وای! | فوریه 2019

SANS SECURITY AWARENESS

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

# کلاهبرداری با اطلاعات شخصی سازی شده

## مقدمه

مجرمان سایبری همچنان با روش های جدید و خلاقانه در حال فریب مردم هستند. روش جدیدی از کلاهبرداری که در حال عمومی شدن است - با عنوان کلاهبرداری با استفاده از اطلاعات شخصی سازی شده(Personalized scam) شناخته میشود. در این روش مجرمان سایبری اطلاعات مربوط به میلیون ها انسان را بدست اورده و یا خریداری میکنند تا از آن برای شخصی سازی حملات استفاده کنند. در ذیل به شما نشان خواهیم داد که این نوع کلاهبرداری ها چگونه کار میکنند و با یک مثال معمولی آن را برای شما باز خواهیم کرد. هرچه بیشتر در خصوص این نوع کلاهبرداری ها بدانید، راحتتر میتوانید آنها را متوقف کنید.

## نحوه عملکرد آن چگونه است؟

کلاهبرداری از طریق ایمیل و یا تلفن چیز جدیدی نیست، مجرمان سایبری سالهاست که از این روشها برای فریب دادن مردم استفاده میکنند. مثالهایی نظیر «شما برنده قرعه کشی شده اید» و یا رسوایی شاهزاده نیجریه از این دست کلاهبرداری ها به حساب می آیند. اما، در این روشهای قدیمی مجرمان سایبری نمیدانند که به چه شخصی حمله کرده اند. در این روش آنها یک پیغام عمومی درست کرده و برای میلیونها نفر ارسال میکنند. با توجه به اینکه این نوع کلاهبرداری ها بسیار کلی هستند، شناسایی آنها نیز راحت خواهد بود. کلاهبرداری شخصی سازی شده اما متفاوت است، مجرمان سایبری در ابتدا تحقیق میکنند که برای هر قربانی چه پیام سفارشی درست کنند. این کار با پیدا کردن و یا خریدن بانک اطلاعاتی افراد نظیر اسم، رمز عبور، شماره تماس و سایر جزییات انجام خواهد شد. این اطلاعات به سادگی و توسط سایتهایی که قبلا هک شده اند در دسترس خواهند بود. این اطلاعات همچنین در سایتهای شبکه های اجتماعی و سوابق دولتی که بصورت عمومی در دسترس هستند قابل دسترسی است. مجرمان سپس هر کسی که را که از او اطلاعات دارند مورد هدف قرار خواهند داد.

یک روش معمول برای مجرمان سایبری ایجاد ترس و سپس اخاذی است که شما را مجبور به پرداختن پول به آنها بکند. روش کار آنها به این شکل است. اطلاعات کاربری و رمزعبور افراد را توسط سایتهای هک شده پیدا میکنند و یا میخرند. با به دست اوردن اطلاعات، برای شما ایمیلی که حاوی اطلاعات شخصی شما، از جمله پسوردی که در آن سایت هک شده داشتید ارسال خواهد شد. مجرمان به اشاره به این پسورد وانمود میکنند که دستگاه شما را هک کرده اند، که در البته واقعیت ندارد. سپس ادعا میکنند که زمانیکه دستگاه شما را هک میکردند شما در حال تماشای سایت های مستهجن بودید. در ادامه ی ایمیل شما را تهدید میکنند که اگر هزینه اخاذی را پرداخت نکنید، شواهدی از فعالیت های شرم اور شما را با دوستان و خانواده شما به اشتراک خواهند گذاشت.

باج خواهی در حالی صورت میگیرد که مجرمان سایبری هرگز دستگاه شما را هک نکردند. آنها حتی نمیدانند که شما چه کسی هستید و یا چه سایتهایی را بازدید کردید. کلاهبردار ها با حداقل اطلاعاتی که از شما دارند تلاش خواهند کرد تا شما را بترسانند و شما را متقاعد کنند که دستگاه شما را هک کرده اند و به این طریق شماه مجبور شوید به آنها پول پرداخت کنید. بخاطر داشته باشید که مجرمان از همین روش میتوانند برای کلاهبرداری تلفنی استفاده کنند.

## چه کاری باید انجام دهید؟

تشخیص دهید که ایمیل و تلفن های از این دست برای کلاهبرداری هستند. طبیعی است از اینکه کسی اطلاعات شخصی شما را در اختیار دارد احساس ترس کنید. به خاطر داشته باشید که فرستنده دورغ میگوید. این نوع حملات بخشی از حملات خودکار در حجم وسیع هستند که بطور مستقیم شما را مورد هدف قرار نداده اند. امروزه برای مجرمان سایبری بدست آوردن و یا خریدن اطلاعات شخصی افراد بسیار کار راحتی است، بنابراین در آینده منتظر حملات بیشتری از نوع کلاهبرداری های شخصی باشید. برخی از سرنخ هایی که باید به دنبالش بگردید عبارتند از:

- **هر زمان ایمیل، پیغام و یا تلفنی با موضوع بسیار فوری دریافت کردید، به آن بسیار مشکوک باشید. اگر کسی از احساساتی نظیر ترس و یا فوریت استفاده میکند، هدفش این است که با ایجاد عجله و دستپاچگی در شما، موجب شود تا شما دچار اشتباه شوید.**
- **زمانیکه شخصی از شما درخواست پرداخت پول بصورت بیت کوین، کارت هدیه و یا روشهایی که قابل ردیابی نیستند میکند.**
- **وقتی ایمیل مشکوکی دریافت میکنید، در گوگل جستجو کنید و ببینید که آیا افراد دیگری هم گزارشاتی شبیه این حملات را داده اند.**

در نهایت رجوع به عقل سلیم بهترین روش دفاع است. در عین حال توصیه ما این است که همیشه از رمزعبورهای منحصربفرد و طولانی برای هر یک از اکانت های آنلاین خود استفاده کنید.اگر نمیتوانید همه کلمات عبور خود را حفظ کنید از برنامه های مدیریت پسورد استفاده کنید. علاوه بر این، هر زمان که ممکن بود احراز هویت دو عاملی را فعال کنید.

## سردبیر مهمان

لنی زلتسر یک کهنه سرباز در حوزه امنیت سایبری است. وی در شرکت Minerva Labs بر روی راهکارهای ضدبدافزار کار میکند و مدرس دوره های امنیت در SANS میباشد. از دیگر تجربیات وی میتوان به سرویسهای مدیریت امنیت و مشاوره اشاره کرد. برای ارتباط با وی میتوانید به آدرس zeltser.com/blog سر بزنید و یا به آدرس توییتر @lennyzeltser مراجعه کنید.

## منابع


مهندسی اجتماعی : https://www.sans.org/u/LW6
نکات مهم برای استفاده از شبکه های اجتماعی: https://www.sans.org/u/LWb
اپراتورهای موتورهای جستجو: https://support.google.com/websearch/answer/2466433
چهارچوب OSINT: https://osintframework.com/
دوره درسی OSINT ارائه شده در SANS: https://www.sans.org/u/LWZ