رویداد

جلوگیری از دامپینگ در تولیدات حوزه «آی‌سی‌تی»

• **ایسنا:** به گفته مدیرعامل پیشین مخابرات ایران تولید داخلی منجر به جلوگیری از ایجاد دامپینگ از سوی شرکت‌های خارجی و افزایش کیفیت تولیدات داخلی می‌شود. صابر فیضی دراین‌باره بیان کرد: «کیفیت تولیدات داخلی در حوزه‌های نرم‌افزاری و سخت‌افزاری بسیار درخورتوجه است». به گفته او ما در این حوزه‌ها در عرصه جهانی حرف برای گفتن داریم؛ اما مسئله مهم حمایت از این تولیدات و شرکت‌های داخلی از طریق تسهیلات بانکی و همچنین تنظیم دقیق و صحیح مقررات در بازار رقابت است که در فصل ششم اصل ۴۴ قانون اساسی بر آن تاکید شده است. او بیان کرد: «بخش دولتی دیگر ظرفیت ایجاد اشتغال برای خیل عظیم فارغ‌التحصیلان دانشگاهی را ندارد؛ بنابراین باید به سرمایه‌گذاری و کارآفرینی بخش خصوصی برای حل مسئله اشتغال و پیشبرد پروژه‌ها بها بدهیم».

او بر ایجاد امنیت در بخش خصوصی برای سرمایه‌گذاری بیشتر در حوزه فناوری اطلاعات و مخابرات تاکید کرد. او افزود: «کسب و کارهای اینترنتی از ظرفیت خوبی برای ایجاد اشتغال برخوردارند؛ اما این حوزه به‌تنهایی نمی‌تواند مسئله اشتغال را در حوزه فناوری اطلاعات پوشش دهد. برای ایجاد اشتغال باید در همه حوزه‌های شبکه‌های داخلی و اینترنت و به طور کل مخابرات و فناوری اطلاعات فعال بود».

کره شمالی تلفن هوشمند می‌سازد

• **مهر:** شرکتی در کره شمالی یک تلفن هوشمند ساخته که شباهت زیادی به آیفون دارد. به گفته این شرکت تمام بخش‌ها و سیستم‌عامل این موبایل در داخل کشور تولید شده‌اند. براساس گزارش ان‌کی‌نیوز، شرکتی در کره شمالی یک تلفن هوشمند داخلی ساخته و عرضه کرده است. این تلفن شباهت بسیار زیادی به آیفون دارد! موبایل مذکور Jindallae3 نام گرفته و به وسیله شرکت دولتی DPRKK ساخته شده است. تصاویر این موبایل با ویژگی‌های بهبودیافته و امنیتی به‌تازگی منتشر شده است. البته اطلاعات دیگری از این دستگاه به غیر از نام آن منتشر نشده است. شرکت سازنده در گزارش خود اعلام کرده سیستم‌عامل این موبایل به طور داخلی ساخته شده است.

جریمه ۲/۴ میلیارد یورویی برای گوگل

• **مهر:** اتحادیه اروپا شرکت بزرگ فناوری را به جرم رعایت‌نکردن قوانین آنتی‌تراست به پرداخت ۲.۴ میلیارد یورو جریمه محکوم کرده است. براساس گزارش بیزینس اینسایدر، اتحادیه اروپا به دلیل رعایت‌نکردن قوانین آنتی‌تراست، گوگل را به پرداخت ۲.۴ میلیارد یورو جریمه محکوم کرده است. البته احتمالا این بخشی از بهایی است که اتحادیه اروپا به دلیل رعایت‌نکردن قوانین از گوگل طلب کرده است. مبلغ این جریمه نیز بی‌سابقه است که البته با توجه به درآمد ۹۰ میلیارد دلاری گوگل در سال این جریمه چندان زیاد به نظر نمی‌رسد؛ اما شواهد حاکی از آن است که با سخت‌ترشدن قوانین مختلف گوگل در آینده با کاهش درآمد روبه‌رو خواهد شد. دلیل این جریمه نیز آن بود که مقامات اتحادیه اروپا معتقدند گوگل از سلطه موتور جست‌وجوی خود به طور ناعادلانه برای ساخت خدمت خرید گوگل استفاده کرده است. تصمیم کمیته آنتی‌تراست اروپا نتیجه تحقیقی هفت‌ساله است. سازمان رقابت اتحادیه اروپا در آوریل ۲۰۱۵ میلادی گوگل را به اختلال در جست‌وجوهای اینترنتی به سود خدمت خرید خود متهم کرد. در آن زمان پیش‌بینی می‌شد گوگل ۹ میلیارد دلار جریمه شود.

کاهش ۵۰درصدی تعرفه اینترنت داخلی

• **زومیت:** مصوبه کاهش ۵۰درصدی تعرفه استفاده از ترافیک اینترنت داخلی که بهمن سال ۱۳۹۵ به کمیسیون تنظیم مقررات ارتباطات ابلاغ شده بود، سرانجام اعمال شد. طبق این مصوبه کمیسیون تنظیم مقررات و ارتباطات رادیویی، تعرفه استفاده از ترافیک داخلی را نصف استفاده از ترافیک اینترنت خارجی محاسبه می‌کند. این مصوبه بهمن سال ۱۳۹۵ برای تصویب به کمیسیون تنظیم مقررات و ارتباطات رادیویی ابلاغ شده بود. معاون نظارت و اعمال مقررات سازمان تنظیم مقررات و ارتباطات رادیویی دراین‌باره گفت: «تقریبا شرکتی در این حوزه نداریم که این کار را انجام نداده باشد. مقدمات و آماده‌سازی و جداسازی ترافیک مقداری بحث فنی داشت؛ زیرا همه شرکت‌ها برای اجرای طرح به یک اندازه پتانسیل نداشتند». حسین فلاح همچنین بیان کرد: «در دستورالعمل‌هایی که به اپراتورها داده شده است، تقریبا موردی وجود ندارد که انجام نشده باشد. شرکت مخابرات ایران در برخی استان‌ها مشکل زیرساختی داشت که براساس برنامه اعلام‌شده تا ۱۵ تیر کار همه استان‌ها کامل می‌شوند».

هجوم ویروس باج‌افزار جدید به رایانه‌های سراسر دنیا

«پتیا» امنیت سایبری جهانی را تسخیر کرد

شرق: رایانه‌های جهان یک بار دیگر مورد هجوم بدافزار ویروسی جدیدی قرار گرفته‌اند که به گفته محققان از واناکرای هم خطرناک‌تر است. این حمله از اوکراین شروع شد و سپس در سراسر دنیا منتشر شده است.این ویروس «پتیا» نام دارد. این در حالی است که سیستم‌های کنترل اشعه‌های رادیواکتیو در چرنوبیل و همین‌طور یک کارخانه داروسازی در آمریکا با مشکل روبه‌رو شده است. این حمله از اوکراین آغاز شد. نخست شبکه توزیع برق، فرودگاه و بانک ملی این کشور و شرکت‌های مخابراتی آن از بروز مشکلاتی خبر دادند که پس از آن سریع در سراسر اروپا منتشر شد. شرکت‌هایی در نروژ، روسیه، دانمارک و فرانسه نیز از بروز مشکلاتی در سیستم‌های خود خبر دادند. این ویروس سیستم‌های رایانه‌ای شرکت‌های داروسازی «مرک‌شارپ» و «دوم» در آمریکا را نیز آلوده کرده است. این ویروس از قربانیان می‌خواهد مبلغی را به‌عنوان باج به یک حساب ناشناس آنلاین واریز کنند تا فایل‌هایشان دوباره قابل دسترسی شود. تا به حال آمار دولتی حاکی از آن است که ۱۹ عملیات پرداخت به این حساب ناشناس انجام شده است. رقم کل این پرداخت‌ها بالغ بر هزاران پوند می‌شود. این در حالی است که محققان امنیت سایبری هشدار داده‌اند ویروس پتیا بزرگ‌تر و خطرناک‌تر از ویروس واناکرای است که چندی‌قبل رایانه‌های جهان را آلوده کرد. گفته شده برخی از قربانیان این باج‌افزار در اوکراین اعلام کردند هکرها بعد از قفل‌کردن رایانه‌ها درخواست ۳۰۰ دلار باج کرده‌اند. همچنین از قربانیان دیگر این باج‌افزار می‌توان به شرکت کشتی‌رانی دانمارک، شرکت سازنده فلز ارواز روسیه و شرکت تولید مواد سینت‌گوبین فرانسه اشاره کرد. خبرگزاری CNBC، به نقل از کسپرسکی اعلام کرد شرکت‌هایی در روسیه، اوکراین، ایتالیا، فرانسه، آلمان، نروژ، لیتوانی، اسپانیا، رومانی، هلند، انگلیس، لهستان و ایالات‌متحده، قربانی این باج‌افزار شده‌اند. سازندگان این باج‌افزارها ادعا می‌کنند در اوایل سال جاری، این دو باج‌افزار موفق شده‌اند به منابع اطلاعاتی مهمی دست پیدا کنند و همین مطلب، نشان‌دهنده موفقیت عملکرد آنهاست. مهاجمان با استفاده از کدهای JanusSecretary شناخته‌شده برای باج‌افزار پتیا، در تلاش برای به‌حداقل‌رساندن رقابت بین باج‌افزارها و ایجاد برتری مطلق برای باج‌افزارهای تولیدی خودشان هستند. در گزارش ارائه‌شده از سوی Malwarebytes، درحال‌حاضر کدهایی از باج‌افزار منتشر شده است که به رمزگشایی فایل‌های آسیب‌دیده می‌پردازد. محققان امنیتی Malwarebytes پس از بررسی و تحقیقات خود اعلام کردند که در حال تهیه رمزگشایی برای محافظت از اطلاعات در برابر باج‌افزارها هستند. همچنین در تحقیقات به این نکته نیز اشاره شده است که در صورت مشاهده قفل‌شدن اطلاعات، از حذف‌کردن آنها خودداری کنید چراکه اطلاعات قفل‌شده قابل بازگردانی هستند. همچنین گروه امنیتی IB در روسیه تأیید کرد ۸۰ کمپانی روسی و اوکراینی تاکنون قربانی شده‌اند و این در حالی است که آمریکایی‌ها یعنی کمپانی سیمانتک آن را باج‌افزار پتیا می‌دانند اما روس‌ها به رهبری کسپرسکی آن را نوع جدیدی از باج‌افزار به نام ExPetr می‌دانند که دنیا با آن دست به گریبان شده است. در مجموع این باج‌افزار با سوءاستفاده از حفره‌ای در ویندوز به نام EternalBlue خود را روی شبکه می‌گستراند. نکته جالب اینکه باج‌افزار واناکرای نیز که ماه پیش در اینترنت منتشر شد، از همین حفره سوءاستفاده کرده بود اما «پتیا» بسیار پیشرفته‌تر از آن است.

پژوهشگران دراین‌باره اعلام کردند شواهد به‌دست‌آمده از تحلیل این بدافزار نشان می‌دهد سازندگان آن از کدهای افشاشده از «آژانس امنیت ملی» آمریکا استفاده کرده‌اند. این موضوع، باعث شکل‌گیری گمانه‌زنی‌هایی در این خصوص شده است که حملات مذکور با استفاده از ابزارهایی انجام شده که مالیات‌دهندگان آمریکایی بهای آن را پرداخت کرده‌اند. «ویکتور زورا» مدیر اجرائی ارشد شرکت «انفوسیف» در کی‌یف دراین‌باره گفت: «گسترش این ویروس در سرتاسر اروپا قابل مشاهده است و من از این موضوع نگران هستم که بدافزار مذکور، به تمام جهان آسیب برساند».

آنچه درباره پتیا باید بدانیم

باج‌افزار پتیا خلاف واناکرای فایل‌ها را رمز نمی‌کند؛ بلکه جدول مسترفایل درایو (MFT) و MBR را هدف قرار داده و آنها را غیرقابل استفاده می‌کند. پتیا MFT را رمز کرده و MBR را با کد مخرب خود جایگزین می‌کند، سپس پیغام درخواست پول را نمایش می‌دهد. با رمزشدن MBR، ویندوز حتی در حالت امن (Safe Mode) نیز بارگذاری نشده و از کار می‌افتد. به‌منظور درخواست پول از قربانی، متن زیر نمایش داده می‌شود: درحال‌حاضر از ۶۱ آنتی‌ویروس ثبت‌شده تنها ۱۵ عدد توانایی شناسایی پتیا را دارند. اگر قربانی‌های فعلی خود را در برابر حمله‌های باج‌افزار واناکرای مقاوم می‌کردند، نتیجه فعلی را شاهد نبودند.

گزارش‌های ابتدایی از تحقیقات کسپرسکی این ویروس را یک نسخه از باج‌افزار Petya نشان می‌داد اما چند ساعت بعد این شرکت ویروس را یک نوع کاملا جدید از باج‌افزار نامید که حالا با نام «NotPetya» شناخته می‌شود. کسپرسکی می‌گوید حداقل دو هزار کاربر تاکنون به این ویروس آلوده شده‌اند.

دو شرکت تحقیقاتی دیگر ادعا می‌کنند این باج‌افزار از همان حفره امنیتی EternalBlue استفاده می‌کند که WannaCry از آن بهره گرفته بود و به همین دلیل به سرعت در حال رشد است. EternalBlue فایل‌های سیستمی مربوط به اشتراک‌گذاری ویندوز با پسوند SMB را مورد حمله قرار می‌دهد که گفته می‌شود به وسیله NSA و برای مقاصد جاسوسی کار گذاشته شده است. مایکروسافت البته با انتشار بسته‌های امنیتی برای ویندوزهای قدیمی حتی ویندوز XP این مشکل را رفع کرده اما هنوز کامپیوترهای فراوانی در سطح دنیا با نرم‌افزار قدیمی و آپدیت‌نشده کار می‌کنند.

این ویروس که همچنین با نام Petrwrap نیز از آن یاد می‌شود، یک برنامه کامپیوتری مخرب است که وقتی اجرا شود، فایل‌های کامپیوتر را با یک کلید خصوصی رمزگذاری می‌کند که برای دسترسی به این فایل‌ها راهی به‌جز رمزگشایی با آن کلید وجود نخواهد داشت. این نرم‌افزار از کاربر تقاضای ۳۰۰ دلار پول از نوع غیرقابل ردیابی بیت‌کوین می‌کند تا کلید را آزاد کند. گفته می‌شود تا زمان انتشار این گزارش حدود ۲۰ تراکنش با مبلغ مجموعا چهار هزار و ۹۰۰ دلار به حساب مهاجمان واریز شده است.

راهبرد جدید امنیت سایبری آمریکا

مدیران بخش خدمات نیروی هوایی آمریکا به‌تازگی اعلام کردند اکنون چندین عنصر کلیدی راهبرد امنیت سایبری خود را به مرحله اجرا درآورده‌اند. این راهبرد با هدف تجزیه و تحلیل و کاهش حملات و ایجاد انعطاف‌پذیری سایبری در سامانه سلاح‌های جدید و سیستم‌هایی که در ابتدای فرایند تولید هستند، طراحی شد. به گزارش سایبربان، پیاده‌سازی راهبرد یادشده دارای چندین بُعد مختلف، ازجمله طیف وسیعی از نوآوری‌هاست که به عملیات‌ها و توسعه سلاح‌ها شتاب می‌دهد. تعدادی از این دستاوردها شامل سخت‌افزار مهندسی می‌شوند؛ به‌گونه‌ای که بتواند وصله‌ها یا به‌روزرسانی‌های امنیتی را به‌سرعت پس از انتشار، یکپارچه کند. با استفاده از خودکارسازی رایانه‌ها، شناسایی و ردیابی مزاحمان سایبری، راه‌اندازی اسکادران‌های سایبری و شناسایی آسیب‌پذیری‌های بالقوه در ابتدای توسعه سلاح یا فناوری‌ها، به شکل بهتری صورت می‌گیرد. فرماندهان نیروی هوایی برای به‌کاربستن بخشی از راهبرد یادشده، واحد جدیدی را ایجاد کرده‌اند که وظیفه دارد با تشخیص، ردیابی و رسیدگی به نفوذ و حملات سایبری، از سامانه سلاح‌ها محافظت کند.

مقامات نیروی هوایی توضیح دادند به‌عنوان بخشی از نوآوری‌های گفته‌شده، انعطاف‌پذیری سایبری بیشتری به سامانه‌های سلاح‌های قدیمی که به صورت روزافزون به فناوری‌های رایانه‌ای وابسته می‌شوند، اضافه می‌شود.

خط سوم حمله به ترکیب مناسبی از متخصصان امنیت سایبری و مهندسان امنیتی در نیروها پرداخته است. همچنین تلاش برای حصول اطمینان از این امر که سلاح‌ها به خودی خود دارای انعطاف‌پذیری سایبری هستند، فرضیه خط چهارم حمله را تشکیل می‌دهد. توسعه سلاح‌ها در طرح بحث‌شده، به «معماری باز» (open architecturee) معروف است که به مهندسان نرم‌افزار و سخت‌افزار اجازه می‌دهد فناوری‌های جدید را به شکل ساده‌تری با یکدیگر سازگار و یکپارچه کنند. در نتیجه، سامانه سلاح‌های در دست توسعه می‌تواند به شکل سریع‌تری با طیف وسیعی از تهدیدات و شرایط عملیاتی مبارزات انطباق پیدا کند. این موضوع در بسیاری از موارد، مطرح می‌کند که به‌روزرسانی سامانه‌ها که با نرم‌افزارهای جدید طراحی شده، به کاهش حملات خاص می‌انجامد. خط پنجم به تلاش برای ایجاد یک محیط امنیتی مشترک برای راهنمایی‌های طبقه‌بندی‌شده اشاره دارد تا از سطوح امنیتی رایج اطمینان حاصل کند. به علاوه، خط ششم، همکاری کارشناسان و مهندسان را با آزمایشگاه تحقیقاتی نیروی هوایی (Air Force Research Laboratory) برای توسعه ابزارهای تحکیم سایبری پیش‌فرض مطرح می‌کند. الن ماری پاولیکوسکی برای مثال توضیح داد تا سال ۲۰۲۰ باید همه پایگاه‌های هوایی در سامانه‌های خود از ابزارهای یادشده بهره‌مند شوند و کارشناسان سایبری نیز به مقابله با حملات سایبری خواهند پرداخت. اصلی‌ترین موضوع خط هفتم نیز به فراهم‌کردن بستری برای پیش‌بینی مناطقی که انتظار حملات سایبری در آنها وجود دارد و همچنین توسعه و آماده‌سازی اطلاعاتی که به آن نیاز پیدا می‌شود، اشاره دارد. او گفت: «ما در برابر حملاتی که انتظار داریم دشمنانمان انجام بدهند، طرح‌های دفاعی خود را ایجاد و برنامه‌ریزی کردیم. ما نیاز داریم درک کنیم تهدیدات به کدام سمت خواهند رفت و سپس می‌توانیم در برابر آنها از خود دفاع کنیم».

دریچه

۱۴ میلیارد دلار صرف تعمیرات آیفون

• شرکت SquareTrade که در زمینه سرویس‌های گارانتی برای دستگاه‌های هوشمند فعالیت دارد، به‌تازگی به سراغ موبایل‌های آیفون رفته و به ارائه اطلاعاتی جالب درباره چگونگی تعامل افراد با موبایل‌هایشان پرداخته است. این شرکت در تحقیقاتی به نام «یک دهه آسیب»، به مقایسه آیفون OG و آیفون۷ در تست سقوط و غوطه‌وری در آب پرداخته است؛ به‌عنوان‌مثال، آیا تابه‌حال می‌دانستید که خریداران آیفون از زمان عرضه این خانواده در سال ۲۰۰۷، بالغ بر ۱۴میلیارد دلار صرف تعمیرات دستگاه‌های خود کرده‌اند؟ یا می‌دانستید که احتمال آسیب‌زدن به موبایلتان، تا شش‌برابر از احتمال سرقت یا گم‌شدن آن بیشتر است؟ اگرچه غالب افراد از قاب‌ها یا محافظ‌های نمایشگر روی آیفون خود استفاده می‌کنند، اما تقریبا نیمی از آنها در مدت‌زمان مالکیت دستگاه، نمایشگر آن را شکسته‌اند. حدود ۶۸ درصد از این افراد می‌گویند که شکستگی به هنگام رسیدگی به چندین کار به صورت هم‌زمان صورت گرفته و ۴۰ درصد می‌گویند که این اتفاق در خانه و در ارتفاعی که به زحمت به یک متر می‌رسید به وقوع پیوسته است. درهمین‌حال، هرچه فعال‌تر باشید، احتمال شکستن نمایشگر آیفون نیز بیشتر است و چتربازان در صدر این فهرست قرار دارند.

از نکات جالب مربوط به این گزارش می‌توان به این موضوع اشاره کرد که افراد بلندقامت‌تر، معمولا احتیاط بیشتری در نگهداری از دستگاه نشان می‌دهند؛ به‌عنوان‌مثال افرادی با قد ۱.۸۰ متر یا بیشتر، تا ۳۲ درصد کمتر نسبت به افرادی با قد ۱.۶۵ متر یا کمتر آیفون خود را می‌شکنند. در نتایج این نظرسنجی همچنین آمده افرادی که یک‌بار نمایشگر دستگاه را می‌شکنند، به صورت میانگین یک‌بار دیگر نیز آن را شکسته‌اند که هزینه تعمیرات ۱۴میلیارددلاری در ۱۰ سال را توضیح می‌دهد! علاوه‌براینها، ۵۷ درصد از دارندگان آیفون که بیشتر از چهار ساعت در روز را در شبکه‌های اجتماعی سپری می‌کنند، در ۱۲ ماه گذشته به موبایل خود آسیب زده‌اند؛ بنابراین شاید بهتر باشد که از این پس به هنگام عبور از خیابان و انتشار تصویری در اکانت اینستاگرامتان، دقت بیشتری به خرج دهید. در نهایت نیز گفتنی است که ۴۴ درصد از دارندگان فعلی آیفون، به خرید آیفون ۸ اپل نیز تمایل دارند.