OUCH!
ماهنامه آگاهی از امنیت اطلاعات برای شما

بله، بدنبال شما هستند!

مقدمه

خیلی مردم به اشتباه خیال میکنند که آنها هدف تبهکاران سایبری قرار نمیگیرند چون آنها و وسایل الکتریکی شان یا حساب های کاربری آنها ارزش آنچنان ندارد. این تفکر درستی نیست. اگر از فن آوری اطلاعات به هر نحوی در خانه یا محل کار استفاده میکنید، مطمئن باشید که شما برای تبهکاران ارزش دارید. اما، این شانس را دارید که قبلا حفاظت خوبی در مقابل این افراد دارید که آن خود شما هستید.

چرا به دنبال شما هستند؟

در حال حاضر، انواع مختلفی از تبهکاران سایبری روی اینترنت وجود دارند که انگیزه های مختلفی هم دارند. چرا آنها بدنبال شما هستند؟ چون با هدف قرار گرفتن شما آنها به منظور خود خواهند رسید. در اینجا دو نمونه متداول از جرایم همراه با انگیزه تبهکاران سایبری بیان میشود.

تبه کاران سایبری: اینها دنبال پول در آوردن هستند به هر اندازه و هر گونه که بتوانند. اینترنت برای آنها جذاب هست چون میتوانند هر کس را در سراسر دنیا بخواهند با فشردن دکمه ای هدف قرار دهند. و راههای زیادی هم برای پول بدست آوردن از طریق جرائم سایبری دارند. بطور نمونه، دزدی از حساب بانکی آنلاین شما یا حساب بازنشستگی، تهیه کارت اعتباری تحت نام شما و ارسال قبض پرداخت برای شما، استفاده از رایانه شما برای نفوذ به رایانه دیگران، نفوذ به حساب کاربری شبکه اجتماعی یا شبکه بازی شما و فروش آن به تبهکاران دیگر. میتوان موارد تبهکاری بیشماری را بیان نمود که تبهکاران میتوانند از شما پول بدست بیاورند. صدها هزار تبهکار هر روزه از خواب به نیت نفوذ به رایانه و حساب کاربری مردم بیدار میشوند از جمله شخص شما.

تبه کاران متمرکز روی هدف: این نوع تبهکاران خیلی حرفه ای هستند و معمولا برای دولتها، گروههای تبهکاری یا رقیبانمان کار میکنند. ممکن است فکر کنید که شغل شما برای آنها خیلی جذابیت نداشته باشد، ولی تعجب خواهید کرد وقتی اهداف آنها را بدانید:

- اطلاعات و داده هایی که شما در محل کار با آن سر و کار دارید، ارزش بسیار زیادی برای شرکتها و دولتهای مختلف دارد.
- تبه کاران ممکن است روی شما تمرکز کنند نه به این خاطر که به رایانه شما نفوذ کنند بلکه از شما برای نفوذ به رایانه یا حساب کاربری همکارانتان یا دیگر رایانه ها استفاده کنند.
- این تبه کاران ممکن است شما را هدف بگیرند به خاطر شرکت یا شریک تجاری که شما با آنها کار میکنید.

من آنتی ویروس دارم، خیالم راحت است

اگر من هدف قرار گرفتم مشکلی نیست، آنتی ویروس و فایروال روی رایانه ام نصب میکنم و محفوظ خواهم بود. اینطور نیست؟ حقیقت این است که متاسفانه نه. خیلی از مردم فکر میکنند اگر بعضی نرم افزارهای حفاظتی را نصب کنند، دیگر امن هستند. متاسفانه، این کاملا درست نیست. تبهکاران سایبری هر روز ماهرتر میشوند، و با ترفندهایی که بکار میبرند میتوانند این نرم افزارهای حفاظتی را دور بزنند. برای نمونه، بدافزارهایی میسازند که آنتی ویروسها نمیتوانند آنها را شناسایی کنند. یا از فیلترهای حفاظتی نرم افزار ایمیل شما با استفاده از فیشینگ های خاص میگذرند، یا به تلفن شما زنگ میزنند و شما را فریب میدهند تا اطلاعات کارت اعتباری شما، یا رمز عبور یا پول شما را بدست بیاورند. ابزارهای فن آوری نقش مهمی در زمینه محافظت از شما بازی میکنند اما در نهایت شما بهترین محافظ خود هستید.

خوشبختانه، امن ماندن خیلی سخت نیست، هوشیاری مرسوم و بعضی رفتار ساده بهترین محافظ شما هستند. اگر ایمیلی یا پیامی یا تلفنی دریافت کردید که از شما واکنش سریع طلب میکنند، یا مشکوک یا غیرعادی است، به احتمال زیاد شما مورد هدف قرار گرفته اید. برای اینکه مطمئن شوید که رایانه و وسائل الکترونیکی شما امن هستند، آنها را به روز نگه دارید و به روز کردن خودکار را فعال کنید. برای حساب های کاربری خود رمز عبارتگونه منحصر بفرد و قوی انتخاب کنید. آگاه بودن از خطرات و راه حل آنها بهترین محافظ خواهد بود. اگر نمیدانید چگونه شروع کنید، برای دریافت مداوم همین ماهنامه وای! که در حال خواندن آن هستید در آدرس sans.org/ouch اقدام کنید.

سردبیر مهمان

مت برومیلی (@mbromileyDFIR) Matt Bromiley کارشناس کشف و بررسی جرائم دیجیتالی و همچنین مسئول پاسخ سریع به وقایع سایبری است، که 8 سال سابقه کار برای سازمانهای مختلف در سراسر دنیا دارد. همچنین او این موضوعات را برای موسسه SANS تدریس میکند.

SANS SECURITY AWARENESS

منابع

بدافزار را متوقف کنید: https://www.sans.org/u/L1J
مهندسی فریب جامعه: https://www.sans.org/u/L1O
کلاهبرداری از طریق تلفن: https://www.sans.org/u/L1T
رمز عبارتگونه: https://www.sans.org/u/L1Y
بدنبال شما هستند (پوستر): https://www.sans.org/u/L23