رویداد

ارزان‌شدن ۲۰ درصدی تعرفه پهنای باند ارتباطات داخلی

• **مهر:** معاون وزیر ارتباطات از کاهش ۲۰درصدی تعرفه پهنای باند ارتباطات داخل کشور برای افزایش ترافیک داخلی در شبکه ملی اطلاعات طبق مصوبه کمیسیون تنظیم مقررات ارتباطات خبر داد. محمدجواد آذری‌جهرمی با اعلام این خبر، گفت: «این مصوبه در جلسه روز دوشنبه ۱۶ اسفند کمیسیون تنظیم مقررات ارتباطات و پیرو پیشنهاد شرکت ارتباطات زیرساخت و توافق با شرکت مخابرات ایران، نهایی شده است». او ادامه داد: «پس از افتتاح فاز دوم شبکه ملی ارتباطات و با هدف توسعه محتوای داخل کشور برای ارائه سرویس در بستر شبکه ملی ارتباطات، پیشنهاد کاهش تعرفه ترنسمیشن زیرساخت با توافق با شرکت مخابرات ایران به سازمان تنظیم مقررات ارتباطات ارائه شد و بعد از جلسات متعدد، روز گذشته کمیسیون تنظیم مقررات تصمیم گرفت برای کاهش هزینه تمام‌شده محتوای داخلی در کشور، تعرفه سرویس انتقال را برای سرویس‌دهندگان این خدمات ۲۰ درصد کاهش دهد». او بیان کرد: «ما قصد داریم با کاهش تدریجی نرخ پهنای باند داخلی، سرویس‌های داخلی ارتباطات به سمتی بروند که اپراتورها دیگر از میزان ترافیک هزینه‌ای از مشترک دریافت نکنند و تنها هزینه‌های مشترک، در قبال سرویس و حق‌اشتراک آن باشد». او گفت: «ما همچنان در حال مانیتور توسعه بازار هستیم و با مدیریت سازمان تنظیم مقررات و توافق با شرکت مخابرات ایران، کاهش مجدد تعرفه پهنای باند ارتباطات داخلی را در حال بررسی داریم و این کاهش قیمت، به اپراتورهای ارتباطی برای توسعه سرویس‌های داخلی و توسعه ترافیک داخلی آزادی عمل می‌دهد». واحد محاسبه تعرفه در این مصوبه براساس مگابیت شده است. برای مثال، مصرف پهنای باند تا صد مگابیت حدود ۲۷ هزار تومان محاسبه می‌شد که اگر این مصرف به صد گیگابیت برسد، قیمت آن ۱۰ هزار تومان محاسبه می‌شد که براساس مصوبه روز گذشته از هر پایه این مصرف، ۲۰ درصد کاهش قیمت محاسبه می‌شود». به گفته او، مصوبه جدید کمیسیون تنظیم مقررات برای کاهش ۲۰درصدی تعرفه پهنای باند ارتباطات داخلی، از اول فروردین سال ۹۶ امکان اجرا دارد.

فروش ۲۲هزارمیلیاردتومانی شرکت‌های فاوا

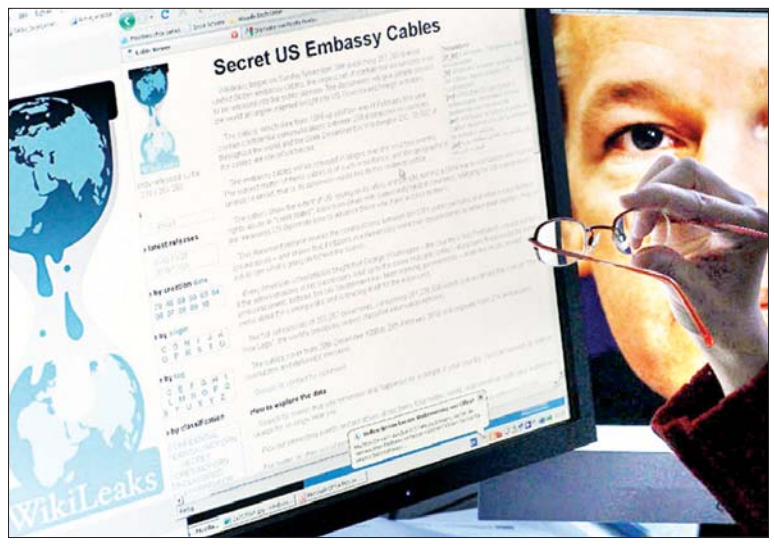
• **شرق:** به گفته رئیس سازمان نظام صنفی رایانه‌ای کشور، هزارو ۴۰۰ اظهارنامه مالیاتی شرکت‌ها جمع‌آوری و بررسی شد و طبق آن، میزان فروش شرکت‌ها ۲۲ هزار میلیارد تومان است. ناصرعلی سعادت در همایش برجام و اقتصاد مقاومتی، سرمایه‌گذاری و اشتغال در حوزه فاوا افزود: «در یک سال گذشته شرکت‌ها ۹۰۰ میلیارد تومان مالیات پرداخت کردند و سود خالص پس از کسر مالیاتشان ۱۲ درصد است. اگر این رقم را به کل کشور تعمیم دهیم و تهران را ۷۰ درصد نسبت به کل صنعت در نظر بگیریم، شرکت‌های صنعت فاوا در سال منتهی به بهمن، حدود ۶۲ هزار میلیارد تومان فروش داشتند و دوهزارو ۶۰۰ میلیارد تومان مالیات پرداخت کردند و سود خالص پس از کسر مالیات آنها، هفت‌هزارو ۵۰۰ میلیارد تومان است. او گفت: «۶۶۵ شرکت به‌عنوان نمونه آماری بررسی شد که طبق آن، سال ۹۵ نسبت به سال ۹۴ رشدی هشت‌درصدی در اشتغال به ثبت می‌رساند». او بیان کرد: «بخش خصوصی با اعتماد به عملکرد دولت در بهبود وضعیت اقتصادی کشور، برای اخذ مجوز فعالیت دوهزارو ۱۰۰ میلیارد تومان هزینه و برای خود ایجاد تعهد کرده است. واضح است که این هزینه پرداخت شده تا پیرو آن، کار و فعالیت انجام شود. اگر این رقم را چهار درصد سرمایه‌گذاری لازم برای فعالیت با پروانه‌های جدید حساب کنیم، جمع سرمایه‌گذاری بخش خصوصی در سه سال آینده، به ۵۲هزارو ۵۰۰ میلیارد تومان می‌رسد».

سیم‌کارت شاتل وارد بازار می‌شود

• **شرق:** با اعطای رسمی «پروانه نوع اول اپراتور مجازی تلفن همراه» از سوی سازمان تنظیم مقررات و ارتباطات رادیویی، شاتل از برنامه خود برای راه‌اندازی نخستین و کامل‌ترین شبکه نسل جدید اپراتور تلفن همراه ایران و عرضه سیم‌کارت‌های نسل جدید با قابلیت برقراری مکالمه، تبادل پیامک و دسترسی به اینترنت بر پایه فناوری‌های 3G و 4G خبر داد. اپراتورهای مجازی نوع اول (Full MVNO) خلاف اپراتورهای مجازی نوع دوم (Light MVNO)، دارای تمام امکانات، تجهیزات فنی و هسته شبکه تلفن همراه بوده و با به‌کارگیری زیرساخت رادیویی شبکه‌های تلفن همراه موجود، خدمات نوآورانه و متمایزی را به مشترکان خود ارائه می‌کنند. سیم‌کارت‌های این شرکت علاوه بر قابلیت برقراری مکالمه و تبادل پیامک به‌عنوان خدمات پایه، آخرین تکنولوژی‌های دسترسی به اینترنت پرسرعت مبتنی بر شبکه‌های 3G، 4G/LTE و 4.5G را به همراه طرح‌ها و خدمات ویژه محتوایی و ارزش‌افزوده، با کیفیت شاتل، در اختیار مشترکان و متقاضیان قرار می‌دهد.

ویکی‌لیکس ۸ هزار سند از سیا را منتشر کرد

جاسوسی از اپل، اندروید، ویندوز و سامسونگ



ویکی‌لیکس هشت‌هزارو ۷۶۱ سند سازمان سیا را که ابعاد تازه‌ای از روش‌های جاسوسی این نهاد را روشن می‌کند، منتشر کرد. براساس گزارش ویکی‌لیکس، سیا از ابزارهایی برای نفوذ به دستگاه‌های ارتباطی ساخته‌شده به وسیله شرکت‌های آمریکایی و اروپایی برای تبدیل آنها به ابزارهای جاسوسی استفاده کرده است. در این مجموعه که با نام Vault7 شناخته می‌شود، هشت‌هزارو ۷۶۱ سند و فایل وجود دارد که به گمان افشاکننده، از شبکه‌ای ایمن درون مقر سازمان سیا در لنگلی (Langly) ایالات ویرجینیا به دست آمده است. این اسناد تعدادی از اکسپلویت‌ها و ابزارهای نفوذ را شرح می‌دهند که شباهت زیادی به کاتالوگ ANT آژانس امنیت ملی دارند؛ مجموعه‌ای که در سال ۲۰۱۳ از سوی هفته‌نامه معتبر اشپیگل آلمان فاش شد. در بین فایل‌های موجود در این مجموعه ویکی‌لیکس، چندین اکسپلویت برای دیوایس‌های مبتنی بر iOS و اندروید دیده می‌شود که بین سال‌های ۲۰۱۴ و ۲۰۱۶ توسعه یافته‌اند. به نظر می‌رسد سازمان سیا در هدف قراردادن دستگاه‌های اندرویدی، با استفاده از ۲۴ اکسپلویت ویژه بسیار موفق بوده؛ ضمن اینکه اکسپلویت‌های iOS نیز به رقم ۱۴ می‌رسد. به گزارش نشریه فوربس، براساس فایل‌های انتشاریافته، سازمان سیا از بدافزاری با نام Weeping Angel برای شنود به وسیله تلویزیون‌های هوشمند سامسونگ استفاده کرده که در سال ۲۰۱۴ با همکاری همتای انگلیسی خود یعنی MI5 کدنویسی شده است. متیو هیکی، محقق امنیت و یکی از مؤسسان «هکر هاوس»، توضیح می‌دهد: Weeping Angel مانند یک اپلیکیشن معمول و نه مانند نرم‌افزاری شبیه به یوتیوب، به صورت غیرمحسوس فعالیت کرده و اقدام به ضبط صدای محیط می‌کند. همچنین می‌تواند به رمز عبور شبکه وای‌فایی دسترسی پیدا کند که تلویزیون از طریق آن به اینترنت متصل شده است. گفتنی است بدافزار اشاره‌شده از این طریق می‌تواند شبکه وای‌فای قربانی را هک کرده و به تمام نام کاربری‌ها و رمز عبورهای ذخیره‌شده در مرورگر تلویزیون، دست یابد. علاوه بر آن، قابلیت دیگری نیز با عنوان «Fake Off» وجود دارد که حتی در زمان خاموش‌بودن تلویزیون نیز به شنود خود ادامه می‌دهد. هیکی با بررسی یادداشت‌های سیا درباره پروژه یادشده، مشاهده کرد در بخشی از آن به کارایی‌نداشتن روش‌های نصب از طریق USB در برخی از فیرمورهای خاص اشاره شده؛ بنابراین گمان می‌برد که Weeping Angel از طریق USB به تلویزیون رخنه کند. با وجود این، او عنوان کرد: کماکان ممکن است راه‌هایی برای آلوده‌شدن تلویزیون از راه دور نیز وجود داشته باشد. نشریه «ورج» هم به نقل از ویکی‌لیکس می‌نویسد: آژانس اطلاعاتی آمریکا آسیب‌پذیری‌های نرم‌افزاری جدی را جمع‌آوری کرده تا بتواند بعدها از آنها سوءاستفاده کند؛ درحالی‌که طبق دستور صریح دولت اوباما، هر نهاد امنیتی در صورت کشف باگ‌های روز صفر، باید شرکت‌های مربوطه را در جریان قرار دهد. در این اسناد آمده است: «تازمانی‌که سازمان سیا آسیب‌پذیری‌ها را از شرکت‌هایی مانند اپل و گوگل مخفی نگه دارد، شرکت‌ها توانایی برطرف‌کردن آنها را ندارند و موبایل‌ها به‌راحتی نفوذپذیر خواهند بود». نکته مهم اینکه اگر سازمان سیا توانسته این آسیب‌پذیری‌ها را کشف کند، قطعا هکرهای دیگر نیز موفق به انجام چنین کاری شده‌اند و از طرفی، موبایل‌های مستعد نفوذ در دستان مقامات دولتی و افراد سرشناس جامعه نیز وجود دارند که احتمال جاسوسی از آنها را تا حد زیادی بالا می‌برد. شرکت اپل، سیستم‌عامل اندروید، ویندوز و حتی تلویزیون‌های هوشمند سامسونگ، ازجمله اهداف این برنامه بوده‌اند. سیا تلاش کرده با نفوذ به این دستگاه‌ها یا دستگاه‌هایی که با این سیستم‌عامل‌ها کار می‌کنند، از آنها برای شنود از کاربران استفاده کند. اپل در واکنش به این خبر، ادعاها مبنی بر اثربخش‌بودن تلاش‌های سیا را برای سوءاستفاده از آسیب‌پذیری‌های موجود در محصولاتش، رد کرده است. سخنگوی اپل دراین‌زمینه گفته است: «اپل به‌شدت متعهد است از حریم خصوصی و امنیت کاربران خود محافظت کند. تکنولوژی‌های به‌خدمت گرفته‌شده درون آیفون‌های امروزی از بهترین سطح امنیت موجود بهره می‌گیرند و ما نیز مرتب تلاش داریم این سطح از استاندارد را حفظ کنیم. محصولات و نرم‌افزارهای ما به‌گونه‌ای طراحی شده‌اند تا در کمترین زمان ممکن، آپدیت‌های امنیتی را به دست مشتریان‌مان برسانند و تقریبا ۸۰ درصد از کاربران ما حالا جدیدترین نسخه از سیستم‌عامل iOS را روی موبایل‌هایشان دارند. تحلیل‌های اولیه ما حکایت از آن دارند که بسیاری از آسیب‌پذیری‌های مطرح‌شده در اسناد ویکی‌لیکس، در جدیدترین نسخه از iOS رفع شده‌اند؛ با این همه، همچنان با سرعت کار می‌کنیم تا همه این موارد را رفع کنیم. ما همواره از کاربرانمان می‌خواهیم جدیدترین نسخه از iOS را دانلود کنند تا مطمئن شوند به جدیدترین آپدیت‌های امنیتی دسترسی دارند». یکی از ابزارهای ساخته‌شده با مشارکت ام‌آی۵ انگلستان، پس از نفوذ به تلویزیون‌های هوشمند سامسونگ، عملا این دستگاه‌ها را به وسیله شنود بدل می‌کند؛ هرچند تلویزیون به ظاهر خاموش است؛ اما در واقع تلویزیون در حالت «خاموشی ساختگی» قرار گرفته و در حال ضبط همه مکالمات و صداهای محیط و ارسال آنها به سیا است. سیا همچنین در سال ۲۰۱۴ تلاش کرده تا به سامانه‌های ناوبری خودروهای پیشرفته نفوذ کند. این کار به سیا اجازه می‌دهد بدون آنکه کسی متوجه شود، کنترل خودرو را به دست گرفته و در صورت نیاز، با تصادفی ساختگی سرنشینان را از بین ببرد. واحد «تجهیزات متحرک» سیا هم ابزارهای متعددی تولید کرده که می‌توانند با نفوذ به تلفن‌های هوشمند، به صورت مخفیانه دوربین و میکروفون تلفن را فعال کنند. ازآنجاکه بسیاری از شخصیت‌های مطرح از گوشی‌های آیفون استفاده می‌کنند، واحد ویژه‌ای برای نفوذ به گوشی‌های آیفون و دیگر تجهیزاتی که با سیستم‌عامل iOS کار می‌کنند، در سیا ایجاد شده است. واحد مشابهی هم برای نفوذ به تجهیزات دارای سیستم‌عامل اندروید ایجاد شده است. تلفن‌های همراه سامسونگ، اچ‌تی‌سی، سونی و دیگر شرکت‌هایی که گوشی‌های اندروید تولید می‌کنند، هدف این واحد بوده‌اند. این روش‌ها به سیا این امکان را داده‌اند تا روش‌های کدگذاری نرم‌افزارهایی مانند واتس‌اپ، سیگنال، تلگرام و دیگر نرم‌افزارهای پیام‌رسان را دور بزنند. همچنین گفته شده سیا علاوه بر مرکز ویرجینیا، از کنسولگری آمریکا در فرانکفورت آلمان به‌عنوان پایگاهی مخفی برای انجام فعالیت‌های سایبری علیه اهداف مدنظر در اروپا، خاورمیانه و آفریقا استفاده می‌کند. ویکی‌لیکس مدعی است از این کنسولگری به‌عنوان پوششی برای هکرهای درحال‌فعالیت در اروپا، خاورمیانه و آفریقا استفاده می‌شود.

> **یکی از ابزارهای ساخته‌شده با مشارکت ام‌آی۵ انگلستان، پس از نفوذ به تلویزیون‌های هوشمند سامسونگ، عملا این دستگاه‌ها را به وسیله شنود بدل می‌کند؛ هرچند تلویزیون به ظاهر خاموش است؛ اما در واقع تلویزیون در حالت «خاموشی ساختگی» قرار گرفته و در حال ضبط همه مکالمات و صداهای محیط و ارسال آنها به سیا است**

دریچه

تلویزیونی با فناوری نانوسل

• کارشناسان بر این عقیده‌اند که استراتژی دوگانه پرمیوم برای تلویزیون، سهم بازارش را در صنعت جهانی تلویزیون افزایش دهد؛ از جمله تلویزیون SIGNATURE OLED W که از این ماه در کره و آمریکا موجود خواهد بود. این تلویزیون، با استفاده از پیشرفته‌ترین فناوری‌های موجود در صنعت نمایشگر، نشانگر هدف اعلای این شرکت برای بهترین تجربه تماشای تلویزیون است. این سری از تلویزیون‌ها برای اولین‌بار در این بازار صدای نوآورانه Dolby Atmos را ارائه می‌کند و باعث کیفیت صدا و تصویر خیره‌کننده‌ای می‌شود؛ Dolby Atmos محل نسبی هر صدا را ایزوله می‌کند تا صدایی چندلایه و غنی تولید کند و صداهای پیچیده دنیای واقعی را انعکاس دهد. نسل سوم تلویزیون SUPER UHD از فناوری نانوسل بهره می‌برد که ذراتی به‌اندازه یک نانومتر را کنترل کرده و بازسازی رنگ را با دقت بی‌نظیری به نمایش می‌گذارد. صفحه‌نمایش نانوسل با جذب طیف نورهای اضافی و در نتیجه ایجاد رنگ‌های خالص‌تر و تمیزتر، به کیفیت تصویر فوق‌العاده‌ای دست پیدا کرده است. قابلیت جذب نور، به صفحه‌نمایش جدید LCD اجازه می‌دهد رنگ‌های خاصی را با دقت بالاتر فیلتر کرده و هر رنگ را همان‌گونه که در اصل بوده، به نمایش بگذارد. فناوری Active HDR به تلویزیون‌ها امکان پردازش صحنه‌به‌صحنه تصویر را می‌دهد و اطلاعات پویایی را در زمان نیاز میسر می‌کند. علاوه بر این، تلویزیون‌های ۲۰۱۷ از پالت کامل فرمت‌های HDR پشتیبانی می‌کند که شامل HDR10، Dolby Vision و HLG یا Hybrid Log Gamma است. این تنوع باقابلیت جدید HDR Effect ترکیب می‌شود و محتوای استاندارد را پردازش می‌کند تا روشنایی را در فضاهای خاص بهتر کند، نسبت تصویر را بهبود بخشد و در نتیجه تمام اینها، تصاویری دقیق‌تر را به نمایش بگذارد. جدیدترین پلتفرم تلویزیون هوشمند webOS، تمام سری تلویزیون‌های فوق‌پیشرفته را به‌طور استثنایی کاربرپسندتر می‌کند. بینندگان می‌توانند با فشاردادن کلید اصلی روی کنترل از راه دور، فورا به سرویس‌های موردعلاقه خود مانند نت‌فلیکس و آمازون پرایم ویدئو دسترسی پیدا کنند و با به دنیایی بزرگ از سرگرمی‌ها و برنامه‌های متنوع با کیفیت خیره‌کننده 4K بگذارند.

امنیت

فلوکی، بدافزاری برای سرقت اطلاعات کارت‌های اعتباری

بات‌نت فلوکی (Floki)، نمونه جدیدی از بدافزارهای بانکداری است که به‌تازگی در بازارهای Dark Net برای فروش گذاشته شده و از طریق پست الکترونیکی گسترش پیدا می‌کند و از آن برای سرقت اطلاعات کارت‌های اعتباری قربانیان استفاده می‌شود. بدافزار بات‌نت فلوکی، مبتنی بر کد مبنای مشابهی است که به وسیله بات‌نت مشهور زئوس (Zeus) استفاده شد؛ کُدی که در سال ۲۰۱۱ منتشر شد. به جای کپی ساده خصوصیاتی که در بات‌نت زئوس وجود داشتند، بات‌فلوکی قابلیت‌های جدیدی اضافه کرد که آن را به ابزار جالبی برای مجرمان تبدیل کرد. به گفته شرکت تلوس (Talos)، اصلاحاتی در مکانیسم ارسال موجود در کد منبع زئوس ایجاد شده است؛ به‌طوری‌که شناسایی بات‌فلوکی را مشکل‌تر می‌کند. به گزارش ایسنا، بات‌فلوکی از سوی توسعه‌دهندگان به قیمت هزار دلار به فروش می‌رسد و مبتنی بر بات‌نت زئوس است. هرچند محققان به‌تازگی متوجه شدند که بات‌فلوکی دارای قابلیت‌های جدیدی ازجمله ضدتشخیص است. شرکت تلوس کد نسخه جدید بدافزار را نیز بررسی کرده و متوجه شده قابلیت عملیات روی شبکه Tor نیز در این بدافزار موجود است، ولی هنوز عملکرد فعالی از آن مشاهده نشده است. محققان شرکت فلش‌پوینت معتقدند نام استفاده‌شده به وسیله این بدافزار، یک نام برزیلی است. همچنین محققان مشخص کردند که ارتباطات عوامل این بات در پرتغال است و آدرس‌های IP و دامنه‌های برزیلی را هدف قرار داده‌اند و در حالت کلی به دستگاه‌هایی که زبان پیش‌فرض آنها روی پرتغالی تنظیم شده است، علاقه‌مند هستند. شرکت فلش‌پوینت عوامل این بات را «اتصال‌دهنده» (رابط) نامید؛ زیرا در تعداد زیادی از انجمن‌های خارج از برزیل، ازجمله انجمن‌های زیرزمینی Dark Web در روسیه و انگلستان، حضور دارند. محققان معتقدند با حضور در وب‌گاه‌های خارجی، این مهاجمان دانش و ابزارهای مختلفی را وارد انجمن‌های برزیل می‌کنند. علاوه بر قابلیت‌هایی که این بدافزار از بات‌نت زئوس گرفته است، دارای قابلیت قلاب‌کردن نیز هست که از این طریق می‌تواند اطلاعات کارت‌های پرداخت را از حافظه به دست آورد. در یک پویش، بات‌نت فلوکی که از سوی فلش‌پوینت مشاهده شده بود، ۲۲۵ بات اطلاعات نزدیک به هزارو ۳۷۵ کارت اعتباری را به سرقت بردند. در حوزه جرائم سایبری مالی، پیشرفت ادامه‌دار بدافزار شناخته‌شده بات‌فلوکی مشاهده می‌شود که از سوی فعالی به نام فلوکی‌بات (flokibot) از سپتامبر ۲۰۱۶ عرضه شده است. سازندگان بدافزار دائما فناوری خود را برای دورزدن، شناسایی و کنترل‌ها تطبیق می‌دهند. این بدافزارهای جدید، قبل از انتشار در اینترنت بدون هشدار قبلی معمولا از سوی فعالانی ساخته می‌شود که در اعماق Dark Web فعالیت دارند و شرکت‌ها را مستأصل می‌کنند. درحالی‌که مجرمان سایبری برزیلی معمولا به اندازه همتاهای روسی خود ماهر نیستند، غالبا فرم‌های جدید بدافزار (برای درنظرگرفتن باج‌افزار نقطه فروش (PoS) و تروجان‌های بانکداری) را طلب کرده و خدمات خود را پیشنهاد می‌دهند. به نظر می‌رسد حضور در انجمن‌های روسی اعماق Dark Web می‌تواند عامل احتمالی در پیشرفت فلوکی باشد.