تیتر جام جم
۲
ویژه‌نامه حوادث روزنامه جام جم
چهارشنبه ۴ خرداد ۱۴۰۱ ● شماره ۹۷۰
هوش سیاه

رونمایی از شگردهای مجرمان مجازی

مجید غمخوار
تپش

تا چندی قبل مجرمان به‌صورت سنتی دست به سرقت و کلاهبرداری می‌زدند و بیشترین شکایت مردم از جرایم خرد مانند جیب‌بری و زورگیری بود، اما رفته‌رفته با پیشرفت تکنولوژی و استفاده روزافزون مردم از فضای مجازی و گسترش اینترنت، مجرمان کسب‌وکار مجرمانه‌شان را به این فضا انتقال دادند. با حضور مجرمان در فضای اینترنت، جرایم نوظهور اینترنتی به‌وجود آمد و این افراد که به دزدان پنهان مشهور شدند، هر روز بعد از لو رفتن یک شگرد خود به شگردی جدیدتر رو آورده و حساب بانکی قربانیان را خالی می‌کنند. دو هفته قبل دلیل کوچ مجرمان به این فضا را بررسی کردیم و امروز از مهم‌ترین شگردهای آنها برای اجرای نقشه مجرمانه‌شان رونمایی خواهیم کرد.

تله‌گذاری؛ از اولین جرایم رایانه‌ای

یکی از اولین جرایم رایانه‌ای که هنوز هم با گذشت سالیان طولانی گاهی افرادی را قربانی خود می‌کند، فیشینگ است. در این روش مجرمان مجازی با طراحی سایت‌های مشابه سایت اصلی با کمترین تغییر، وقتی فردی برای پرداخت اینترنتی اقدام می‌کند او را با خطای عملیات پرداخت روبه‌رو می‌کنند. این درحالی است که از آن سو

مجرمان فیشینگ به تمامی اطلاعات او دسترسی پیدا کرده و به‌راحتی دقایقی بعد حساب او را خالی می‌کنند. این روش تا قبل از یک بار مصرف کردن رمزهای اینترنتی اصلی‌ترین روش کلاهبرداری اینترنتی بود. البته هنوز هم هستند شهروندانی که قربانی فیشینگ می‌شوند و با یک کلیک اشتباه پول‌های خود را از دست می‌دهند. تنها راه جلوگیری از گرفتار نشدن در دام کلاهبرداران فیشینگ رعایت پروتکل http و واردکردن سایت مورد نظر به‌صورت دستی از سوی خود افراد است. البته ما یک روش دیگر را به شما آموزش می‌دهیم. هنگام ورود اطلاعات، یکی از موارد را اشتباه وارد کنید. اگر همه نکات را رعایت کرده و با خطای ورود اشتباه اطلاعات روبه‌رو شدید، با خیال راحت‌تری می‌توانید عملیات بانکی را انجام دهید. اگر شک کردید که در دام مجرمان فیشینگ گرفتار شده‌اید، سریع رمز خود را تغییر دهید.

کلاهبرداری نیجریه‌ای

در این روش که در اواسط دهه ۹۰ بسیار باب بود، فقط تجار و مدیران شرکت‌ها، طعمه کلاهبرداران بودند. این روش اولین بار از سوی اتباع نیجریه انجام شد و به همین دلیل به کلاهبرداری نیجریه‌ای معروف شد. مجرمان اینترنتی در این روش با شناسایی تجار و شرکت‌های بزرگ و دسترسی به ایمیل آنها، با تغییرات کوچک در آدرس شرکت‌هایی که با آنها مشغول داد‌وستد هستند، خودشان را نماینده شرکت معرفی و با اعلام شماره حساب جدید، از آنها می‌خواهند معاملات با شماره حساب بانکی جدید انجام شود.

البته در این روش هم با یک اقدام ساده می‌توان از سرقت هزاران دلار سرمایه جلوگیری کرد. برای ارسال ایمیل باید به‌صورت دستی آدرس ایمیل را وارد کرده و به‌هیچ‌وجه نباید پاسخ ایمیل را با گزینه ریپلای داد و بهتر است اگر به ایمیلی مشکوک شدید، برای جواب دادن آدرس ایمیل را به‌صورت دستی وارد کنید.

دستگاه سرقت اطلاعات و خریدهای میلیونی

یکی دیگر از روش‌های مورد اقبال کلاهبرداران، اسکیمر است. در این روش، مجرمان با قرار دادن قطعه‌ای به نام اسکیمر، کارت‌بانکی را کپی کرده و به‌آسانی به تمام اطلاعات کارت دسترسی پیدا می‌کنند و بعد از این‌که خودتان رمز را به فرد می‌گویید، اجازه می‌دهید تا آنها هم کارت‌بانکی شما را داشته باشند.

مجرمان اسکیمری که بیشتر در پوشش دستفروش کنار خیابان ظاهر می‌شوند، بعد از کپی‌کردن اطلاعات بانکی آنها را روی کارتی خام پیاده کرده و بعد با دانستن رمز اول که خودتان گفته‌اید، با کارت‌تان شروع به خرید طلا و اقلام باارزش می‌کنند. تنها راه گرفتار نشدن در دام اسکیمری‌ها این است که همیشه خودتان رمز کارت را وارد کنید و اجازه ندهید کسی رمز را مشاهده کند یا بفهمد. اگر همه اطلاعات کارت در اختیار مجرمان باشد تا زمانی که رمز اول را ندانند، امکان برداشت از حساب را ندارند.

شگردی نخ‌نما اما پرسود

اواخر دهه ۸۰ روش برنده‌شدن در قرعه‌کشی و کشاندن افراد پای دستگاه به قدری فراگیر شد که پلیس با ساخت برنامه و هشدارهای روزانه قصد داشت از گرفتارشدن مردم با این روش جلوگیری کند. در این روش، مجرمان که اغلب آنها در زندان بودند با طعمه‌های خود تماس گرفته و به بهانه این‌که در قرعه‌کشی برنامه‌های صداوسیما یا شرکت‌های بزرگ برنده شده‌اید افراد را پای دستگاه عابربانک می‌کشاندند تا جایزه خود را دریافت کنند اما با چرب‌زبانی و تغییر زبان دستگاه، به‌جای این‌که پولی به حساب افراد ساده لوح بیاید، پول از حساب آنها خارج و به حساب کلاهبرداران واریز می‌شد.

با هشدارهای پلیس بالاخره این روش در حال فراموشی بود اما بازهم کلاهبرداران تلفنی با ورود شبکه‌های اجتماعی این روش را احیا و این‌بار به اسم اپراتورهای تلفن‌همراه و صداوسیما از واتساپ با قربانیان خود تماس گرفته و با صحنه‌سازی وانمود می‌کنند آنها برنده مسابقه یا قرعه‌کشی کالایی شده و به بهانه واریز جایزه طعمه را سرکیسه می‌کنند.

تنها راه گرفتارنشدن در دام این مجرمان این است که بدانیم برای دریافت جایزه یا واریز پول به حساب‌مان نباید به عابربانک مراجعه کنیم و تنها کافی است شماره‌کارت را بدهیم. اگر کسی از ما خواست برای دریافت جایزه پای دستگاه عابربانک برویم یا اطلاعات کارت را در اختیارش بگذاریم کلاهبردار است و نباید این اقدامات را انجام دهیم.

پیامک‌های حاوی بدافزار

مدتی است با گسترش استفاده از فضای مجازی و دولت‌الکترونیک، کلاهبرداران به این فکر افتادند که از این فضا استفاده کرده و با روش‌های جدید مردم را نقره‌داغ کنند. در جدیدترین روش کلاهبرداری افراد با ارسال پیامک‌های حاوی بدافزار اقدام به کسب اطلاعات بانکی افراد و اطلاعات گوشی آنها کرده و کلاهبرداری می‌کنند. در این روش که بیشتر با نام سامانه ثنای قوه قضاییه انجام می‌شود افراد لینکی حاوی آدرس اشتباه و بدافزار را برای افراد پیامک کرده و فرد بعد از کلیک روی لینک گرفتار بدافزار و مجرمان اینترنتی می‌شود.

در این روش افراد به بهانه مشاهده سامانه ثنا، اطلاعات بانکی افراد را سرقت و حساب‌شان را خالی می‌کنند.

بارها از سوی پلیس فتا و قوه قضاییه اعلام شده است که ابلاغیه‌های قضایی به‌هیچ‌عنوان با شماره‌های شخصی ارسال نمی‌شود و تنها با سرشماره‌هایی که آن‌هم عنوان دارد ارسال می‌شود و اگر لینکی با شماره‌های شخصی یا پیامک تبلیغاتی برایتان ارسال شد بدانید کلاهبرداری است و افراد می‌خواهند حساب‌تان را خالی کنند.