سه روشی که مهاجمان سایبری شما را هدف قرار میدهند

مقدمه

حملات مهندسی اجتماعی، که در آن دشمنان افراد را فریب می دهند تا کاری را که نباید انجام دهند، یکی از رایج ترین روش هایی است که مهاجمان سایبری برای هدف قرار دادن افراد استفاده می کنند. این مفهوم هزاران سال است که توسط کلاهبرداران و فریبکاران استفاده شده است. چیزی که جدید است این میباشد که اینترنت این را برای یک مجرم سایبری در هر نقطه از جهان بسیار آسان می کند تا خود را به جای هر کسی که می خواهد جا زده و هر کسی را که می خواهد هدف قرار دهد. در زیر سه نوع متداول از روش های مهندسی اجتماعی که مهاجمان سایبری برای درگیر کردن و فریب شما از آنها استفاده می کنند، آورده شده است.

حملات فیشینگ

فیشینگ سنتی ترین حمله مهندسی اجتماعی است. زمانی است که مهاجمان سایبری برای شما ایمیلی ارسال می کنند و سعی می کنند شما را فریب دهند تا اقدامی را انجام دهید که نباید انجام دهید. در ابتدا فیشینگ نامیده می شد زیرا مانند ماهیگیری در یک دریاچه بود: شما یک طعمه و قلاب انداخته اید اما نمی دانستید ممکن است چه چیزی را بگیرید. استراتژی پشت این تاکتیک این بود که هر چه مجرمان سایبری ایمیل های فیشینگ بیشتری ارسال کنند، افراد بیشتری قربانی می شدند. حملات فیشینگ امروزی بسیار پیچیده‌تر و هدفمندتر شده‌اند (که گاهی اوقات به آن فیشینگ نیزه می‌گویند)، و مهاجمان سایبری اغلب ایمیل‌های فیشینگ خود را قبل از ارسال سفارشی می‌کنند.

اس ام اس فیشینگ (اسمیشینگ)

Smishing اساساً فیشینگ مبتنی بر پیامک است که در آن به جای ایمیل یک پیام متنی ارسال می شود. مهاجمان سایبری در برنامه هایی مانند Google Messages، iMessage یا WhatsApp پیام های متنی به گوشی شما ارسال می کنند. دلایل مختلفی وجود دارد که چرا smishing محبوب شده است. اولین مورد این است که فیلتر کردن حملات پیام رسانی بسیار دشوارتر از فیلتر کردن حملات ایمیل است. دوم، پیام‌هایی که مهاجمان سایبری ارسال می‌کنند اغلب بسیار کوتاه هستند، به این معنی که دلایل بسیار کمی وجود دارد و تشخیص قانونی بودن یا نبودن پیام را بسیار سخت‌تر می‌کند. سوم، پیام‌رسانی اغلب غیررسمی‌تر و مبتنی بر عمل است، بنابراین مردم عادت دارند سریع به پیام‌ها پاسخ دهند یا بر اساس آن عمل کنند. در نهایت، مردم در شناسایی حملات ایمیل های فیشینگ بهتر و بهتر می شوند، بنابراین مهاجمان سایبری به سادگی به سمت یک روش جدید، پیام رسانی می روند.

حملات تلفنی(ویشینگ)

Vishing یا فیشینگ مبتنی بر صدا تاکتیکی است که از تماس تلفنی یا پیام صوتی به جای ایمیل یا پیام متنی استفاده می کند. حملات Vishing زمان بسیار بیشتری را برای اجرای مهاجم نیاز دارد، زیرا آنها مستقیماً با قربانی صحبت می کنند و با آن تعامل دارند. با این حال، این نوع حملات نیز بسیار مؤثرتر هستند، زیرا ایجاد احساسات قوی از طریق تلفن، مانند احساس فوریت، بسیار آسان تر است. هنگامی که یک مهاجم سایبری با شما تماس تلفنی برقرار می کند، تا زمانی که به خواسته خود نرسیده باشد، اجازه نمی دهد از تلفن خارج شوید.

شناسایی و جلوگیری از این مدل حملات

خوشبختانه، مهم نیست که مهاجمان سایبری از کدام یک از سه روش استفاده می‌کنند، سرنخ‌های رایجی وجود دارد که می‌توانید آنها را شناسایی :

- اضطراری: هر پیامی که احساس فوریت فوق العاده ای ایجاد می کند که در آن مهاجمان سعی می کنند شما را مجبور به اقدامی سریع و اشتباه کنند. به عنوان مثال، پیامی است که ادعا می کند از طرف دولت است، مبنی بر اینکه مالیات شما به تاخیر افتاده است و اگر فوراً پرداخت نکنید در نهایت به زندان خواهید افتاد.

- فشار:هر پیامی که یک کارمند را برای نادیده گرفتن یا دور زدن سیاست ها و رویه های امنیتی شرکت تحت فشار قرار دهد.

- کنجکاوی: هر پیامی که مقدار زیادی کنجکاوی ایجاد می کند یا به نظر می رسد بیش از حد خوب است که واقعی و درست باشد، مانند یک بسته UPS تحویل نشده یا اطلاعیه ای مبنی بر اینکه شما بازپرداخت آمازون را دریافت می کنید.

- لحن: هر پیامی که به نظر می‌رسد از طرف شخصی که می‌شناسید، مانند یک همکار، می‌آید، اما جمله‌بندی شبیه آنها نیست، یا لحن کلی یا امضای آن اشتباه است.

- اطلاعات حساس هر پیامی که اطلاعات بسیار حساسی مانند رمز عبور یا کارت اعتباری شما را درخواست کند.

- عمومی: پیامی که از یک سازمان قابل اعتماد می‌آید اما از یک سلام عمومی مانند «مشتری عزیز» استفاده می‌کند. اگر آمازون بسته ای برای شما دارد یا خدمات تلفنی مشکلی در قبض دارد، نام شما را می دانند.

- آدرس ایمیل شخصی: هر ایمیلی که به نظر می رسد از طرف یک سازمان، فروشنده یا همکار قانونی است، اما از یک آدرس ایمیل شخصی مانند gmail.com@ یا hotmail.com@ استفاده می کند.

با جست‌وجوی این سرنخ‌های رایج، می‌توانید راه طولانی را برای محافظت از خود پیش ببرید.

سردبیر مهمان

مری جین سوارز پارتین مدیر برنامه زنان در امنیت سایبری (WiCyS) است. تمرکز نقش او فراهم کردن منابع، ابتکارات و برنامه‌های طراحی شده برای جذب، حفظ و پیشرفت زنان در زمینه امنیت سایبری است. او مشتاق ایجاد محیطی فراگیر است که در آن همه احساس ارزشمندی، استقبال و دیده شدن کنند.

منابع

جلوی حملات تماس تلفنی فریبکارانه را بگیرید: https://www.sans.org/newsletters/ouch/stop-phone-call-scams
حملات فیشینگ فریبکارانه تر میشوند: /https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier
محرکهای احساسی: چگونه مهاجمان سایبری شما را فریب میدهند: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
من هک شده ام،حالا چکار کنم؟: /https://www.sans.org/newsletters/ouch/im-hacked-now-what

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو