SANS SECURITY AWARENESS

OUCH!

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

کلاهبرداری با نقاب مدیرعامل / BEC

کلاهبرداری با نقاب مدیرعامل (BEC) چیست؟

نوع جدیدی از حمله سایبری از طریق ایمیل به نام کلاهبرداری با نقاب مدیرعامل یا نفوذ به ایمیل کسب و کار (BEC) در حال افزایش هست. این نوع حملات ایمیل های هدفمند هستند که قربانی خود را به انجام خواسته های مجرم فریب میدهند. در اغلب موارد مجرمان سایبری در پی پول هستند. چیزی که این حملات را بسیار خطرناک میکند این است که مجرمین سایبری قبل از حمله در مورد قربانی خود تحقیق میکنند. برای فن آوری های امنیتی موجود هم جلوگیری از این نوع حملات خیلی سخت است چون مثل حملات متداول هیچ پیوست ایمیل آلوده و یا لینک مخرب برای تشخیص حمله وجود ندارد. در اینجا در مورد این حمله توضیح می دهیم.

مجرم اینترنتی با استفاده از شبکه های اجتماعی و اطلاعات موجود روی اینترنت در مورد قربانی و افرادی که با قربانی در تعامل هستند مانند رئیس محل کارش یا مشاور املاک و مستغلات او تحقیق میکنند. مجرم سایبری سپس ایمیلی را تهیه میکند و ادعا میکند که یکی از این افراد است که به او ایمیل ارسال می کند. ایمیل فوری است و از قربانی میخواهد فورا اقدامی کند، مانند پرداخت صورتحساب، تغییر فرد گیرنده مبلغ و یا قربانی را متقاعد به پاسخ و ارسال اطلاعات محرمانه و حساس میکند. نقطه مشترک همه این نوع حقه ها این است که شما را در حالت اضطرار میگذارند تا آنچه میخواهند را برایشان انجام دهید. در اینجا با دو مثال توضیح میدهیم چگونه این حقه ها کار میکند.

انتقال پول: مجرم سایبری به دنبال پول هست. آنها در مورد شرکت شما تحقیق میکنند، بطورمثال کسانی که در حسابداری شرکت یا هر کس که مسئول پرداخت ها یا انتقال وجوه هست را شناسایی میکنند. سپس مجرمان ایمیلی را میسازند که در آن تظاهر به رئیس فرد یا مسئول ارشد اجرایی میکنند و در ایمیل به آنها می گوید که فورا پولی را به حساب بانک جدیدی منتقل کند. این ایمیل آنها را تحت اضطرار قرار میدهد تا مرتکب اشتباه شده و پول به حساب مجرم سایبری واریز کنند.

کلاهبرداری مالیاتی: مجرمان اینترنتی در این نوع حقه، در پی اطلاعات شخصی و مالیاتی مردم هستند. یکی از سریعترین راه ها برای این کار سرقت اطلاعات کارکنان شرکت است. مجرمان اینترنتی کارکنان اداره استخدامی و منابع انسانی را با تحقیق شناسایی میکنند. سپس ایمیل های جعلی به این افراد فرستاده و تظاهر میکنند مدیر اجرایی ارشد و یا شاید کسی از اداره حقوق هستند. این ایمیل داستانی از وضعیتی اضطراری میسازد که اطلاعات مالیاتی همه کارکنان باید فوراً به او ارسال شود. کارکنان اداره استخدامی و منابع انسانی فکر می کنند که آنها این اسناد حساس را به مدیر اجرایی ارشد ارسال میکنند در حالیکه در واقع آنها اسناد را به مجرمان سایبری فرستاده اند.

حفاظت از خودتان

پس چگونه می توانید از خود محافظت کنید؟ عقل سلیم بهترین مدافع است. اینجا شایع ترین نشانه های این نوع حمله که باید به دنبالش باشید گفته میشود.

ایمیل بسیار کوتاه و اضطراری (اغلب تنها چند جمله) است و امضا پایین ایمیل می گوید ایمیل از دستگاه تلفن همراه فرستاده شده است.

یک حس قوی از ضرورت و فوریت وجود دارد که شما را به نادیده گرفتن و یا دور زدن سیاست های کارفرمای شما ترغیب میکند. حتی اگر به نظر می رسد ایمیل از رئیس خود و یا حتی مدیر عامل می آیند، همیشه سیاست ها و روش های مربوطه را دنبال کنید.

ایمیل مربوط به کار است اما با استفاده از آدرس ایمیل شخصی مانند @gmail.com یا @hotmail.com ارسال شده است.

ایمیل به نظر می رسد از مدیر ارشد، همکار یا فروشنده ای که شما می شناسید یا با او کار میکنید آمده است، اما لحن پیام مانند آنها نیست.

اطلاعات و دستورالعمل پرداخت ارائه شده است و متفاوت از آنهایی است که شما قبلا در اختیار دارید، مانند درخواست فوری پرداخت به حساب بانکی متفاوت.

اگر به چنین مواردی برخوردید و گمان اینکه مورد حمله قرار گرفته اید دارید با مجرم هیچ گونه تماسی برقرار نکنید و فوری با مسئول خود موضوع را در میان بگذارید. اگر شما در خانه مورد این نوع حقه قرار گرفتید و قربانی پرداخت پولی هم شدید، بلافاصله آن را به بانک خود سپس به مجریان قانون گزارش دهید.

سردبیر مهمان

دان کاوندر (Don Cavender) افسر ویژه سابق اف بی آی، با بیش از 22 سال سابقه در کشف جرائم دیجیتال و جرائم رایانه ای است. او اخیرا روی گروههای سازمان یافته مجرم سایبری به عنوان هماهنگ کننده BEC (نفوذ از طریق ایمیل کاری) در واشنگتن دی سی خدمت کرده است. او در زمینه کشف جرائم دیجیتال تدریس و پژوهش میکند. او را میتوانید در لینکدین و توییتر دنبال کنید: @don_cavender
https://www.linkedin.com/in/donald-cavender

منابع

مهندسی اجتماعی: https://www.sans.org/u/HE3

توقف فیشینگ: https://www.sans.org/u/HE8

جلوگیری از بدافزارها: https://www.sans.org/u/HEd

قفل کردن ورود به حساب: https://www.sans.org/u/HEi