ذره‌بین

سعودی‌ها، پگاسوس و جمال خاشقجی

عربستان سعودی اتهاماتی را که اخیرا در پی انتشار نتایج تحقیقاتِ مرتبط با استفاده از بدافزار جاسوسی پگاسوس متوجه این کشور شده، رد کرده است. نتایج تکان‌دهنده این تحقیقات نشان می‌دهد که عربستان سعودی از بدافزار صهیونیستی «پگاسوس» برای نظارت بر فعالیت روزنامه‌نگاران و فعالان حقوق بشر بهره برده است. ریاض اما در واکنش به این ادعا که گمانه‌زنی درخصوص آن با توجه به پرونده قتل جمال خاشقجی، روزنامه‌نگار منتقد حکومت عربستان بیش از پیش تقویت شده، تاکید دارد که این اتهامات بی‌اساس و دروغین است. خبرگزاری رسمی عربستان سعودی با انتشار گزارشی بدون اشاره به نام بدافزار اسرائیلی به نقل از یک مقام دولتی در این کشور ادعاهای مطرح‌شده در مطبوعات و رسانه‌ها مبنی بر این‌که نهادی در دربار از نرم‌افزاری خاص برای کنترل مکالمات و ارتباطات افراد استفاده کرده را رد کرد. به گفته این منبع که خبرگزاری رسمی عربستان نامی از وی نبرده «این ادعاها دروغ و بی‌اساس است» و ریاض «این نوع اعمال را تایید نمی‌کند.»

براساس نتایج تحقیقی که هفته گذشته از سوی کنسرسیومِ ۱۷ رسانه بین‌المللی ازجمله روزنامه‌های لوموند فرانسه، گاردین بریتانیا و واشنگتن‌پستِ ایالات‌متحده آمریکا منتشر شد، عربستان سعودی یکی از کشورهایی است که از بدافزار جاسوسی پگاسوس برای نظارت بر فعالیت روزنامه‌نگاران، سیاستمداران زن و مرد، فعالان حقوق بشر یا روسای برخی شرکت‌ها و موسسات بزرگ استفاده کرده است.

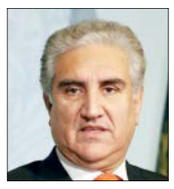
فرانس‌پرس در گزارشی با انعکاس واکنش عربستان به ادعاهای مطرح درخصوص استفاده این کشور از بدافزار پگاسوس آورده است که مقامات ریاض به‌خصوص پس از رسمیت‌یافتن ولیعهدی محمد بن‌سلمان در سال ۲۰۱۷ بی‌امان مخالفان و فعالان حقوق‌بشر در این کشور را سرکوب می‌کنند. حکومت پادشاهی عربستان سعودی همچنین بارها به دنبال‌کردن مخالفان در شبکه‌های اجتماعی یا حتی نفوذ در میان کاربران شبکه اجتماعی توییتر از طریق سربازان سایبری متهم شده است. گفتنی است که وزارت دادگستری آمریکا به‌تازگی دو کارمند سابق شرکت توییتر را به جاسوسی برای دولت عربستان متهم کرده بود.

جمال خاشقجی، منتقد دولت عربستان سعودی و ساکن آمریکا در اکتبر ۲۰۱۸ در کنسولگری عربستان سعودی در استانبول کشته و تکه‌تکه شد. به گزارش یورونیوز براساس تحقیقات انجام‌شده که در گزارش سازمان‌های رسانه‌ای آمده، برای کنترل دو زن نزدیک به خاشقجی و دیگر اعضای حلقه نزدیک او از بدافزار پگاسوس استفاده شده است. یکی از این زنان حنان العتر، مهماندار هواپیمایی مصر و همسر خاشقجی بوده است. بررسی‌های سازمان عفو بین‌الملل نشان می‌دهد که شش ماه پیش از قتل خاشقجی، تلفن خانم العتر مخفیانه توسط یکی از کاربران پگاسوس هدف قرار داده شده بود.

شخصی که از این بدافزار استفاده می‌کرده از نوامبر ۲۰۱۷ تا آوریل ۲۰۱۸ برای خانم العتر چهار پیام حاوی پیوندهای مخرب ارسال کرده است. عفو بین‌الملل می‌گوید قادر به تشخیص موفقیت هک نیست. خانم العتر به واشنگتن‌پست گفت: «جمال پیش از این به من هشدار داده بود که این اتفاق می‌افتد.»

او همچنین گفت که باور دارد آنها از همه مسائل میان او و جمال خاشقجی مطلع هستند. گرچه خاشقجی متأهل بود اما یک نامزد هم به نام خدیجه چنگیز داشت که پژوهشگر ترک بود. او ۲ اکتبر ۲۰۱۸ در خارج از کنسولگری عربستان منتظر خاشقجی بود اما وقتی نامزدش از ساختمان کنسولگری عربستان خارج نشد موضوع را به مقام‌های ترکیه خبر داد. براساس تجزیه و تحلیل‌هایی که متخصصان امنیتی سازمان عفو بین‌الملل انجام داده‌اند، چند روز پس از قتل آقای خاشقجی، گوشی آیفون خانم چنگیز توسط یک کاربر پگاسوس هک شده بود.

روند صلح افغانستان وارد مرحله حیاتی شده است



شاه‌محمود قریشی، وزیر خارجه پاکستان گفت: اسلام‌آباد خواهان صلح و ثبات در افغانستان است و تمام مقامات افغان باید برای برقراری صلح پایدار در این کشور تلاش کنند. وی افزود: روند صلح افغانستان وارد مرحله حیاتی شده است. وزیر خارجه پاکستان با اشاره به پرونده ربودن دختر سفیر افغانستان تصریح کرد: روند تحقیقات به‌زودی به پایان خواهد رسید و گزارش مربوطه نیز با دولت افغانستان به اشتراک گذاشته خواهد شد./فارس

دفع تجاوز هوایی صهیونیست‌ها توسط سوریه

منابع سوری از مقابله پدافند هوایی این کشور با اهداف متخاصم در آسمان حمص خبر دادند. یک منبع امنیتی اعلام کرد که پدافند هوایی سوریه با موشک‌های رژیم صهیونیستی که قصد هدف قراردادن برخی مواضع نظامی در اطراف شهر حمص را داشت، مقابله کرد. وی همچنین افزود که پدافند هوایی سوریه توانست بیشتر موشک‌ها را پیش از رسیدن به هدف رهگیری و منهدم کند. این تجاوز تلفات انسانی به‌همراه نداشته و خسارات آن محدود به زیان مادی بوده است./سانا

جاسوسی رژیم صهیونیستی و سران سعودی از کشورهای غربی، به سوژه داغ این روزها تبدیل شده است

ابعاد پرونده جاسوسی رژیم صهیونیستی از کشورهای غربی هر روز جدی‌تر می‌شود

آلودگی گوشی‌های سران غرب به ویروس اسرائیلی

سعید سبحانی

بین‌الملل

طی روزهای اخیر، شاهد انتشار اخباری تکان‌دهنده درخصوص جاسوسی هدفمند برخی دولت‌ها و سازمان‌ها از دیگر کشورها و مقامات، آن هم به وسیله یک جاسوس افزار صهیونیستی به نام «پگاسوس» هستیم. گرچه مقامات رژیم اشغالگر قدس و سازمان جاسوسی موساد دراین خصوص فعلا سکوت کرده‌اند اما با افشای عمق جاسوسی‌های صورت‌گرفته از مقامات دیگر کشورهای جهان، جایی برای لاپوشانی بسیاری از حقایق مربوط به این اقدامات غیرقانونی باقی نخواهد ماند.

بدافزار پگاسوس که توسط یک شرکت صهیونیستی ساخته‌شده از سوی برخی دولت‌ها و دستگاه‌های امنیتی با هدف جاسوسی مورد استفاده قرار گرفته است. این بدافزار با آلوده‌کردن گوشی موبایل، علاوه بر دسترسی به تمام اطلاعات می‌تواند حتی میکروفن تلفن را مخفیانه فعال کند. در فرانسه خبر حضور اسم امانوئل ماکرون در فهرست افراد هدف‌گرفته‌شده جنجال بزرگی به پا کرده است.

جاسوسی صهیونیست‌ها چگونه افشا شد؟

افشاگری در باره پگاسوس توسط شبکه‌ای از خبرنگاران انجام گرفته که Forbidden Stories نام دارد و با سازمان عفو بین‌الملل همکاری می‌کند. سازمان گزارشگران بدون مرز نیز از این شبکه حمایت می‌کند. روزنامه لوموند، رادیوی دولتی فرانسه و ۱۵ رسانه معتبر دیگر در سطح بین‌المللی، نتایج تحقیقات را منتشر کرده‌اند. Forbidden Stories و سازمان عفو بین‌الملل به فهرستی دست‌یافته‌اند که شامل ۵۰ هزار شماره تلفن است. به گزارش رادیو فرانسه، این شماره‌ها از سال ۲۰۱۶ توسط ۱۲ مشتری پگاسوس دست‌چین شده و روشن نیست که این ۱۲ کاربر دولت‌ها هستند یا اشخاص حقیقی اما همه آن ۵۰ هزار تلفن را باید به‌طور بالقوه هدف اقدامات جاسوسی دانست. در واقع فهرست یادشده حاوی تلفن‌هایی است که نفوذ به آنها موردنظر بوده؛ حال کدامیک از آنها عملا توسط پگاسوس آلوده شده، معلوم نیست.

بدافزار پس از نصب چه‌کاری انجام می‌دهد؟

آلن وودوارد، استاد امنیت سایبری در دانشگاهی در بریتانیا در گفت‌وگو با یورونیوز می‌گوید: «پگاسوس احتمالا یکی از توانمندترین ابزارهای دسترسی از راه دور است. به این فکر کنید که گویی تلفن خود را در دست شخص دیگری قرار داده‌اید.» به این ترتیب از این بدافزار می‌توان برای خواندن پیام‌ها و ایمیل‌های هدف و جست‌وجوی عکس‌هایی که گرفته‌اند و استراق سمع تماس‌های آنها و ردیابی موقعیت مکانی آنها و حتی فیلمبرداری از طریق دوربین آنها استفاده کرد. وودوارد گفت که توسعه‌دهندگان پگاسوس «بهتر و بهتر در پنهان‌کردن» تمام ردپای نرم‌افزار عمل می‌کنند؛ بنابراین تأیید این‌که آیا یک تلفن خاص درگیرشده یا نه، دشوار است. به همین دلیل هنوز مشخص نیست که چه تعداد از دستگاه‌های افراد شنود شده‌اند. گرچه گزارش‌های جدید رسانه‌های بین‌المللی حکایت از این نکته دارند که بیش از ۵۰ هزار شماره تلفن از طریق شرکت اسرائیلی کنترل می‌شده است. با این حال سازمان عفو بین‌الملل به عنوان یکی از سازمان‌های تحقیق در مورد پگاسوس اعلام کرد که در همین ماه ردپای حملات موفقیت‌آمیز به آیفون‌های اپل را یافته است.

آیا می‌توان نرم‌افزارهای جاسوسی را حذف کرد؟

از آنجا که دانستن اینکه یک تلفن، بدافزار را حمل می‌کند بسیار دشوار است، شناختن راه قطعی حذف شدن آن نیز دشوار است. وودوارد گفت که بدافزار پگاسوس بسته به نسخه، ممکن است خود را روی سخت‌افزار تلفن یا در حافظه آن نصب کند. به این ترتیب اگر در حافظه ذخیره شده باشد، راه‌اندازی مجدد تلفن می‌تواند به‌طور تئوری آن را پاک کند؛ بنابراین او توصیه می‌کند افرادی که در معرض خطر هستند، مانند مدیران مشاغل و سیاستمداران، مرتبا دستگاه‌های خود را خاموش و روشن کنند. وودوارد گفت: «برای بسیاری از مردم بیش از حد انتظار است اما نرم‌افزارهای ضدبدافزار برای دستگاه‌های تلفن همراه وجود دارند. اگر شما فردی در معرض خطر هستید شاید بخواهید برخی نرم‌افزارهای ضدبدافزار را روی تلفن خود نصب کنید.

در صورتی که ثابت شود تلفن امانوئل ماکرون هدف جاسوسی سایبری قرار داشته، این پرونده ابعاد بسیار جدی‌تری خواهد یافت. علاوه بر امانوئل ماکرون، شماره تلفن‌های رؤسای جمهور عراق و آفریقای جنوبی در فهرست دیده می‌شود. همچنین شماره‌های نخست‌وزیران پاکستان، مصر، مراکش و یا تلفن سعد حریری نخست‌وزیر پیشین لبنان هم در فهرست است

وقتی قرعه به نام مکرون می‌افتد!

شرکت اسرائیلی «ان‌اس‌او» که سازنده بدافزار است با موافقت وزارت دفاع رژیم صهیونیستی، پگاسوس را به برخی حکومت‌ها و دستگاه‌های امنیتی فروخته است. دولت مراکش دست‌داشتن در این ماجرا را تکذیب کرده اما گفته می‌شود که حتی شخص پادشاه محمد ششم و برخی از نزدیکانش هدف جاسوسی نهادهای امنیتی مراکش بوده‌اند. روزنامه لوموند می‌نویسد که دو سازمان امنیتی مهم کشور در مظان اتهام قرار دارند؛ اداره کل مطالعات و اسناد که سرویس اطلاعات خارجی و ضدجاسوسی مراکش محسوب می‌شود و اداره کل نظارت داخلی که امنیت داخل کشور را به عهده دارد. کارشناسان سوءظن بیشتری نسبت به سازمان دوم دارند. مسوولان شبکه افشاگری تأیید کرده‌اند که یکی از شماره‌های رئیس جمهوری فرانسه در فهرست دیده می‌شود اما این امر نیز معلوم نمی‌کند که تلفن ماکرون واقعا آلوده بوده یا خیر. نخست‌وزیر فرانسه ژان کاستکس گفت که رئیس جمهوری دستور انجام تحقیقات گسترده را صادر کرده است. در صورتی که ثابت شود تلفن امانوئل ماکرون هدف جاسوسی سایبری قرار داشته این پرونده ابعاد بسیار جدی‌تری خواهد یافت. علاوه بر امانوئل ماکرون، شماره تلفن‌های رؤسای جمهور عراق و آفریقای جنوبی در فهرست دیده می‌شود. همچنین شماره‌های نخست‌وزیران پاکستان، مصر، مراکش یا تلفن سعد حریری، نخست‌وزیر پیشین لبنان هم در فهرست است. شرکت اسرائیلی ان‌اس‌او مدعی شده که پگاسوس را برای مبارزه با مجرمان و تروریست‌ها طراحی‌کرده و آن را فقط به دستگاه‌های امنیتی یا دولت‌هایی فروخته که کارنامه خوبی در حوزه حقوق بشر دارند اما این توضیحات هیچ‌کس را قانع نکرده است.

چه کشورهایی از جاسوس افزار صهیونیست‌ها استفاده کرده‌اند؟

مراکش، مکزیک، هند، اندونزی، عربستان، امارات، قزاقستان، آذربایجان، کشورهای آفریقایی توگو و رواندا و حتی مجارستان که عضو اتحادیه اروپاست، مشتری شرکت ان‌اس‌او بوده‌اند. با این حال هنوز اطلاعات دقیقی در مورد هویت خریداران و کاربران بدافزار منتشر نشده است. در مواردی معلوم شده که برخی نهادها، حتی بدون اطلاع دولت از پگاسوس استفاده کرده‌اند. در هند، ظاهرا نخست‌وزیر نارندرا مودی، مسوول اصلی و آمر جاسوسی‌هاست. به نوشته لوموند، نارندرا مودی دولتی در دولت ایجاد کرده و بسیاری از رقبا، روزنامه‌نگاران یا فعالان اجتماعی و سیاسی را هدف گرفته است. دولت‌هایی از سراسر جهان با اتهاماتی شوکه‌کننده مبنی بر استفاده آنها از بدافزار ساخت اسرائیل برای جاسوسی از تلفن‌های کنشگران سیاسی و حقوق بشر، روزنامه‌نگاران و مدیران شرکت‌ها مواجه هستند.

بدافزار پگاسوس چگونه کار می‌کند؟

اما بدافزار پگاسوس دقیقا چگونه کار می‌کند؟ چگونه وارد تلفن افراد می‌شود و پس از آن چه‌کاری می‌تواند انجام دهد؟ محققان بر این باورند که نسخه‌های ابتدایی این نرم‌افزار هک برای اولین بار سال ۲۰۱۶ شناسایی شده است.

در آن زمان از پیام‌های متنی تله‌گذاری‌شده استفاده می‌شد تا روی تلفن‌های هدف نصب شوند؛ البته برای این‌که نرم افزار جاسوسی بارگذاری شود، گیرنده باید روی پیوند موجود در پیام کلیک می‌کرد اما این روش، شانس نصب موفقیت‌آمیز آن را محدود می‌کرد، به‌خصوص که کاربران تلفن نسبت به کلیک روی پیوندهای مشکوک بیش از پیش احتیاط می‌کردند.

نسخه‌های جدیدتر پگاسوس که توسط شرکت اسرائیلی ان‌اس‌او تهیه شده از نقاط ضعف نرم‌افزارهای معمول نصب‌شده روی تلفن‌های همراه استفاده کرده است. سال ۲۰۱۹ سرویس پیام‌رسانی واتس‌اپ از شرکت ان‌اس‌او شکایت و اعلام کرد که از یکی از نقاط آسیب‌پذیر در سیستم عاملش، برای نصب نرم‌افزارهای جاسوسی روی حدود ۱۴۰۰ تلفن استفاده شده است.

پگاسوس با تماس ساده با هدف از طریق واتس‌اپ می‌توانست خود را مخفیانه روی تلفن بارگذاری کند، حتی اگر کاربر هرگز به تماس پاسخ نداده باشد. اخیرا گزارش شده که پگاسوس از نقاط ضعف نرم‌افزار پیامک اینترنتی اپل، «آی‌مسیج» نیز استفاده کرده است. این موضوع به‌طور بالقوه امکان دسترسی به یک میلیارد آیفون اپل را که در حال حاضر مورد استفاده قرار می‌گیرند، می‌دهد. این کار حتی بدون کلیک یک دکمه نیز امکان‌پذیر است.

جنجال بر سر جاسوسی مراکشی‌ها

بسیاری از تحلیلگران امنیتی تایید کرده‌اند که اخبار افشاشده، نشان‌دهنده جاسوسی هدفمند دستگاه‌های امنیتی مراکش از مقامات فرانسوی است. قطعا رژیم صهیونیستی (به‌عنوان مصدر توزیع این بدافزار)، در جریان این جاسوسی قرار داشته است. روزنامه لوموند چاپ پاریس می‌نویسد موبایلی که رئیس جمهور فرانسه از سال ۲۰۱۷ استفاده می‌کند و در چند روز گذشته نیز از آن استفاده شده، مورد شنود قرار داشته است.

طبق گزارش لوموند، سرویس اطلاعاتی مراکش با کمک نرم‌افزار پگاسوس مکالمات مکرون را گوش می‌داده است: «اقدام خصمانه مراکش علیه رئیس یک دولت اروپایی.» همچنین دویچه‌وله به نقل از گروه روزنامه‌نگاران تحقیقی می‌گوید بررسی‌ها نشان می‌دهند که مراکش می‌تواند مکالمات و مبادلات تلفنی مکرون یا شارل میشل را شنود کرده باشد اما معلوم نیست هدف از این کار چه بوده است. دولت مراکش هیچ موضعی در این زمینه نگرفته و سفارت این کشور در پاریس نیز در تماس رسانه‌ها به این اکتفاکرده که بگوید: «مساله ادعاهایی بی‌اساس هستند و گزارش‌ها قاطعانه تکذیب می‌شوند.»

شماره تلفن الکساندر بنالا، محافظ سابق مکرون نیز در فهرست افشا شده هاست. سایر مقامات ارشد فرانسوی مورد شنود عبارتند از ادوارد فیلیپ، نخست‌وزیر سابق فرانسه، ژان ایو لودریان، وزیرخارجه، برونو لومیر، وزیر اقتصاد و ژان میشل بلانکه، وزیر آموزش‌وپرورش. هنوز روشن نیست که آیا تلفن مکرون به‌طور فعال و مداوم کنترل‌شده یا خیر. جاسوسی از همه شماره تلفن‌ها هنوز تاییدنهایی نشده و برای این امر لازم است دستگاه‌های تلفن از نظر ردیابی نرم‌افزار بررسی شوند. وزیر محیط‌زیست فرانسه با آنالیز موبایل خودش موافقت‌کرده و کارشناسان امنیت فناوری اطلاعات از سازمان عفو بین‌الملل توانسته‌اند ثابت کنند که پگاسوس جولای ۲۰۱۹ در تلفن همراه او فعال بوده است. کاخ الیزه در نخستین موضع‌گیری، مساله را بسیار نگران‌کننده خوانده است.

سایر سیاستمداران ارشد اروپایی نیز هدف جاسوسی بوده‌اند: شارل میشل، نخست‌وزیر سابق بلژیک و رئیس شورای اروپا و پدر او لویی میشل که تا سال ۲۰۱۹ ریاست گروه مشترک پارلمانی کشورهای آفریقایی، کارائیب، اقیانوسیه و اتحادیه اروپا را بر عهده داشت.

چگونه شرکت ان‌اس‌او چنین بدافزاری را توسعه داد؟

شرکت‌های فناوری چند میلیارد دلاری مانند اپل و گوگل هر سال مبالغ زیادی پول سرمایه‌گذاری می‌کنند تا مطمئن شوند در برابر هکرهایی که می‌توانند سیستم‌هایشان را از کار بیندازند، آسیب‌پذیر نیستند آنها حتی به هکرها اگر به شرکت‌ها در مورد نقص نرم‌افزارهایشان پیش از اینکه بتوانند از آن برای حمله استفاده کنند، هشدار دهند پاداش‌های خوبی می‌پردازند.

وودوارد گفت اپل به شهرت ایمنی خود افتخار می‌کند و «تلاش‌های نسبتا زیادی» کرده تا نقاط ضعف خود را شناسایی کند اما «به ناچار یک یا دو» اشکال در چنین نرم‌افزارهای پیچیده‌ای وجود خواهد داشت.

به گزارش یورونیوز، البته تحلیلگران بر این باورند که شرکت ان‌اس‌او که کارکنان آن را اعضای نخبه سابق ارتش رژیم صهیونیستی تشکیل می‌دهند، احتمالا «شبکه تاریک» را که در آن هکرها اغلب اطلاعات مربوط به نقایص امنیتی را پیدا کرده و می‌فروشند، کاملا تحت‌نظر دارند. وودوارد بر این باور است که همه افراد یک تلفن به‌روز با نرم‌افزار به‌روز شده روی آن ندارند. به گفته او برخی از نقاط آسیب‌پذیر قدیمی که اپل و گوگل آنها را با اندروید ترمیم کرده است، هنوز هم می‌توانند وجود داشته باشند.