شناسایی و توقف حملات پیام رسانی

حملات پیام رسانی چیست؟

Smishing (کلمه ای است که ترکیبی از پیامک و فیشینگ میباشد) حملاتی هستند که زمانی رخ می دهند که مهاجمان سایبری از پیام کوتاه، پیامک یا فناوری های پیام رسانی مشابه استفاده می کنند تا شما را فریب دهند تا اقدامی را که نمیبایست انجام دهید، انجام بدهید. شاید آنها بتوانند شما را فریب دهند تا جزئیات کارت اعتباری خود را ارائه دهید، از شما بخواهند با یک شماره تلفن تماس گرفته تا اطلاعات بانکی خود را دریافت کنید، یا شما را متقاعد کنند که یک فرم نظر سنجی آنلاین را تکمیل کرده تا اطلاعات شخصی شما را جمع آوری کنند. درست مانند حملات فیشینگ ایمیل، مجرمان سایبری اغلب با احساسات شما بازی می‌کنند تا به عنوان مثال با ایجاد حس فوریت یا کنجکاوی، شما را وادار به عمل کنند. با این حال، چیزی که حملات پیام‌رسانی را بسیار خطرناک می‌کند این است که اطلاعات بسیار کمتر و سرنخ‌های محدودتری در متن نسبت به ایمیل وجود دارد، و این باعث میشود تشخیص موارد اشتباه و خطا برای شما بسیار سخت تر شود.

یک کلاهبرداری رایج، پیغامی است که به شما می‌گوید برنده یک آیفون شده‌اید، و برای دریافت آن کافیست روی پیوند کلیک کرده و یک فرم نظرسنجی را پر کنید. در واقعیت، تلفنی وجود ندارد و این نظرسنجی برای جمع آوری اطلاعات شخصی شما طراحی شده است. مثال دیگر پیامی است مبنی بر اینکه بسته ای را نمی توانند تحویل دهند و یک لینک به یک وب سایت ارائه میدهند که در آن از شما خواسته می شود اطلاعات لازم برای تکمیل تحویل بسته، از جمله جزئیات کارت اعتباری خود را برای پوشش «هزینه های خدمات» ارائه دهید. در برخی موارد، این سایت‌ها حتی ممکن است از شما بخواهند یک برنامه تلفن همراه غیرمجاز را نصب کنید تا دستگاه شما را آلوده کرده و تحت کنترل خود درآورند.

حتی گاهی اوقات مجرمان سایبری حملات تلفنی و پیام رسانی را با هم ترکیب می کنند. به عنوان مثال، ممکن است یک پیام متنی اضطراری از بانک خود دریافت کنید که از شما می پرسد آیا اجازه پرداختی غیرعادی را داده اید یا خیر. این پیام از شما می‌خواهد برای تایید پرداخت، با جواب بله یا خیر پاسخ دهید. اگر شما پاسخ دهید، اکنون مجرم سایبری می داند که مایل به تعامل هستید و با شما تماس می گیرد که وانمود می کند که از بخش پیشگیری از کلاهبرداری بانک تماس گرفته است. سپس آنها سعی می کنند اطلاعات مالی و کارت اعتباری یا حتی اطلاعات ورود و رمز عبور بانکی تان را از شما دریافت کنند.

شناسایی و توقف حملات پیام رسانی

در اینجا چند سوال وجود دارد که باید از خود بپرسید تا رایج ترین سرنخ های حمله های پیام رسانی را پیدا کنید:

- آیا این پیام باعث ایجاد احساس فوریت شدید در تلاش برای عجله کردن یا تحت فشار قرار دادن شما برای انجام کاری میشود؟آیا این پیام شما را به وب‌سایت‌هایی که درخواست اطلاعات شخصی، کارت اعتباری، رمز عبور یا سایر اطلاعات حساسی را که نباید به آنها دسترسی داشته باشند، میبرد؟
- آیا این پیام به نظر بیش از حد خوب به نظر میرسد؟ نه، در حقیقت شما یک آیفون جدید رایگان برنده نشدید.
- آیا وب سایت یا سرویس پیوند شده به آن شما را مجبور به پرداخت با استفاده از روش های غیر معمول مانند بیت کوین، کارت های هدیه یا انتقال وسترن یونیون (مانند حواله ارز از یک کشور به کشور دیگر) می کند؟

- آیا این پیام از شما کد احراز هویت چند مرحله‌ای را می‌خواهد که به تلفن شما ارسال شده یا توسط برنامه بانکی شما ایجاد شده است؟
- آیا این پیام مشابه "یک شماره اشتباه" است؟ اگر چنین است، به آن پاسخ ندهید یا سعی نکنید با فرستنده تماس بگیرید فقط آن را حذف کنید.

اگر پیامی از یک سازمان رسمی دریافت کردید که به شما هشدار می دهد، مستقیماً با آنها تماس بگیرید. از شماره تلفن موجود در پیام استفاده نکنید، به جای آن از یک شماره تلفن مطمئن استفاده کنید. به عنوان مثال، در صورت دریافت پیامک از بانک خود مبنی بر اینکه برای حساب بانکی یا کارت اعتباری شما مشکلی بوجود آمده، یک شماره تلفن قابل اعتماد در وب سایت بانک خود، صورتحساب و یا از پشت کارت اعتباری یا بانکی خود برداشته و مستقیما با آنها تماس بگیرید. همچنین به یاد داشته باشید که اکثر سازمان‌های دولتی، مانند سازمان‌های مالیاتی یا مجری قانون، هرگز از طریق پیامک با شما ارتباط برقرار نمیکنند، بلکه فقط از طریق پست قدیمی با شما تماس خواهند گرفت.

وقتی صحبت از حملات پیام رسانی می شود، بهترین دفاع خود شما هستید.

سردبیر مهمان

جف لوماس یک کارآگاه در گروه تحقیقات سایبری اداره پلیس متروپولیتن لاس وگاس است و دوره جمع‌آوری و تحلیل اطلاعات منبع باز SANS SEC487 (OSINT) را تدریس می‌کند. جف در مورد جرایم مالی با فناوری پیشرفته از جمله به خطر انداختن ایمیل های تجاری، حملات پیامکی، باج افزار، و دزدی پیچیده ارزهای دیجیتال و موارد پولشویی تحقیق می کند.

منابع

آن حمله فیشینگ را متوقف کنید: https://www.sans.org/security-awareness-training/resources/stop-phish
حملات مهندسی اجتماعی: https://www.sans.org/newsletters/ouch/social-engineering-attacks
Vishing-حملات تماس تلفنی و کلاهبرداری: https://www.sans.org/newsletters/ouch/vishing

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو