جاسوسی گسترده انگلیس از تمامی کاربران اینترنت

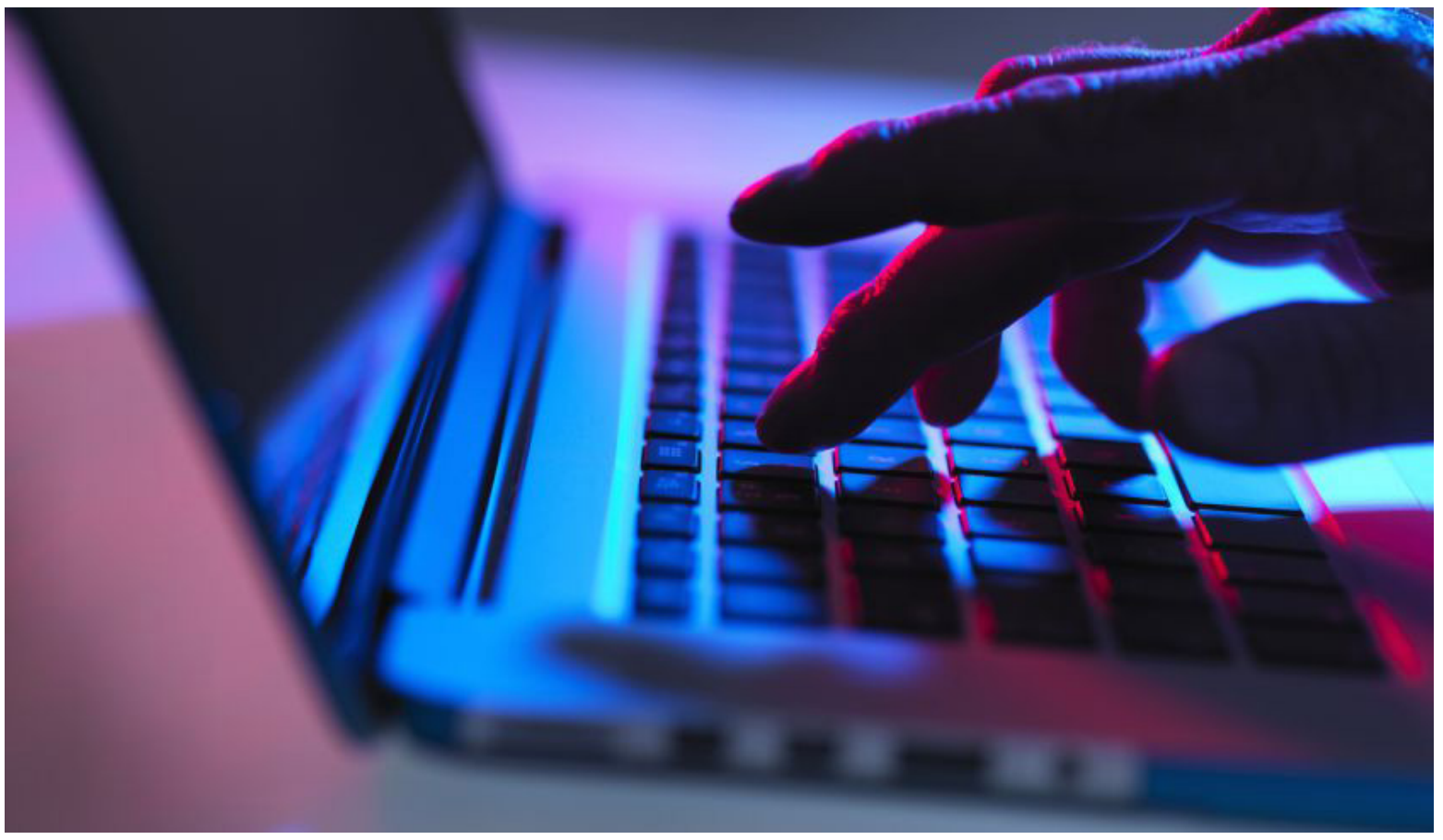
اگر شما جزء افرادی هستید که از سال ۲۰۰۷ به بعد از وب استفاده کرده‌اید ستاد ارتباطات انگلیس به احتمال بسیار زیاد از شما جاسوسی کرده است. اسناد جدیدی که در سایت اینترسپت متعلق به ادوارد اسنودن و گلن گرینوالد منتشر شده نشان می‌دهد که برنامه‌ای موسوم به Karma Police توسط ستاد ارتباطات دولت انگلیس برای جاسوسی از تمامی کاربران اینترنت طراحی شده است. در قالب این برنامه تمامی عادات کاربری افراد در جهان مورد بررسی و جاسوسی قرار گرفته است. سایت اینترسپت این برنامه جاسوسی را بزرگ‌ترین برنامه جمع‌آوری اطلاعات از اینترنت لقب داده است. زیرا در قالب برنامه یاد شده از تمامی کاربران قابل رویت در فضای مجازی جاسوسی شده است. برنامه Karma Police در ابتدا برای جاسوسی از کاربرانی طراحی شد که به شبکه‌های رادیویی اینترنتی گوش می‌کردند و ماهیت تحقیقاتی داشت تا مشخص شود چه افرادی از رادیوهای اینترنتی برای انتشار پیام‌های تبلیغاتی نامناسب استفاده می‌کنند. ستاد ارتباطات انگلیس از این طریق قصد داشت اطلاعاتی در مورد محتوای مذهبی و اسلامی در فضای مجازی و افرادی که به این اطلاعات گوش می‌کنند یا آن‌ها را جمع‌آوری می‌کنند، گردآوری کند. گام بعدی شناسایی حساب‌های کاربری این افراد در اسکایپ و حساب‌های کاربری‌شان در شبکه‌های اجتماعی بود. بر طبق اسناد ستاد ارتباطات دولت انگلیس تا سال ۲۰۰۹ از طریق این برنامه جاسوسی بیش از ۱/۱ تریلیون مورد جاسوسی از مرورگرهای اینترنتی کاربران صورت گرفته است. تا سال ۲۰۱۰ از طریق این سیستم هر روز ۳۰ میلیارد سابقه در مورد هر کاربر جمع‌آوری شد.

تحقیقات در مورد سوءاستفاده گوگل از اندروید

کمیسیون فدرال ارتباطات آمریکا می‌گوید تحقیقات در مورد احتمال سوءاستفاده گوگل از برتری اندروید در بازار سیستم‌عامل‌های همراه برای بازاریابی دیگر محصولاتش را آغاز کرده‌است. این کمیسیون معتقد است که روش‌های مورد استفاده گوگل بدین منظور غیرعادلانه و غیررقابتی بوده است. گوگل از این شیوه برای افزایش استفاده از خدماتی همچون جست‌وجوی گوگل و خدمات نقشه خود بهره‌برداری کرده است. کارشناسان می‌گویند گوگل به طور مستقیم از سیستم‌عامل اندروید سود تجاری کسب نمی‌کند، زیرا استفاده از این نرم‌افزار رایگان است. اما با توجه به نصب آن روی بیش از ۸۰ درصد از گوشی‌های هوشمند در جهان و ۵۲ درصد از گوشی‌ها در آمریکا بازار مناسبی برای استفاده از خدمات و محصولات مبتنی بر این سیستم‌عامل به وجود آمده است. گوگل استفاده از بسیاری از خدمات دیگر خود را هم به استفاده از اندروید منوط کرده یا خدمات مذکور را روی اندروید با کیفیت و امکانات بیشتری ارائه می‌دهد. اندروید بر خلاف سیستم‌عامل iOS اپل اکوسیستم بازی دارد و طراحی برنامه‌ها و خدمات برای آن محدودیتی ندارد. این در حالی است که اپل برنامه‌ها و خدمات طراحی شده برای iOS را به دقت کنترل می‌کند. گوگل به ازای باز بودن سیستم اندروید آن را با خدمات دیگرش همچون نقشه، جیمیل، جست‌وجو و... گره زده است. طی ماه‌های اخیر برخی شرکت‌های سازنده برنامه‌های همراه به همین علت از گوگل به وزارت دادگستری آمریکا شکایت کرده‌اند. به همین علت کمیسیون فدرال ارتباطات آمریکا برای بررسی موضوع وارد عمل شده است. گوگل هنوز در این زمینه اظهارنظری نکرده است.

امنیت؛ هیچ کس، هیچ کجا!

پنج یافته جالب توجه در مورد حملات سایبری



حملات سایبری در انواع و اقسام مختلف و با وسعت زیاد طی سال‌های اخیر به یکی از بزرگ‌ترین معضلات دنیای جدید تبدیل شده است. وسعت، شدت و گستردگی حملات سایبری به قصد سرقت اطلاعات طی این چند سال به حدی زیاد شده است که اکنون بسیاری از کاربران در خصوص فاش شدن اطلاعات حساس شخصی خود و افتادن آن‌ها به دست مجرمان سایبری بی‌تفاوت و به‌گونه‌ای بی‌حس شده‌اند. این موضوع از گزارشی که اخیرا موسسه و شرکت امنیت سایبری Trend Micro منتشر کرده است و طی آن به تجزیه و تحلیل یک دهه سرقت اطلاعات سایبری پرداخته است، مشخص می‌شود. این گزارش یادآور شده است که شرکت‌های تجاری به این دلیل که اطلاعات آن‌ها بیش از هر چیز برای هکرها سودآور است، بیشتر در معرض حمله و تهدیدات سایبری قرار دارند. اما در این میان همچنین کاربران به عنوان قربانیان اصلی حملات سایبری مطرح‌اند.

این گزارش مجموعه‌ای مشتمل بر ۴۶۰۰ مورد سرقت اطلاعات و هک بزرگ را از سال ۲۰۰۵ و از پایگاه اطلاعات Privacy Right Clrariinghouse مورد تجزیه و تحلیل قرار داده است. این اطلاعات و موارد شامل سرقت‌های بزرگ اطلاعاتی نظیر سرقت اطلاعات از وب سایت مشهور Ashley Madison را در بر می‌گیرد. پنج مورد از جالب‌ترین یافته‌های این گزارش به شرح زیر است.

علاقه هکرها به حمله به شبکه‌ها و صنایع درمان و سلامت

کسب و کارهای مربوط به حوزه سلامت یکی از مهم‌ترین اهداف هکرها را تشکیل می‌دهد و البته به دنبال آن نهادهای دولتی و خرده‌فروشی‌های جزو بزرگ‌ترین اهداف حملات سایبری است. حوزه سلامت گنجینه‌ای از اطلاعات شخصی است که در راستای اختلاس‌ها و تخلفات مالی یک هدف بسیار خوب و پر و پیمان برای هکرها به حساب می‌آید. اطلاعات موجود در این سامانه‌ها همچون شماره‌های هویتی، آدرس، نام و تاریخ تولد، بهترین و مطلوب‌ترین گزینه‌ها را برای دسترسی به اطلاعات مالی کاربران در اختیار هکرها قرار می‌دهد.

رشد ۱۶۹ درصدی هک کارت‌های اعتباری از ۵ سال گذشته

از سال ۲۰۱۰ تا کنون هکرها به شکلی گسترده با استفاده از ابزارهای الکترونیکی با نام Skimmers و همچنین مداخله و نفوذ به ترمینال‌های تراکنش مالی در فروشگاه‌های بزرگ، اطلاعات مالی مربوط به کارت‌های اعتباری را به سرقت برده‌اند. یکی از نمونه‌های جالب سرقت اطلاعات کارت‌های اعتباری که در این گزارش به آن اشاره شده است، مورد نصب یک بدافزار روی سامانه ثبت نام دیجیتال یکی از فروشگاه‌های بزرگ تجاری در ایالات متحده آمریکاست.

بدافزارها ابزارهای مورد علاقه هکرها

اگر یک ایمیل مشکوک دریافت کردید که ادعا می‌کرد از سوی بانک برای شما ارسال شده است به هیچ وجه روی هیچ کدام از لینک‌های داخل آن ایمیل کلیک نکنید. چرا که در غیر این صورت به احتمال بسیار زیاد سیستم شما آلوده به یک بدافزار خواهد شد و با نصب این بدافزار در سیستم، هکرها به سادگی قادر به گشت و گذار در بین فایل‌ها و اطلاعات شخصی ما و سرقت موارد جالب توجه خواهند شد. این روش معمول که از آن تحت عنوان Phishing یاد می‌شود به هکرها این امکان را می‌دهد که به سهولت و بدون نیاز به دسترسی فیزیکی به سیستم قربانی اطلاعات مورد نظر خود را استخراج و سرقت کنند. طبق گزارش یاد شده، بدافزارهایی نظیر Worm ها هنوز هم جزو محبوب‌ترین و شایع‌ترین ابزارهای هکرها برای سرقت اطلاعات هستند.

بازارهای فراگیر و در حال رشد خرید و فروش اطلاعات

هکرها و مجرمان سایبری معمولا اطلاعات سرقت شده از کاربران نظیر اطلاعات مالی و هویتی قربانیان خود را در بازارهایی که در Deep Web قرار دارد به فروش می‌رسانند. Deep Web یا همان Dark Web مکانی است در اینترنت که عملا با جست‌وجو از طریق موتورهای جست‌وجوگر یافت نمی‌شود و در معرض دید عموم قرار ندارد. گزارش Trend Micro یاد آور شده است که اطلاعات هویتی و مالی قربانیان مربوط به حساب‌های eBay، PayPal، Facebook، Amazon، FedEx و NetFlix اکنون به شکلی گسترده در این بازارهای آنلاین غیرمجاز و غیرقابل رویت خرید و فروش می‌شوند. قاعدتا اطلاعات مربوط به یک حساب کاربری به اندازه اطلاعات مربوط به سامانه‌های سلامت و بانکی ارزشمند نیست اما برای یک هکر و در راستای آسیب جدی به قربانیان به اندازه کافی کارآمد است. برای مثال یک هکر می‌تواند از طریق اطلاعات حساب کاربری Facebook به سادگی به همه سایت‌هایی که از حساب کاربری فیسبوک قربانی استفاده می‌کنند دسترسی پیدا کند. از این مسیر اطلاعات ارزشمند دیگری در مورد قربانی و فعالیت‌های وی - احتمالا فعالیت‌های مالی - در اختیار هکرها قرار می‌گیرد. یکی از این نمونه‌ها که در این گزارش از آن یاد شده مربوط به سرقت اطلاعات Uber و سوء استفاده مالی از آن است.

از گوشی هوشمند و لپتاپ خود مانند چشمانتان حفاظت کنید

هرچند معمول‌ترین و شایع‌ترین روش هکرها برای سرقت اطلاعات عبارت است از اغفال قربانیان و نصب بدافزار روی گوشی هوشمند یا لپتاپ آن‌ها، اما دسترسی فیزیکی به این دستگاه‌ها و ابزارها گنجینه بزرگی از اطلاعات باد آورده را در اختیار آن‌ها قرار می‌دهد. ابزارها و دستگاه‌های سرقت شده یا گم شده نظیر لپتاپ‌ها، گوشی‌های هوشمند، USB Flash و سایر سخت‌افزارهای مشابه، در صدر موضوعات مورد علاقه هکرها و مجرمان سایبری قرار دارد. در این فهرست روش‌هایی مانند Phishing و نصب بدافزار در رده دوم قرار دارد.

افزایش سرعت رایانه‌ها تا ۱۰۰۰ برابر

پیشرفت قابل توجه رایانه‌ها در ۵۰ سال گذشته تا حد زیادی مدیون توانایی ساخت ترانزیستورهای سیلیکونی کوچک است. روش جدید طراحی و ساخت تراشه‌های رایانه‌ای می‌تواند به پردازش دست‌کم ۱۰۰۰ برابر سریع‌تر از بهترین تراشه‌های موجود در بازار بینجامد. این روش جدید که روی موادی به نام لوله‌های کربنی نانو متکی است به دانشمندان این امکان را می‌دهد که تراشه را سه‌بعدی بسازند. ماکس شولا کریکی از طراحان این تراشه و دانشجوی دکترای مهندسی الکترونیک در دانشگاه استنفورد کالیفورنیا گفت: طراحی سه‌بعدی این تراشه دانشمندان را قادر می‌سازد که حافظه (ممووری) را که داده‌ها را ذخیره می‌کند در یک فضای کوچک در کنار پردازنده‌های قدرتمند تعبیه کنند. شولا کر افزود: کاهش فاصله بین این دو قطعه می‌تواند زمان پردازش را به شکل قابل توجهی پایین بیاورد. پیشرفت قابل توجه رایانه‌ها در ۵۰ سال گذشته تا حد زیادی مدیون توانایی ساخت ترانزیستورهای سیلیکونی کوچک است که عملکردهای منطقی رایانه‌ها را انجام می‌دهند. براساس قانون مور (قانونی که اولین بار توسط گوردون ای مور محقق آمریکایی در سال ۱۹۶۵ ارائه شد، تعداد ترانزیستورها در یک تراشه سیلیکونی هر دو سال تقریبا دو برابر خواهد شد. مطابق پیش‌بینی این محقق ترانزیستورها روز به روز کوچک‌تر شده و به کوچک‌ترین بخش رایانه‌ها که اندازه‌شان حتی پنج نانومتر شده تبدیل شده‌اند و سایز کاربردی‌ترین تراشه‌ها در حال حاضر تنها هفت نانومتر است. کارشناسان می‌گویند، اما کاهش سایز به این معنی است که اثرات کوانتومی ذرات در این مقیاس می‌تواند عملکرد آن‌ها را مختل کند. بنابراین این احتمال وجود دارد که قانون مور تا ۱۰ سال آینده به پایان خودش برسد. شولا کر گفت: مانع اصلی سر راه سریع‌تر شدن رایانه‌ها سرعت کم پردازنده نیست بلکه مشکل حافظه است.

یک کمپین بدافزاری هزاران وب سایت را آلوده کرد

فعالیت کمپین بدافزاری جدید وردپرس هزاران سایت و بازدیدکنندگان آن را در معرض خطر قرار داده است. این کمپین VisitorTracker نامیده شده است و وب سایت‌ها را از طریق آسیب‌پذیری‌های جدید موجود در پلاگین‌های نصب شده بر روی وردپرس آلوده می‌کند. بنا به نظر محققان هزاران وب‌سایت به این بدافزار جدید آلوده شده‌اند که ۹۵ درصد آن‌ها مبتنی بر وردپرس است و از این میان ۱۷ درصد از لیست سیاه گوگل قرار گرفته است. مدیران وب‌سایت‌ها باید اطمینان حاصل کنند که تمامی پلاگین‌ها به آخرین نسخه به روز شده است. این کمپین جدید توسط SucuriLabs شناسایی شده و تقریبا از ۲۰ روز پیش شروع به فعالیت کرده است اما نرخ آلودگی وب‌سایت‌ها در چند روز گذشته افزایش قابل توجهی داشته است. بر این اساس از ۱۵ سپتامبر تا ۱۷ سپتامبر نرخ آلودگی‌ها از ۱۰۰۰ وب سایت در روز به ۶۰۰۰ وب‌سایت در روز افزایش یافته است. وب‌سایت‌ها توسط بدافزار visitorTracker_isMob آلوده شده‌اند و این بدافزار باعث می‌شود تا بازدیدکنندگان به سمت صفحه‌ای حاوی بسته سوءاستفاده NuclearExploit Kit هدایت شوند. پس از آن که کاربر به صفحه مخرب وارد شود، بسته سوءاستفاده به طور بالقوه سیستم قربانی را بررسی کرده و آسیب‌پذیری‌های اصلاح نشده‌ای را که می‌تواند از آن‌ها سوءاستفاده کند، جست‌وجو می‌کند. اگر نرم‌افزار اصلاح نشده و به روز نشده‌ای یا آسیب‌پذیری اصلاح نشده‌ای یافت شود، سیستم قربانی در معرض خطر قرار می‌گیرد و به طور بالقوه می‌تواند منجر به افشای اطلاعات شود.

رصدخانه

نمایشگاه «تلکام» افتتاح شد

شانزدهمین نمایشگاه بین‌المللی صنایع مخابرات و اطلاع‌رسانی (تلکام) امروز با حضور دبیر شورای‌عالی فضای مجازی آغاز به کار کرد. برخلاف سال‌های قبل که به‌طور معمول این نمایشگاه با حضور وزیر ارتباطات و فناوری اطلاعات افتتاح می‌شد، امسال به دلیل همراهی وزیر ارتباطات با هیئت همراه رئیس جمهوری، دبیر جدید شورای‌عالی فضای مجازی این نمایشگاه را افتتاح کرد. در مراسم افتتاحیه این نمایشگاه نصرالله جهانگرد- رئیس سازمان فناوری اطلاعات و معاون وزیر ارتباطات- نیز به نمایندگی از وزارت ارتباطات حضور دارد. نمایشگاه تلکام بزرگ‌ترین نمایشگاه صنایع مخابراتی منطقه خاورمیانه به‌شمار می‌رود که امسال در آن ۲۱۲ شرکت و واحد تولیدی داخلی و حتی شرکت خارجی یا نمایندگی‌های آنان از ۱۸ کشور جهان به معرفی دستاوردهای خود در این نمایشگاه پرداخته‌اند. نمایشگاه تلکام ۲۰۱۵ از امروز تا هفتم مهرماه در محل دائمی نمایشگاه‌های بین‌المللی تهران برگزار می‌شود.

کالاهای فاقد گارانتی قاچاق محسوب می‌شوند

فروشندگان کالاهای فاقد گارنتی تا پایان آذرماه برای پاکسازی واحدهای خود فرصت دارند. اتحادیه صنف فناوران رایانه با هدف ساماندهی به بازار کالاهای دیجیتال و فناوری در کشور به فروشندگان و فعالان صنف کالاهای کامپیوتری اطلاعیه صادر کرد. براین اساس این اتحادیه اعلام کرد: فروشندگان کالاهای سرمایه‌ای که به‌صورت عمده یا خرده فعالیت می‌کنند، مکلف‌اند تا پایان آذرماه سال جاری متناسب با نوع کالا، خدمات پس از فروش ارائه کنند. با پایان این مهلت، کالاهای فاقد گارانتی، کالای قاچاق محسوب می‌شوند. همچنین واحدهای صنفی که کالا با کارت‌های گارانتی بی‌ارزش و فاقد اعتبار به مصرف‌کنندگان ارائه می‌دهند، با معرفی اتحادیه به سازمان تعزیرات حکومتی، علاوه بر ضبط کالا، ۴ برابر ارزش کالا جریمه شده و در صورت فروش کالا پس از مهلت مقرر شده، واحد صنفی طبق قانون پلمب می‌شود.

اطلاعات پرچم‌داران جدید مایکروسافت فاش شد

لو رفتن یک اسلاید مربوط به گوشی‌های هوشمند لومیا ۹۵۰ و ۹۵۰ ایکس ال اطلاعات سخت‌افزاری این دو پرچم‌دار جدید را فاش کرد. لومیا ۹۵۰، از نمایشگری ۵/۲ اینچ با رزولوشن ۱۴۴۰ در ۲۵۶۰ پیکسل بهره می‌برد. چیپست این تلفن همراه، اسنپدراگون ۸۰۸ بوده که سیستم- بر- چیپی با پردازنده ۶ هسته‌ای است. به همراه این چیپست، سه گیگابایت رم و ۳۲ گیگابایت حافظه داخلی به این تلفن همراه افزوده شده‌اند. Lumia ۹۵۰ XL اما از سخت‌افزار قوی‌تری نسبت به مدلی که در مورد آن صحبت کردیم استفاده می‌کند. نمایشگر، ۵/۷ اینچ با همان رزولوشن 2K است اما تفاوت اصلی در میان این دو دستگاه، استفاده از اسنپدراگون ۸۱۰ بوده که در واقع، می‌تواند نسبت به نمونه کوچک‌تر قدرت پردازشی بیشتری را به ارمغان آورد. باتری در لومیا ۹۵۰ برابر با ۳۰۰۰ میلی‌آمپر است و این حجم در نمونه XL، به ۳۳۰۰ میلی‌آمپر می‌رسد.