خبرنامه مدیریتی سراج
مرکز نرم‌افزار و سرویس وخدمات سازمان فضای مجازی سراج
اخبار فناوری اطلاعات و ارتباطات
هفته نامه | سال دوم | شماره نود و پنجم | ۷ اسفند ۱۳۹۵
۹۵

حمله به بانک‌های لهستان کار گروه لازاروس بوده است

نفوذگران در حمله‌ای علیه بانک‌های لهستانی شرکت کرده‌اند، آن‌ها در این حمله خطوط کد را به نحوی تغییر داده‌اند که این‌طور به نظر برسد که حمله توسط عوامل روسی انجام شده است. واقعیت این است که این خطوط از کد حس زبان مادری را به کارشناسان القاء نمی‌کند و آن‌ها بایست برای بررسی بیشتر از یک مترجم برخط استفاده کنند.

یک کمپین پیچیده‌ی سایبری سازمان‌های مالی کشورهای متعددی را هدف قرار داده است، اما به‌طور خاصی روی لهستان تمرکز کرده است. به نظر می‌رسد که تیم پشت این حمله از روی عمد کلمات و دستور زبان روسی را به کد بدافزار خود اضافه کرده تا محققان را گمراه کند.

به گفته‌ی کارشناسان دستورات و رشته‌های متعددی در این بدافزار وجود دارند که به کمک ابزارهای برخط به زبان روسی ترجمه شده‌اند. در برخی از موارد این مترجم‌های ناکارآمد معنی کلمات را به کلی دگرگون کرده‌اند. این موضوع دقیقاً نشان می‌دهد که نویسندگان و دست‌اندرکاران این حمله روسی‌زبان نیستند و استفاده از زبان روسی از سوی آن‌ها فقط و فقط برای رد گم‌کردن بوده است.

سرنخ‌هایی که به لازاروس می‌رسند

نسبت دادن حملات گسترده به کمپین‌های سایبری کار دشواری است، اما اضافه‌شدن واژگان روسی به این کد به وضوح تلاشی بوده تا کارشناسان مسیر درست را برای رسیدن به مقصد گم کنند. در واقع تمام سرنخ‌ها باعث می‌شود توجه‌ها معطوف به لازاروس شوند؛ لازاروس یک گروه شناخته‌شده در صنعت امنیت است. در گذشته این گروه حملاتی را علیه بخش‌های دولتی و سازمان‌های خصوصی کشورهای مختلف مانند آمریکا ترتیب داده است.

حتی حمله‌ای که در سال ۲۰۱۴ علیه سونی پیکچرز انجام شد، حمله‌ای که طی آن داده‌های حساسی افشا شد و عملکرد رایانه‌های شرکت سونی مختل گردید، با لازاروس مرتبط بوده است؛ البته هیچ مدرکی برای این ادعا وجود ندارد.

عربستان سعودی هدفِ حملات سایبری و پویش‌های جاسوسی

یک پویش جاسوسی که گفته می‌شود به کشور ایران و حملات شمعون2 مرتبط است، سازمان‌های مختلف در خاورمیانه به‌ویژه عربستان سعودی را هدف قرار داده است.

محققان امنیتی در شبکه‌ی پالوآلتو این پویش جاسوسی را ردیابی می‌کردند. سابقه‌ی فعالیت‌های این پویش به اواسط سال 2016 میلادی برمی‌گردد. این پویش در اصطلاح «سگِ شکاریِ جادویی» نام دارد که سازمان‌های انرژی، دولتی و فناوری را در کشور عربستان سعودی هدف قرار داده است.

گروهی که در پشت این پویش فعالیت دارد از ابزارهای بسیار ویژه‌ای از جمله ابزار دسترسیِ راه‌دور Pupy که متن‌باز نیز هست استفاده می‌کنند. در حالی‌که محققان پالوآلتو هنوز این حملات را به کشوری نسبت نداده‌اند، شرکت امنیتی دیگری این پویش را تحلیل و بررسی کرده و آن را با عملیات COBALT GYPSY مرتبط می‌داند و مطمئن است این عملیات نیز توسط ایرانیان انجام شده است.

در حملات اخیر از اسناد ورد و اکسل حاویِ ماکروهای مخرب استفاده می‌شود. این ماکروها تلاش دارند با استفاده از پاورشِل ابزارهای جانبیِ بیشتری را تنظیم و نصب کنند. این پرونده‌ها در قالب کارت‌های تبریک، درخواست‌های شغلی و اسناد رسمی دولتی از طرف وزارت بهداشت و درمان، بین کاربران عربستان سعودی توزیع می‌شود.

مهاجمان از ابزارهای ویژه‌ای برای رسیدن به اهداف خود استفاده می‌کنند. از جمله‌ی این ابزارهای می‌توانند نصب‌کننده‌های بدافزار، باتنت IRC و یک بار داده حاوی ابزار دسترسیِ راه دور، مبتنی بر پایتون با نام Pupy را برشمرد.

شایان ذکر است که برخی از دامنه‌های مورد استفاده در این حمله، توسط محققان امنیتی، زمانی که حملات شمعون2 را بررسی می‌کردند شناسایی شده بود. بردار توزیع حمله، استفاده از اسنادِ حاوی ماکروهای مخرب و پاورشِل نیز در هر دوی این حملات مشابه است.

محققان پالوآلتو روابطی را بین این پویش جاسوسی و گروه نفوذِ ایرانی با نام Rocket Kitten کشف کرده‌اند.

نفوذگرانِ چینی با یک تروجان جدید، سازمان‌های ژاپن را هدف قرار دادند

محققـان امنیتـی پالوآلتـو روز پنج‌شـنبه گـزارش دادنـد یـک گـروه نفـوذِ چینـی، تروجـان جدیـدی را طراحـی کـرده کـه افـراد و سـازمان‌ها در کشـور ژاپـن را هـدف قـرار می‌دهـد.

ایـن گـروه نفـوذ بـا نام‌هایـی همچـون menuPass، Stone Panda و APT10 شـناخته می‌شـود و از سـال 2009 فعالیـت خـود را آغـاز کـرده اسـت. ایـن گـروه نفـوذ در ابتـدای امـر صنایـع دفاعـی آمریـکا و سـایر کشـورها را هـدف قـرار داده بـود ولـی از سـال 2014 حملـه بـه سـازمان‌های کشـور ژاپـن را آغـاز کـرده اسـت.

ایـن گـروه نفـوذ بـه اسـتفاده از بدافزارهـای PlugX و PoisonIvy معروف اسـت کـه توسـط پویش‌هـای دیگـر نیـز اسـتفاده می‌شـود. بـا ایـن حـال، در حمـلات اخیـر menuPass، از تروجـان جدیـدی بـا نـام ChChes اسـتفاده می‌شـود کـه منحصـر بـه همیـن گـروه اسـت.

در حملات اخیـر، بخش‌هـای دانشـگاهی، یـک شرکـت دارویـی و همچنیـن یـک سـازمانِ تابعـه‌ی ژاپـن واقـع در آمریـکا هـدف قـرار گرفته‌انـد. در ایـن حمـلات از رایانامه‌هـای فیشـینگ بـا آدرس‌هـای جعلـی از طـرف سـازمان صلـح جهانـی و کاخ سـفید اسـتفاده می‌شـود.

سرنخ‌هایـی وجـود دارد کـه نشـان می‌دهـد بدافـزار ChChes از یـک درهم‌سـازی مشـترک بـا سـایر ابزارهـای menuPass اسـتفاده می‌کنـد. همچنیـن محققـان امنیتـی، مشـابهت‌های بسـیاری را در زیرسـاختِ حملـه‌ی جدیـد بـا حمـلات قبلـی کشـف کرده‌انـد.

تروجـانِ ChChes در یـک سـند ورد مخفـی شـده و بـا یـک گواهی‌نامـه از طـرف گـروه نفـوذ ایتالیایـی امضـاء شـده اسـت. ایـن گواهی‌نامـه زمانـی افشـاء شـد کـه ایـن شرکـت ایتالیایـی در سـال 2015 مـورد نفـوذ قـرار گرفـت. محققـان امنیتـی معتقدنـد از ایـن بدافـزار بـرای سـخت‌تر کـردن انتسـاب حمـلات اسـتفاده شـده اسـت.

بدافـزار ChChes عـلاوه بـر جمـع‌آوری اطلاعـات حسـاس از سـامانه‌ی آلـوده، دارای ماژول‌هایـی اسـت کـه بـه رمزنـگاری ارتباطـات، اجـرای دسـتورات شِـل، بارگـذاری و بارگیـریِ پرونده‌هـا و اجـرای DLL هـا کمـک می‌کنـد. محققـان پالوآلتـو معتقدنـد تروجـان ChChes تنهـا بـرای بارگیـریِ بدافزارهـای دیگـر مـورد اسـتفاده قـرار می‌گیـرد چـرا کـه دارای هیـچ سـازوکاری بـرای مانـدگاری بـر روی ماشـین قربانـی نیسـت.

حمله‌ی بدافزار اندرویدی به دستگاه‌های ارتشِ رژیم صهیونیستی

براسـاس گـزارش آزمایشـگاه کسپرسـکی، از اواسـط سـال قبـل، نزدیـک بـه 100 سـامانه‌ی نظامـی رژیـم صهیونیسـتی هـدف حمـلات سـایبری قـرار گرفتـه و از ایـن سـامانه‌ها داده‌هـای حساسـی خـارج و بـرای کارگزارهـای دسـتور و کنـترل مهاجـمان ارسـال شـده اسـت. در ادامـه نیـز بـر روی ایـن دسـتگاه‌ها، تروجان‌هـا به‌روزرسـانی شـده و قابلیت‌هـای آن‌هـا افزایـش یافتـه اسـت.

کارشناسـان امنیتـی معتقدنـد پویـشِ ایـن مهاجـمان ادامـه داشـته و در مـوجِ جدیـدی از حمـلات، دسـتگاه‌های اندرویـدی را هـدف قـرار داده‌انـد. تلفن‌هـای هوشـمند و تبلت‌هـا پـس از آلـوده شـدن، بـه دسـتگاهی بـرای جاسوسـی تبدیـل شـده و مهاجـمان می‌تواننـد از قابلیت‌هـای صوتـی، ویدئویـی و حتـی پیامـک آن اسـتفاده کننـد.

در ایـن حمـلات از روش‌هـای مهندسـی اجتماعـی نیـز اسـتفاده می‌شـود به‌طوری‌کـه سربـازان ارتـش در شـبکه‌های اجتماعـی تحریـک می‌شـوند تـا گواهی‌نامـه‌ی حسـاب‌های خـود را افشـاء کـرده و برنامه‌هـای مخـرب را بـر روی سـامانه‌ها نصـب کننـد. بـه گـزارش کسپرسـکی، رده‌هـای مختلفـی از ارتـشِ رژیـم صهیونیسـتی هـدف ایـن حمـلات قـرار گرفته‌انـد و بیشـتر ایـن سـامانه‌ها در بخش‌هایـی کـه در نـوار غـزه خدمـت می‌کننـد، قـرار دارد.

بدافزارِ اندرویدی چگونه کار می‌کند؟

قربانیـان در شـبکه‌های اجتماعـی فریـب می‌خورنـد تـا برنامه‌هـای مخـرب را بارگیـری و نصـب کننـد. هنگامی‌کـه برنامـه‌ی مخـرب APK بارگیـری شـد، ایـن برنامـه نیـاز دارد تـا به‌طـور دسـتی نصـب شـود. ایـن برنامـه در هنـگام نصـب مجوزهایـی را بـرای حـذف و نصـبِ بسـته‌ها، نوشـتن در حافظه‌هـای خارجـی، دسترسـی بـه اینترنـت و وضعیـت شـبکه درخواسـت می‌کنـد.

بسـته بـه نـوع دسـتگاه، کارگـزار مخـرب مشـخص می‌کنـد چـه نسـخه‌ای از بـارِ داده بـرای ایـن دسـتگاه مناسـب اسـت. نصب‌کننـده‌ی بدافـزار در ادامـه فهرسـتی از برنامه‌هـای نصب‌شـده بـر روی دسـتگاه را ارسـال می‌کنـد. باتوجـه بـه برنامه‌هایـی کـه بـر روی دسـتگاه نصـب شـده، بدافـزار در قالـب برنامـه‌ی جعلـیِ یوتیـوب و یـا برنامه‌هـای گفتگـو و یـا سـایر برنامه‌هـا بارگیـری و نصـب می‌شـود.

یکـی از بـار داده‌هـا در قالـب به‌روزرسـانیِ برنامـه‌ی واتـس‌اپ، اپراتـور را قـادر می‌سـازد تـا به‌طـور دسـتی دسـتورات دلخـواه خـود را اجـرا کنـد و وظایفـی را بـرای جمـع‌آوری اطلاعـات از منابـع مختلـف زمان‌بنـدی کنـد.