پگاسوس یک نرم‌افزار هک یا جاسوس‌افزار است که توسط شرکت صهیونیستی ان‌اس‌او توسعه یافته‌است و به دولت‌ها فروخته می‌شود. این جاسوس‌افزار قادر است میلیاردها گوشی از جمله سیستم‌های عامل اندروید و آی‌اواس را هدف قرار دهد

سال ۲۰۱۹ واتس‌اپ آشکار کرد که نرم‌افزار ان‌اس‌او با استفاده از حمله‌ای موسوم به روز صفر، به بیش از ۱۴۰۰ گوشی همراه، بدافزار ارسال کرده‌است

پگاسوس چطور به تلفن‌های همراه وارد می‌شود؟

نفوذ به قلب داده‌ها

شیرین هنرمنداصل
روزنامه‌نگار

پگاسوس یکی از نمونه‌هایی است که نشان می‌دهد چگونه همه ما در برابر جاسوس افزارها آسیب‌پذیر هستیم. این جاسوس‌افزار شگفت انگیز، می‌تواند به اطلاعات شخصی ما در گوشی‌های هوشمند مانند پیام‌ها، ایمیل‌ها و هر چیزی که فکرش را بکنید، دسترسی پیدا کند. جاسوس‌افزارها می‌توانند مستقیم از اتفاقات روزمره زندگی‌های ما باخبر شوند. دور زدن رمزنگاری‌هایی که از اطلاعات ارسالی در اینترنت محافظت می‌کنند، برای پگاسوس کاری آسان است.

اخیرا روزنامه گاردین در گزارشی نوشته که محققان امنیتی شواهدی از تلاش‌هایی برای نصب یا نصب‌های موفق پگاسوس در گوشی روزنامه‌نویسان و تاجران پیدا کرده‌اند. فعالان و افراد دیگر نیز هدف جاسوسی‌های مخفیانه پگاسوس قرار می‌گیرند. این در حالی است که هدف پگاسوس، تعقیب قانونی مجرمان و تروریست‌ها عنوان شده‌بود. فهرستی از بیش از ۵۰ هزار شماره موبایل که به احتمال زیاد هدف مشتریان پگاسوس بوده‌است با ۱۷ خبرگزاری به‌اشتراک گذشته شد. شماره موبایل ۱۰ نخست‌وزیر، سه رئیس جمهور و یک پادشاه در این میان به چشم می‌خورد. خبرگزاری‌ها و رسانه‌های مختلف، هویت بسیاری از افراد این فهرست و آلوده شدن آنها را با جاسوس‌افزار پگاسوس تایید کردند. ۶۷ گوشی از اسامی ذکر شده بررسی و در ۳۷ گوشی، نشانه‌های نصب پگاسوس یا تلاش برای نصب آن مشاهده شد. طبق گزارش واشنگتن پست، ۳۴ گوشی از این ۳۷ گوشی، از برند آیفون بودند.

پگاسوس چیست؟

پگاسوس شاید قدرتمندترین جاسوس‌افزار دنیا باشد. زمانی که وارد گوشی شما شود، بدون آن که متوجه شوید، گوشی شما را تبدیل به یک دستگاه نظارتی خواهدکرد. این نرم‌افزار جاسوسی می‌تواند پیام‌ها و عکس‌های شما را کپی و تماس‌های شما را ضبط کند. ممکن است با دوربین شما فیلمبرداری یا میکروفن را فعال و مکالمات روزمره شما را ضبط کند. پگاسوس می‌تواند مکان فعلی و جایی را که قبلا بوده‌اید و اشخاصی که با آنها ملاقات کرده‌اید، به‌دقت مشخص کند. پگاسوس یک نرم‌افزار هک یا جاسوس‌افزار است که توسط شرکت صهیونیستی ان‌اس‌او توسعه یافته‌است و به دولت‌ها فروخته می‌شود. این جاسوس‌افزار قادر است میلیاردها گوشی از جمله سیستم‌های عامل اندروید و آی‌اواس را هدف قرار دهد. نسخه اولیه پگاسوس سال ۲۰۱۶ توسط محققان کشف شد که روش آلوده‌کردن آن، ترغیب کاربر به کلیک روی لینک آلوده در پیام یا ایمیل بود. فیشینگ هدفمند نامی بود که آن زمان بر آن نهاده شد.

نسخه اولیه پگاسوس سال ۲۰۱۶ توسط محققان کشف شد که روش آلوده‌کردن آن، ترغیب کاربر به کلیک روی لینک آلوده در پیام یا ایمیل بود. فیشینگ هدفمند نامی بود که آن زمان بر آن نهاده شد

پگاسوس چگونه نفوذ می‌کند؟

حملات ان‌اس‌او با گذر زمان پیشرفته‌تر می‌شوند. در حدی که دیگر لازم نیست صاحب گوشی روی لینکی کلیک کند تا آلوده شود. به این نوع حملات، حمله روز صفر گفته می‌شود. زیرا هنوز سازنده اپلیکیشن از باگ‌ها یا مشکلاتی که باعث می‌شود گوشی آلوده شود، آگاهی ندارد؛ بنابراین نمی‌تواند از این حملات جلوگیری کند. سال ۲۰۱۹، واتس‌اپ آشکار کرد نرم‌افزار ان‌اس‌او با استفاده از حمله‌ای موسوم به روز صفر، به بیش از ۱۴۰۰ گوشی همراه، بدافزار ارسال کرده‌است. با یک تماس واتس‌اپ، بدون آن که تماس پاسخ داده‌شود، کد آلوده پگاسوس می‌تواند روی گوشی نصب شود. اخیرا نرم‌افزار ان‌اس‌او ، نرم افزار iMessage اپل را هم هدف قرار داده‌است که از این طریق می‌تواند به میلیون‌ها گوشی دسترسی داشته‌باشد. اپل می‌گوید به‌صورت پیوسته نرم افزار خود را به‌روزرسانی می‌کند تا از چنین حملاتی جلوگیری کند.

چگونه پگاسوس به گوشی‌ها نفوذ می‌کند؟

برای شرکت‌هایی مانند ان‌اس‌او، اپلیکیشن‌های پیش‌فرض مانند آی‌مسیج یا اپلیکیشن‌های پرطرفدار مانند واتس‌اپ یک گزینه مناسب به شمار می‌روند. زیرا تعداد گوشی‌هایی که پگاسوس می‌تواند به آنها حمله کند، به طرز قابل توجهی افزایش می‌یابد. آنالیز گوشی‌های هوشمند قربانیان نشان می‌دهد ان‌اس‌او از طریق اپلیکیشن‌های محبوب به آنها حمله کرده‌است. هنگام آلوده شدن گوشی، اپلیکیشن تصاویر و موسیقی اپل از ترافیک شبکه استفاده می‌کنند. محققان ادعا می‌کنند احتمالا ان‌اس‌او از روش‌های مختلف دیگری برای نفوذ به گوشی قربانی استفاده‌می‌کند. زمانی که فیشینگ هدفمند و حمله روز صفر موفق به جاسوسی نمی‌شود، پگاسوس می‌تواند روی گیرنده بی‌سیم نزدیک قربانی نصب شود یا طبق بروشور ان‌اس‌او، مامور شرکت می‌تواند گوشی قربانی را بدزد و پگاسوس را بر آن نصب کند. زمانی که پگاسوس با موفقیت نصب شود، می‌تواند به همه اطلاعات مانند پیامک‌ها، فهرست مخاطبان، سابقه تماس، تقویم‌ها، ایمیل‌ها، چت‌های پیام‌رسان‌ها مانند واتس‌اپ، اطلاعات جی‌پی‌اس، عکس‌ها و ویدئوها و مرورگرهای قربانی دسترسی پیدا کنند. پگاسوس حتی می‌تواند با استفاده از میکروفن و دوربین گوشی، فعالیت‌های اطراف گوشی را ضبط کند. به عبارت دیگر، دسترسی‌های پگاسوس بیش از صاحب گوشی است.

آیا می‌توان از جاسوسی پگاسوس جلوگیری کرد؟

ان‌اس‌او تلاش‌های بسیاری برای غیرقابل تشخیص کردن این جاسوس‌افزار کرده و اکنون تشخیص پگاسوس بسیار سخت است. طبق گفته‌های محققان امنیتی، پگاسوس می‌تواند حتی درون حافظه موقت گوشی جا خوش کند. در این حالت، اگر گوشی خاموش شود، همه آثار پگاسوس نیز ناپدید خواهدشد. یکی از بزرگ‌ترین چالش‌ها برای روزنامه‌نگاران و مدافعان حقوق بشر این است که پگاسوس به نقاط آسیب‌پذیر کشف نشده گوشی حمله می‌کند. در این صورت، حتی کاربری که شدیدا به فکر حفظ امنیت گوشی هوشمند خود است، نخواهد توانست از حمله پگاسوس جلوگیری کند. چگونه می‌توانیم از جاسوسی پگاسوس از گوشی هوشمند خود جلوگیری کنیم؟ بسیاری از افراد شبیه این سوال را از کارشناسان می‌پرسند. ولی طبق گفته‌های محققان امنیتی، هیچ‌کاری نمی‌توانید بکنید. به‌روزرسانی سیستم‌عامل و استفاده از تایید هویت دو مرحله‌ای شاید بتواند گوشی هوشمند شما را از دست هکرهای کوچک نجات دهد؛ ولی محافظت از گوشی در برابر جاسوس‌افزارهای قدرتمند مانند پگاسوس که به‌دقت ساخته شده‌اند، غیرممکن به نظر می‌رسد. ان‌اس‌او تایید می‌کند ممکن است از پگاسوس استفاده‌های نادرستی شود. این شرکت ادعا کرد طی ۱۲ ماه گذشته، دو مشتری را به علت نگرانی‌ها درباره نقض حقوق‌بشر حذف کرده‌است. ادوارد اسنودن، کسی که اطلاعاتی از برنامه‌های جاسوسی آژانس امنیت ملی آمریکا را سال ۲۰۱۳ لو داده‌بود، ادعا کرد اگر فروش جاسوس‌افزارها ممنوع نشود، به‌زودی برای جاسوسی از میلیون‌ها فرد از آنها استفاده خواهدشد. اسنودن گفت: «در گوشی‌هایی مانند آیفون، نرم‌افزارهای یکسانی وجود دارد. پس اگر آنها راهی برای هک کردن یک گوشی آیفون پیدا کنند، راهی برای هک همه آیفون‌ها پیدا کرده‌اند.»