

جاسوسی سازمان «سیا» از همه مردم جهان

پیامک‌های رئیس جمهوری به مردم رایگان است

خبر

وزیر ارتباطات و فناوری اطلاعات گفت: پیامک‌هایی که رئیس جمهوری به مناسبت‌های مختلف برای عموم مردم ارسال می‌کند، رایگان است و بابت ارسال آنها، هیچ هزینه‌ای به دولت

تحویل نمی‌شود.

به گزارش «ایران»، محمود واعظی در حاشیه نشست هیأت دولت در مورد ابهامات مربوط به هزینه پیامک‌های تلفن همراه که از سوی رئیس جمهوری به مردم ارسال می‌شود، گفت: از همان ابتدا اپراتورها پیشنهاد کردند که رئیس جمهوری می‌تواند از طریق شبکه اپراتورها، بدون هزینه به مردم پیام دهد که دکتر روحانی گفتند من حرفی ندارم. وی افزود: اپراتورها در ایران حتی در دنیا، رویه‌ای دارند که برخی از پیامک‌ها نظیر پیامک رایگان «محیط زیست» یا «روز شهید» را به طور رایگان ارسال می‌کنند.

تشکیل ستاد پیگیری ارتباطات نوری

رئیس سازمان تنظیم مقررات و ارتباطات رادیویی (رگولاتوری)، از تشکیل ستاد نوری حوزه ICT به منظور خدمات‌رسانی و پاسخگویی بهتر و مناسب‌تر به مشترکین اپراتورهای ارتباطی و فناوری اطلاعات در نوروز ۹۶ خبر داد.

به گزارش «ایران»، علی اصغر عمیدیان با اشاره به اینکه این ستاد با حضور نمایندگان رگولاتوری، اپراتورهای تلفن همراه و شرکت مخابرات ایران تشکیل شده است، گفت: براساس ابلاغ سازمان رگولاتوری، اپراتورهای تلفن همراه موظف شده‌اند با برنامه‌ریزی مناسب در ایام نوروز بویژه در جاده‌های پرتردد و نقاط سیاحتی و زیارتی مسافرپذیر نسبت به بهبود وضعیت شبکه و خدمات و همچنین افزایش ظرفیت با استفاده از ایستگاه‌های متحرک اقدام کنند.

وی افزود: پیش‌بینی کشیک‌های نوری در تمامی بخش‌های فنی، نگهداری، تجاری، توسعه، فروش و پشتیبانی برای ارائه خدمات مناسب مشترکین و حضور مستمر در دفاتر و نقاط پاسخگویی در کل کشور با اولویت مکان‌های پرتردد توریستی، زیارتی و سیاحتی نیز از مواردی است که اپراتورها ملزم به اجرای آن هستند. معاون وزیر ارتباطات با اشاره به اینکه در ایام نوروز مصرف خدمات صوتی، پیامکی و اینترنت مشترکین نسبت به روزهای عادی افزایش می‌یابد، تصریح کرد: بر همین اساس اپراتورهای تلفن همراه موظف شده‌اند برنامه‌های ویژه‌ای را برای تخصیص ظرفیت مناسب و مدیریت خدمات داشته باشند که البته این موضوع از چند ماه قبل در دستور کار اپراتورها قرار گرفته و با شناسایی نقاط مرتبط برای بهبود افزایش ظرفیت و خدمات اقدام کرده‌اند.

رئیس سازمان تنظیم مقررات و ارتباطات رادیویی گفت: سامانه تلفنی ۱۹۵ و پایگاه اینترنتی ۱۹۵.ir نیز برای دریافت نظرات مردم و ثبت و رسیدگی به شکایات مشترکین در ایام نوروز فعال است.

میثم لطفی

سایت اینترنتی «ویکی‌لیکس» هفته گذشته یکی از بزرگ‌ترین افشاکاری‌های خود را انجام داد و اسنادی را در رابطه با فعالیت‌ها و ابزارهای جاسوسی سازمان اطلاعات مرکزی آمریکا (CIA) در دستگاه‌های الکترونیکی معمول از جمله گوشی‌های هوشمند، رایانه‌های لوحی، گیرنده‌های تلویزیونی و... منتشر کرد. این مرکز با انتشار بیانیه‌ای توضیح داد: «سازمان اطلاعات مرکزی آمریکا به تازگی کنترل بخش وسیعی از ابزارهای نفوذی و جاسوسی خود شامل بدافزارها، ویروس‌ها، تروجان‌ها، سیستم‌های کنترل از راه دور بدافزار و اسناد مرتبط با آنها را از دست داده است و ما توانستیم به تمام اطلاعات منتشر شده در این زمینه دسترسی پیدا کنیم. این مجموعه استثنایی چندصد میلیون خط‌خط و برنامه را شامل می‌شود.»

ویکی‌لیکس ادعا می‌کند که سازمان اطلاعات مرکزی آمریکا با انجام تحقیقات گسترده موفق شده است آسیب‌پذیری‌های جدید نرم‌افزارهای کاربردی را شناسایی کند و از این طریق به اطلاعات کاربران دسترسی داشته باشند. این اتفاق در حالی صورت گرفته است که رئیس جمهوری سابق آمریکا -باراک اوباما- تمام نهادهای دولتی این کشور را موظف کرده بود در صورت شناسایی هرگونه حفره نرم‌افزاری، شرکت مربوطه را مطلع کند. با تمام این افشاکاری‌ها، آیا ویکی‌لیکس هم‌اکنون از همه مردم جهان جاسوسی می‌کند؟

تفاوت‌های جاسوسی

مرکز ویکی‌لیکس توسط شخصی به نام «جولین آسانز» مدیریت می‌شود و هم‌اکنون اسناد محرمانه سازمان CIA را در قالب بسته‌های موسوم به Vault ۷ منتشر کرده است که تمام اطلاعات مربوط به فعالیت‌های جاسوسی و همکاری سازمان مربوطه در آن وجود دارد. به گفته ویکی‌لیکس، در این

طرح خود را به گونه‌ای دنبال می‌کند که بر اساس آن طیف گسترده‌ای از دستگاه‌های الکترونیکی مورد حملات جاسوسی قرار می‌گیرند که از جمله آنها می‌توان به رایانه شخصی، تلویزیون، گوشی هوشمند و... اشاره کرد. اسناد منتشر شده همچنین نشان داد هر دو سیستم عامل اندروید و iOS در مقابل این فعالیت‌های جاسوسی آسیب‌پذیر هستند و کارمندان اطلاعاتی آمریکا براحتی به داده‌های ذخیره شده در دستگاه‌های مبتنی بر این دو سیستم عامل دسترسی پیدا می‌کنند. ولی جاسوسی با طیف به این گستردگی اهداف ویژه‌ای را هم دنبال می‌کند. هر بار که سازمان CIA بدافزارهای خود را منتشر می‌کند این احتمال وجود دارد تا شرکت نرم‌افزاری



عکس: ZNet

سازمان CIA برنامه‌های دقیقی برای انتشار بدافزارها و دیگر برنامه‌های نرم‌افزاری مخرب در دست دارد که برنامه‌های مخرب‌ترین پلتفرم‌های موجود راهک کنند

نیم‌نگاه

سازمان اطلاعات مرکزی آمریکا طرح خود را به گونه‌ای دنبال می‌کند که بر اساس آن طیف گسترده‌ای از دستگاه‌های الکترونیکی مورد حملات جاسوسی قرار می‌گیرند که از جمله آنها می‌توان به رایانه شخصی، تلویزیون، گوشی هوشمند و... اشاره کرد

از فعالیت مذکور مطلع شود و با انتشار وصله‌های امنیتی جلو فعالیت بدافزار را بگیرد. این اتفاق دقیقاً سال گذشته در آگوست ۲۰۱۶ صورت گرفت. در آن زمان اپل یک به روزرسانی جهانی برای سیستم عامل iOS منتشر کرد که اتفاق مذکور پس از سه هفته گسترده به آیفون در کشورهای عربی صورت گرفت.

در این اسناد همچنین مشخص شد سازمان اطلاعات مرکزی آمریکا موفق شده است به سیستم داخلی تمام تلویزیون‌های سامسونگ با قابلیت اتصال به اینترنت ورود پیدا کند و همکاری با شرکت‌های دیگر در زمینه تلویزیون‌ها به این معنی است که کارمندان اطلاعاتی آمریکا می‌توانند به تمام اتفاقات محیط پیرامون تلویزیون دسترسی پیدا کنند. در بخش

دیگری از این اسناد گفته شده است که دولت آمریکا به صورت مخفیانه حتی سیستم‌های رایانه‌های خودروها را هم هک می‌کند تا آنها را زیر نظر بگیرد. بررسی‌های ویکی‌لیکس نشان داد سازمان CIA برای آنکه بتواند این فعالیت‌های جاسوسی را انجام دهد، از کدهای برنامه‌نویسی شده بسیار پیچیده استفاده می‌کند و از این طریق امکان جلوگیری از فعالیت‌های هکری آن بسیار کاهش می‌یابد.

عامل انتشار اسناد محرمانه

ویکی‌لیکس می‌گوید این اسناد را از یک شبکه ایزوله شده و فوق امنیتی به دست آورده و شبکه مذکور در «هوش سایبری» وابسته به سازمان CIA قرار داشته است. مرکز مذکور در اصل بازوی جاسوسی سازمان اطلاعات مرکزی آمریکا محسوب می‌شود که جرایم سایبری را مدیریت می‌کند و در صورت بروز هرگونه حمله سایبری به دولت آمریکا، جلو آن می‌ایستد. این طور که بررسی‌های اخیر نشان داده است، اسناد محرمانه مذکور از طریق هرکس و پیمانکاران دولت قبلی آمریکا به دست آمده‌اند که این افراد از طریق شیوه‌های مجاز اطلاعات یاد شده را منتشر کردند. در این میان یکی از هرکس‌های وابسته به دولت قبلی آمریکا با ویکی‌لیکس همکاری‌های نزدیک داشته و بخش اعظم آرشیو محرمانه سازمان CIA را در اختیار آنها گذاشته است. هنوز به درستی مشخص نشده است چه کسی این اسناد را برای نخستین بار منتشر کرد. با وجود این پلیس فدرال آمریکا (FBI) می‌گوید اطلاعات مذکور احتمالاً بر اساس فعالیت‌های جاسوسی، یکی از کارمندان سرقت از پیمانکاران دولتی یا شکستن قفل سرورهای مرکزی لورفته است.

از من هم جاسوسی می‌شود؟

آژانس امنیت ملی آمریکا برای انجام فعالیت‌های هکری خود روش‌های متفاوتی را پیش می‌گرفت و با وجود این سازمان CIA در برنامه‌ریزی‌های مجزای خود به صورت نظارتی عمل می‌کند. این اتفاق باعث می‌شود حضور جاسوسی سازمان CIA احساس نشود و این مرکز بتواند بدون ایجاد هرگونه اختلال تمام فعالیت‌های مختلف را زیر نظر بگیرد. این سازمان با استفاده از تکنیک یاد شده توانسته است میلیون‌ها دستگاه گیرنده تلویزیونی را هک کند و روش خود را از روش سازمان NSA کارآمدتر می‌داند.

آژانس اطلاعاتی مذکور به صورت ویژه بر گوشی‌های هوشمند و رایانه‌های لوحی تأکید دارد و از این طریق می‌تواند تمام ارتباطات صورت گرفته بین کاربران را زیر نظر بگیرد. ویکی‌لیکس می‌گوید در هیچ بخشی از این اسناد اعلام نشده است که ابزارهای ارتباطی رمزگذاری شده از جمله واتس‌آپ و سیکنال مورد حملات هکری سازمان CIA قرار گرفته‌اند و به عبارت دیگر این سازمان در فعالیت‌های جاسوسی خود توانسته است به اطلاعات چنین اپلیکیشن‌هایی دسترسی پیدا کند. به هر حال ویکی‌لیکس هشدار داده است که سازمان‌های اطلاعاتی آمریکا از تمام کاربران جهان جاسوسی می‌کنند و بدون آنکه افراد مطلع شوند، می‌توانند به اطلاعات دستگاه موبایلی آنها دسترسی داشته باشند. «مات بلیز»، یکی از مشهورترین کارشناسان امنیتی جهان وابسته به شرکت کسپرسکی روی صفحه اختصاصی خود در شبکه اجتماعی توییتر توضیح داد: «تنها اقدامی که کاربران در مقابل این فعالیت‌های جاسوسی می‌توانند انجام دهند، این است که به صورت دائم نرم‌افزار خود را به‌روز کنند ولی متأسفانه باید اعتراف کرد حتی این اتفاق هم نمی‌تواند جلو فعالیت‌های مخرب سازمان‌های اطلاعاتی آمریکایی را بگیرد.»

جدول سودوکو

ارقام ۱ تا ۹ را طوری در خانه‌های سفید قرار دهید که هر رقم در سطرها، ستون‌ها و مربع‌های کوچک ۳ در ۳ یکبار دیده شود

۱	۵	۳	۶	۷	۸	۵	۸	
۸	۷	۸	۳	۵	۵	۱	۷	
۷	۶	۵	۸	۱	۸	۷	۳	
۷	۸	۶	۱	۵	۸	۷	۵	
۵	۳	۱	۷	۸	۶	۸	۷	
۵	۸	۷	۷	۸	۵	۱	۳	۶
۶			۲		۷		۸	
۸	۵	۸	۵	۷	۳	۱	۹	
۳	۱	۷	۸	۹	۵	۴		

آسان

۸	۸	۷	۵	۵	۱	۶	۳
۵	۶	۵	۱	۳	۷	۸	۸
۳	۷	۱	۸	۶	۸	۵	۷
۱	۸	۶	۵	۸	۷	۳	۵
۷	۳	۷	۵	۸	۱	۵	۷
۸	۵	۵	۳	۸	۱	۶	۷
۶	۷	۲	۶	۵	۷	۲	۷
۷	۱	۸	۶	۵	۷	۳	۸

متوسط

۵				۴	۶		
۹				۶	۷		
	۶	۳			۹		
		۷		۸			۱
				۴			
۱		۳		۲			
		۹		۸	۳		
	۸		۹				۷
		۶	۸				۴

سخت