سراج

۹ بهمن ۱۳۹۵

شماره ۹۷

تسلیت به ایران، آتش‌نشانان شهید پرکشیدند...

خبرنامه کارشناسی

اخبار فناوری اطلاعات و ارتباطات

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج

هفته نامه | شماره نود و هفتم | سال دوم | ۴۵ صفحه

Expert Bulletin News

Information Communication Technology

2th year 2017 | Weekly bulletin

در این شماره می‌خوانید:

بارگیری مخفیانه‌ی برنامه‌ها از فروشگاه گوگل پلی توسط بدافزار اندرویدی

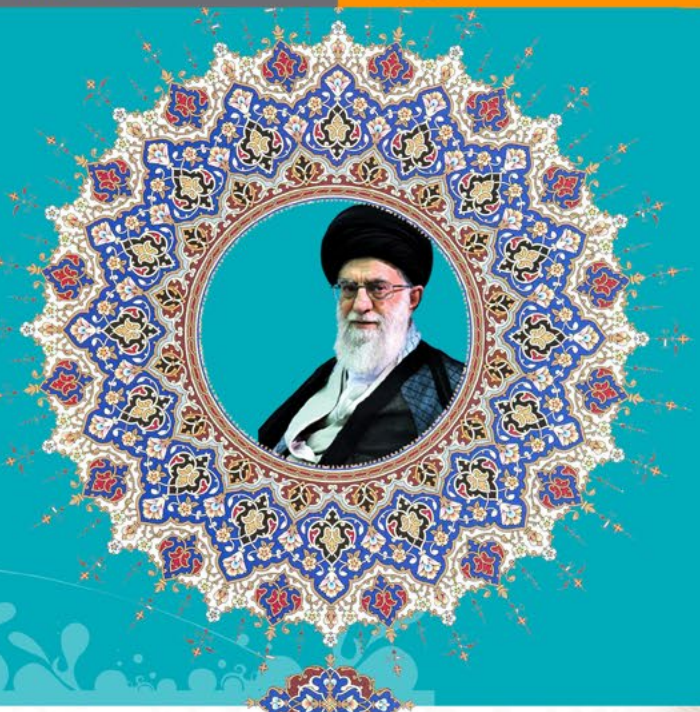
سیمانتک گواهی‌نامه‌های اشتباه صادر شده را باطل کرد

ناتو: نفوذگران سایبری هر ماه ۵۰۰ بار به اتحادیه حمله می‌کنند

ویجت نظردهی، بسیاری از وب‌گاه‌ها را در معرض خطر قرار داد

بسم الله الرحمن الرحیم

آگاهی و بصیرت



بنده بارها این جبهه های سیاسی و صحنه های سیاسی را مثال می زنم به جبههٔ جنگ. اگر شما در جبههٔ جنگ نظامی، هندسه زمین در اختیارتان نباشد، احتمال خطاهای بزرگ هست.

مقام معظم رهبری (مد ظله العالی)

فهرست مطالب

فصل اول: اخبار عمومی

بازگشت بدافزار اندرویدی HummingBad به گوگل‌پلی. ۶
بارگیریِ مخفیانه‌ی برنامه‌ها از فروشگاه گوگل‌پلی توسط بدافزار اندرویدی. . . . ۸
بازگشتِ دوباره‌ی سرویس رایانامه‌ی «لاوابیت».. . . . . ۹
شکستن قفل الگویی اندروید با 5 بار تلاش توسط مهاجمان.. . . . . ۱۱
نفوذ به انجمن‌های بازی کلش رویال. ۱۲
آسیب‌پذیری در فیس‌بوک و حذف ویدئوها توسط نفوذگران. ۱۳

فصل دوم: مدیریت امنیت

سیمانتک گواهی‌نامه‌های اشتباه صادرشده را باطل کرد. ۱۵
حمله‌ی منع سرویس توزیع‌شده به بانک Lloyds در سه روز متوالی. ۱۶
گروه نفوذ Greenbug به بدافزاری که عربستان سعودی را هدف قرار داده، کمک می‌کند ۱۷
در سال 2017 همچنان 200 هزار سامانه دارای آسیب‌پذیری Heartbleed هستند ۱۹
پشتیبانیِ پیش‌فرض از HTTPS بر روی وب‌گاه‌های دولتی آمریکا اجباری شد. . . ۲۰

فصل سوم: سیاست سایبری

سپر طلایی چین و ممنوعیت استفاده از شبکه‌ی خصوصی مجازی.. . . . . ۲۲
یاهو تحت بازرسی: چرا نقض داده‌ی عظیم در این شرکت دیر اطلاع‌رسانی شده است؟ ۲۳
در برنامه‌ی پاداش در ازای اشکال ارتش آمریکا 118 آسیب‌پذیری وصله شد ۲۵
دستگیری نفوذگر روسی، نویسنده‌ی بدافزار NeverQuest. ۲۷
نفوذ به حساب توییتر بی‌بی‌سی و خبر جعلی تیراندازی به دونالد ترامپ. ۲۸
ناتو: نفوذگران سایبری هر ماه 500 بار به اتحادیه حمله می‌کنند.. . . . . ۲۹
نفوذ به حساب توییتر نیویورک تایمز و خبر جعلی حمله‌ی موشکی روسیه به آمریکا ۳۰
دادستان منتخب ترامپ: باید در رمزنگاری‌ها دربِ پشتی داشته باشیم.. . . . . ۳۱

فصل چهارم: اخبار فنی

شرکت اپل آسیب‌پذیری‌های حیاتی را در هسته‌ی سامانه عامل‌ها وصله می‌کند ۳۳

فهرست مطالب

آسیب‌پذیری که اپل را مجبور کرد ویژگی جدید خود را در فروشگاه اپل حذف کند ۳۵
حمله به پایگاه داده‌ها همچنان ادامه دارد: هدوپ و CouchDB ۳۷
اهداف بعدی مهاجمان
در افزونه‌ی مخفی شرکت ادوبی، آسیب‌پذیری XSS کشف شد ۳۸
توقف اعتماد اوراکل به پرونده‌های JAR امضاءشده با MD5 از اردیبهشت ماه ۳۹
ویجت نظردهی، بسیاری از وب‌گاه‌ها را در معرض خطر قرار داد ۴۰

فصل پنجم: اخبار تحلیلی

برایان کربس، نویسنده‌ی واقعی بدافزار Mirai را کشف کرد ۴۲
بازگشت باتنت Necurs و توزیع باج‌افزار و تروجان بانکی ۴۴
انتشار کد منبع یک بدافزار بانکی اندروید ۴۵

فصل اول

اخبار عمومی

اخبار عمومی

بازگشت بدافزار اندرویدی HummingBad به گوگل‌پلی

بدافزار اندرویدی HummingBad که سال گذشته نزدیک به 10 میلیون دستگاه اندرویدی را آلوده کرده بود و ماهانه برای نویسندگان این بدافزار نزدیک به 300 هزار دلار سود داشت، دوباره برگشته است.

محققان امنیتی نسخه‌ی جدیدی از بدافزار HummingBad را کشف کردند که در بیش از 20 برنامه‌ی اندرویدی در بازار گوگل‌پلی مخفی شده است. این برنامه‌های آلوده پیش از اینکه گروه امنیتی گوگل از این قضیه مطلع شوند و برنامه‌ها را حذف کنند، توسط 12 میلیون کاربر بی‌خبر بارگیری شده‌اند.

نسخه‌ی جدید بدافزار با نام HummingWhale توسط محققان امنیتی شرکت چک‌پوینت کشف شده و دارای ویژگی‌های جدیدی است. این ویژگی‌های جدید به بدافزار اجازه می‌دهد کلاه‌برداری‌های تبلیغاتی را بهتر از قبل انجام داده و سود بیشتری برای توسعه‌دهندگان به همراه داشته باشد.

محققان امنیتی چک‌پوینت اعلام کردند برنامه‌های اندرویدی که آلوده به بدافزار HummingWhale با نام توسعه‌دهندگان چینی و جعلی بر روی فروشگاه گوگل‌پلی با ساختار نام متداول و معمولی منتشر شده‌اند ولی رفتارهای آغازین این برنامه‌ها تا حدودی مشکوک به‌نظر می‌رسد.

محققان چک‌پوینت در پستی که روز دوشنبه منتشر شد گفتند: «این بدافزار چندین رویداد مانند Time_Tick, Screen_Off و Install_Referrer را در بخش راه‌اندازی دستگاه ثبت می‌کند که مشکوک هستند.»

اجرای برنامه‌های مخرب در داخل ماشین مجازی

بدافزار HummingWhale بسیار زرنگ‌تر و حیله‌گرتر از بدافزار HummingBad است چرا که از یک پرونده‌ی APK مبدل اندروید استفاده می‌کند که این پرونده برنامه‌های دیگری را بر روی دستگاه تلفن همراه قربانی بارگیری و نصب می‌کند. اگر قربانی متوجه این قضیه شده و فرآیند مربوط به آن را از کار بیندازد، پرونده‌ی APK خود را در داخل یک ماشین مجازی قرار می‌دهد تا شناسایی آن سخت‌تر شود.

پرونده‌ی نصب‌کننده از یک افزونه‌ی اندروید با نام DroidPlugin که توسط شرکت امنیتی چینی Qihoo 360 توسعه داده شده، استفاده می‌کند تا برنامه‌های مخرب را در داخل ماشین مجازی بارگذاری کند. این پرونده به بدافزار HummingWhale اجازه می‌دهد برنامه‌های مخرب دیگر را بدون ارتقاء مجوزها بر روی ماشین مجازی بارگذاری کرده و عملیات مخرب خود را بر روی گوگل‌پلی مخفی سازد.

به لطف استفاده از ماشین مجازی، دیگر نیازی نیست بدافزار HummingWhale دستگاه اندرویدی را روت کند و می‌تواند تمامی برنامه‌های مخرب مورد نیاز را بر روی

دستگاه قربانی نصب کند.

زمانی که دستگاه قربانی آلوده شد، کارگزار دستور و کنترل، تبلیغات جعلی و برنامه‌های مخرب را به سمت کاربر ارسال می‌کند که بر روی ماشین مجازی در حال اجرا شدن است. در ادامه نیز شناسه‌های ارجاعی جعلی و منحصربفرد برای کاربر ایجاد می‌کند تا در کلاه‌برداری‌های تبلیغاتی از آن استفاده کرده و سود بدست آورد.

شبیه به بدافزار HummingBad، هدف بدافزار HummingWhale نیز بدست آوردن پول بیشتر از طریق کلاه‌برداری‌های تبلیغاتی و نصب برنامه‌های جعلی است. در کنار تمامی این قابلیت‌های مخرب، بدافزار HummingWhale تلاش می‌کند محبوبیت خود را در گوگل‌پلی از طریق نظردهی و امتیازدهی افزایش دهد.

اخبار عمومی

بارگیریِ مخفیانه‌ی برنامه‌ها از فروشگاه گوگل‌پلی توسط بدافزار اندرویدی

دستگاه‌های اندرویدی هدف بدافزار جدیدی قرار گرفته‌اند که به‌طور مخفیانه از فروشگاه گوگل‌پلی برنامه‌هایی را خریداری کرده و بارگیری می‌کند. این بدافزار همچنین اطلاعات حساس کاربران بر روی دستگاه‌های اندرویدی مانند اطلاعات حساب‌های پیکربندی‌شده‌ی گوگل را به سرقت می‌برد.

این بدافزار با نام Skyfin با کمک بدافزارهای دیگری با نام Android.DownLoader توزیع شده و دستگاه‌های اندرویدی را آلوده می‌کند و معمولاً از طریق برنامه‌های موجود در فروشگاه‌های ثالث گسترش می‌یابد. به عبارت دیگر، کاربرانی که برنامه‌ها را از فروشگاهی بجز گوگل‌پلی بارگیری می‌کنند در معرض خطر هستند.

محققان امنیتی از شرکت Dr.Web می‌گویند بدافزار Skyfin می‌تواند برای بارگیری برنامه‌ها به‌طور خودکار بر روی دستگاه قربانی، فرآیند گوگل‌پلی را آلوده کند. با این حال، این برنامه‌ها بر روی دستگاه قربانی نصب نمی‌شوند و در پوشه‌ی بارگیری او قرار می‌گیرند تا قربانی متوجه تغییراتی در تلفن همراه خود نشود.

این شرکت امنیتی می‌گوید: «این بدافزار شناسه‌ی منحصربفرد دستگاه قربانی و اطلاعات حساب‌های گوگل را به سرقت می‌برد. این بدافزار همچنین کدهای احراز هویت داخلی برای ارتباط با گوگل‌پلی را نیز شنود می‌کند. در ادامه این ماژول داده‌های سرقتی را به سمت مؤلفه‌ی اصلی Android.Skyfin.1.origin ارسال می‌کند. در ادامه نیز مؤلفه‌ی اصلی این داده‌ها را به همراه اطلاعاتی از دستگاه قربانی به سمت کارگزار دستور و کنترل می‌فرستد.»

این بدافزار به دستورات خاصی گوش می‌دهد و می‌تواند بر روی گوگل‌پلی برنامه‌های ویژه‌ای را جستجو کند، برنامه را بخرد، قوانین مربوط به برنامه را قبول کرده و به آن رأ دهد. در این شرایط بدون اینکه قربانی از آلودگی دستگاه خود خبر داشته باشد، بدافزار می‌تواند با عملیات خود، باعث محبوبیت بیش از حد یک برنامه در فروشگاه گوگل‌پلی شود.

علاوه بر این مشخص شده که بدافزار Skyfin می‌تواند بر روی تبلیغات موجود در برنامه‌ها کلیک کند. به عبارت دیگر نویسندگان این تبلیغات می‌توانند با آلوده کردن دستگاه‌ها به بدافزار، سود خود را افزایش دهند. شرکت امنیتی می‌گوید: «این بدافزار کلیک بر روی بنر تبلیغات گوگل را شبیه سازی می کند و با بارگیری برنامه های موجود در گوگل‌پلی باعث افزایش نصب‌های برنامه و محبوبیت آن می‌شود.»

تنها راه برای ایمن ماندن در برابر چنین بدافزارهایی این است که تا جایی که امکان دارد از بارگیری برنامه‌ها از فروشگاه‌های ثالث خودداری کنید و هیچ‌گاه بر روی برنامه‌های APK مشکوک کلیک نکنید.

اخبار عمومی

بازگشت دوباره‌ی سرویس رایانامه‌ی «لاوابیت»

سرویس رایانامه‌ی رمزنگاری‌شده «لاوابیت» مستقر در تگزاس که در سال 2013 حکم دادگاه مبنی بر ارائه‌ی کلیدهای SSL برای جاسوسی در رایانامه‌های ادوارد اسنودن را نپذیرفت و تعطیل شد، روز جمعه مجدداً راه‌اندازی شد. مدیرعامل شرکت لاوابیت، لادار لویسون مسئول سرویس کلیدهای SSL بود که نهادهای دولتی می‌توانستند با استفاده از آن به گذرواژه‌های اسنودن دست یابند. هرچند مقامات FBI اصرار داشتند که از این طریق می‌خواهند به گذرواژه‌های حساب اسنودن دست یابند ولی به هر حال، با این کار حساب‌های کاربران دیگر نیز برای FBI قابل دست‌یابی بود.

با این حال شرکت لاوابیت تصمیم گرفت بجای همکاری با FBI و در معرض خطر قرار دادن تمامی مشتریان خود، سرویس رایانامه‌ی خود را از کار بیندازد و از این طریق نزدیک به 410 هزار کاربر قادر به دست‌یابی به حساب‌های رایانامه‌ای خود بر روی این سرویس نبودند. اینک لویسون اعلام کرده سرویس لاوابیت را با معماری جدیدی احیاء کرده و مدیریت کلیدهای SSL را بهبود داده است. همچنین به این سرویس، ویژگی‌های حفظ حریم خصوصی کاربران نیز افزوده شده است به‌طوری که به کاربران اجازه می‌دهد بدون ترس از شنود، رایانامه‌های خود را ارسال کنند.

لویسون در حال انتشار کد منبع استاندارد رایانامه‌ی جهانی است به‌طوری که متن‌باز بوده و از رمزنگاری انتها به انتها پشتیبانی می‌کند. این سرویس رایانامه ضدنظارت بوده و تمامی اَبَرداده‌ها را در رایانامه مخفی می‌کند تا آژانس‌های اطلاعاتی مانند NSA و FBI نتوانند متوجه شوند کدام‌یک از کاربران لاوابیت با هم در حال ارتباط هستند.

این سرویس جدید با نام محیط رایانامه‌ای اینترنت تاریک (DIME) قرار بود به همراه یک برنامه‌ی کارگزار رایانامه به نام Magma، دو روز پیش بر روی گیت‌هاب منتشر شود. لویسون در یک پست وبلاگی نوشت: «DIME تنها استاندارد خودکار، فدارال و رمزنگاری‌شده است که برای کار با تمامی ارائه‌دهندگان سرویس طراحی شده است و نشت اطلاعات و اَبَرداده‌ها را به حداقل می‌رساند. با رمزنگاری تمامی اجزای یک رایانامه از جمله بدنه‌ی پیام، اَبَرداده‌ها و اطلاعات لایه‌ی انتقال، DIME امنیت کاربران را تضمین می‌کند و نشت اطلاعات کاربران را به حداقل می‌رساند.»

به گزارش لویسون کارگزار Magma برای این طراحی شده تا کاربران غیرفنی که فاقد کارخواه رایانامه هستند بتوانند به راحتی از این سرویس رایانامه‌ای استفاده کنند. استاندارد DIME شامل یک حالت رمزنگاری «اعتماد کامل» است که در این حالت لازم است کاربران به رمزنگاری و مدیریت کلید در این سرویس اعتماد کنند.

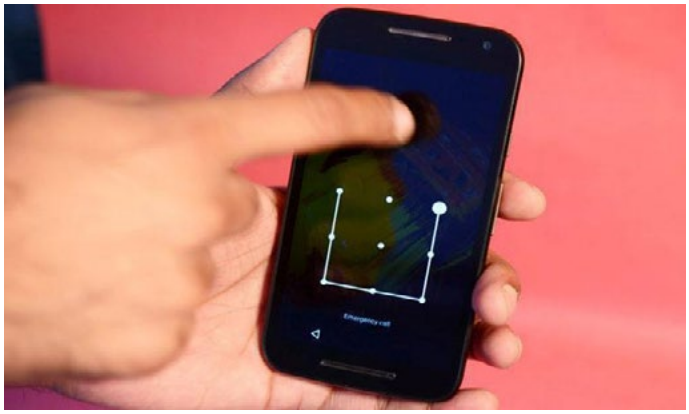
لویسون می‌گوید: «کارگزار رمزنگاری را در سمت شما انجام خواهد داد و ضروری است شما اعتماد کنید و اطمینان داشته باشید که این سرویس، گذرواژه‌های شما را بازنویسی نکرده و در طول فرآیند رمزنگاری به پیام‌های شما دسترسی نخواهد داشت.»

با این حال، استاندارد DIME به کاربرانی که می‌خواهند بر روی مدیریت کلید کنترل کامل داشته باشند، حالت‌های «محتاط» و «پارانوئید» را نیز ارائه می‌دهد که در این حالت کلیدهای کاربران به هیچ جای دیگری منتقل نخواهد شد. حالت پارانوئید به این معنی است که لاوابیت هیچ‌گاه کیلدهای خصوصی کاربران را بر روی کارگزاهای خود ذخیره نخواهد کرد.

در ابتدا، سرویس جدید لاوابیت تنها برای مشتریان موجود این شرکت و در حالت «اعتماد کامل» قابل دست‌یابی خواهد بود. ولی اگر شما قبل از متوقف شدن این سرویس، مشتری این شرکت نبوده‌اید می‌توانید پیش‌ثبت‌نام کنید و منتظر راه‌اندازی احتمالی این سرویس برای کاربران دیگر باشید.

اخبار عمومی

شکستن قفل الگویی اندروید با ۵ بار تلاش توسط مهاجمان



اگر از آن دسته کاربرانی هستید که بر روی دستگاه‌های اندرویدی از سامانه‌ی قفل الگویی استفاده می‌کنید، باید به شما هشدار دهیم که ممکن است دستگاه شما در معرض خطر باشد. این نتایج براساس تحقیقات کارشناسان امنیتی از چند دانشگاه بدست آمده است.

براساس مقاله‌ای که منتشر شده، محققان کشف کردند که مهاجمان می‌توانند با الگوریتم‌های بینایی ماشین با 5 بار تلاش، سامانه‌ی قفل الگویی شما را بشکنند. در این مقاله آمده است:

«وقتی صاحب دستگاه در مکانی مانند یک کافه مشغول نوشیدن قهوه است و قفل الگویی را بر روی دستگاه می‌کشد، می‌توان از این کار مخفیانه ویدئو ضبط کرد. مهاجم می‌تواند در حالی‌که تظاهر می‌کند با تلفن همراه خود مشغول بازی است، این ویدئو را ضبط کند. در ادامه مهاجم می‌تواند با نرم‌افزار بینایی ماشین، اثرانگشت کاربر را نسبت به تلفن همراه ردیابی کند. این نرم‌افزار در عرض چند ثانیه الگوهای پیشنهادی برای باز کردن قفل دستگاه قربانی را تولید خواهد کرد. مهاجم می‌تواند این حمله را بدون ضبط ویدئو و مشاهده‌ی محتوای صفحه‌ی تلفن همراه در فاصله‌ای برابر با دو نیم متر نیز انجام دهد. اگر برای ضبط ویدئو از دوربین‌های SLR استفاده شود، نتایج در فواصل 9 متری نیز قابل قبول خواهد بود.»

گزارش‌ها حاکی از آن است که محققان توانستند بر روی دستگاه‌های مختلف نزدیک به 120 الگوی منحصربفرد را شناسایی کنند و در 95 درصد از موارد می‌توانند با 5 تلاش، الگوی مربوط به دستگاه کاربران مختلف را تشخیص دهند. در ادامه‌ی این مقاله می‌خوانیم:

«بسیاری از افراد از الگوهای پیچیده (خطوط زیادی بین نقطه‌ها) استفاده می‌کنند تا تکرار آن توسط کسی که این الگو را مشاهده کرده سخت شود. با این حال محققان دریافتند که شکستن چنین الگوهایی بسیار راحت‌تر است چرا که گزینه‌ها و حالت‌های موجود برای الگویتم ردیابی اثرانگشت تحت این شرایط محدودتر می‌شود.»

محققان در آزمایش‌های خود توانستند 87.5 درصد از الگوهای نیمه‌پیچیده را بشکنند و 60 درصد از الگوهای ساده نیز در اولین تلاش قفلشان باز شد.

راه‌کارهای دفاعی

باوجود اینکه یافته‌های محققان نگرانی‌های کاربران را افزایش می‌دهد ولی با انجام برخی از راه‌کارهای دفاعی می‌توان از چنین رخدادهایی پیشگیری کرد. اگر نگران لو رفتن گذرواژه‌ی الگویی خود هستید می‌توانید هنگام رسم آن جلوی صفحه‌ی نمایش را با دست دیگر خود بپوشانید. همواره از خود این سؤالات را بپرسید: کدام تنظیمات امنیتی برای دستگاه من مناسب است؟ چگونه این تظیمات را پیکربندی نمایم؟ چگونه بررسی کنم که تنظیمات مورد استفاده درست هستند؟

اخبار عمومی

نفوذ به انجمن‌های بازی کلش رویال

شرکت سوپرسل که سازنده‌ی بازی‌های فوق‌محبوبی مانند کلش رویال است، در شهریور ماه دچار نقض داده شده و احتمال می‌رود داده‌های کاربران آن افشاء شده باشد.

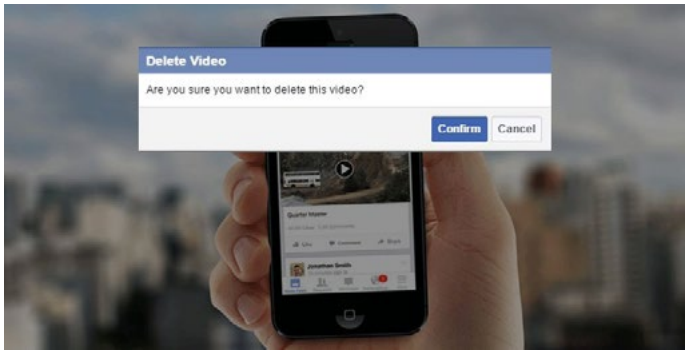
مدیر انجمن‌های این شرکت در اطلاعیه‌ای اعلام کرد نفوذگران توانستند با بهره‌برداری از آسیب‌پذیری‌ها به وب‌گاه نفوذ کنند ولی در حالی‌که تلاش داشتند به حساب‌های کاربری نیز دست یابند، حساب‌های کاربری در حال حاضر در امنیت کامل هستند. تنها آدرس‌های رایانامه و گذرواژه‌های رمزنگاری‌شده افشاء شده و داده‌های دیگری به سرقت نرفته است.

تاکنون هیچ فرد یا گروهی مسئولیت این نفوذ سایبری را برعهده نگرفته و مشخص نیست چه تعداد حساب کاربری در اثر این حمله تحت تأثیر قرار گرفته است اما شرکت سوپرسل اعلام کرده تمامی کاربران باید گذرواژه‌های حساب‌های کاربری خود را تغییر دهند. همچنین به کاربران توصیه شده به هیچ‌وجه از گواهی‌نامه‌های یکسان بر روی وب‌گاه‌های مختلف استفاده نکنند و اگر قبلاً از گذرواژه‌ی حساب‌های بازی خود در جای دیگری استفاده کردند، تمامی آن‌ها را تغییر دهند.

نفوذگران اغلب تلاش می‌کنند گذرواژه‌های کاربران بر روی سرویس‌های برخط و محبوب همچون گوگل و یاهو را به سرقت ببرند و اینک این نقض داده ممکن است سرویس‌های دیگری بجز کلش رویال را نیز تحت تأثیر قرار دهد. برای تغییر گذرواژه‌ی حساب انجمن کلش رویال، می‌توانید از این پیوند اقدام کنید.

اخبار عمومی

آسیب‌پذیری در فیس‌بوک و حذف ویدئوها توسط نفوذگران



یک محقق امنیتی آسیب‌پذیری را در فیس‌بوک کشف کرد. این آسیب‌پذیری به مهاجمان اجازه می‌دهد ویدئوهای منتشرشده بر روی دیوار یک حساب کاربری را حذف کنند.

این آسیب‌پذیری توسط محقق امنیتی با نام دان ملامد در تیر ماه سال جاری کشف شده است. این آسیب‌پذیری به مهاجم اجازه می‌دهد از راه دور و بدون نیاز به مجوز و احراز هویت، ویدئوهای به اشتراک گذاشته‌شده را حذف کند. علاوه بر این، نفوذگر می‌تواند قابلیت ارسال نظرات بر روی این ویدئوها را نیز از کار بیندازد.

بهره‌برداری از این آسیب‌پذیری چگونه امکان‌پذیر است؟

برای بهره‌برداری از این آسیب‌پذیری، ملامد ابتدا در صفحه‌ی فیس‌بوک خود یک رویداد عمومی را ایجاد کرد و در بخش مباحثه‌ی این رویداد یک ویدئو بارگذاری کرد. در زمان بارگذاری این ویدئو، این محقق با استفاده از Fiddler درخواست POST را بدست آورده و بجای شناسه‌ی ویدئوی خود، شناسه‌ی ویدئوی دیگر در شبکه‌ای اجتماعی را قرار داد.

با این حال کارگزار فیس‌بوک به این عمل با خطای «محتوای مورد نظر در دسترس نیست» پاسخ می‌دهد اما ویدئوی قربانی با موفقیت پست شده و به‌خوبی نمایش داده می‌شود. زمانی‌که این عملیات انجام شد، ملامد پست مربوط به رویداد خود را حذف می‌کند. به همراه حذف پست رویداد، ویدئوی مورد نظر نیز حذف خواهد شد.

قسمت اصلی ماجرا زمانی است که این ویدئو از روی دیوار قربانی در شبکه‌ی اجتماعی نیز حذف خواهد شد. ملامد می‌نویسد: «در قسمت پایین پست، گزینه‌ای برای خاموش کردن نظردهی نمایش داده می‌شود، که شما می‌توانید آن را نیز انتخاب کنید.»

برای مشاهده‌ی مراحل این حمله و بهره‌برداری از این آسیب‌پذیری، می‌توانید ویدئوی مربوط به اثبات مفهومی این آسیب‌پذیری را مشاهده کنید. ملامد به‌طور مسئولانه این آسیب‌پذیری را به گروه امنیتی فیس‌بوک اطلاع داد و این گروه با آغاز سال جدید، در عرض دو هفته این آسیب‌پذیری را وصله کردند. پس از وصله‌ی آسیب‌پذیری نیز شرکت فیس‌بوک در برنامه‌ی پاداش در ازای اشکال خود مبلغ 10 هزار دلار به ملامد جایزه داد.

این اولین بار نیست که چنین آسیب‌پذیری در فیس‌بوک کشف می‌شود که به نفوذگران اجازه می‌دهد ویدئوهای کاربران را در این شبکه‌ی اجتماعی حذف کنند. محققان امنیتی در برنامه‌ی پاداش در ازای اشکال فیس‌بوک، به‌طور مداوم چنین آسیب‌پذیری‌هایی را کشف کرده و برای امن‌تر کردن این شبکه‌ی اجتماعی گزارش می‌دهند.

فصل دوم

مدیریت امنیت

مدیریت امنیت

سیمانتک گواهی‌نامه‌های اشتباه صادرشده را باطل کرد

سیمانتک تعداد زیادی از گواهی‌نامه‌ها را که به اشتباه صادر شده بودند باطل کرد. این گواهی‌نامه‌ها شامل دامنه‌هایی مانند example.com و test.com بود. این اولین بار نیست که صدور گواهی‌نامه در این شرکت تحت بررسی‌های دقیق، انجام نشده است.

گواهی‌نامه‌های اشتباه در سامانه‌ی شفافیت گواهی‌نامه توسط مدیرعامل SSLMate مورد بررسی قرار گرفت. این کارشناس امنیتی چندین گواهی‌نامه برای دامنه‌ی example.com کشف کرد که توسط مالک این وب‌گاه مجاز شمرده نمی‌شدند. او در ادامه گواهی‌نامه‌هایی را برای دامنه‌های test1.com، test.com و سایر دامنه‌ها که حاوی رشته‌ی test بودند را شناسایی کرد.

این محقق امنیتی نزدیک به 100 گواهی‌نامه‌ی اشتباه را کشف کرد که توسط سیمانتک و شرکت‌های تابعه‌ی آن از جمله GeoTrust و Thawte صادر شده بودند. در این گواهی‌نامه‌های مشکل‌ساز، چندین رکورد با مقدار test وجود داشت که به‌نظر می‌رسید این گواهی‌نامه‌ها به منظور آزمایش و بررسی صادر شده‌اند.یکی از کارشناسان سیمانتک که مدیریت بخش قوانین PKI را بر عهده دارد، گفت این گواهی‌نامه‌ها توسط یکی از شرکای این شرکت با نام WebTrust صادر شده است. این کارشناس در ادامه اعلام کرد امتیازات این شریک تجاری برای صدور گواهی‌نامه کاهش یافت و محدود شد و گواهی‌نامه‌های اشتباه نیز باطل شدند.سیمانتیک گفت: «ما امتیازات این شریک تجاری را برای صدور گواهی‌نامه محدود کردیم و همچنان در حال بررسی این مسئله هستیم. در حالی‌که این شرکت تمامی گواهی‌نامه‌های اشتباه را باطل کرده ما نیز تمامی گواهی‌نامه‌های صادرشده در 24 ساعت گذشته را باطل کرده‌ایم. بررسی‌های ما ادامه دارد.»

کارشناس سیمانتک به مالکان دامنه‌ها توصیه کرد تا رکوردهای ثبت‌شده برای شفافیت گواهی‌نامه را بررسی کرده و ببینند برای وب‌گاه‌های آن‌ها گواهی‌نامه‌های اشتباهی صادر نشده باشد. در مهر ماه سال 94 گوگل از شرکت سیمانتک درخواست کرد تا در صدور گواهی‌نامه‌های خود دقت بیشتری داشته باشد. این درخواست زمانی اعلام شد که شرکت تابعه‌ی سیمانتک با نام Thawte برای دامنه‌ی google.com گواهی‌نامه‌های اشتباه صادر کرده بود. این شرکت مدعی شده بود تنها با اهداف آزمایشی این گواهی‌نامه‌ها را صادر کرده است ولی پس از بررسی‌ها، این شرکت چندین کارمند خود را از کار برکنار کرد.در بهمن ماه سال 94 بخش تجارت گواهی‌نامه‌های سیمانتک مجدداً خبرساز شد زمانی که این شرکت از سازندگان مرورگرهای وب درخواست کرد تا 9 گواهی‌نامه‌ی SSL دیگر امضاءشده با SHA-1 برای Worldpay صادر کند. این درخواست زمانی صورت گرفت که قبل از مهلت زمانی در تاریخ 10 دی ماه سال 94، پردازنده‌ی پرداخت در به‌روزرسانی برخی از دستگاه‌ها با شکست مواجه شده بود.

مدیریت امنیت

حمله‌ی منع سرویس توزیع‌شده به بانک Lloyds در سه روز متوالی

بانک Lloyds در سه روز متوالی هدف حملات منع سرویس توزیع‌شده قرار گرفته است. نفوذگران تلاش داشتند با از کار انداختن این وب‌گاه باعث اختلال در دسترسی مشتریان به این بانک شوند.

خبرگزاری‌ها اعلام کردند این اتفاقات دو هفته پیش رخ داده و از 22 دی ماه آغاز و در 25 دی پایان یافته است. این بانک بزرگ در انگلستان توسط نفوذگران بین‌المللی هدف حمله‌ی منع سرویس توزیع‌شده قرار گرفته ولی هنوز اعلام نشده منشأ این حمله کجا بوده است. نفوذگران تلاش دارند با ارسال ترافیک زیاد به سمت وب‌گاه از دسترسی مشتریان به وب‌گاه این بانک جلوگیری کرده و در نهایت باعث درهم شکستن وب‌گاه بانک شوند. در ادامه نفوذگران مایل هستند مانده حساب و پرداخت‌های مشتریان را رویت کنند.

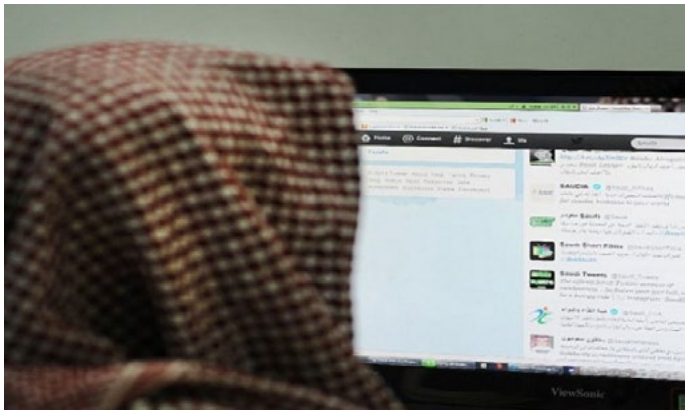
حملات منع سرویس توزیع‌شده به ابزار محبوبی برای مهاجمان سایبری تبدیل شده که می‌خواهند سرویس یا وب‌گاهی را از کار بیندازند. این حملات بسیار رایج هستند و ما در مورد این حملات در خبرها بسیار می‌شنویم. هرچند در حمله‌ی اخیر شاهد هستیم که نفوذگران نمی‌خواستند صدمات زیادی به وب‌گاه بانک وارد کنند. خوشبختانه برخلاف حملاتی که بر روی بانک‌ها انجام می‌شود، در این حمله هیچ مشتری پول خود را از دست نداده است. به‌طور مثال، بانک Tesco هدف حمله‌ی مهاجمان قرار گرفته بود و نزدیک به 3.1 میلیون دلار از حساب 9 هزار مشتری به سرقت رفته بود.

به گزارش مقامات رسمی بانک Lloyds، تنها تعداد محدودی از مشتریان در طول این 3 روز با مشکل مواجه شدند. در اکثر موارد، زمانی‌که مشتریان می‌خواستند بر روی وب‌گاه بانک وارد حساب خود شوند، در دسترسی به حساب با مشکل مواجه شده بودند.

در حال حاضر، مقامات بانک Lloyds در کنار مراجع قانونی در تلاش هستند تا عوامل این حمله را شناسایی کنند. باید منتظر ماند و دید آیا پلیس می‌تواند این مهاجمان سایبری را پیدا کند یا کشف آن‌ها یک مسئله‌ی حل‌نشده باقی خواهد ماند.

مدیریت امنیت

گروه نفوذ Greenbug به بدافزاری که عربستان سعودی را هدف قرار داده، کمک می‌کند



گواهی‌نامه‌های به سرقت رفته که در حملات بدافزار Shamoon علیه کشورهای حوزه‌ی خلیج فارس مورد استفاده قرار می‌گرفت، به‌نظر می‌رسد توسط گروه نفوذی با نام Greenbug بدست آمده باشد.

بدافزار Shamoon که با نام مستعار Disttrack نیز شناخته می‌شود، یک بدافزار حذف‌کننده‌ی دیسک است که از سال 2012 شناسایی شده است و آن زمان حدود 35 هزار رایانه‌ی صنعت نفت و گاز عربستان سعودی را از کار انداخت. Shamoon 2 نیز نسخه‌ی جدیدی از این بدافزار است که اخیراً کشور عربستان سعودی را هدف قرار داده است.

موج اول حملات توسط بدافزار Shamoon 2 در تاریخ 27 آبان و موج دوم در 9 آذر ماه اجرا شد. این حملات که به‌نظر می‌رسد از طرف کشور ایران انجام شده باشد، با استفاده از بدافزار Disttrack حذف دیسک‌های سامانه‌های آلوده را شروع می‌کند.

این بدافزار برای هدف قرار دادن سامانه‌های مشخصی که گواهی‌نامه‌های آن‌ها معلوم است، برنامه‌ریزی شده و شرکت امنیتی سیمانتک معتقد است، این اطلاعات در حملات قبلی که توسط گروه Greenbug انجام شده، بدست آمده است.

این گروه جاسوسی از یک تروجان دسترسی راه دور به نام Ismdoor و سایر ابزارها برای هدف قرار دادن کشورهای خاورمیانه استفاده کرده است. مهاجمان سامانه‌های حمل‌ونقل هوایی، سرمایه‌گذاری، دولتی و سازمان آموزش و پرورش در کشورهای مختلف از جمله عربستان سعودی، ایران، عراق، بحرین، قطر، کویت و ترکیه و یک شرکت عربستانی در استرالیا را هدف قرار دادند.

گروه Greenbug رایانامه‌هایی جعلی با عنوان کسب‌وکار تجاری برای کاربران ارسال می‌کند تا از این راه کاربران را فریب داده و بدافزار مورد نظر را بر روی سامانه‌های آن‌ها بارگیری و نصب کند. در این رایانامه یک پرونده‌ی آرشیوی RAR که حاوی یک سند پی‌دی‌اف و یک پرونده‌ی کمکی HTML است برای قربانی ارسال می‌شود. این اسناد حاوی تروجان Ismdoor هستند.

برای جلوگیری از تشخیص، این بدافزار در جریان داده‌ی متناوب (ADS) مخفی شده است. به محض اجرای این پرونده، بدافزار Ismdoor یک دربِ پشتی را باز کرده و برای ارتباط با کارگزار دستور و کنترل از ابزار پاورشِل استفاده می‌کند. هدف از طراحی این تروجان بارگیری و نصب بدافزارهای دیگر است که می‌توانند به‌عنوان کی‌لاگر و سرقت اطلاعات حساس کاربران مورد استفاده قرار بگیرند.

محققان سیمانتک معتقدند گروه نفوذ Greenbug گواهی‌نامه‌های مورد نیاز برای حمله را در حملات قبلی که توسط تروجان Ismdoor انجام شده از سامانه‌های مدیریتی سازمان‌ها بدست آورده‌اند.

شبکه‌ی پالوآلتو اوایل این ماه گزارش داده بود که بدافزار Shamoon 2 محصولات مجازی‌سازی را هدف قرار داده تا کار بازیابی داده‌ها برای سازمان‌ها سخت‌تر و سخت‌تر شود. روز دوشنبه عربستان سعودی به تمامی سازمان‌های این کشور هشدار داده که احتمال وقوع حملات جدید وجود دارد. این هشدار برای وزارت کار این کشور، یک شرکت مواد شیمیایی و سایر نهادها ابلاغ شده است.

مدیریت امنیت

در سال 2017 همچنان 200 هزار سامانه دارای آسیب‌پذیری Heartbleed هستند

نزدیک به دو سال و نه ماه از افشای آسیب‌پذیری Heartbleed گذشته و هنوز هم 200 هزار سامانه دارای این آسیب‌پذیری هستند.

تلاش‌ها برای وصله‌ی آسیب‌پذیری از سال 2014 تاکنون کاهش یافته است. این آسیب‌پذیری با شناسه‌ی CVE-2014-0160 برنامه‌ی OpenSSL را تحت تأثیر قرار داده و به مهاجمان اجازه‌ی سرقت گذرواژه‌ها، کوکی‌های ورود، کلیدهای خصوصی رمزنگاری و سایر اطلاعات را می‌دهد.

پویش‌های ابزار Shodan نشان می‌دهد نزدیک به 200 هزار نمونه‌ی OpenSSL وصله نشده و دارای آسیب‌پذیری Heartbleed هستند. این پویش نشان می‌دهد 42032 سرویس در آمریکا، 15380 سرویس در کره، 14116 سرویس در چین و 14072 سرویس در آلمان در معرض خطر قرار دارند.

تقریباً 75 هزار سرویس از گواهی‌نامه‌های منقضی‌شده‌ی SSL و لینوکس x.3 استفاده می‌کنند. یک سال قبل 10 کارگزار سرویس OpenSSL VPN هنوز دارای آسیب‌پذیری Heartbleed بودند.

ماجرای وصله نکردن آسیب‌پذیری‌ها از آن چیزی که فکر می‌کنیم بدتر است. از تیر ماه یک آسیب‌پذیری شناخته‌شده‌ی مایکروسافت آفیس مورد بهره‌برداری می‌گیرد که آفیس 2012 را تحت تأثیر قرار می‌دهد. این نشان می‌دهد کاربران هیچ توجهی به به‌روزرسانی برنامه‌ها ندارند، کاری که حتی دزدان دریایی هم آن را انجام می‌دهند.

ردموند در سال 2015 هشدار داد که ماکروهای ورد دوباره به صحنه‌ی تهدیدات سایبری برگشته و نزدیک به نیم میلیون رایانه را در سراسر جهان آلوده کرده‌اند. در سال 2106 نیز شاهد پویش‌های مخربی بودیم که از ماکروهای مخرب آفیس بهره‌برداری می‌کردند.

مدیریت امنیت

پشتیبانیِ پیش‌فرض از HTTPS بر روی وب‌گاه‌های دولتی آمریکا اجباری شد

تمامی وب‌گاه‌های دولتی آمریکا که امسال راه‌اندازی خواهند شد، قرار است به‌طور پیش‌فرض از HTTPS استفاده کنند. این روند برای تقویت وب‌گاه‌های دولتی که به دفعات مورد نفوذ قرار گرفته، انجام شده است. دولت باراک اوباما تا 11 دی ماه به تمامی وب‌گاه‌های دولتی مهلت داده بود تا به‌طور پیش‌فرض از HTTPS استفاده کنند ولی به گزارش مقامات غیررسمی، تنها 60 درصد از این وب‌گاه‌ها به سمت HTTPS مهاجرت کردند. با این حال، از آغاز سال 2017 بر روی تمامی وب‌گاه‌های دولتی .gov قابلیت HTTPS فعال خواهد بود.

اداره خدمات عمومی آمریکا اعلام کرد قابلیت HTTPS بر روی تمامی زیردامنه‌های وب‌گاه‌های دولتی، حتی در اینترانت‌ها فعال خواهد شد چرا که نداشتن HTTPS در اینترانت‌ها نیز خطرساز است. اداره خدمات عمومی، راه‌اندازی این طرح را در بهار سال 2017 اعلام کرده و 30 روز قبل از اجرا شدن به تمامی مشتریان این وب‌گاه‌ها اطلاع‌رسانی خواهد شد.

اداره‌ی خدمات عمومی آمریکا تنها سازمانی نیست که مدیران وب‌گاه‌ها را به حرکت به سمت HTTPS تشویق می‌کند بلکه سازمان‌های بزرگ دیگر نیز این کار را انجام می‌دهند. به‌عنوان مثال شرکت گوگل بر روی وب‌گاه‌هایی که HTTPS آن‌ها فعال نیست، هنگامی که کاربر گذرواژه یا اطلاعات کارت اعتباری خود را وارد می‌کند، برای جلوگیری از سرقت اطلاعات و جعل هویت به کاربران هشدار می‌دهد.

فصل سوم

امنیت سایبری

امنیت‌سایبری

سپر طلایی چین و ممنوعیت استفاده از شبکه‌ی خصوصی مجازی

مدت طولانی است که کشور چین به قوانین سخت‌گیرانه در خصوص سانسور اینترنت با استفاده از یک دیواره‌ی آتش قوی و بزرگ در این کشور شناخته می‌شود. این دیواره‌ی آتش، سپر طلایی چین نام دارد و محدودیت‌ها و سانسورهای مختلفی را در دسترسی کاربران به وب‌گاه‌های خارجی اعمال می‌کند.

این دیواره‌ی آتش بزرگ نزدیک به 171 مورد از هزار وب‌گاه برتر دنیا از جمله گوگل، فیس‌بوک، توییتر، تامبلر و دراپ‌باکس را مسدود کرده است. بنابراین برای دور زدن این محدودیت‌ها و دسترسی به این وب‌گاه‌ها، صدها هزار نفر از شهروندان چینی از شبکه‌ی خصوصی مجازی (VPN) استفاده می‌کنند.

به گزارش خبرگزاری‌ها، اخیراً دولت چین اعلام کرده در تلاشی گسترده سعی دارد تمامی شبکه‌های خصوصی مجازی را از کار بیندازد و با این کار دسترسی به وب‌گاه‌های خارجی برای کاربران چینی بسیار سخت خواهد شد.

در برنامه‌ای با عنوان «پاک‌سازی» اتصالات اینترنت در چین، وزارت صنایع و فناوری این کشور اعلام کرد در یک تلاشِ 14 ماهه تمامی اتصالات VPN را از کار انداخته است.

سرویس‌های VPN با رمزنگاری ترافیک کاربر و مسیریابی این ترافیک از طریق اتصالات راه دور، مکان کاربر در چین را مخفی کرده و می‌توانند محدودیت‌ها و سانسورها را دور بزنند.

در قانون جدید، استفاده و راه‌اندازی سرویس VPN محلی بدون تأیید دولت، غیرقانونی محسوب شده و نیاز است تمامی اتصالات و کابل‌های VPN موجود در چین همگی دارای مجوز از نهادهای دولتی باشند.

علاوه بر این تمامی ارائه‌دهندگان سرویس اینترنت (ISP)، ارائه‌دهندگان سوریس اَبر و نمایندگی‌های فروش VPN باید خود-بازرسی داشته و بر عملیات غیرقانونی بر روی کارگزارهای خود نظارت داشته باشند. ممنوعیت استفاده از سرویس VPN و اتصالات کابلی به سرعت اجرا شده و تا 11 فروردین ماه سال 97 برقرار خواهد بود.

علاوه بر ممنوعیت VPN، وزارت فناوری اطلاعات چین گفت نظارتی بر روی ارائه‌دهندگان سرویس اینترنت، شبکه‌های تحویل محتوا و مراکز داده‌ی اینترنتی انجام خواهد داد تا مجوز آن‌ها در حوزه‌های تعریف‌شده توسط نهادهای دولتی را بررسی کند.

امنیت‌سایبری

یاهو تحت بازرسی: چرا نقض داده‌ی عظیم در این شرکت دیر اطلاع‌رسانی شده است؟

یاهو در شرایط سختی به سر می‌برد و در بررسی‌های سازمان بورس و اوراق بهادار آمریکا، از یاهو سؤال شده چرا در گزارش این نقض داده به مشتریان و سهام‌داران خود کُند عمل کرده است.

سازمان بورس و اوراق بهادار آمریکا بررسی‌هایی را برای نقض داده‌ی یاهو راه‌اندازی کرده است. این سازمان بیشتر تلاش می‌کند بفهمد آیا افشای این نقض داده توسط یاهو مطابق با قوانین امنیتی و مدنی بوده است یا خیر. یاهو مدعی شده که در یک دوره‌ی سه ماهه با ارائه‌ی اسنادی با سازمان‌های اطلاعاتی، دولت‌های خارجی و سازمان‌های فدرال و ایالتی همکاری داشته تا به آن‌ها اطلاعاتی راجع‌به این حادثه‌ی امنیتی بدهد.

سال گذشته، شرکت یاهو دو نقض داده‌ی بزرگ را در تاریخ امنیت اینترنت، به کاربران خود اطلاع داد. این نقض داده‌ها بقدری بزرگ بود که گفته می‌شد نهادهای حکومتی و دولتی پشت این نفوذها بوده‌اند.

اولین نقض داده در شهریور ماه گزارش شد. آن زمان گفته می‌شد در این نفوذ نزدیک به 500 میلیون کاربر تحت تأثیر قرار گرفته‌اند. یاهو اعتراف کرد نفوذگران در این حمله اطلاعاتی مانند نام، آدرس رایانامه، شماره تلفن ، تاریخ تولد، گذرواژه‌های درهم‌سازی‌شده به علاوه‌ی سؤالات و پاسخ‌های رمزنگاری شده یا نشده را به سرقت برده‌اند. ولی اطلاعات حساسی مانند اطلاعات حساب‌های بانکی و کارت‌های اعتباری از آسیب نفوذگران دور مانده‌اند.

مشکل اینجاست که تقویباً یک ماه قبل از اطلاع‌رسانی رسمی یاهو، نفوذگران اطلاعات 200 میلیون حساب کاربری یاهو را در وب تاریک به فروش گذاشتند. این اطلاعات مربوط به سال 2014 بود. این شرکت اعلام کرد در حال بررسی شرایط بوده درحالی‌که دو ماه قبل از آن، یاهو از این نقض داده‌ی عظیم باخبر شده است.

نفوذ دوم که در نوع خود بی‌سابقه‌ترین نفوذ تاریخ است، در آذر ماه اطلاع‌رسانی شد. یاهو در ادامه اعتراف کرد که نزدیک به 1 میلیارد حساب کاربری در معرض خطر قرار گرفته و این سرقت در سال 2013 رخ داده است. اطلاعات به سرقت‌رفته مشابه اطلاعات نفوذ قبلی بود. یاهو معتقد است این نفوذها پس از دسترسیِ یک نهاد ثالث به کدهای اختصاصی، اتفاق افتاده و این گروه در ادامه از این کد برای جعل کوکی‌ها استفاده کرده‌اند.

یاهو در حال حاضر در شرایط بسیار بدی قرار داد و از طرفی نیز با وریزون در خصوص معامله‌ی یاهو صحبت می‌کند. اینک چندین سؤال از یاهو باقی مانده است. یک اینکه چرا اطلاع‌رسانی این نقض داده‌های عظیم اینقدر به‌طول انجامیده است و دوم اینکه یاهو برای محافظت از کاربران خود در سراسر جهان چه کارهایی باید انجام می‌داد؟

اوایل این ماه، گزارشی منتشر شد مبنی بر اینکه هسته‌ی اصلی و تجاری یاهو در حال واگذاری به وریزون به قیمت 4.8 میلیارد دلار است و بقیه‌ی بخش‌های باقی‌مانده از این شرکت، Altaba نام‌گذاری خواهد شد. Altaba یک شرکت سهام‌داری است که نزدیک به 15 درصد از سهام آن متعلق به شرکت علی‌بابا و 35 درصد آن متعلق به یاهو در ژاپن است.

امنیت‌سایبری

در برنامه‌ی پاداش در ازای اشکال ارتش آمریکا ۱۱۸ آسیب‌پذیری وصله شد

ارتش آمریکا روز پنج‌شنبه نتایج اولین برنامه‌ی پاداش در ازای اشکال خود را به اشتراک گذاشت. این برنامه از 1 دی ماه به مدت 3 هفته در حال برگزاری بود و خبرها حاکی از آن است که این برنامه با موفقیت انجام شده است.

پس از موفقیت برنامه‌ی نفوذ به پنتاگون، این دومین برنامه‌ی پاداش در ازای اشکال بود که در سطح سازمان‌های دولتی انجام می‌شد. مقامات دولتی پورتال‌ها و پایگاه داده‌های خود را در اختیار نفوذگران کلاه سفید و محققان امنیتی قرار دادند تا بر روی آن تست نفوذ انجام داده و آسیب‌پذیری‌های ممکن را کشف کنند.

وزیر سابق ارتش آمریکا گفت: «ارتش در این برنامه توانست با گروهی از فناوری‌ها و محققان امنیتی به‌طور مستقیم در ارتباط باشد، موضوعی که شاید قبلاً از آن خودداری می‌کرد.»

ارتش آمریکا روز پنج‌شنبه اعلام کرد بیش از 400 گزارش آسیب‌پذیری دریافت کرده است که 118 مورد از آن‌ها منحصربفرد و عملیاتی هستند. به شرکت‌کنندگانی که اشکالی منحصربفرد را گزارش داده‌اند، بیشترین مقدار جایزه به مبلغ 100 هزار دلار پرداخت شده است. ارتش از 371 محقق امنیتی دعوت کرده بود تا در این برنامه شرکت کنند و 25 نفر از شرکت‌کنندگان از کارکنان دولتی از جمله 17 نفر نیروهای ارتش بودند.

ارتش همچنین جزئیات سطح بالایی از چندین آسیب‌پذیری بر روی وب‌گاه goarmy.com را به اشتراک گذاشت. این آسیب‌پذیری‌ها توسط یکی از شرکت‌کنندگان کشف شده بود و زنجیره‌ای از این آسیب‌پذیری‌ها دسترسی به وب‌گاه‌های داخلی وزارت دفاع آمریکا را بدون احراز هویت در اختیار مهاجمان قرار می‌داد.

برنامه‌های نفوذ به پنتاگون و برنامه‌ی پاداش در ازای اشکال ارتش توسط HackerOne برگزار شده است. HackerOne در یک پست گفت: «در سطح شبکه یک پروکسی باز وجود داشت که فرآیند مسیریابی نیز از طریق آن انجام می‌شد. به دلیل وجود آسیب‌پذیری در این پروکسی، محققان امنیتی می‌توانستند به شبکه‌های داخلی ارتش دست یابند. به خودی خود، هر یک از آسیب‌پذیری‌ها قابل توجه بودند ولی وقتی با یکدیگر ترکیب می‌شدند مسئله‌ای جدی رخ می‌داد.»

در ادامه‌ی پست به اهمیت بررسی اشکالات و آسیب‌پذیری‌های امنیتی توسط محققان حرفه‌ای تأکید شد که نسبت به روش‌های خودکار کشف آسیب‌پذیری‌ها بسیار بهتر عمل می‌کنند. برنامه‌ی پاداش در ازای اشکال ارتش آمریکا برای محققان امنیتی بخش خصوصی و تعدادی از محققان دولت و ارتش باز بود. این برنامه نیز همانند برنامه‌ی نفوذ به پنتاگون با موفقیت انجام شد. در برنامه‌ی نفوذ به پنتاگون 138 آسیب‌پذیری وصله شد و در مجموع 150 هزار دلار به محققان امنیتی پرداخت شد.

وزیر سابق ارتش آمریکا در ادامه افزود: «ما می‌دانیم

آن‌طور که باید و شاید نمی‌توانیم به تجارت خود ادامه داده و با روند سریع و رو به رشد فناوری حرکت کنیم. هنوز هم کسانی در سراسر دنیا وجود دارند که می‌خواهند به وب‌گاه، داده‌ها و اطلاعات ما دست یابند. با اینکه ما بسیار آموزش دیده‌ایم اما هنوز هم این قابلیت‌ها کافی نیست.»

امنیت‌سایبری

دستگیری نفوذگر روسی، نویسنده‌ی بدافزار NeverQuest

یک نفوذگر روسی که توسط FBI به جرم نفوذ به رایانه‌ها تحت تعقیب بود، اوایل این هفته در اسپانیا دستگیر و راهی زندان شد. هنوز در رابطه با استرداد این نفوذگر به آمریکا تصمیمی اتخاذ نشده است.

گواردیا سیویل، افسر آژانس اطلاعاتی اسپانیا، در فرودگاه بارسلونا این نفوذگر 32 ساله با نام استانیسلاو لیسو را با حکم بازداشت پلیس اینترپل و به درخواست FBI دستگیر کرده است.

لیسو به جرم ایجاد و انجام فعالیت مخرب با تروجان بانکی NeverQuest دستگیر شده است. این بدافزار مؤسسات مالی در سرتاسر جهان را هدف قرار داده و بالغ بر 5 میلیون دلار ضرر و زیان به بار آورده است.

این دستگیری پس از آن انجام شد که مقامات اطلاعاتی آمریکا اعلام کردند نفوذگران روسی پشت نفوذهای آبان ماه به انتخابات ریاست جمهوری آمریکا بوده‌اند و احتمالاً در انتخاب دونالد ترامپ به‌عنوان رئیس جمهور آمریکا تأثیرگذار بوده‌اند.

با این حال پلیس اسپانیا در بیانیه‌ای رسمی اعلام کرد با بررسی‌هایی که از سال 2014 شروع شده بود، FBI لیسو را تحت تعقب قرار داده بود. تروجان بانکی NeverQuest به کلاه‌برداران سایبری اجازه می‌داد به رایانه‌های افراد و مؤسسات مالی دسترسی یافته و داده‌های بانکی آن‌ها را به سرقت ببرند.

این بدافزار از طریق شبکه‌های اجتماعی، رایانامه‌ها و پروتکل‌های انتقال پرونده توزیع می‌شود و می‌تواند محتوای وب‌گاه‌های بانکی را دست‌کاری کرده و فرم‌های جعلی در آن قرار دهد. از طریق این فرم‌ها، مهاجمان می‌توانند گواهی نامه های حساب‌های کاربران را به دست آورند.

این بدافزار همچنین به مهاجمان اجازه می‌دهد با استفاده از کارگزار پردازش شبکه‌ی مجازی، کنترل دستگاه آلوده را در اختیار بگیرند. در ادامه از این رایانه‌ها برای ورود به حساب‌های بانکی و مالی قربانیان و کلاه‌برداری استفاده می‌شود.

افسر اسپانیایی در توضیحات خود گفت: «در بررسی که بر روی کارگزارهای لیسو در فرانسه و آلمان انجام دادیم، فهرستی از اطلاعات را در پایگاه داده‌های آن مشاهده کردیم که در این بین مانده حساب قربانیان نیز به چشم می‌خورد. در یکی از کارگزارهایی که لیسو استفاده می‌کرد، میلیون‌ها گواهی‌نامه‌ی ورود به حساب‌های کاربران مشاهده شد که شامل نام کاربری، گذرواژه، سؤال و پاسخ امنیتی در حساب‌های بانکی و مالی قربانیان بود.»

گزارش‌های حاکی از آن است که لیسو به‌عنوان مدیر سامانه و توسعه‌دهنده‌ی وب در یک شرکت روسی مشغول به کار بود. این نفوذگر روسی تا زمان برگزاری دادگاه عالی اسپانیا، در منطقه‌ی شمال شرقی کاتالونیا تحت نظر خواهد بود. در این دادگاه عالی قرار است در خصوص استرداد لیسو به آمریکا تصمیم‌گیری شود.

امنیت‌سایبری

نفوذ به حساب توییتر بی‌بی‌سی و خبر جعلی تیراندازی به دونالد ترامپ

دیروز حساب توییتر متعلق به بی‌بی‌سی مورد نفوذ قرار گرفت و در آن پیامی بسیار عجیب منتشر شد. در این پیام آمده است: «آخرین اخبار: رئیس جمهور منتخب، دونالد ترامپ در اثر تیراندازی از ناحیه‌ی بازو زخمی شد.»

این پیام مدت کوتاهی پس از انتشار حذف شد و این خبرگزاری اعلام کرد این پیام نادرست بوده و از طرف نفوذگرانی که کنترل حساب کاربری را در دست داشتند منتشر شده است.

بی‌بی‌سی اعلام کرد در حال حاضر نمی‌داند چه کسانی پشت این حملات هستند و گفت: «ما در حال پیگیری ماجرا هستیم و گام‌هایی را طی می‌کنیم تا مطمئن شویم چنین اتفاقاتی دیگر رخ نخواهد داد.»

گروه نفوذ OurMine کنترل حساب مورد نفوذ قرار گرفته را در دست گرفتند و توییتی را از آن منتشر کردند که این نقض را افشاء کرد. در پیام گروه OurMine آمده است: «ما فعالیت‌های غیرعادی را در این حساب کاربری شناسایی کردیم. این حساب توسط یک نفر مورد نفوذ قرار گرفته بود و ما سعی کردیم این اشکال را برطرف کنیم.» گروه OurMine با فاصله‌ی کوتاهی از انتشار پیام زنده بودن ترامپ، توییت خود را ارسال کرد.

براساس گزارش بی‌بی‌سی که پس از این نفوذ با گروه OurMine تماس گرفت، این گروه نفوذ آمریکایی مسئول نفوذ به حساب توییتر بی‌بی‌سی و انتشار خبر کشته شدن دونالد ترامپ نبوده است.

گروه نفوذ OurMine گفت: «ما در مرحله‌ی اول به حساب بی‌بی‌سی نفوذ نکردیم. ما بعد از مشاهده‌ی فعالیت‌های مشکوک در این حساب، دوباره به آن نفوذ کردیم تا مطمئن شویم که نفوذ رخ داده یا خیر. ولی متأسفانه این حساب مورد نفوذ قرار گرفته بود. ما فقط توییتی در این حساب ارسال کردیم و اطلاع دادیم که این حساب مورد نفوذ قرار گرفته است. ما هیچ‌گاه به هیچ حسابی بدون دلیل نفوذ نمی‌کنیم. ما یک گروه نفوذ امنیتی هستیم.»

گروه OurMine در گذشته توانسته بود به چند حساب کاربری سطح بالا در توییتر نفوذ کند. از جمله‌ی این حساب‌های توییتر، می‌توان نت‌فلیکس، Marvel و سایر شرکت‌ها را نام برد. هرچند، این گروه نفوذ هیچ‌گاه سعی نکرده اخبار نادرست یا بدافزار را از طریق این نفوذها توزیع کند و بیشتر نشان دادن ضعف امنیتی در حساب‌های قربانی مدنظر این گروه بوده است.

تاکنون هیچ گروه یا فردی مسئولیت این نفوذ را برعهده نگرفته است و بی‌بی‌سی نیز اعلام کرده در حال حاضر کنترل حساب کاربری را بدست آورده است. تمامی توییت‌های ارسالی از طرف نفوذگران حذف شده و این شرکت بدنبال راهی برای کشف چگونگی وقوع حمله است.

امنیت‌سایبری

ناتو: نفوذگران سایبری هر ماه ۵۰۰ بار به اتحادیه حمله می‌کنند

سخنگوی ارتش اتحادیه‌ی ناتو اعلام کرد ناتو به هدفی برای تمام نفوذگران در سراسر دنیا تبدیل شده است و به‌طور میانگین هر ماه 500 حمله‌ی سایبری علیه این اتحادیه انجام می‌شود. این حملات در سال گذشته نسبت به سال 2015 افزایش 60 درصدی داشته است.

برای شناسایی مهاجمان بررسی‌های زیادی صورت گرفته است ولی در بسیاری از موارد، کشف اینکه حمله توسط چه کسانی انجام شده، کار بسیار دشواری است. سخنگوی این اتحادیه گفت: «دولت‌های خارجی، مهاجمان سایبری و تروریست‌ها می‌توانند منشأ این حملات باشند با این حال انتساب حملات کار سختی است. البته بسیاری از کشورها دارای منابع بزرگی در حوزه‌ی سایبری هستند و مسئولیت بسیاری از حملات علیه ناتو برعهده‌ی چنین کشورهایی است.»

ناتو اواسط سال 2016 تصمیم گرفت حملات سایبری را نیز مانند حملات مسلحانه‌ی معمولی قلمداد کند و به نفوذگران خارجی هشدار داد در صورت حمله به دولت‌های عضو اتحادیه، طبق ماده‌ی 5 با آن‌ها برخورد خواهد شد.

در اغلب موارد این‌گونه تصور می‌شود که دولت روسیه پشت بسیاری از نفوذهای سایبری است. همان‌طور که در انتخابات ریاست جمهوری آمریکا نیز گفته می‌شود کرملین با کمک شهروندان خود در آمریکا، در روند انتخابات دخالت کرده و نفوذهای متعددی را علیه حزب دموکرات انجام داده است.

همزمان دولت‌های اروپایی نیز در خصوص حملات سایبری روسیه و نفوذ به رایانه‌های این کشورها هشدار دادند. کشورهای اروپایی ادعا می‌کنند دولت روسیه سعی دارد با نفوذهای سایبری در روند انتخابات کشورهای دیگر اختلال ایجاد کند.

در طرف دیگر، دولت روسیه تمامی این ادعاها و اتهامات را رد کرده و اعلام کرد دولت روسیه خود هدف حملات سایبری دولت‌های خارجی قرار گرفته است. دولت روسیه در دی ماه اعلام کرد شواهدی پیدا کرده که سرویس‌های اطلاعاتی از کشورهای خارجی تلاش می‌کنند مؤسسات مالی و بانک‌های روسیه را از کار بیندازند.

امنیت‌سایبری

نفوذ به حساب توییتر نیویورک تایمز و خبر جعلی حمله‌ی موشکی روسیه به آمریکا

نیوریورک تایمز در حال بررسی نفوذ به حساب توییتر خودش است که توسط OurMine انجام شده و در روز یکشنبه خبرهایی جعلی را منتشر کرده است.

حساب @nytvideo حساب ویدئویی توییتر متعلق به روزنامه‌ی آمریکایی نیویورک تایمز است که بیش از 250 هزار دنبال‌کننده دارد. دیروز ساعت 9:40 در این حساب یک خبر جعلی درباره‌ی حمله‌ی موشکی روسیه علیه آمریکا منتشر شد. این خبر در مورد حمله‌ی موشکی باعنوان بیانیه‌ای از طرف ولادیمیر پوتین منتشر شده بود. این خبرهای جعلی به سرعت حذف شد در حالی‌که در توییت‌های دیگری به دخالت گروه OurMine در انتشار خبرهای جعلی اشاره شده بود. این گروه نفوذ که در دی ماه نیز به حساب توییتر نت‌فلیکس حمله کرده بود، در تلاش است با این کار به شناساندن وب‌گاه و سرویس‌های نفوذ خود بپردازد و در حال حاضر با نفوذهای خود به حساب‌های سطح بالای توییتر شناخته می‌شود.

در فهرست قربانیان این گروه که به حساب‌های توییتر آن‌ها نفوذ شده می‌توان مدیرعامل فیس‌بوک، مارک زوکربرگ، مدیرعامل فعلی و سابق توییتر و مدیرعامل گوگل را مشاهده کرد. در پیامی که توسط OurMine ارسال شده بود، تأیید شد که این گروه مسئول نفوذ به حساب موسیقی سونی در توییتر بوده و خبرهای جعلی در خصوص مرگ بریتنی اسپیرز منتشر کرده است.

امنیت‌سایبری

دادستان منتخب ترامپ: باید در رمزنگاری‌ها دربِ پشتی داشته باشیم

جف سشنز، دادستان کلِ منتخب ترامپ، معتقد است استفاده از رمزنگاری‌های قوی بسیار عالی است ولی باید مقامات راهی برای شکستن آن داشته باشند.

باتوجه به اهمیت رمزنگاری، سشنز معتقد است نهادهای امنیتی و بررسی‌کننده‌ی جرائم باید راهی برای دور زدن این حفاظت‌ها داشته باشند. به‌نظر می‌رسد دیدگاه‌های سشنز با دیدگاه رئیس جمهور فعلی آمریکا، دونالد ترامپ هماهنگ است.

در بحثی که بین اپل و FBI در باز کردن قفل آیفون تیرانداز در حادثه‌ی سان‌برنادیو پیش آمد، ترامپ معتقد بود اپل باید با نهادهای اطلاعاتی همکاری می‌کرد و در غیر این‌صورت تحریم می‌شد. ترامپ می‌گوید: «آن‌ها فکر می‌کنند کی هستند؟ هیچ‌کس. ما باید در چنین مواردی بتوانیم تلفن همراه را باز کنیم.»

تمامی دیدگاه‌های ترامپ در خصوص رمزنگاری، امنیت برخط و هرچیز مرتبط با رایانه به‌روز نبوده و نشان می‌دهد او هیچ درکی از این مباحث ندارد. این موضوع را می‌توان از حساب توییتر او فهمید. دیدگاه‌های سشنز نیز بازتابی از دیدگاه‌های ترامپ است هرچند او به‌طور صریح در این‌باره اظهارنظر نکرده است.

از سشنز سوال شد که آیا استفاده از رمزنگاری قوی را برای حفاظت از آمریکا در برابر حملات سایبری مفید می‌داند و او در پاسخ گفت: «رمزنگاری موضوعی مهم و ارزشمند است. همچنین ضروری است که نهادهای امنیتی و بررسی‌کننده‌ی جرائم قادر باشند در صورت لزوم و برای پیشبرد امنیت ملی و تحقیقات جنایی آن را رمزگشایی کنند.»

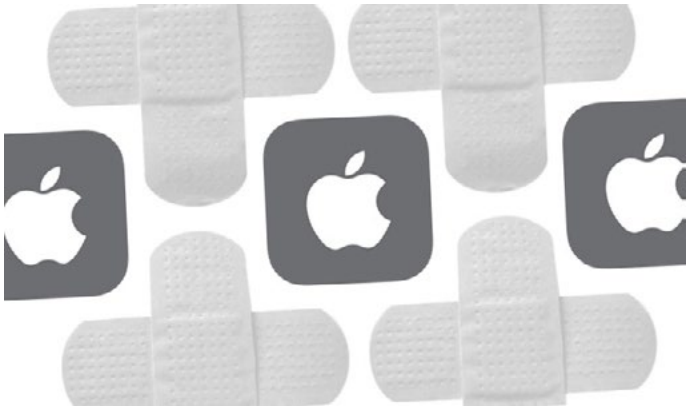
بنابراین تنها راهی که به ذهن همگان برای دور زدن رمزنگاری می‌رسد، استفاده از دربِ پشتی در ویژگی‌های امنیتی است و این خواست نهادهای اطلاعاتی نیز هست. با قدرت گرفتن افرادی همچون سشنز نمی‌توان گفت که در آینده چه اتفاقی خواهد افتاد. قوانین تضعیف امنیت سایبری بدون شک مخالفت‌هایی بدنبال خواهد داشت.

فصل چهارم

اخبار فنی

اخبار فنی

شرکت اپل آسیب‌پذیری‌های حیاتی را در هسته‌ی سامانه عامل‌ها وصله می‌کند



شرکت اپل دیروز نسخه‌ی جدید iOS و macOS Sierra منتشر کرد و در آن تعدادی آسیب‌پذیری هم‌پوشان را در این سامانه عامل‌های تلفن همراه و رومیزی برطرف کرده بود.

این به‌روزرسانی بخشی از به‌روزرسانی امنیتی بزرگ‌تر است که سافاری، iCloud در ویندوز و watchOS را نیز شامل می‌شود.

مهم‌ترین و جدی‌ترین آسیب‌پذیری‌ها دو آسیب‌پذیری در هسته با شناسه‌های CVE-2017-2370 و CVE-2017-2360 است. این آسیب‌پذیری‌ها به یک برنامه‌ی مخرب، اجازه‌ی اجرای کد در بالاترین سطح از امتیازات هسته را می‌دهد. این دو آسیب‌پذیری سرریز بافر و استفاده پس از آزادسازی توسط محققان امنیتی گوگل گزارش شده و در iOS نسخه‌ی 10.2.1 و در macOS Sierra نسخه‌ی 10.12.3 وصله شده است.

یک آسیب‌پذیری حیاتی سریز بافر در libarchive با شناسه‌ی CVE-2016-8687 در iOS و macOS Sierra نیز وصله شده است. اپل گفت: «از بسته خارج کردن یک آرشیو جعلی و مخرب، ممکن است به اجرای کد دلخواه منجر شود.»

اپل همچنین 11 آسیب‌پذیری را در پیاده‌سازی iOS مربوط به WebKit وصله کرده است که شش مورد از این آسیب‌پذیری‌ها می‌تواند منجر به اجرای کد دلخواه شود. 3 مورد دیگر از آسیب‌پذیری‌ها نیز با محتوای وب جعلی قابل بهره‌برداری بوده و برای خارج کردن اطلاعات از سامانه‌ی قربانی مورد استفاده قرار می‌گیرد.

بسیاری از آسیب‌پذیری‌های Webkit در مرورگر وب سافاری در نسخه‌ی 10.0.3 نیز وصله شده است. در به‌روزرسانی‌ها و وصله‌های iOS، اپل یک آسیب‌پذیری در ویژگیِ باز کردن قفل خودکار را وصله کرده است. مهاجمان با بهره‌برداری از این آسیب‌پذیری می‌توانند ساعت اپل را بر روی مچ دست کاربر در حالتی که خاموش است، باز کنند.

همچنین یک آسیب‌پذیری دیگر وصله شده که می‌تواند باعث درهم شکستن برنامه‌ی مخاطبان شود. یک آسیب‌پذیری دیگر نیز در وای‌فای برطرف شده که با بهره‌برداری از آن، حتی زمانی‌که دستگاه کاربر خاموش است، تصویری از صفحه‌ی خانگی او نمایش داده می‌شود.

در به‌روزرسانی macOS Sierra چند آسیب‌پذیری اجرای کد در مؤلفه‌های دیگر وصله شده است. این مؤلفه‌ها عبارتند از پیاده‌سازی بلوتوث، راه‌اندازهای گرافیکی و ویرایشگر متن Vim. در به‌روزرسانی سافاری نیز یک آسیب‌پذیری در نوار آدرس با شناسه‌ی CVE-2017-2359 وصله شده است. این آسیب‌پذیری زمانی‌که کاربر از یک وب‌گاه مخرب بازدید کند و مهاجم نیز آدرس URL را جعل کرده باشد قابل بهره‌برداری است.

tvOS نیز به نسخه‌ی 10.1.1 به‌روزرسانی شده و همان

آسیب‌پذیری‌های هسته و webkit در این سامانه عامل تلویزیون اپل نیز وصله شده است. watchOS به نسخه‌ی 3.1.3 به‌روزرسانی شده که در آن 33 آسیب‌پذیری که شامل 17 آسیب‌پذیری اجرای کد بوده، برطرف شده است. برنامه‌ی iCloud برای ویندوز نیز به نسخه‌ی 6.1.1 برای ویندوزهای 7 و بالاتر به‌روزرسانی شده است. همچنین 4 آسیب‌پذیری Webkit در سایر محصولات این سامانه عامل برطرف شده که منجر به اجرای کد دلخواه می‌شد.

اخبار فنی

آسیب‌پذیری که اپل را مجبور کرد ویژگی جدید خود را در فروشگاه اپل حذف کند

اخیراً شرکت اپل ویژگی را در دستگاه‌های آیفون و آی‌پد ارائه کرد که بقدری دارای اشکال بود که این شرکت راهی بجز حذف کردن کامل این ویژگی پیدا نکرد.

در آبان ماه، شرکت اپل ویژگی به اسم «اعلان» را در فروشگاه برنامه‌های کاربردی خود ارائه کرد. کاربران با فعال کردن این ویژگی که دکمه‌ی نارنجی روشنی داشت، می‌توانستند از طریق رایانامه‌ی iCloud اگر برنامه یا بازی جدیدی در فروشگاه در دسترس قرار می‌گرفت، از آن مطلع شوند.

محققان امنیتی چندین آسیب‌پذیری در ویژگی اعلان iTunes و رایانامه‌های iCloud کشف کردند که به مهاجمان اجازه می‌دهند از طریق بدافزار، کاربران دیگر اپل را نیز آلوده کنند.

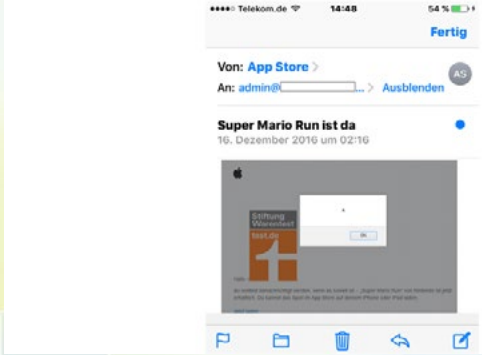
محققان امنیتی در مشاوره‌نامه‌ی خود نوشتند: «بهره‌برداری موفقیت‌آمیز این آسیب‌پذیری‌ها می‌تواند منجر به سرقت نشست، حملات پایدار فیشینگ، حملات پایدار هدایت به سمت منابع دیگر و دستکاری ماژول‌ها در سرویس‌های مختلف شود.»

این حمله چگونه کار می‌کند؟

وقتی شما بر روی گزینه‌ی اعلان برای برنامه‌ای که هنوز منتشر نشده کلیک می‌کنید، این تابع به‌طور خودکار اطلاعاتی از قبیل نام دستگاه شما و شناسه‌ی رایانامه‌ی iCloud را بازیابی می‌کند تا زمانی که برنامه‌ی جدیدی ارائه شد، به شما خبر دهد.

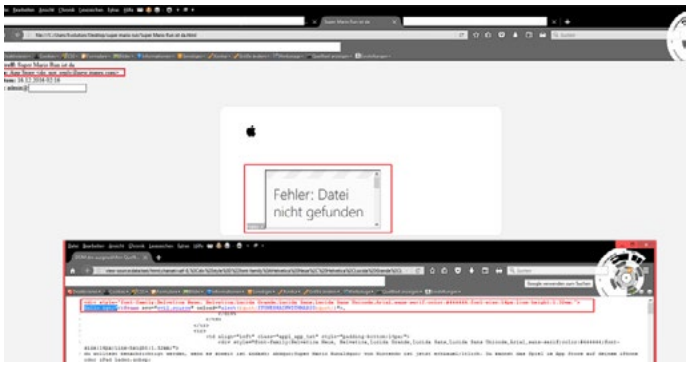
با این حال بازیابی نام دستگاه در برابر اشکالات اعتبارسنجی ورودی بسیار آسیب‌پذیر است و به یک نفوذگر اجازه می‌دهد یک بار داده‌ی مخرب جاوا اسکریپت را در این فیلد تزریق کند که این کد می‌تواند پس از بهره‌برداری از آسیب‌پذیری، بر روی دستگاه قربانی اجرا شود.

علاوه بر این، یک نفوذگر راه دور می‌تواند شناسه‌ی رایانامه‌ی iCloud قربانی را با آدرس رایانامه‌ی اصلی خود تنظیم کند در حالی‌که به هیچ تأییدی از سمت قربانی نیاز نیست. اینجاست که اشکال دوم رخ می‌دهد.



بنابراین زمانی‌که یک برنامه‌ی منتشرنشده در دسترس قرار می‌گیرد، اپل رایانامه‌ای به آدرس قربانی ارسال خواهد کرد ولی نفوذگر آدرس رایانامه‌ی قربانی را با رایانامه‌ی اصلی خود تنظیم کرده است. بنابراین قربانی رایانامه‌ای

از طرف اپل دریافت خواهد کرد که توسط نفوذگر در بخش نام دستگاه آن بار داده‌ی مخرب درج شده است. در تصویر زیر اجرای بار داده‌ی مخرب را در سمت قربانی مشاهده می‌کنید و اینجا اشکال سوم مشاهده می‌شود. در اشکال سوم کارخواه رایانامه‌ی اپل در بررسی محتوای رایانامه‌ی ارسال‌شده به سمت کاربران با شکست مواجه شده است.



محققان امنیتی گفتند: «بهره‌برداری از آسیب‌پذیری‌های اعتبارسنجی ورودی و کدگذاری رایانامه، به حساب کاربری اپل با امتیازات سطح پایین نیاز دارد و مقدار تعامل با کاربر نیز کم یا متوسط است.»

این محقق امنیتی عنوان کرد اولین بار در مهر ماه که شرکت اپل این ویژگی را رونمایی کرد، کد بهره‌برداری را آماده کرده بود. تقریباً در 25 آذر زمانی که بازی سوپر ماریو در فروشگاه اپل منتشر شد، او مطمئن شد که بهره‌برداری او به درستی کار می‌کند. گزارش‌ها حاکی از آن است که اپل از این اشکالات مطلع شده و در حال برطرف کردن آن‌ها است.

اخبار فنی

حمله به پایگاه داده‌ها همچنان ادامه دارد: هدوپ و CouchDB اهداف بعدی مهاجمان

برنامه‌های هدوپ و CouchDB به آخرین اهداف مهاجمان سایبری برای سرقت و حذف داده‌ها تبدیل شده‌اند. هفته‌ی گذشته محققان امنیتی اعلام کردند نزدیک به 28 هزار پایگاه داده‌ی MongoDB و موتور جستجوی Elasticsearch مورد نفوذ قرار گرفته است. این پایگاه داده‌ها منابعی محافظت‌نشده و متن‌باز بودند. روز جمعه، محقق امنیتی با نام ویکتور گورز اعلام کرد 126 مورد نصب هدوپ و 452 مورد CouchDB مورد نفوذ قرار گرفتند. همچون حملات قبلی، مهاجمان برای نفوذ به نصب های هدوپ و CouchDB از گواهی‌نامه‌های پیش‌فرض یا بسیار ساده استفاده کرده‌اند.

گروهی از محققان امنیتی که این حملات را بررسی می‌کردند، گفتند: «علت اصلی حمله مشابه نمونه‌ی MongoDB است. پیکربندی‌های پیش‌فرض به مهاجمان بدون احراز هویت، اجازه‌ی دسترسی می‌دهد. به عبارت دیگر یک مهاجم با مهارت‌های پایه‌ای می‌تواند شروع به حذف پرونده‌ها کند.»

برخلاف حملات به MongoDB که مهاجمان پس از حذف پرونده ها، برای بازگرداندن پرونده‌های رونویسی‌شده از قربانیان باج درخواست می‌کردند، در نمونه‌ی هدوپ تمامی داده‌ها حذف می‌شوند. یک یادداشت نیز در پوشه‌ای برای کاربر گذاشته شده است.

ولی در مورد CouchDB حمله مشابه حملات MongoDB و Elasticsearch است و مهاجم برای برگرداندن داده‌ها از قربانیان باج درخواست می‌کند درحالی‌که پرونده‌ها حذف شده‌اند و با پرداخت باج پرونده‌ها برگردانده نخواهد شد.یک محقق امنیتی دیگر عنوان کرد هدوپ دارای ویژگی‌های امنیتی و حفاظت از داده‌ی بسیاری است. بر روی این بستر می‌توان تمامی داده‌های موجود را رمزنگاری کرد. می‌توان سامانه‌ی مدیریت کلید را از سامانه‌ی اصلی جدا کرد. همچنین قابلیت‌های ویژه‌ی احراز هویت و کنترل دسترسی در آن وجود دارد. بنابراین، سامانه‌های هدوپ که مورد نفوذ قرار گرفته‌اند از این قابلیت‌های امنیتی بهره‌ای نبرده‌اند.

گورز اعلام کرد ردیابی این حملات را از روز سه‌شنبه با اولین حمله بر روی هدوپ و CouchDB آغاز کرده است. پویش‌های Shodan نشان می‌دهد 5160 نمونه هدوپ و 4530 نمونه CouchDB محافظت‌نشده و باز وجود دارد. گورز گفت به نظر می‌رسد بسیاری از حملات علیه هدوپ دستی انجام می‌شود. با این حال حملات علیه CouchDB مشابه حملات MongoDB و Elasticsearch به‌طور خودکار صورت می‌گیرد.

این محقق اعلام کرد نفوذگری با نام Kraken0 حمله به CouchDB را به یک کیت باج‌افزاری اضافه کرده و در وب تاریک به فروش می‌رساند. حذف پایگاه داده‌های عظیم مشکلی بسیار بزرگ محسوب می‌شود چرا که نفوذگران به راحتی و با استفاده از گواهی‌نامه‌های پیش‌فرض می‌توانند این حملات را انجام دهند.

اخبار فنی

در افزونه‌ی مخفی شرکت ادوبی، آسیب‌پذیری XSS کشف شد

محققان پروژه‌ی Zero گوگل کشف کردند افزونه‌ی گوگل کروم که ادوبی هفته‌ی قبل به‌طور مخفیانه در به‌روزرسانی امنیتی خود قرار داده بود، دارای آسیب‌پذیری XSS است. شرکت ادوبی پس از اطلاع از وجود این آسیب‌پذیری، بی‌سروصدا آن را وصله کرد.

در به‌روزرسانی امنیتی که شرکت ادوبی در 21 دی ماه برای محصولات آکروبات و ریدر منتشر کرد، 29 آسیب‌پذیری وصله شد. با این‌حال برخی از کاربران از این ماجرا گله می‌کردند که ادوبی یک افزونه‌ی گوگل کروم را در مرورگرهای آن‌ها نصب کرده است. این افزونه برای تبدیل صفحه‌ی وب به سند پی‌دی‌اف استفاده می‌شود. این افزونه که تنها بر روی سامانه‌های ویندوزی کار می‌کند از کاربر مجوزهایی را برای دسترسی به داده‌های وب‌گاه‌های بازدیدی، مدیریت بارگیری‌ها و ارتباط با برنامه‌های جانبی درخواست می‌کند. این افزونه همچنین داده‌هایی را از سامانه‌ی کاربران جمع‌آوری می‌کند و ادوبی ادعا کرده این جمع‌آوری داده شامل اطلاعات شخصی افراد نمی‌شود.

این افزونه نزدیک به 30 میلیون بار نصب شده است.

پس از بررسی‌ها مشخص شد که افزونه تحت تأثیر آسیب‌پذیری XSS قرار گرفته است و به اسناد جاوا اسکریپت با امتیازات سطح بالا، اجازه‌ی اجرا شدن را می‌دهد. کارشناسان امنیتی این آسیب‌پذیری را با درجه‌ی اهمیت جدی طبقه‌بندی کردند.

این آسیب‌پذیری در 23 دی ماه به شرکت ادوبی گزارش شده و پس از چند روز وصله شد. این اولین بار نیست که محققان امنیتی در افزونه‌های مرورگرها آسیب‌پذیری کشف می‌کنند. تقریباً یک سال قبل، کارشناسان نشان دادند یک افزونه که به‌طور خودکار توسط ضدبدافزار AVG نصب شده بود، تمامی اطلاعات تاریخچه‌ی مرورگر و اطلاعات شخصی کاربران را افشاء می‌کرد.

اخبارفنی

توقف اعتماد اوراکل به پرونده‌های JAR امضاءشده با MD5 از اردیبهشت ماه

اوراکل تصمیم گرفت به توسعه‌دهندگان جاوا فرصت بیشتری بدهد تا مطمئن شوند که پرونده‌های JAR آن‌ها با الگوریتم MD5 امضاء نشده است. محیط زمان اجرای جاوا (JRE) در اردیبهشت ماه به پشتیبانی از این پرونده‌های JAR خاتمه خواهد داد.

شرکت اوراکل در شهریور ماه اطلاعیه‌ای مبنی بر توقف پشتیبانی از پرونده‌های JAR که با الگوریتم MD5 امضاء شده‌اند خبر داد. نزدیک به یک دهه است که آسیب‌پذیری‌های تصادم در این الگوریتم‌ها کشف شده است. اوراکل در سال 2006 استفاده از الگوریتم MD5 برای پرونده‌های JAR به‌طور پیش‌فرض را متوقف کرد و اینک قصد دارد به‌کلی هیچ استفاده‌ای از این الگوریتم درهم‌سازی نداشته باشد.

با انتشار همزمان SE 8u131 به همراه به‌روزرسانی‌های امنیتی اوراکل در اردیبهشت ماه، با پرونده‌های JAR که با الگوریتم MD5 امضاء شده‌اند، همچون پرونده‌های امضاءنشده و غیرقابل اعتماد برخورد خواهد شد. اوراکل قصد داشت پشتیبانی از MD5 در پرونده‌های JAR را با آغاز سال 2017 متوقف کند ولی تعدادی از توسعه‌دهندگان جاوا از اوراکل درخواست کردند تا مهلت بیشتری به آن‌ها بدهد تا تغییرات لازم را اعمال کنند.

به توسعه‌دهندگان جاوا توصیه شده تا امضای پرونده‌های JAR را با الگوریتم MD5 مورد بررسی قرار دهند و این پرونده‌ها را با الگوریتم قوی‌تری مجدداً امضاء کنند و کلیدهای با طول بزرگ‌تر استفاده کنند. با استفاده از ابزار Zip و دستور زیر می‌توانید امضاهای MD5 موجود را حذف کنید:

```
zip -d test.jar 'META-INF/*.SF' 'META-INF/*.RSA' "META-INF/*.DSA
```

سایر تغییرات مبتنی بر رمزنگاری که توسط اوراکل در شهریور ماه برای JRE و JDK برنامه‌ریزی شده شامل غیرفعال کردن زنجیره‌ی گواهی‌نامه‌های SHA-1 است که در JDK به‌طور پیش‌فرض مورد استفاده قرار گرفته و همچنین افزایش حداقل طول کلید برای SSL و TLS به 1024 بیت است.

اوراکل در آخرین به‌روزرسانی وصله‌های امنیتی خود در سال 2017 تعداد 270 آسیب‌پذیری را وصله کرد که 158 مورد از این آسیب‌پذیری‌ها توسط مهاجمان بدون احراز هویت قابل بهره‌برداری است. تعداد زیادی از این آسیب‌پذیری‌ها در محصول E-Business Suite اوراکل وجود داشت که توجه محققان امنیتی زیادی را به خود جلب کرده بود.

اخبار فنی

ویجت نظردهی، بسیاری از وب‌گاه‌ها را در معرض خطر قرار داد

یک آسیب‌پذیری XSS ذخیره‌شده در یک ویجت محبوب نظردهی کشف شد که بسیاری از وب‌گاه‌ها را در معرض خطر قرار می‌داد. این آسیب‌پذیری به سرعت توسط توسعه‌دهندگان این محصول وصله شد.

ابراهیم مارزوک 14 ساله یک آسیب‌پذیری XSS ذخیره‌شده را در بخش نظردهی یک وب‌گاه اشتراک کد با نام PasteCoin کشف کرد. دوست ابراهیم که او نیز 14 سال سن دارد، بعداً کشف کرد که این آسیب‌پذیری فقط PasteCoin را تحت تأثیر قرار نداده و تمامی وب‌گاه‌هایی که از یک ویجت محبوب، برای افزودن جعبه‌ی نظردهی به وب‌گاه خود استفاده می‌کنند، در معرض خطر قرار دارند.

این جعبه‌ی نظردهی HTML به‌گونه‌ای طراحی شده تا برای جلوگیری از حملات XSS ورودی‌های کاربر را پالایش کند ولی بار داده‌ای که توسط این دو نوجوان مورد استفاده قرار گرفته، توانست پالاینده‌ی این ویجت را دور بزند:

<<//;(img src=x onerror=alert(1>><<”

این نوجوانان در پست وبلاگی توضیح دادند: «پالاینده‌ی تگ‌های باز و بسته را می‌توان با استفاده از دو تگِ علامت بزرگ‌تر (>) و کوچک‌تر (<) دور زد. علاوه بر این، پالاینده‌ای که ویژگی‌ها را بررسی می‌کند با استفاده از نقطه-ویرگول (؛) و دو علامت اسلش (//) در انتهای ویژگی‌ها می‌توان دور زد.»

این آسیب‌پذیری از طریق یک برنامه‌ی پاداش در ازای اشکال با نام Detectify که به تازگی راه‌اندازی شده است، به توسعه‌دهندگان ویجت جعبه‌ی نظردهی HTML گزارش شد. توسعه‌دهندگان نیز در عرض دو ساعت این اشکال را وصله کردند.

بررسی‌های این نوجوانان از طریق گوگل نشان داد که نزدیک به 2 میلیون وب‌گاه از این ویجت نظردهی استفاده می‌کنند. سکیوریتی‌ویک نیز چنین جستجویی را انجام داد و نتیجه‌ها حاکی از آن بود که نزدیک به 760 هزار وب‌گاه از جعبه‌ی نظردهی HTML استفاده می‌کنند و برخی از این وب‌گاه‌ها تکراری بودند. ولی بهرحال در نهایت می‌توان گفت که وب‌گاه‌های زیادی از این ویجت استفاده می‌کنند.

این اولین بار نیست که محققان امنیتی آسیب‌پذیری‌هایی را در ویجت‌های نظردهی وب‌گاه‌ها کشف می‌کنند. در سال 2013 دو محقق امنیتی، دو آسیب‌پذیری پایدار و انعکاسی XSS را در جعبه‌ی نظردهی HTML کشف کرده بودند.

فصل پنجم

اخبار تحـــلیلی

اخبار تحلیلی

برایان کربس، نویسنده‌ی واقعی بدافزار Mirai را کشف کرد

محقق امنیتی مشهور، برایان کربس جزئیات بررسی‌های خود در خصوص نویسنده‌ی بدافزار Mirai، آنا سنپایی را منتشر کرد. در ماه‌های گذشته بات Mirai توجه رسانه‌ها را به خود جلب کرده است. این بدافزار و بات‌نت برای تشدید حملات منع سرویس توزیع‌شده علیه ارائه‌دهنده‌ی سرویس DNS با نام Dyn مورد استفاده قرار گرفت و باعث قطعی اینترنت در بخش وسیعی گردید.

به دنبال این حمله بسیاری از سرویس‌های معروف اینترنت مانند توییتر، آمازون، نت‌فلیکس و غیره برای ساعاتی قابل دسترسی نبودند. این بات‌نت اینترنت اشیاء مدتی قبل نیز وب‌گاه محقق امنیتی، برایان کربس را هدف حمله‌ی منع سرویس توزیع‌شده قرار داده بود که موجب شد او بررسی‌هایی را برای شناسایی نویسنده‌ی این بدافزار ترتیب دهد.

یک نفوذگر در مهر ماه کد منبع این بدافزار را به‌طور عمومی منتشر کرد و برایان کربس تصمیم گرفت این کد را در انجمن معروف نفوذگران Hackforum مورد تحلیل و بررسی قرار دهد. یکی از کاربران انجمن Hackforum پیوندی مربوط به کد منبع بدافزار Mirai منتشر کرده بود.

کربس گزارش داد: «انتشار کد منبع بدافزار روز جمعه در انجمن Hackforum اطلاع داده شد. نام این بدافزار Mirai است و پیوسته در حال پویش دستگاه‌های آسیب‌پذیر اینترنت اشیاء است. این دستگاه‌ها معمولاً با گواهی‌نامه‌های پیش‌فرض کارخانه و یا با نام کاربری و گذرواژه های هاردکدشده محافظت می‌شوند.»

برایان کربس معتقد است هویت واقعی آنا سنپایی که پیوند مربوط به Mirai را منتشر کرده، کشف کرده است. کربس اعلام کرد نام واقعی او پاراس جی‌ها و صاحب یک شرکت امنیتی با نام ProTraf است. این شرکت در حوزه‌ی کاهش تهدیدات منع سرویس توزیع‌شده فعالیت می‌کند.

کربس در وب‌گاه خود می‌نویسد: «پس از ماه‌ها جمع‌آوری اطلاعات در خصوص نویسنده‌ی بدافزار Mirai من از عمار زوبری در مورد پاراس جی‌ها اطلاعاتی بدست آوردم. زوبری گفت جی‌ها قبول کرده که مسئول بات‌نت Mirai و حمله‌ی منع سرویس توزیع‌شده‌ی علیه دانشگاه راتگرز بوده است. زوبری می‌گوید وقتی در دانشگاه راتگرز در سال 2015 جی‌ها را ملاقات کرده، جی‌ها در مورد راه‌اندازی چند حمله‌ی منع سرویس توزیع‌شده به او فخرفروشی کرده است. زوبری دلیل انجام این حملات توسط جی‌ها را نمی‌داند ولی فکر می‌کند او می‌خواسته آزمایش کند با انجام این حملات تا کجا می‌تواند پیش برود.»

به گزارش کربس، فردی با نام مستعار آنا سنپایی از نام مستعار Ogmemes123123 و آدرس رایانامه‌ی

ogmemes123123@gmail.com نیز استفاده کرده است. کربس می‌گوید این نویسنده از نام مستعار OG_Richard_Stallman نیز استفاده کرده که به بنیان‌گذار برنامه‌های متن‌باز اشاره مستقیم دارد. آدرس رایانامه‌ی ذکرشده برای ایجاد حساب‌های کاربری در فیس‌بوک با نام‌های مستعار مورد استفاده قرار گرفته است.

حساب کاربری مربوط به OG_Richard_Stallman نشان می‌دهد که این فرد از سال 2015 تحصیل در رشته‌ی مهندسی کامپیوتر را در دانشگاه راتگرز آغاز کرده است. این همان دانشگاهی است که پاراس جی‌ها در آن تحصیل می‌کند. سامانه‌های دانشگاه راتگرز از سال 2015 مورد حملات منع سرویس توزیع‌شده قرار می‌گرفت و این مهاجم به مسئولین دانشگاه پیشنهاد داده بود تا یک محصول و راه‌حل برای کاهش تهدیدات منع سرویس توزیع‌شده خریداری کنند.

کربس همچین اشاره کرد مهارت‌هایی که جی‌ها در صفحه‌ی لینکدین خود ثبت کرده همان مهارت‌هایی است که در انجمن HackForums برای آنا سنپایی ثبت شده است. تحلیل‌های دقیق و جامع کربس در خصوص این نفوذگر را در وب‌گاه او می‌توانید مطالعه کنید.

اخبار تحلیلی

بازگشت باتنت Necurs و توزیع باج‌افزار و تروجان بانکی

گروه امنیت سیسکو اعلام کرد متوجه ترافیکی از باتنت خفته‌ی Necurs شده است. این محققان در خصوص احتمال پیدایش پویش‌های باج‌افزاری جدید توسط این باتنت هشدار دادند.

در پستی که سیسکو منتشر کرده می‌خوانیم: «تحقیقات گروه تالوس نشان می‌دهد فعالیت هرزنامه‌های Locky مجدداً افزایش یافته است ولی به شدتی که قبلاً داشت نرسیده است. سرانجام چند روز پیش ما شاهد پویش‌های هرزنامه‌ای بودیم که باج‌افزار Locky را توزیع می‌کردند. تفاوت فاحش در این هرزنامه‌ها مربوط به مقدار و حجم توزیع باج‌افزار است. ما به‌طور معمول صدها و هزاران هرزنامه را شاهد هستیم.»

در زمان نگارش این خبر، محققان امنیتی تنها هزار نمونه از پیام‌های هرزنامه‌ای باتنت Necurs را پیدا کرده‌اند اما شرایط ممکن است خطرناک‌تر از وضعیت فعلی بشود. باتنت Necurs یک از بزرگ‌ترین معماری‌های تهدید در دنیاست که برای توزیع تروجان بانکی Dridex و باج‌افزار Locky مورد استفاده قرار می‌گرفت و از تاریخ 12 خرداد ماه سال جاری ناپدید شده بود.

در مهر ماه سال 94، تعدادی از آژانس‌های اطلاعاتی و مراجع قانونی با کمک هم باتنت Necurs را تخریب کردند ولی این باتنت دوباره به صحنه‌ی تهدیدات سایبری بازگشت و با قدرت هرچه تمام به توزیع باج‌افزار Locky پرداخت. در حال حاضر نیز باتنت Necurs توسط مهاجمان سایبری برای توزیع باج‌افزار Locky استفاده می‌شود و در هفته‌ی گذشته تعداد حملات سایبری افزایش چشمگیری داشته است.محققان سیسکو گفتند: «تا اوایل دی ماه، ما شاهد هیچ فعالیتی از باج‌افزار Locky نبودیم ولی در چند روز گذشته پویش‌های هرزنامه‌ای را مشاهده کرده‌ایم که به توزیع این باج‌افزار می‌پردازند. تنها تفاوتی که وجود دارد در تعداد هرزنامه‌های ارسالی است. قبلاً می‌دیدیم برای توزیع باج‌افزار صدها و هزاران هرزنامه ارسال می‌شد ولی در حال حاضر کمتر از هزار هرزنامه برای توزیع باج‌افزار Locky مشاهده شده است. با این کاهش در تعداد هرزنامه‌ها، شاید در آینده شاهد تغییرات دیگری در این پویش‌ها باشیم.»

محققان سیسکو در بررسی‌های اخیر خود دو پویش را مشاهده کرده‌اند که تا حدودی با پویش‌های قبلی تفاوت دارند. در یکی از این پویش‌ها یک پرونده‌ی zip که در هرزنامه موجود است، یک نصب‌کننده‌ی بدافزار را بر روی رایانه‌ی قربانی قرار می‌دهد. وقتی پرونده‌ی zip باز شود، یک پرونده‌ی JSE این قابلیت را دارد که باج‌فزار Locky و تروجان Kovter را بر روی سامانه‌ی قربانی بارگیری و نصب کند.

در پویش دوم بجای استفاده از پرونده‌ی zip از یک پرونده‌ی RAR استفاده می‌شود. اگر قربانی پرونده‌های موجود در آن را استخراج کند با یک پرونده‌ی جاوا اسکریپت به نام doc_details.js مواجه خواهد شد.

اخبار تحلیلی

انتشار کد منبع یک بدافزار بانکی اندروید

محققان امنیتی هشدار دادند که کد منبع یک بدافزار بانکی اندروید به‌طور برخط منتشر شده است. به همراه این کد منبع، اطلاعاتی در خصوص استفاده از آن نیز قرار دارد. به عبارت دیگر این احتمال وجود دارد که در چند روز آینده شاهد افزایش حملات بدافزارها بر روی دستگاه‌های اندرویدی باشیم.

شرکت امنیتی Dr.Web اعلام کرد بدافزاری را شناسایی کرده که کد منبع آن نیز منتشر شده است. این بدافزار به‌طور مستقیم به برنامه‌های قانونی اندورید در فروشگاه‌های ثالث تزریق شده و در حال توزیع است.

این بدافزار با نام Android.BankBot.149.origin تلاش می‌کند بر روی رایانه‌های آلوده امتیازات مدیریتی را بدست آورد. وقتی بدافزار به امتیازات کامل دست یافت، از روی صفحه‌ی خانگی، آیکون برنامه‌ی کاربردی را حذف می‌کند و تلاش دارد کاربر را فریب دهد که این برنامه به‌کلی حذف شده است.

از سوی دیگر، این بدافزار در پس‌زمینه فعال باقی می‌ماند و به یک کارگزار دستور و کنترل متصل شده و برای دریافت دستورات منتظر می‌ماند. این بدافزار می‌تواند وظایف مختلفی از جمله ارسال و دریافت پیامک، سرقت اطلاعات مخاطبان، ردیابی دستگاه، برقراری تماس تلفنی، نمایش دیالوگ‌های فیشینگ و سرقت اطلاعات حساس مانند اطلاعات کارت‌های بانکی را انجام دهد.

این شرکت امنیتی توضیح داد: «مانند سایر بدافزارهای بانکی اندروید، بدافزار Android.BankBot.149.origin با ردیابی فعالیت برنامه‌های پرداخت برخط و برنامه‌های بانکی، اطلاعات گواهی‌نامه‌های کاربران را به سرقت می‌برد. در بررسی نمونه‌ای از این بدافزار مشخص شد که تعداد زیادی از برنامه‌های بانکی را کنترل می‌کند. زمانی‌که بدافزار استفاده از برنامه‌های بانکی را شناسایی کرد، یک فرم فیشینگ را نمایش داده و اطلاعات کارت بانکی و گذرواژه‌های قربانی را دریافت کرده و در قسمت بالای برنامه‌ی مورد نظر نمایش می‌دهد.»

وقتی یکی از برنامه‌های معروف مانند فیس‌بوک، اینستاگرام، واتس‌اپ، یوتیوب و حتی گوگل‌پلی راه‌اندازی شد، بدافزار دیالوگ فیشینگ شبیه به دیالوگ خرید از گوگل‌پلی را نمایش می‌دهد و اطلاعات کارت‌های بانکی را از کاربر درخواست می‌کند.

علاوه بر این، بدافزار می‌تواند پیام‌های متنی را ردیابی کرده و آن‌ها را برای مهاجم ارسال کند. در ادامه نیز این پیام‌ها از روی تلفن همراه حذف خواهد شد. این عملیات در مورد اطلاعات بانکی می‌تواند بسیار خطرناک محسوب شود. این شرکت امنیتی هشدار داد این تنها یک نمونه از بدافزار مبتنی بر این کد منبعِ منتشرشده است و کاربران باید در بارگیری برنامه‌های اندروید از فروشگاه‌های ثالث بسیار مراقب باشند.

Expert Bulletin News

Information Communication Technology

2th year 2016 | Weekly bulletin

اخبار فناوری اطلاعات و ارتباطات

هفته نامه | شماره نود و هفتم | سال دوم | ۴۵ صفحه

خبرنامه هفتگی کارشناسی

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج