خبرنامه مدیریتی سراج
مرکز نرم‌افزار و سرویس وخدمات سازمان فضای مجازی سراج

اخبار فناوری اطلاعات و ارتباطات

۹۳

هفته نامه | سال دوم | شماره نود و سوم | ۲۳ بهمن ۱۳۹۵

درخواست FBI از گوگل: داده‌های موجود بر روی کارگزارهای خارجی را در اختیار ما قرار دهید

در دنیای کنونی که نظارت‌های مختلفی توسط کشور آمریکا و نهادها و سازمان‌های اطلاعاتی در حال انجام است، بسیاری از کشورها از شرکت‌های فناوری مانند گوگل، مایکروسافت و اپل درخواست کرده‌اند تا کارگزارهای خود را به داخل این کشورها منتقل کنند. این درخواست‌ها برای حفاظت بیشتر از داده‌های شهروندان در داخل مرزهای این کشورها بوده است.

سال گذشته مایکروسافت توانست FBI و نهادهای دولتی آمریکا را در دادگاهی شکست دهد. مایکروسافت اعلام کرد این سازمان‌ها نمی‌توانند شرکت‌های فناوری را مجبور کنند که کارگزارهای متعلق به کاربران غیرآمریکایی را تحت نظر آن‌ها نگهداری و ذخیره کنند. با این حال، این دادخواست دولت فدرال آمریکا و FBI نگرانی‌هایی را درخصوص حریم خصوصی کاربران به‌وجود می‌آورد.

یک دادرس آمریکایی روز جمعه اعلام کرد گوگل مجبور است آدرس رایانامه‌ی کاربران را که در کارگزارهایی خارج از آمریکا ذخیره شده‌اند، در اختیار FBI قرار دهد. این دادرس آمریکایی اشاره کرد با انتقال رایانامه‌ها از کارگزارهای خارجی به FBI، این سازمان می‌تواند رایانامه‌های کاربران را به‌طور محلی بخواند بدون اینکه هیچ هرج‌ومرجی ایجاد شود چرا که حساب‌های کاربری دارای واسطی نیستند که بتوان سرقت داده‌ها را از طریق آن متوجه شد.

این دادستان در صحبت‌های خود گفت: «گوگل به‌طور منظم داده‌های مشتریان را از یک مرکز داده به مرکز داده‌ی دیگر منتقل می‌کند بدون اینکه کاربر از آن مطلع باشد. این انتقال‌ها تحت کنترل کاربران قرار ندارد و اگر هم چنین کنترلی وجود داشته باشد موقتی و محدود است.»

در مرداد ماه FBI به گوگل دستور داده بود در راستای بررسی جرائم با این نهاد همکاری داشته باشد ولی گوگل تنها اطلاعاتی که بر روی کارگزارهای داخل آمریکا وجود داشت را در اختیار بازرسان FBI قرار داده بود. بنابراین دولت آمریکا در تلاش است گوگل را وادار کند تا اطلاعات کارگزارهای خارج از آمریکا را نیز در اختیار FBI قرار دهد.

بدافزارهای چینی سامانه‌های کشور روسیه را هدف قرار داده‌اند

یک گروه جاسوسیِ سایبری منتسب به چین، با بدافزارها و روش‌های جدید، سامانه‌های نظامی و هوافضا در کشورهای روسیه و بلاروس را هدف قرار داده است.

در تیر ماه سال جاری، محققان گروه پروف‌پوینت گزارش دادند که مهاجمانِ این گروه با استفاده از تروجانِ پیشرفته‌ی NetTraveler روسیه و سایر کشورهای همسایه را هدف قرار داده‌اند. اینک محققان کشف کردند که این گروه جاسوسی همزمان از بارگیری‌کننده‌ای به نام ZeroT و کامپایلر کمکی HTML متعلق به شرکت مایکروسافت (chm.) برای توزیع بدافزار PlugX استفاده می‌کند.

مهاجمان پرونده‌ی .chm را برای قربانیان ارسال می‌کنند که حاوی پرونده‌ی HTML و یک پرونده‌ی اجرایی دیگر است. زمانی که پرونده‌ی کمکی HTML باز شود، یک متن به زبان روسی نمایش داده شده و از کاربر خواسته می‌شود از طریق کنترل حساب کاربری (UAC) اجازه‌ی اجرای برنامه‌ی ناشناخته‌ای را صادر کند. اگر قربانی با این درخواست موافقت کند، بارگیری‌کننده‌ی ZeroT بر روی سامانه‌ی قربانی نصب خواهد شد.

مشابه حملات قبلی، این گروه جاسوسی از اسناد ورد جعلی نیز استفاده می‌کنند. این اسناد توسط ابزار تولیدکننده‌ی بهره‌برداری با نام MNKit ایجاد می‌شود. این ابزار به محققان کمک کرده تا ارتباط بین چند گروه نفوذ و جاسوسی را کشف کنند که ممکن است خارج از کشور چین باشند.

رایانامه‌ها و پرونده‌های جعلی که در این حملات از آن‌ها استفاده می‌شود، به کشورهای مستقل مشترک‌المنافع ارجاع داده می‌شود که اتحادیه‌ای از جماهیر شوروی سابق، دولت روسیه و وزارت دفاع روسیه است.

این گروه جاسوسی همچنین برای توزیع ZeroT از ویژگی خود-استخراجی پرونده‌های آرشیوی RAR استفاده می‌کند. در بسیاری از پرونده‌های آرشیوی یک پرونده‌ی اجرایی با نام Go.exe وجود دارد که برای دور زدن کنترل حساب کاربری (UAC) در ویندوز به‌کار می‌رود.

توسعه‌ی بدافزاری برای جاسوسی از سامانه‌های مک توسط نفوذگران ایرانی

گزارش‌ها حاکی از آن است که نفوذگران ایرانی بدافزاری را برای جاسوسی از سامانه‌های مک طراحی کرده‌اند. طراحی بدافزار برای جاسوسی از سامانه‌های مک، توانایی نفوذگران ایرانی را نشان می‌دهد که پا را فراتر گذاشته و سامانه‌هایی به‌غیر از ویندوز را برای جاسوسی هدف قرار داده‌اند. اغلب مردم فکر می‌کنند سامانه‌های مک جزو امن‌ترین دستگاه‌ها هستند.

این بدافزار که توسط طراحان آن MacDownloader نام گرفته، بر روی یک وب‌گاه جعلی در حال توزیع بوده است. این وب‌گاه جعلی، فعالیت‌های یک شرکت هوافضای آمریکایی را که در حوزه‌ی دفاعی به فروش توربین جت و تجهیزات صنعتی دیگر می‌پردازد، تقلید می‌کند. کارشناسان امنیتی معتقدند این بدافزار مخالفان دولت ایران و سایر فعالان را هدف قرار داده است.

این بدافزار سامانه‌ی قربانی را از طریق یک برنامه‌ی بارگیری جعلی فلش آلوده می‌کند. این برنامه زمانی‌که کاربر با وارد کردن گذرواژه‌ی iCloud Keychain با کارگزار خارجی در حال ارتباط است، نمایش داده می‌شود. مرورگر سافاری و سرویس‌های سامانه‌ی macOS به‌طور خودکار گذرواژه‌ها را بر روی Keychain اپل برای وب‌گاه‌ها، سامانه‌های پرونده، راه‌اندازهای رمزنگاری‌شده و سایر موارد ذخیره می‌کنند تا در مواقع دیگر که کاربر برای ورود به حساب خود به این گذرواژه نیاز دارد از آن استفاده شود.

این بدافزار جعبه‌های ورود به حساب کاربری که دیگر از رده خارج شده‌اند را به کاربر نمایش می‌دهد تا کاربر ترغیب شده و اطلاعات بیشتری از حساب کاربریِ خود را افشاء سازد. به‌نظر می‌رسد هدف بدافزار MacDownloader شناسایی طیف وسیعی از کاربران و به دست آوردن گواهی‌نامه‌های حساب‌های کاربری است.

در این گزارش آمده است: «در نمونه‌ای از بدافزار MacDownloader می‌توان فهمید که این بدافزار توسط ایرانی‌ها توسعه داده شده است و از روی نام افزونه‌ی flashplayer.app می‌توان متوجه شد که یک فرد فارسی‌زبان این نام‌گذاری را انجام داده است. زیرساخت‌های این بدافزار و طیف کاربرانی که هدف قرار داده این گمان را قوی‌تر می‌کند که بدافزار توسط گروه نفوذ ایرانی به نام Charming Kitten طراحی شده است. گفته می‌شود این گروه توسط نهادهای امنیتی ایران مورد حمایت قرار می‌گیرد.»

نفوذ به ایستگاه‌های رادیویی در آمریکا و انتشار پیام‌های معترضانه علیه ترامپ

تنها دو هفته از آغاز ریاست جمهوری دونالد ترامپ می‌گذرد و او با تصمیم‌گیری‌های خود، باعث هرج‌ومرج در این کشور شده است. یکی از این تصمیمات عجیب ترامپ ممنوعیت ورود شهروندان 7 کشور مسلمان از جمله عراق، ایران، لیبی، یمن، سومالی، سوریه و سودان به آمریکاست. در پی این دستور در فرودگاه‌های این کشور بسیاری از پناهندگان و افرادی که ویزای اقامت در آمریکا را داشتند، توسط نیروهای پلیس دستگیر شدند.

اینک در اعتراض به این تصمیماتِ ترامپ، جمعی از معترضان از آسیب‌پذیری‌های موجود بر روی ایستگاه رادیویی FM بهره‌برداری کرده‌اند تا از این طریق اعتراض خود را به گوش ترامپ و دیگران برسانند. ایستگاه رادیویی در کارولینای جنوبی، ایندیانا، تگزاس، تنسی و کنتاکی اخیراً مورد نفوذ قرار گرفته و از آن پیام‌هایی علیه ترامپ پخش شده است.

نفوذگران با بهره‌برداری از آسیب‌پذیری‌های شناخته‌شده در دستگاه‌های Barix Exstreamer، توانستند به ایستگاه‌های رادیویی دست یابند. این آسیب‌پذیری به نفوذگران اجازه می‌دهد پرونده‌های صوتی را کدگشایی کرده و از طریق LPFM انتقال دهند.

در هفته‌های اخیر بیش از دوازده ایستگاه رادیویی چنین نفوذی را تجربه کرده‌اند و برخی از این ایستگاه‌ها نیز برای متوقف کردن انتشار این پیام‌ها مجبور شدند امواج رادیویی خود را از کار بیندازند. نفوذگر یا گروه نفوذی که عامل این حملات بوده هنوز مشخص نیست.