا سوال کنید «آیا مهم هست که بدانم چه هست؟» امروز توضیح می دهیم که اینترنت مخفی چیست و چه چیزی برای شما مهم است.

اینترنت مخفی چیست؟

اینترنت مخفی شامل سامانه های اینترنتی است که برای ارتباط و یا به اشتراک گذاری اطلاعات به طور مخفی و ناشناس استفاده می شود. یک اینترنت مخفی وجود ندارد؛ چیزی شبیه فیس بوک نیست که در یک جا و توسط یک سازمان یا شرکت اداره شود. در عوض اینترنت مخفی مجموعه ای از سیستم های مختلف و شبکه های مدیریت شده توسط افراد مختلف است که برای اهداف مختلف مورد استفاده قرار می گیرند. این سیستم ها هنوز به اینترنت متصل هستند و بخشی از اینترنت محسوب میشوند، اما معمولا آنها را با استفاده از موتورهای جستجوی معمول پیدا نمی کنید. حتی اغلب به نرم افزار خاصی در رایانه خود نیاز دارید تا آنها را پیدا کنید یا به آنها دسترسی پیدا کنید. یک مثال پروژه Tor است. برای دسترسی به اینترنت مخفی، مرورگر Tor را دانلود و نصب کنید. هنگام اتصال به سرورهای وب با استفاده از مرورگر Tor، ترافیک رمزگذاری شده شما از طریق رایانه های دیگر که آنها هم از Tor استفاده می کنند عبور میکند. هنگامی که ارتباطات شما از طریق این رایانه های در طی مسیر عبور میکنند، آدرس IP منبع ارسال داده (که ادرس کامپیوتر شما است) تغییر می کند و به این معنی است که هنگامی که داده های شما به وب سایت مقصد می رسد، کسی آدرس اینترنتی شما را نمیداند و اینگونه فعالیت آنلاین شما ناشناس است. نمونه های دیگر سیستم های موجود در اینترنت مخفی عبارتند از Freenet، Zeronet و I2P.

چه کسی از آن استفاده می کند؟

مجرمان سایبری بزرگترین کاربراینترنت مخفی هستند. آنها وب سایت ها و انجمن های گفتگویی را برای اجرای فعالیت های جنایتکارانه خود مانند خرید دارو یا فروش حجم انبوه اطلاعات هک شده نگهداری می کنند - که همه ناشناس و مخفی هستند. به عنوان مثال، زمانی که یک مجرم سایبری بانکی یا فروشگاهی آنلاین را هک می کند، آنها تا آنجا که میتوانند اطلاعات سرقت می کنند و سپس این اطلاعات را به دیگر مجرمان سایبری در سایت های اینترنت مخفی می فروشند.

البته اینترنت مخفی قانونی هم وجود دارد. به عنوان مثال، شهروندان کشورهایی که سانسور درآنجا شایع هستند، می توانند از شبکه های وب مخفی برای به اشتراک گذاشتن اطلاعات استفاده کنند و ببینند چه چیزی در دنیا اتفاق می افتد و در عین حال از حریم خصوصی خود محافظت کنند و ناشناس باقی بمانند. روزنامه نگاران، خبرنگاران و افرادی که در مورد حریم خصوصی شان حساس هستند می توانند از اینترنت مخفی برای افزایش ناشناسی ماندن خود و دور زدن سانسور استفاده کنند. علاوه بر این، این افراد می

توانند از فن آوری هایی مانند مرورگر Tor استفاده کنند نه تنها برای دسترسی به وب سایت های مخفی، بلکه بطور ناشناس اینترنت معمولی را مرور کنند.

باید چکار کنم؟

به غیر از اینکه دلیل خاصی برای دسترسی به Dark Web داشته باشید، ما به شما در برابر آن هشدار می دهیم. برخی از وب سایت های اینترنت مخفی برای اهداف غیر قانونی مورد استفاده قرار می گیرند، بسیاری از سایت ها از رایانه شما در یک شبکه ی peer-to-peer برای رسیدن به اهداف خود سوء استفاده می کنند و در بعضی موارد ممکن است کامپیوتر شما مورد آزمایش قرار گیرد یا مورد حمله قرار گیرد. برخی از شرکت ها خدمات نظارتی ارائه می دهند تا به شما اطلاع دهند که آیا نام و یا اطلاعات دیگر شما توسط جنایتکاران اینترنتی دزدیده شده است و در وب سایت Dark Web یافت می شود. ارزش واقعی این خدمات جای سوال دارد. بهترین راه محافظت از خود، این است که فرض کنید که برخی از اطلاعات شما در حال حاضر در وب مخفی موجود است که توسط مجرمان اینترنتی استفاده می شود. در نتیجه . . .

- **از هر گونه تماس تلفنی یا ایمیل که تظاهر به یک سازمان رسمی میکند و شما را برای انجام کاری تحت فشار و اضطراب، مانند پرداخت جریمه میگذارد خودداری کنید. مجرمان حتی ممکن است از اطلاعاتی که در مورد شما پیدا کرده اند، برای ایجاد نقشه ای کاملا حساب شده استفاده کنند.**
- **کارت اعتباری و رسیدها و صورتحساب های بانکی خود را کنترل کنید. حتی حساب بانکی خود را طوری تنظیم کنید که هر تراکنشی که در حساب شما اتفاق می افتد پیامی به شما ارسال شود. به این ترتیب شما می توانید تشخیص دهید که آیا کلاهبرداری مالی رخ داده یا خیر. اگر رخ داد، آن را به شرکت کارت اعتباری یا بانک خود بلافاصله گزارش دهید.**
- **رتبه ی اعتباری (credit score)خود را بپوشانید. این تاثیری بر نحوه استفاده از کارت اعتباری شما ندارد و یکی از موثرترین اقداماتی است که می توانید برای محافظت از خود مقابل سرقت هویت استفاده کنید.**

سردبیر مهمان

مایکل هافمن (@WebBreacher) محقق اصلی در شرکت Spotlight Infosec LLC است، مدرس معتبر موسسه SANS و نویسنده محتوای دروس دوره های SANS OSINT است. اشتیاق مایک به اطلاعات سایبری و منبع باز در پروژه های او، برنامه های آموزشی و سبک آموزشی او نمایان است.

منابع

حملات شخصی: https://www.sans.org/u/RfW
مهندسی اجتماعی: https://www.sans.org/u/Rg1
سرقت هویت: https://www.identitytheft.gov
پوشیدن رتبه اعتباری: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
مرورگر تور: https://www.torproject.org/
دوره OSINT موسسه سنز: https://sans.org/sec487