حمله فیشینگ سنتی را فراموش کنید، زمان ترس از والینگ است

والینگ: نسل جدیدی از حملات سایبری!

در دنیای امنیت اطلاعات، همیشه قاعده‌ای کلی وجود دارد. شرکتی امنیتی، یک مکانیزم امنیتی می‌سازد و چندی بعد مجرمان سایبری ابزاری برای گذر از این مکانیزم امنیتی طراحی می‌کنند. شاید در گذشته درباره فیشینگ، فیشینگ قلاب‌دار و راه‌های مختلفی که هکرها با استفاده از آن‌ها کاربران را فریب می‌دادند، مطالب زیادی خوانده باشید. حملات فیشینگ قدمتی بسیار طولانی دارند و مجرمان خیلی پیش‌تر از آنکه کامپیوترها پا به عرصه ظهور نهند، از این مدل حملات استفاده می‌کردند.

اما به نظر می‌رسد اکنون دیگر زمان حملات فیشینگ سنتی به سر رسیده است و باید در انتظار حملات والینگ و دیگر مکانیزم‌های پیچیده مهندسی اجتماعی باشید که در نزدیکی شما قرار دارند. اما پرسش اصلی این است که اساساً والینگ چیست و چرا خطرناک‌تر از فیشینگ سنتی است. در این مقاله به واکاوی این مدل از حملات خواهیم پرداخت.

هکرها در حال ساخت قایق بزرگ‌تری هستند

بدون اغراق می‌توان گفت تنها زمانی از وجود این چنین حملاتی آگاه خواهید شد که با تمامی روش‌های مهندسی اجتماعی که در آن کلاهبرداران آنلاین از ایمیل‌ها، تماس‌های تلفنی، پیام‌های فوری و حتی چاپ سنتی از طریق دستگاه فکس کلاهبرداری‌های می‌کنند، آشنا باشید. روش‌های مهندسی اجتماعی جدید، به مجرمان سایبری حیات تازه‌ای بخشیده‌اند. امروزه، آنلاین بودن برای بسیاری از افراد و سازمان‌های بزرگ چالش سختی محسوب می‌شود؛ در بسیاری از کسب‌وکارها حتی اختلالی چنددقیقه‌ای ممکن است خسارات زیادی به همراه آورد. مکانیزم حمله فیشینگ عمدتاً بر شهرت و نام تجاری سازمان‌ها، مشاغل شخصی و سودهای مالی شرکت‌ها و سازمان‌ها تأثیرگذار است. مجرمان سایبری به دو دلیل در این مدل حملات قدرتمند ظاهر می‌شوند. اول آنکه به حساب‌های ایمیلی که در معرض خطر قرار گرفته‌اند، دسترسی پیدا کرده‌اند و دوم آنکه موفق شده‌اند به کانال‌های شغلی معتبر و قانونی دست پیدا کنند. هدف اصلی مجرمان سایبری در این مدل حملات، فریب دادن متخصصان است.

[illegible].

والینگ چه حرف تازه‌ای برای گفتن دارد؟

به نظر می‌رسد حملات فیشینگ سنتی، هر ترفندی را که هکر نیاز دارد، در اختیارش قرار داده است. پس چرا باید از والینگ واهمه داشته باشیم؟ به‌تازگی اخباری منتشر شده است که نشان می‌دهد در سبک جدیدی از حملات، هکرها نیازی ندارند که کاربران روی لینک‌های آلوده کلیک کرده یا نرم‌افزارهای مخرب را اجرا کنند. در عوض، برای اولین

بار مجرمان سایبری سیستم‌های آنلاین را به‌طور گسترده تحت نظارت قرار داده‌اند. این کار با هدف به دست آوردن اعتبار اینترنتی مورد نیاز هکرها انجام می‌شود. بعد از به دست آوردن این اعتبار، هکرها به سراغ کاربران نهایی می‌روند که ارزش زیادی دارند. آن‌ها کاربران سطح بالا را مجاب می‌کنند که مدیرعامل شرکت ایمیلی برایشان ارسال کرده و به این شکل آن‌ها را متقاعد می‌سازند که باید وجه مورد نیاز مدیرعامل را برای او انتقال داده یا اجازه یک معامله را بدهند.

مطلب پیشنهادی

مقابله با حملات DDoS و فیشینگ
دو پروژه‌ای که امنیت شبکه ملی اطلاعات را تضمین می‌کنند!

بر خلاف فیشینگ سنتی که ایمیل‌هایی با آدرس‌های فریبنده برای قربانیان ارسال می‌کند، در والینگ هکرها به دنبال اعتبار هستند. این اعتبار از هر ابزار دیگری قدرتمندتر است. این موضوع را با ذکر یک نمونه واقعی تشریح می‌کنیم.
داستان مربوط به شرکت «Alpha Payroll» است. کاربری چندی پیش فریب درخواستی را خورده بوده که در ظاهر این چنین بود که مدیرعامل شرکت برای او ایمیلی ارسال کرده است. متن ایمیلی که برای کاربر ارسال شده بود، به این شکل بود: «تهیه یک نسخه کپی از تمامی فرم‌های W-2 2015 که شرکت Alpha Payroll تولید کرده، بر عهده مشتریان این شرکت است.»

کالبد شکافی یک پیام

ایمیل ارسال‌شده به ظاهر درست است و هیچ‌گونه نشانه‌ای از یک حمله در آن به چشم نمی‌خورد. اما جزئیات فنی چه می‌گویند؟ بعد از دریافت این ایمیل، در روز هشتم آوریل، بعد از آنکه یکی از مشتریان این شرکت گزارش داد کارمندان آن‌ها اظهارنامه‌های مالیاتی جعلی را با شماره تأمین اجتماعی آن‌ها به ثبت رسانده‌اند، یک سلسله تحقیقات داخلی صورت گرفت که خبر از فیشینگ موفقی می‌داد. تعدادی از کارشناسان گزارش دادند که یک مکانیزم داخلی برای به اشتراک‌گذاری اطلاعات W-2 در داخل مجموعه به فعالیت مشغول است که می‌تواند دلیلی برای پیاده‌سازی این حمله باشد. متأسفانه در این حادثه شرکت Alpha Payroll کارمند قربانی خود را اخراج کرد! کریس توماس، کارشناس امنیتی در این باره گفت: «اگر قرار باشد هر کارمند قربانی فیشینگ را اخراج کنید، در مدت زمان کوتاهی هیچ کارمندی وجود نخواهد داشت.» متن کامل این داستان را در این **آدرس** مطالعه کنید.

نهادهای امنیتی هشدار می‌دهند

در آوریل سال جاری میلادی، «Phoenix Division» که یکی از واحدهای مبارزه با جرایم سایبری در پلیس فدرال است، به‌طور رسمی به سازمان‌ها و مشاغل بزرگ درباره رشد چشمگیر کلاه‌برداری و سوءاستفاده از ایمیل‌های BEC، سرنام Business Email Compromise، هشدار داد.
Phoenix Division در بخشی از گزارش خود آورده است: «کلاه‌برداران و مجرمان سایبری مترصد فرصتی هستند تا ایمیل‌های شرکت‌ها را جعل کنند یا با استفاده از روش‌های مهندسی اجتماعی اطلاعات مربوط به هویت مدیرعامل، وکیل شرکت یا فروشندگان قابل اعتماد را به سرقت ببرند یا جعل کنند. این مجرمان سایبری عمدتاً به دنبال کارمندانی هستند که در بخش‌های مالی به فعالیت اشتغال داشته و وظیفه نقل و انتقال پول شرکت‌ها را بر عهده دارند. آن‌ها به شیوه‌ای کاملاً حرفه‌ای و هماهنگ با ادبیات شرکت هدف، با افراد شاغل در بخش مالی به صحبت می‌پردازند و در ادامه به نقل و انتقال غیرقانونی پول‌ها مبادرت می‌ورزند. در حال حاضر چند مدل مختلف از این چنین کلاه‌برداری‌هایی شناسایی شده است. قربانیان این چنین حملاتی را شرکت‌های بزرگ، شرکت‌های فعال در حوزه فناوری، استارت‌آپ‌های کوچک و سازمان‌های غیرانتفاعی تشکیل می‌دهند. در بیشتر مواقع مجرمان سایبری شرکت‌هایی را به عنوان هدف خود انتخاب می‌کنند که با تأمین‌کنندگان خارجی در ارتباط هستند یا به‌طور روزانه تراکنش‌های مالی را انجام می‌دهند.

است. این مکانیزم حمله بر مبنای جعل هویت مدیرعامل، وکیل شرکت یا فروشنده معتبر عمل می‌کند. این مکانیزم حمله هم به صورت برون‌سازمانی و هم به صورت درون‌سازمانی انجام می‌گیرد. در حالت درون‌سازمانی اطلاعات از سوی افراد داخل شرکت که به بسیاری از منابع دسترسی دارند، برای هکرها فرستاده می‌شود.

سازمان‌ها در برابر این مدل حملات چه تدابیری باید اتخاذ کنند؟

پیشنهاد می‌کنیم در برابر حملات والینگ به این نکات توجه کنید:

1. به کارکنان خود آموزش‌های امنیتی لازم را ارائه کنید و به آن‌ها هشدار دهید: همواره به دنبال برنامه آموزشی هوشمند و به‌روز در زمینه حملات سایبری باشید. این برنامه آموزشی باید این ظرفیت را داشته باشد تا انواع مختلفی از حملات فیشنگ را شناسایی کند.

2. والینگ و مکانیزم‌های جدید مهندسی معکوس را برای کارکنان خود تشریح کنید: در حملات والینگ سعی کنید به غیر از مسئولان ارشد، به کارکنان سطوح پایین نیز آموزش‌های لازم را ارائه دهید. کارکنان پایین‌مرتبه همواره با مشاهده ایمیلی که از طرف مدیرعامل ارسال شده است، این‌گونه استنباط می‌کنند که مدیرشان کاری را از آن‌ها درخواست کرده است که باید در اسرع وقت انجام دهند.

3. همواره فرایندهایی را که مربوط به نقل‌وانتقال وجوه و دیگر تراکنش‌های مالی در جریان هستند، بررسی کنید: پیوسته به این نکته توجه کنید که ممکن است خطر درون خود سازمان باشد. در نتیجه سعی کنید نقاطی را که در زمینه تراکنش‌های برون‌سازمانی فعالیت می‌کنند، به دقت بررسی کنید.

4. با گروه واکنش سریع سازمان خود در تعامل باشید: همواره سعی کنید به صورت دوره‌ای با اعضای گروه واکنش سریع امنیتی سازمان خود، مانورهای تمرینی انجام دهید. گلوگاه‌هایی را که آسیب‌پذیر به نظر می‌رسند، با روش مهندسی معکوس آزمایش کنید. در این حالت بهتر است کارکنان خود را با حملات فیشینگی که خود ترتیب داده‌اید، آزمایش کنید. در این مانور ضمن آنکه تکنیک‌های کلیک روی لینک‌ها یا بازدید سایت‌های متفرقه کارکنان خود را آزمایش می‌کنید، سعی کنید از تکنیک‌های ترکیبی نیز استفاده کنید. برای مثال از کارکنان خود سؤال کنید: «اگر هکر بودید سعی می‌کردید با چه روشی به اطلاعات دست پیدا کنید؟»

==========

شاید به این مقالات هم علاقمند باشید:

بدافزار Nymaim همچنان قربانی می‌گیرد + راه‌حل

بانک‌های عضو شبکه «سوئیفت» هک شدند

نه فرمان خطرناک لینوکس که هرگز نباید اجرا شوند!

سیگنال‌های وای‌فای از روی دست شما تقلب می‌کنند!

چگونه برای خودمان امضای دیجیتالی بسازیم؟

روبات خانگی سونی رقیب جدی اکو آمازون است!

چگونه پریزهای خانگی در معرض حملات هکری قرار می‌گیرند؟

مجرمان سایبری حملات فیشینگ را سازمان‌دهی می‌کنند!

تاریخ انتشار:

23 شهریور 1395

نشانی منبع: https://www.shabakeh-mag.com/security/4534