صبح ساحل فناوری
پنجشنبه ۲۹ آذر۹۷|سال سی وچهارم|شماره ۳۶۶۰
Email : Info.Sobhesahel@Gmail.Com

در کشورهای دنیا یا حداقل در کشورهای پیشرفته، فرهنگی به نام «باگ باونتی» جا افتاده است. به این معنا که شرکتی به عنوان واسطه وارد میدان می شود و سازمان های مختلف که احتمال وجود آسیب پذیری امنیتی یا نفوذ هکر در بدنه امنیتی شان می رود، در این شرکت ثبت نام می کنند

«آی‌گپ» مجهز به تماس تصویری شد

سرویس تماس تصویری به صورت رایگان در اختیار کاربران قرار می‌گیرد و تنها هزینه ترافیک اینترنت مربوط به این تماس را پرداخت خواهند کرد. پیام‌رسان بومی آی‌گپ تماس تصویری‌ای را ارائه کرد که از فناوری P۲P برای برقراری ارتباط امن بین ۲ کاربر استفاده می‌کند و کیفیت تماس به صورت هوشمند متناسب با پهنای باند تنظیم می‌شود.

پیام رسان بومی آی‌گپ اعلام کرد: سرویس تماس تصویری در پلتفرم‌های اندروید، آی او اس و دسکتاپ برای برخی از کاربران به صورت آزمایشی از روز سه شنبه ۲۷ آذرماه به‌مناسبت شب یلدا در اختیار تمامی کاربران آی‌گپ قرار گرفت.

به گزارش ایتنا از فارس، تماس تصویری آی‌گپ از معماری P۲P بهره می‌برد تا علاوه بر امنیت بالا، استاندارد کیفی مطلوبی در اختیار کاربر قرار دهد و با توجه به پهنای باند در دسترس کاربر، کیفیت تماس به صورت هوشمند تنظیم می‌شود.

سرویس تماس تصویری به صورت رایگان در اختیار کاربران قرار می‌گیرد و تنها هزینه ترافیک اینترنت مربوط به این تماس را پرداخت خواهند کرد.

هکری که از سوی وزیر تقدیر شد

وزیر ارتباطات نوشت:
«تلاش شما برای ارتقای سطح امنیت خدمات قابل تقدیره

◆ گروه فناوری:

آسیب پذیری امنیتی (باگ) منجر به اتفاقات جبران ناپذیری می شود و معضلی است که تمام دنیا با آن درگیر هستند. در کشورمان،یک کارشناس این حوزه به تازگی درباره کلیات یک آسیب پذیری امنیتی در پایگاه داده مخابرات توئیت کرد و مورد تقدیر وزیر ارتباطات و فناوری اطلاعات قرار گرفت.

اساسا هکر کلاه سفید به متخصص امنیت کامپیوتر گفته می شود که به منظور تست و ارزیابی امنیت یک شبکه و سیستم محافظت شده تلاش در هک آن می کند. این نوع هکرها از مهارت های خود برای برقراری بیشتر امنیت و مبارزه با هکرهای کلاه سیاه استفاده می کند. هدف آن ها حفظ امنیت است.

شاهین زاده جوان ۲۹ ساله ای است که در رشته مهندسی اپتیک و لیزر تحصیل کرده است و در توئیتر خود، یک آسیب پذیری امنیتی را با رونوشت به وزیر ارتباطات افشا کرد: « شرکت مخابرات ایران، مثل بسیاری از سازمان های دیگر آسیب پذیر بوده و استخراج اطلاعات میلیون ها کاربر به راحتی امکان پذیر است. شما با این کد وریفای کن ....» و ادامه ماجرا. وزیر ارتباطات دقایقی بعد برای او نوشت: «تلاش شما برای ارتقای سطح امنیت خدمات قابل تقدیره. برای رسیدگی به این گزارش با شما تماس خواهند گرفت.»

باگ را رایگان نمی دهند

این سرآغاز افشای باگی بود که در سیستم مخابرات کشف شد. شاهین زاده در گفت و گو با خبرنگار گروه علمی ایرنا درباره کشف حفره های امنیتی گفت: زمانی که باگی در سیستم های مختلف کشف می شود، ما سعی می کنیم با مسئولان مربوطه ارتباط بگیریم تا باگ را رفع کنند. در خارج از کشور به ازای کشف باگ، سازوکاری برای پاداش به هکر وجود دارد. اما در کشور ما چنین امکانی نیست و به همین دلیل هکر کلاه سفید باید موضوع را از طریق شبکه‌های اجتماعی به گوش مسئولین برساند. هر چند سازمان ها معمولا برخورد مناسبی ندارند و بیشتر تمایل دارند که باگ به شکل رایگان به آن ها داده شود. در حالی که در سیستم شان بودجه قابل توجهی برای این مسئله در نظر گرفته شده است.

وی با این توضیحات ادامه داد: حدود یک ماه قبل در یکی از سرورهای اصلی یکی از اپراتورها یک آسیب پذیری جدی پیدا کردم. از طریق این سرویس کل شبکه مشخص بود. این آسیب پذیری۷۰ میلیون رکورد داشت و راهی بود به کل شبکه آن اپراتور. من به واسطه یکی از دوستانم با مرکز ماهر ارتباط برقرار کردم. با این مرکز، یک جلسه حضوری گذاشتیم و شواهدی ارائه دادم تا ادعایم را ثابت کنم. آن ها قانع شدند، با آن اپراتور تماس گرفتند و یک جلسه با مدیران آن ترتیب دادند. البته اپراتور جلسه را لغو کرد و تا الان هم خبری از آن ها نیست. تا جایی که من می دانم و پیگیری کردم، مرکز ماهر نامه ای به سازمان تنظیم مقررات زده تا آن ها را جریمه کند.

آسیب پذیری خطرناک

شاهین زاده که ۱۳سال در این زمینه مشغول فعالیت است، درباره توئیتی که نوشت و نتیجه ای که افشای این باگ داشت، گفت: قصد خرید یک سرویس اینترنتی را داشتم. در کنار فرایند خرید سرویس مشغول نگاه کردن به بخشی از قسمت های سایت شدم و فهمیدم آن ها یک آسیب پذیری خطرناک دارند که در عرض نیم ساعت اجازه نفوذ به سرور را می دهد. به واقع، بیشتر از این عصبانی شدم که دیدم اطلاعات من هم مانند خیلی های دیگر در دسترس است و متوجه شدم چه سو استفاده های زیادی از این اطلاعات می توان انجام داد.

«بعد از آن یک توئیت درباره تمام باگ هایی که در این مدت از دو اپراتور و مخابرات به دست آورده بودم ، با سندی (دو رقم آخر پسوورد سرور) که ثابت می کرد حرف های من درست است، نوشتم و وزیر را منشن کردم. صبح زود همان روز به من ریپلای دادند، بابت کاری که کردم تشکر کردند و من را به معاون خودشان آقای جوانبخت ارجاع دادند. چند ساعت بعد آقای جوانبخت در دایرکت توئیتر از من شماره تماس گرفت . البته مدیر امنیت مخابرات هم با من تماس گرفت اما هنوز موفق نشدیم به شکل کامل با هم صحبت کنیم».

وی تاکید کرد: از نظر من سازمان های خیلی حساس باید روالی برای تست سرورهای شان داشته باشند و این امکان را فراهم کنند تا اگر کسی باگی در سازمان های مهم کشف کرد بتواند آن را مطرح کند و هزینه ای در قبال این سرویس دریافت کند تا وسوسه نشود که از اطلاعات به شکل دیگری استفاده کند. مانند چند سال قبل که اطلاعات کاربران یکی از اپراتورها روی سایت رفت و حسابی سر و صدا کرد.

اگر به هکرهای کلاه سفید بها ندهیم، در واقع ممکن است ناخودآگاه آن ها را به سمت سو استفاده از باگ ها سوق دهیم که این کار به زیان خود ماست

یک معضل جهانی

مجتبی مصطفوی، کارشناس امنیت سایبری نیز در گفت و گو با خبرنگار ایرنا در خصوص این شکل افشاگری در تمام دنیا، گفت: در کشورهای دنیا یا حداقل در کشورهای پیشرفته، فرهنگی به نام «باگ باونتی» جا افتاده است. به این معنا که شرکتی به عنوان واسطه وارد میدان می شود و سازمان های مختلف که احتمال وجود آسیب پذیری امنیتی یا نفوذ هکر در بدنه امنیتی شان می رود، در این شرکت ثبت نام می کنند. از آن سمت هکرهای کلاه سفید یا بچه های امنیت کار که با این شرکت ها همکاری دارند شروع می کنند به پیدا کردن «باگ» یا بهتر بگویم پیدا کردن آسیب پذیری امنیتی آن سازمان. آن ها بعد از پیدا کردن آسیب پذیری، مبلغی را به عنوان جایزه دریافت می کنند تا برای ادامه فعالیت های خود انگیزه داشته باشند.این کارشناس در خصوص وجود چنین امکانی در کشورمان گفت : ما در ایران چنین چیزی را به صورت قوی نداریم چون سازمان هایی که مشتری اصلی آن هستند، از این سیستم استفاده نمی کنند. دلیل دیگری هم دارد. وقتی یک هکر کلاه سفید، باگی را شناسایی می کند که می تواند اطلاعاتی را افشا کرده یا سرویسی را از کار بیندازد هیچ راه قانونی برای اعلام این مشکل وجود ندارد. از طرفی اگر بخواهد از مجرای قانونی اقدام کند معمولا با این تهدید رو به رو می شود که «با چه اجازه ای چنین چیزی را چک کرده اید» و ممکن است کارشان به پلیس کشیده شود. در این شرایط برای کلاه سفیدها نه تنها جایزه ای در کار نیست، حتی ممکن است تنبیه هم بشوند.وی در ادامه گفت: به دلایلی که گفتم هکرهای کلاه سفید به اجبار و برای معیشت خودشان با کشورهای خارجی کار می کنند و آسیب پذیری سیستم های آن کشورها را برطرف می کنند. به این صورت است که مشکلات در کشور خودمان باقی می ماند.

«اگر به هکرهای کلاه سفید بها ندهیم، در واقع ممکن است ناخودآگاه آن ها را به سمت سو استفاده از باگ ها سوق دهیم که این کار به زیان خود ماست. همین آسیب پذیری امنیتی جدید را که در یک اپراتور شناسایی شده است، در نظر بگیرید. این هکر سعی کرد آسیب پذیری را به مرکز خودش اعلام کند، اما حتی موفق نشد با آن ها ارتباط بگیرد. در نهایت هم مجبور شد آن را در توئیتر اعلام کند تا شاید کسی مطلع شود. حالا فکرش را بکنید که یک هکر کلاه سیاه قبل از آقای شاهین زاده، این آسیب پذیری را به دست آورده باشد؟ می دانید با اطلاعات ۷۰ میلیون نفر چه کارهایی می توان انجام داد؟ در این باگ، اطلاعات تمامی خریداران سیم کارت آن اپراتور در دسترس است. این اطلاعات را هر هکری می تواند به دست بیاورد و از آن سو استفاده کند.»

مصطفوی یادآور شد: اساسا یکی از مشکلاتی که هکرهای کلاه سفید با آن درگیر هستند، مشکل درآمدی است. آن ها کارشان این است اما نمی توانند از این طریق کسب درآمد کنند. اگر حسن نیت داشته باشند معمولا با شرکت های خارجی کار می کنند و درآمدشان را از آن طریق به دست می آورند، اما ممکن است گاهی هکر به این فکر کند که من آسیب پذیری امنیتی را پیدا کردم، سازمان مورد نظر هم که آسیب پذیری را نمی پذیرد و بهتر است آن را به فروش برسانم. در کشور ما برای شناسایی یک آسیب پذیری بزرگ سطح بالا جایزه ۲۰۰هزار تومانی مشخص می کنند، این مبلغ برای فردی که بیش از یک هفته زمان برای کشف آسیب پذیری گذاشته، واقعا شبیه شوخی است.

به گفته این کارشناس، در کشورهای دیگر برای یک آسیب پذیری با سطح مخاطره بالا به راحتی مبلغی معادل هزار دلار و برای آسیب پذیری مهم تر و بزرگ تر تا ۲۰/۱۰هزار دلار نیز جایزه تعیین می کنند. زمانی فاجعه رخ می دهد که یک کلاه سفید نا امید از همه جا، از باگی که کشف کرده، بدترین استفاده را کند و مثلا اطلاعات شخصی میلیون ها نفر را لو دهد.

حرکت های «باگ باونتی» حدود دو سال قبل در کشور ما آغاز شد. مصطفوی در این باره گفت: معتبرترین کاری که در این خصوص انجام شد، تشکیل سامانه کلاه سفید در مرکز آپا در دانشگاه امیرکبیر است. البته تا جایی که اطلاع دارم استقبال خوبی از آن صورت نگرفته است. البته برخی نهادهای دولتی نیز در حوزه کشف آسیب پذیری ها فعالیت می کنند، از جمله «مرکز ماهر» در سازمان فناوری اطلاعات ایران مشغول رسیدگی به امور این چنینی است. این نهادها به شکل جداگانه از یکدیگر کار می کنند و یکپارچه شدن شان می تواند کمک بزرگی در این عرصه باشد.

وزیر یک نفر است

وزیر جوان ارتباطات تاکنون واکنش های خوبی نسبت به این مسائل نشان داده است. این اعتقاد مصطفوی است و درباره اش می گوید: «چند بار این اتفاق رخ داده و وزیر معمولا از فردی که آسیب پذیری امنیتی را افشا کرده تشکر کرده است. این کار بسیار خوب و ناشی از درک بالای ایشان است اما کافی نیست. کاری که کلاه سفیدها انجام می دهند تفریح نیست، آن ها باید بتوانند کارشان را به عنوان یک شغل ادامه دهند و از این راه درآمد کسب کنند.

وی با بیان این که آسیب پذیر بودن امنیت و به مخاطره افتادن آن، به قدری خطرناک است که می تواند باعث قطعی برق کل کشور شود و می تواند یک پالایشگاه را از کار بیندازد، افزود: باید این فرهنگ را جا بیندازیم که امنیت کالای لوکسی نیست که در گوشه ای پنهان کنیم.

تحلیل آنتی ویروس های تقلبی موجود روی مارکت های ایرانی

◆ گروه فناوری:

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای (ماهر) وابسته به سازمان فناوری اطلاعات ایران نتایج بررسی های خود را درباره آنتی ویروس های تقلبی و شبه آنتی ویروس های موجود در مارکت های ایرانی منتشر کرد.

به گزارش ایرنا، اپ استورهای اندرویدی این روزها پر شده اند از انبوهی از اپلیکیشن های تقلبی که یا در حقیقت بد افزارند و یا در عمل کاری را که قول می دهند، نمی کنند. این وسط وقتی پای آنتی ویروس ها و اپلیکیشن های تقلبی وسط می آید موضوع از این هم جدی تر می شود. در واقع همین حالا هم اینترنت پر شده است از انبوه آنتی ویروس های تقلبی. سال پیش وقتی در نتیجه شناسایی بدافزار WannaCry اوج گرفت، شرکت امنیتی RiskIQ اعلام کرد که از میان ۴۲۹۲ اپلیکیشن آنتی ویروس فعال روی اینترنت، ۵۲۵ تای آن ها در حقیقت بدافزارند. این یعنی از هر۱۰ برنامه آنتی ویروسی که پیدا می کنید یکی احتمالا تقلبی و بدافزار است. از میان آن اپ ها ۵۵ آپ روی اپ استور خود گوگل قرار داشتند و ما بقی روی اپ استورهای متفرقه قرار گرفته بودند. اپ استورهای داخلی ما هم طبیعتا جزو همین مارکت ها بودند. اما دقیقا وضعیت آنتی ویروس های واقعی و تقلبی موجود روی مارکت های ایرانی چگونه است؟

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای (ماهر) وابسته به وزارت ارتباطات و فناوری گزارشی را تحت عنوان بررسی آنتی ویروس های اندرویدی منتشر شده در مارکت های ایرانی ارائه کرده است که در قالب آن حدود ۱۲۰ آنتی ویروس منتشر شده در مارکت های ایرانی جمع آوری و مورد بررسی اولیه قرار گرفتند.

براساس گزارش مرکز ماهر، این بررسی نشان می دهد که بسیاری از برنامه هایی که تحت عناوین مختلف در مارکت های اندروید منتشر می شوند از روی برنامه های منبع باز ساخته می شوند. این برنامه ها صرفاً با تغییر نام و آیکون به عنوان برنامه های مختلف منتشر می شوند.

در بسیاری از موارد هدف از این کار استفاده از سرویس های تبلیغاتی داخل این برنامه ها و درآمدزایی برای منتشرکننده برنامه است. هرچند این برنامه ها به صورت مداوم توسط افراد مختلف منتشر می شوند در اغلب موارد هیچ کارایی نداشته و حتی ممکن است بدافزار باشند.

در این مستند برنامه های منتشرشده تحت عنوان آنتی ویروس مورد بررسی قرار گرفته اند. بررسی و مقایسه این برنامه ها نشان می دهد که آنها عمدتاً کارایی لازم را نداشته و یا عملکرد جعلی دارند و تنها با هدف جذب کاربر و کسب درامد از تبلیغات توسعه یافته اند. نحوه بررسی تشابه این آنتی ویروس ها در ابتدا بر اساس تشابه لیست api هایی که فراخوانی می کردند و سپس برای اطمینان کامل، بر اساس بررسی کد و نحوه عملکرد دقیق برنامه ها بوده است.

از میان ۱۲۰ آنتی ویروس بررسی شده روی مارکت های ایرانی، ۶۰ آنتی ویروس با توجه به شباهت بالایی که به یکدیگر داشتند، به هفت دسته تقسیم شدند. هرکدام از این دسته ها خصوصیات خاص خود را داشتند که در شرح گزارش آمده است.

تحلیل دسته های مختلف از آنتی ویروس های ایرانی منتشر شده در مارکت های نشان می دهد که بسیاری از آنها بارها با اسامی مختلف و توسط افراد مختلف منتشر شده اند، از این رو می توان نتیجه گرفت که این برنامه ها از روی برنامه های منبع باز (اوپن سورس) ساخته شده اند و صرفا با تغییر نام و آیکون منتشر شده اند. در اغلب موارد هدف از این کار استفاده از سرویس های تبلیغاتی داخل این برنامه ها و درآمدزایی از طریق نمایش تبلیغ به کاربران است. استفاده از سرویس ها تبلیغاتی مثل عدد و سرویس ارسال نوتیفیکیشن پوشه (برای ارسال تبلیغات نوتیفیکیشنی) در این برنامه ها بسیار رایج است.

برخی دیگر از آنتی ویروس ها با کد یکسان بیش از ۱۵ بار روی مارکت های ایرانی منتشر شده اند. متاسفانه بسیاری از این آنتی ویروس ها عملکرد درستی برای تشخیص بدافزارهای اندرویدی ندارند و همه هفت دسته ای که در اینجا بررسی شدند یا کاملا بدون هیچ تحلیلی هستند و یا تحلیل بسیار ابتدایی دارند که قابل قبول نیست و نمی تواند از دستگاه اندرویدی در برابر تهدیدات دفاع کند.

درمجموع این ۶۰ آنتی ویروس بیش از یک میلیون نصب داشتند که نشان از گستردگی کار تبلیغاتی و تجاری این برنامه ها است.

ماجرای عجیب شکایت از اپل!

◆ گروه فناوری:

به تازگی شکایت عجیبی بر علیه شرکت اپل به دادگاه ارائه شده که بر اساس آن اپل به علت دروغگویی در مورد ابعاد و تعداد پیکسل‌های گوشی‌های آیفون ایکس، ایکس اس و مکس باید غرامت بپردازد.

این شکایت تقدیم دادگاهی در شمال کالیفرنیا شده است. بر اساس محتوای این شکایت اپل در تبلیغات بازرگانی خود به طور کامل در مورد ابعاد نمایشگرها و تعداد پیکسل های هر سه مدل تازه آیفون که امسال به بازار آمده دروغ گفته است.اپل در برابر این شکایت هنوز واکنشی از خود نشان نداده است.

به گزارش ایتنا از مهر، در این شکایت ۵۵ صفحه ای به طور مفصل توضیح داده شده که اپل بخش هایی از قاب جلویی گوشی که فاقد هرگونه پیکسل است را هم به عنوان بخشی از نمایشگر منظور کرده است. شاکی با همین استدلال مدعی شده نمایشگر آیفون ایکس ۵.۸ اینچ نبوده و ابعاد آن در واقع ۵.۶۸۷۵ اینچ است که ۰.۳ اینچ کمتر از ادعای اپل است.

در بخش دیگری از این شکایت نامه تصریح شده که دقت آیفون ایکس ۲۴۳۶ در ۱۱۲۵ پیکسل نیست و با توجه به کوچک تر بودن نمایشگر این گوشی از آنچه ادعا شده این دقت هم ادعایی دروغین است.

این اولین بار نیست که شکایاتی از این دست بر علیه اپل تقدیم دادگاه می شود. این شرکت قبلا هم به علت مشکلات نرم افزاری برخی مدل های آیفون، خم شدن این گوشی در زمان قراردادن آن در جیب عقب شلوار، خش افتادن سریع نمایشگر و غیره مورد پیگرد قضایی قرار گرفته بود.

گوشی‌هایی که از طرح رجیستری جا مانده‌اند!

◆ گروه فناوری:

وزیر ارتباطات گفت: امکان فعال‌سازی گوشی‌های خاموش و جامانده در طرح رجیستری، در کارگروه سازمان تنظیم مقررات ارتباطات در حال بررسی فنی است.

محمدجواد آذری جهرمی در جمع خبرنگاران درباره تعیین تکلیف گوشی هایی که به دلیل خاموش بودن، امکان رجیستری در شبکه تلفن همراه کشور را ندارند، گفت: ما در ابتدای طرح رجیستری، یک دوره ۳ ماهه برای پایش درنظر گرفتیم و از مردم خواستیم که در این بازه زمانی گوشی های خود را روشن کنند تا این گوشی ها در شبکه فعال شود.وی ادامه داد: اما با وجود اطلاع رسانی کاملی که انجام شد برخی افراد، این گوشی‌ها را روشن نکردند و هم اکنون با توجه به افزایش قیمت گوشی در بازار به دلیل نوسانات نرخ ارز، قصد دارند از گوشی های خاموش مانده استفاده کنند اما این گوشی‌ها در شبکه غیرفعال است.

به گزارش ایتنا از مهر، جهرمی گفت: در این زمینه کارگروه فنی سازمان تنظیم مقررات و ارتباطات رادیویی با همکاری اپراتورهای تلفن همراه تشکیل شده تا بتوانند برمبنای پردازش های ممکن، موارد موردنظر از گوشی های قدیمی جامانده در طرح رجیستری را آنالیز کنند تا مشخص شود که این گوشی ها قابلیت فعالسازی دارند یا خیر.وی با اشاره به اینکه سیستم ثبت و رجیستری از تطابق شماره تلفن همراه کاربر و شماره شناسه IMEI گوشی وی، عملیاتی می شود، توضیح داد: اگر بخواهیم این فرآیند را به صورت کامل باز بگذاریم، عده ای سودجو که به دنبال قاچاق کالا هستند، از این امکان استفاده کرده و گوشی های قدیم را با IMEI جدید وارد شبکه می کنند. این کدهای جعلی باعث بروز باگ در داخل سیستم می شود.وزیر ارتباطات افزود: اما با این حال برای افرادی که به رغم مهلت داده شده، به هر دلیلی گوشی خود را فعال نکردند و هم اکنون با مشکل مواجه شده اند نیز باید فکری کرد. به همین دلیل کارگروه فنی رگولاتوری درحال بررسی بر نحوه تعیین تکلیف این گوشی ها است.وی درباره توقف ثبت رجیستری گوشی های مسافری در سامانه همتا نیز گفت: گوشی هایی که تحت عنوان مسافر اما خارج از روال مورد تایید وزارت صمت، وارد کشور می شوند، بار مسافر محسوب نمی شوند و برای آنها قانون بار مسافر پیاده سازی نخواهد شد.

جهرمی با بیان اینکه برخی انتقادات به این است که کانال های اصلی واردات گوشی کار نمی کنند و این موضوع باعث ایجاد اخلال در بازار شده است، افزود: تاکید ما بر این است که همه باید مسئولیت واقعی خود را انجام دهند و به جای شیوه های جایگزین، اگر مشکلی وجود دارد باید حل شود.