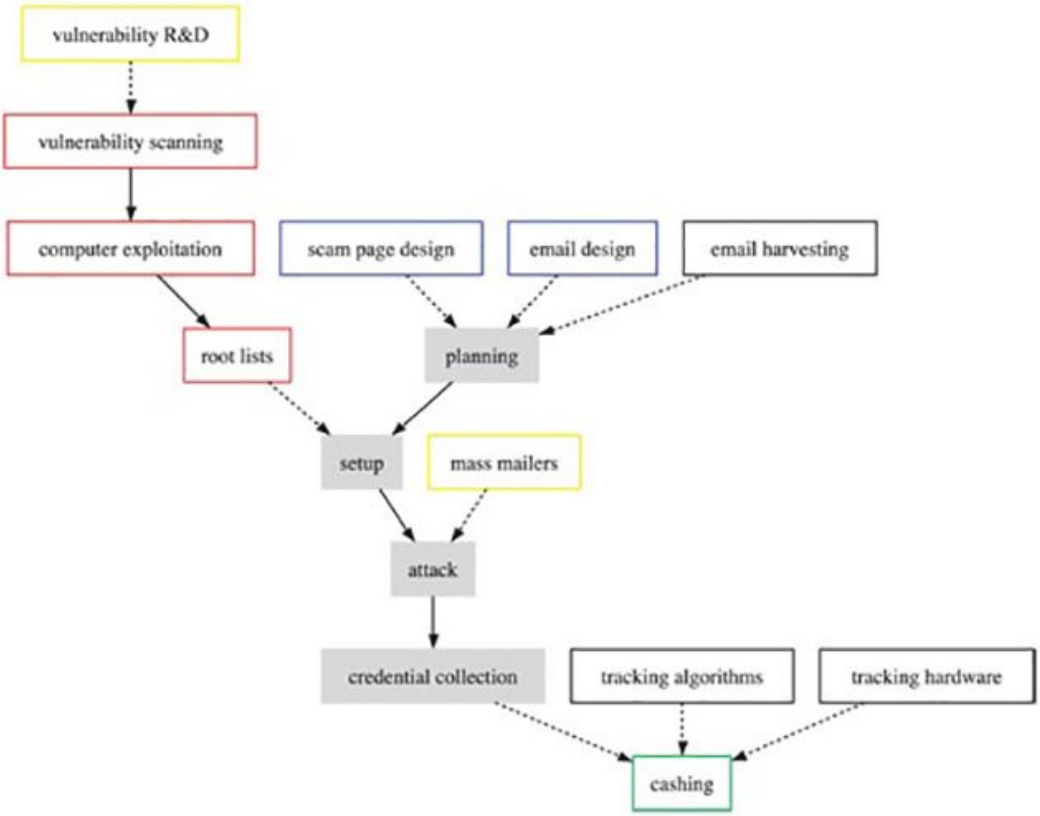
به لینک‌های درون ایمیل‌ها اعتماد نکنید!

آشنایی با حملات فیشینگ قلاب‌دار

فیشینگ گونه‌ای از حملات کامپیوتری است که با هدف دسترسی به حساب‌ها و اطلاعات حساس مورد استفاده قرار می‌گیرد. اما فیشینگ قلاب‌دار (Phishing Spear) نوع پیچیده‌تری از فیشینگ است که برای نفوذ به مراکز حساس و دسترسی به اطلاعات مهم مورد استفاده قرار می‌گیرد. حتی کارمندان شرکت‌های امنیتی نیز در خطر به دام افتادن در دام این مدل از حملات قرار دارند.

آیا دپارتمان فناوری‌اطلاعات شرکت به شما درباره کلیک نکردن روی لینک‌های مشکوکی که درون ایمیل‌ها قرار دارد هشدار می‌دهد؟ حتی زمانی‌که ایمیل از یک منبع رسمی ارسال شده و حاوی یک ویدیوی جالب بوده یا ایمیل از سوی منبعی ارسال شده است که به طور کامل به آن اعتماد دارید؟ اگر لینک مشکوک است، کلیک نکنید. زیرا این ایمیل‌ها اغلب در زمینه کلاهبرداری ارسال می‌شوند تا شما را برای کلیک روی یک ضمیمه مخرب فریب داده یا به مشاهده یک سایت مخرب ترغیب کنند. به نظر سایت متعلق به یک بانک یا سایت مربوط به یک دامنه ایمیلی باشد که برای فریب کاربر به افشای اطلاعات حساس از قبیل نام‌کاربری، گذرواژه یا اطلاعات حساب بانکی مورد استفاده قرار گرفته و به سادگی و در اختفای کامل بدافزارها را روی سیستم قربانی قرار می‌دهند.

ایمیل‌ها و اتاق‌های گفت‌وگو از اصلی‌ترین منابع مورد استفاده برای حملات فیشینگ به شمار می‌روند. کافی است از کارمندان مراکز حساس دولتی سوال کنید چه کسی روی ایمیل فیشینگ که به ظاهر از طرف وزرات امورخارجه ارسال شده بود و به هکرها اجازه داد به داخل چند شبکه دولتی نفوذ کنند، کلیک کرد. فیشینگ قلاب‌دار برای اهدافی بزرگ‌تر از یک فیشینگ معمولی مورد استفاده قرار می‌گیرد. در حالی‌که فیشینگ معمولی اساسا شامل ایمیل‌های مخربی است که به طور اتفاقی برای حساب‌های ایمیل ارسال می‌شود، ایمیل‌های فیشینگ قلاب‌دار به گونه‌ای طراحی شده‌اند که نشان می‌دهند از طرف شخصی ارسال شده‌اند که گیرنده او را می‌شناسد و به او اعتماد دارد؛ یک همکار، مدیر تجاری یا بخش منابع انسانی از بارزترین سمبل‌های مورد استفاده در این ایمیل‌ها هستند. این ایمیل‌ها حتی می‌توانند شامل یک خط یا یک محتوایی باشند که به طور ویژه روی منافع یا صنعتی که برای هکر شناخته شده است تمرکز دارد. برای قربانیانی که ارزش بیشتری برای هکرها دارند، هکرها ممکن است انواع مختلف حساب‌هایی که شخص روی شبکه‌های اجتماعی دارد را مورد مطالعه قرار دهند، تا اطلاعات مورد نیاز درباره قربانی یا قربانیان را به دست آورده؛ نام مناسبی که قربانی یا قربانیان به آن‌ها اعتماد دارند را انتخاب کرده یا در مجموعه رفتاری که موضوعات مورد علاقه قربانی بوده جست‌وجو کرده تا به آسانی بتوانند اعتماد قربانی را جلب کرده و او را فریب دهند.



در برآوردی که به تازگی صورت گرفته است، 91 درصد از حملات هک با یک فیشینگ یا یک فیشینگ قلاب‌دار روی ایمیل‌ها انجام می‌شود. اگرچه دیوارهای آتش و دیگر محصولات امنیتی پیرامون یک شبکه کامپیوتری قرار گرفته و برای جلوگیری از ورود هر نوع ترافیک مخرب به شبکه‌های کامپیوتری به طور مثال از طریق پورت‌های آسیب‌پذیر عمل می‌کنند، اما ایمیل‌ها حالت قانونی داشته و به ترافیک روی آن‌ها اعتماد می‌شود و از این رو اجازه داده می‌شود به شبکه وارد شوند. سیستم‌های فیلتر کردن ایمیل‌ها می‌توانند تعدادی از این تلاش‌های فیشینگ را شناسایی کرده و دفع کنند، اما امکان شناسایی و دفع همه آن‌ها را ندارند. حملات فیشینگ در بیشتر موارد موفقیت‌آمیز هستند، به دلیل این‌که کارمندان روی ایمیل‌هایی که مشکوک بودن آن‌ها قطعی است، باز هم با وجود هشدارهایی که با کلیک کردن روی آن‌ها مشاهده می‌کنند، کلیک می‌کنند (به عبارت دیگر می‌توان این نوع حملات را متأثر از یک مهندسی اجتماعی تعبیر کرد).

یکی از شناخته شده‌ترین این موارد، به حمله فیشینگ قلاب‌داری که با وجود ماهیت مشکوک بودن موفق شد در سال 2011 شرکت امنیتی RSA را مورد حمله قرار دهد باز می‌گردد. هکرها دو ایمیل فیشینگ قلاب‌دار متفاوت را برای چهار کارمند شرکت اصلی EMC ارسال کردند. ایمیل‌ها شامل یک فایل مخرب به نام Recruitment 2011 plan.xls بود که در اصل اکسپلویت zero-day بود. زمانی‌که یکی از این چهار دریافت‌کننده روی ضمیمه کلیک می‌کردند، اکسپلویت ضمیمه شده حمله خود را بر اساس یک آسیب‌پذیری موجود در نرم‌افزار ادوبی فلش که یک در پشتی در سیستم قربانی ایجاد می‌کرد، انجام می‌داد. RSA در وبلاگ خود درباره این حمله نوشت: « ایمیل به اندازه کافی برای گمراه کردن یکی از این چهار کارمند برای باز کردن پوشه Junk فریبنده بود تا فایل اکسل آلوده را باز کند.» در پشتی به حمله‌کننده‌ها یک جای پا برای این‌که نقشه راهی برای سیستم‌هایی که ارزش بیشتری دارند را ارائه می‌کرد. این حمله غافلگیر کننده با موفقیت انجام شد و اطلاعات مربوط به فناوری رمز SecureID و اطلاعات مربوط به رمزهای SecureID کاربران را به سرقت برد. حمله همه را شوکه کرد، زیرا همه تصور می‌کردند که مقام‌های ارشد RSA برای آموزش کارکنان در زمینه ایمیل‌های مشکوک آن‌را ارسال کرده است. حتی یکی از کارمندان نه تنها ایمیل مشکوک را باز کرد، بلکه آن‌را از پوشه زباله‌ها بازیابی کرد و بعد از آن فیلتر ایمیل خود را برای این منظور مورد بازبینی قرار داد. شدت حمله به قدری پر اهمیت بود که لوک‌هد مارتین، پیمانکار حوزه دفاع در آن زمان اعلام کرد عامل حمله به شبکه‌اش داده‌های محرمانه‌ای بودند که هکرها بعد از نفوذ به RSA آن‌ها را به دست آورده بودند.

یکی دیگر از قربانیان شگفت‌آور حملات فیشینگ قلاب‌دار آزمایشگاه ملی اوک ریج در ایالت تنسی بود. این آزمایشگاه در سال 2011 مورد یک حمله هکری قرار گرفت. در آن سال یک ایمیل فیشینگ که به نظر می‌رسید از بخش منابع انسانی ارسال شده و شامل یک لینک به یک صفحه وب است؛ جایی‌که بدافزار مخرب در آن قرار داشت و این‌گونه سیستم قربانیان را مورد حمله قرار داد. هکرها ایمیل‌هایی را به 530 نفر از 5 هزار کارمند آزمایشگاه ارسال کردند و 57 نفر از آن‌ها روی لینک مخرب درون ایمیل کلیک کردند. اما تنها دو ماشین با این بدافزار آلوده شدند، اما همین دو مورد برای ورود هکرها به درون شبکه آزمایشگاه کافی بود. آن‌ها زمانی از وجود این حمله مطلع شدند که مدیرشبکه اعلام کرد چندین مگابایت از داده‌های شبکه آزمایشگاه به سرقت رفته است. این هک همه را شوکه کرده بود زیرا آزمایشگاه فدرال با سطح امنیت بالا در زمینه انرژی‌های طبقه‌بندی شده کار می‌کند. این آزمایشگاه از قضا همچنین تحقیقاتی در زمینه امنیت سایبری را در دستور کار خود دارد که در میان این موارد تحقیقات مربوط به حملات فیشینگ نیز قرار داشتند.

تاریخ انتشار:

24 فروردین 1394

نشانی منبع: https://www.shabakeh-mag.com/security/526