سراج

۱۱ دی ۱۳۹۵

شماره ۹۳

خبرنامه کارشناسی

اخبار فناوری اطلاعات و ارتباطات

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج

هفته نامه | شماره نود و سه | سال دوم | ۶۰ صفحه

Expert Bulletin News

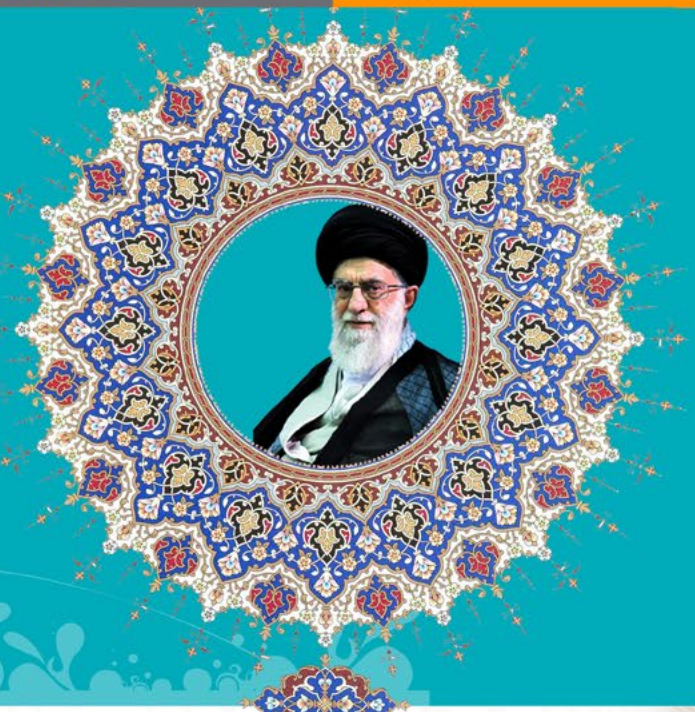
Information Communication Technology

2th year 2016 | Weekly bulletin

در این شماره می‌خوانید:

بسم الله الرحمن الرحیم

آگاهی و بصیرت



در جنگ روانی و آن چه که امروز به آن جنگ نرم گفته می شود در دنیا، دشمن به سراغ سنگرهای معنوی می آید که آنها را منهدم کند؛ به سراغ ایمان ها، معرفت ها، عزم ها، پایه ها و ارکان اساسی یک نظام و یک کشور [می آید].

مقام معظم رهبری (مد ظله العالی)

فهرست مطالب

فصل اول: اخبار عمومی

فصل دوم: مدیریت امنیت

فصل سوم: سیاست سایبری

فصل چهارم: اخبار فنی

فهرست مطالب

فصل پنجم: اخبار تحلیلی

فصل اول

اخبار عمومی

اخبار عمومی

نفوذگران در روز کریسمس به ایکس‌باکس و پلی‌استیشن حمله خواهند کرد

برای علاقه‌مندان به بازی‌های رایانه‌ای خبر بدی داریم! دوباره کریسمس در راه است و در بین کادوهای دریافتی پلی استیشن و ایکس‌باکس‌های جدید را خواهیم دید. ولی باز هم امکان دارد مثل هرسال نتوانید به کنسول برخط بازی متصل شوید.

در تعطیلات کریسمس سال 2014 نفوذگران گروه جوجه مارمولک، شبکه ی بازی پلی‌استیشن و ایکس‌باکس را هدف حمله‌ی منع سرویس توزیع‌شده قرار دادند و این بازی برای علاقه‌مندان از حالت برخط خارج گردید.

این بار نیز یک گروه نفوذ جدید که چند روز پیش سرویس تامبلر را هدف قرار داده بود و 2 ساعت باعث قطعی این وب‌گاه شد، علاقه‌مندان به بازی‌های رایانه‌ای را تهدید کرده که حمله‌ی منع سرویس توزیع‌شده در مقیاس بالا را علیه شبکه‌ی پلی‌استیشن و ایکس‌باکس انجام خواهد داد.

این گروه نفوذ با نام استار پاترول، ویدئویی در یوتیوب منتشر و اعلام کردند در روز کریسمس در حملات هماهنگ، شبکه‌ی پلی‌استیشن سونی و ایکس‌باکس مایکروسافت را هدف منع سرویس توزیع‌شده قرار خواهند داد.

روز چهارشنبه گروه نفوذ استار پاترول وب‌گاه تامبلر را از حالت برخط خارج کرد و عنوان شد که در پس این حمله هدف خاصی دنبال نمی‌شد و صرفاً بخاطر تفریح و سرگرمی این وب‌گاه را هدف حمله‌ی منع سرویس توزیع‌شده قرار دادند.

تاکنون هیچ یک از شرکت‌های سونی و مایکروسافت به این تهدید پاسخی نداده است. با این حال، هر دوی این شرکت‌ها قبلاً وعده داده بودند که حفاظت از سامانه‌های خود را افزایش و بهبود خواهند داد ولی قطعی و اختلال کوتاه‌مدت در هر کریسمس اتفاق می‌افتد.

با آگاهی از قابلیت‌های نفوذگران در راه‌اندازی حملات منع سرویس توزیع‌شده که گاهاً به 1 ترابیت بر ثانیه نیز می‌رسد، هر دو شرکت باید آماده باشند تا حمله‌ی گسترده و عظیمی را بر روی کارگزارهای خود تجربه کنند.

پاییز بود که حمله‌ی منع سرویس توزیع‌شده علیه ارائه‌دهنده‌ی سرویس DNS با نام Dyn بخش زیادی از اینترنت را قطع و ده‌ها وب‌گاه را از حالت برخط خارج کرد. حمله‌ی منع سرویس توزیع‌شده که توسط بات‌نتی با 100 هزار بات از دستگاه‌های اینترنت اشیاء انجام می‌شود، این توانایی را دارد که اینترنت میلیون‌ها کاربر را قطع کند.

اینک باید صبر کنیم و ببینیم علاقه‌مندان به بازی‌های رایانه‌ای در تعطیلات کریسمس می‌توانند از آن لذت ببرند یا خیر!

اخبار عمومی

توسعه‌ی سامانه عامل CyanogenMod متوقف می‌شود

سامانه عامل Cyanogen که یک ROM اندرویدی ویژه و محبوب است، اعلام کرد با شروع سال جدید سرویس خود را متوقف می‌کند. این سامانه عامل با هدف اجرای نسخه‌ی بهبودیافته‌ای از سامانه عامل اندروید گوگل راه‌اندازی شده بود اما بخاطر برخی مسائل فنی و حقوقی، این شرکت تصمیم گرفت سرویس خود را متوقف کند.

سامانه عامل CyanogenMod یک سامانه‌ی تجاری نیست و ویژگی‌هایی را پیاده‌سازی کرده که بر روی ثابت‌افزارهای رسمی موجود در تلفن‌های همراه قابل دسترسی نیست. این سامانه عامل توسط گروهی از توسعه‌دهندگان به رهبری استیو کوندیک که یکی از بنیان‌گذاران Cyanogen است، مدیریت می‌شود.

در بیانیه‌ی رسمی این سامانه عامل که بر روی وب‌گاه این شرکت منتشر شده، آمده است: «به عنوان بخشی از تداوم پروژه، تمامی بخش‌های این پروژه و پشتیبانی‌های آن تا تاریخ 31 دسامبر سال جاری متوقف خواهد شد. پروژه‌ی متن‌باز و تمامی کدهای آن برای کسانی که بخواهند CyanogenMod را به‌طور شخصی بسازند، در دسترس خواهد بود.» اطلاعیه‌ی متوقف شدن این پروژه به‌طور رسمی در پستی کوتاه بر روی وب‌گاه این شرکت اعلام شد.

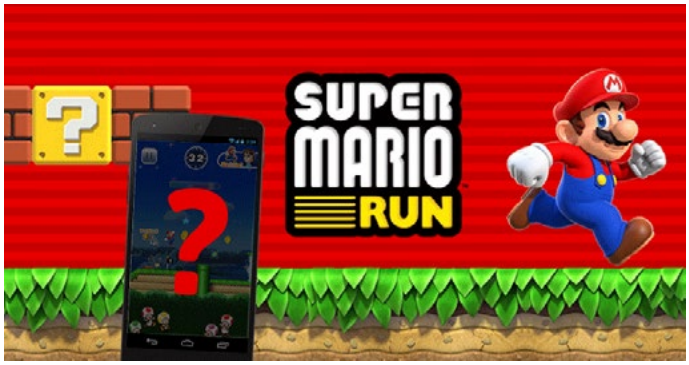
از این پس برای سامانه عامل Cyanogen به‌روزرسانی امنیتی منتشر نخواهد شد و کاربرانی که از نسخه‌ی تلفن همراه این سامانه عامل استفاده می‌کردند، باید به نسخه‌ی متن‌باز آن سوئیچ کنند.

انجمن CyanogenMod در تلاش است مشتقاتی از کد منبع CyanogenMod را تولید کرده و وصله‌هایی را برای آن ارائه دهد. جامعه‌ی اندروید معتقد است نسخه‌ی جدید سامانه عامل با نام LineageOS می‌تواند به سامانه عامل قبلی جانی دوباره ببخشد ولی این طرح هنوز در مراحل ابتدایی قرار دارد. به گفته‌ی گروه توسعه‌دهنده‌ی CyanogenMod، سامانه عامل جدید Lineage چیزی بیش از یک نام تجاری جدید است.

اگر شما نیز علاقه‌مند هستید می‌توانید در وب‌گاه این پروژه نگاهی به LineageOS بیندازید. توزیع‌های این سامانه عامل نیز بر روی مخازن گیت‌هاب قابل دسترسی است.

اخبار عمومی

نسخه‌ی اندرویدی بازی «سوپر ماریو» یک بدافزار است



پس از موفقیت بازی Pokémon Go اینک زمان محبوبیت بازی «سوپر ماریو» فرا رسیده است. این بازی از محبوبیت زیادی بین علاقه‌مندان برخوردار شده و تأثیرات عظیم اجتماعی را بدنبال داشته است. این بازی در هفته‌های گذشته طوفانی به پا کرده چرا که نسخه‌ی iOS آن هفته‌ی قبل منتشر شده است.

شاید باور نکنید ولی این بازی در 4 روز ابتدایی انتشار خود، 40 میلیون بار در کل دنیا بارگیری شده است. ولی اگر بازی سوپر ماریو را برای دستگاه اندروی خود بارگیری کردید، بسیار مراقب باشید! این برنامه قطعاً یک بدافزار است.

از آنجایی که در حال حاضر این بازی فقط برای نسخه‌ی iOS منتشر شده و نسخه‌ی اندرویدی آن بر روی فروشگاه گوگل پلی وجود ندارد، بسیاری از کاربران اندرویدی ناامید شده‌اند. در نتیجه بسیاری از علاقه‌مندان به بازی ماریو که دستگاه اندرویدی دارند، صبر نکرده و این بازی را از بازارهای دیگری بجز گوگل پلی بارگیری کرده‌اند.

اما کاربران باید توجه داشته باشند، برنامه‌هایی که تحت عنوان بازی سوپر ماریو در فروشگاه‌های شخص ثالث توزیع شده، فقط مانند یک برنامه‌ی قانونی بنظر می‌رسد ولی در واقع بر روی دستگاه قربانی به یک بدافزار تبدیل خواهد شد.

برای بارگیری این برنامه لازم است تا کاربر تنظیمات امنیتی دستگاه خود را تغییر دهد و اجازه دهد این برنامه از فروشگاه‌های غیرقابل اعتماد بارگیری و نصب شود.

برخی از این برنامه‌های آلوده می‌توانند کنترل کامل دستگاه قربانی را در دست گیرند چرا که در ابتدای امر امتیازات بالایی برای خواندن، ویرایش و ارسال و دریافت پیام، ضبط ویدئو و گرفتن عکس و ردیابی مکان کاربر از طریق GPS دریافت می‌کنند.

یکی از این برنامه‌ها با نام «سوپر ماریو» آیکن‌های اضافی را ایجاد می‌کند، پاپ‌آپ و تبلیغاتی را نمایش می‌دهد، برنامه‌های مخرب دیگری را بر روی دستگاه قربانی نصب می‌کند و بدون هیچ‌گونه تعاملی با کاربر عملیات سرزده‌ای را انجام می‌دهد. به گزارش ترندمیکرو امسال نزدیک به 90 هزار نمونه برنامه‌ی «سوپر ماریو» مخرب شناسایی شده است.

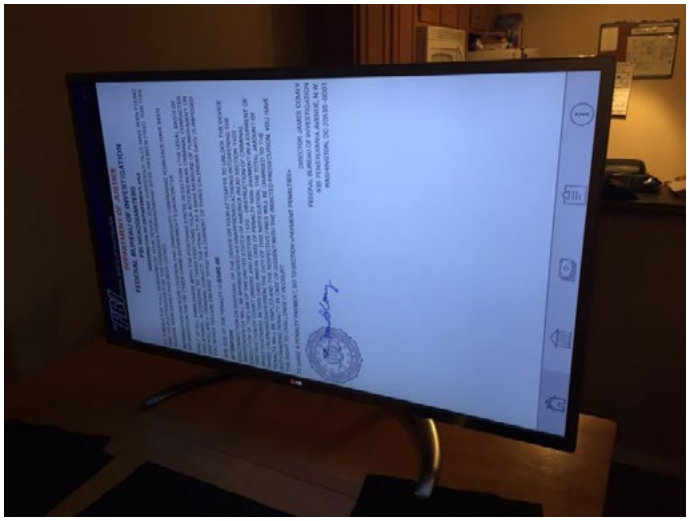
محققان ترندمیکرو می‌گویند کاربران با کلیک بر روی این آیکون‌ها و تبلیغات به وب‌گاه‌های مخرب و مستهجن هدایت می‌شوند و در حالت کلی هدف این آیکون‌ها و تبلیغات نصب برنامه‌های مخرب بر روی دستگاه قربانی است.

یک برنامه‌ی دیگر با عنوان «سوپرماریو» توسط ترندمیکرو کشف شده که در ابتدا از کاربر می‌خواهد برنامه‌ای با نام 9Apps را نصب کند. این برنامه در ادامه مجوزهای بیشتری از جمله ضبط صدا، خواندن و ویرایش تقویم و حتی دسترسی کامل به کارت SD را درخواست می‌کند.

بجـای بارگیـری و نصـب بـازی سـوپر ماریـو از فروشـگاه‌های شـخص ثالـث، کاربـران اندرویـد بایـد منتظـر بماننـد تا نسـخه‌ی اندرویـدی ایـن برنامـه بـر روی گـوگل پلـی منتـشر شـود. بارگیـری برنامـه تنهـا بـه نصـب بدافـزار بـر روی رایانـه‌ی شـما ختـم نمی‌شـود و ایـن شروع تهدیـدات و خطرهـای مختلـف اسـت. پـس لازم اسـت از بخـش تنظیـمات دسـتگاه خـود بـه بخـش امنیـت رفتـه و مطمـئن شـوید کـه گزینـه‌ی «منابـع ناشـناس» غیرفعـال اسـت.

اخبار عمومی

آلودگی تلویزیون‌های هوشمند گوگل به بدافزار



به احتمال زیاد شما تلویزیون‌های هوشمند گوگل را به یاد نمی‌آورید که یک شکست بزرگ برای این شرکت محسوب می‌شود. با این حال هستند کسانی که دستگاه‌هایی را خریداری کرده‌اند که بر روی آن تلویزیون گوگل اجرا می‌شود.

تعداد تلویزیون‌هایی که از تلویزیون هوشمند گوگل بهره می‌برند، امروزه بسیار کاهش یافته است ولی در همین تعطیلات کریسمس حداقل یک تلویزیون دیده شده که به‌طور غیرمنتظره‌ای با صفحه‌ی سیاه مواجه شده است. یکی از صاحبان تلویزیون‌های LG که از تلویزیون هوشمند گوگل بهره می‌برد، در توییتر نشان داد که تلویزیون خانه‌ی آن‌ها هنگام نصب یک برنامه‌ی نمایش فیلم، آلوده به بدافزار شده است. باتوجه به عکس و پستی که او منتشر کرده به نظر می‌رسد که این بدافزار یک باج‌افزار باشد که در ازای بازیابی دستگاه از قربانی باج درخواست می‌کند.

از آنجایی که این باج‌افزار لزوماً برای تلویزیون‌های هوشمند توسعه داده نشده و بر روی دستگاه‌های اندرویدی مانند تبلت و تلفن‌های همراه هوشمند نیز وجود دارد، به نظر می‌رسد که این تلویزیون به‌طور کامل از کار افتاده است و راه‌حلی برای بازیابی آن وجود ندارد. باتوجه به ورودی‌های محدود بر روی تلویزیون، بوت مجدد دستگاه نیز نمی‌تواند کاری انجام دهد و دوباره پیام باج‌خواهی نمایش داده خواهد شد.

در این شرایط تنها چیزی که می‌تواند کمک کند، فلش کردن ثابت‌افزار تلویزیون است که با استفاده از تصویر ثابت‌افزار که توسط LG ارائه می‌شود، قابل انجام است. به‌طور عجیبی شاهد این هستیم که شرکت LG بدون دریافت پولِ سرویس، نمی‌خواهد به صاحب تلویزیون کمک کند تا از شرّ باج‌افزار خلاص شود. مالک تلویزیون در توییتی گفت می‌تواند با این حق سرویس یک تلویزیون جدید بخرد.

این بحث‌ها به این معنی نیست که تمامی تلویزیون‌های هوشمند و به‌ویژه آن‌هایی که از اندروید بهره می‌برند، بد هستند چرا که چنین اتفاقاتی در حالت عادی خیلی کم پیش می‌آید. اگر مالکان تلویزیون‌های هوشمند برنامه‌ها را از فروشگاه‌های غیرقابل اعتماد بارگیری و نصب نکنند این اتفاق به هیچ عنوان رخ نمی‌دهد.

در این مورد واقعاً ضروری است که LG وارد عمل شده و به این کاربر کمک کند. باتوجه به این موضوع که دستگاه او بسیار قدیمی بوده و مدت زیادی است که تولید نمی‌شود و هزینه‌ی سرویس آن شاید بیشتر از قیمت یک تلویزیون جدید باشد.

اخبار عمومی

نفوذ هوشمندانه به فیس‌بوک: می‌توانید آدرس رایانامه‌ی هر کاربری را مشاهده کنید

با وجود برنامه‌ی پاداش در ازای اشکال فیس‌بوک، امسال کریسمس برای تامی دیُس، محقق امنیتی زودتر فرار سیده است. او با کشف یک آسیب‌پذیری در فیس‌بوک توانست 5 هزار دلار جایزه بگیرد. این آسیب‌پذیری به او اجازه می‌داد آدرس رایانامه‌های خصوصی هریک از کاربران فیس‌بوک را مشاهده کند.

دیُس گفت: «این نفوذ به من اجازه می‌تواند تا تمامی آدرس‌های رایانامه‌ی کاربران فیس‌بوک را بدست آورم. مهم نیست که رایانامه‌های شما چقدر خصوصی باشند. من می‌توانم به تمامی آن‌ها دست یابم.»

دیُس در روز جشن شکرگزاری گفت که یک آسیب‌پذیری را در فیس‌بوک کشف کرده و آن را در قالب برنامه‌ی پاداش در ازای اشکال به این شرکت گزارش داده است. با گذشت چند هفته و بررسی‌های انجام شده توسط فیس‌بوک و توضیح روند بهره‌برداری، فیس‌بوک اعلام کرده بود که 5 هزار دلار به این محقق جایزه خواهد داد. روز سه‌شنبه فیس‌بوک به وعده‌ی خود عمل کرد.

این آسیب‌پذیری مربوط به گروه‌های فیس‌بوک است که کاربران می‌توانند ایجاد کنند. این ویژگی به کاربران اجازه می‌دهد بر روی بستر شبکه‌های اجتماعی، گروه خویشاوندی ایجاد کنند. دیُس کشف کرد که به عنوان ادمین یک گروه فیس‌بوک می‌تواند هر کاربر فیس‌بوک را به گروه دعوت کرده و به او نقش ادمین را بدهد و این کاربر بتواند عملیاتی مانند ویرایش پست و عضوگیری را انجام دهد.

این دعوت‌ها توسط سامانه‌ی فیس‌بوک مدیریت شده و به صندوق ورودی پیام های گیرنده‌ی دعوت‌نامه ارسال می‌شود و این حساب‌ها با آدرس‌های رایانامه‌ی کاربران در ارتباط است. در بسیاری از موارد کاربران ترجیح می‌دهند آدرس رایانامه‌شان خصوصی باقی بماند. دیُس کشف کرد برخلاف تمام تنظیمات حریم خصوصی که کاربران فیس‌بوک انجام می‌دهند، او می‌تواند به آدرس‌های رایانامه‌ی کاربران دست یابد. حال اینکه این کاربران جزو دوستان او باشند یا نباشند.

دیُس کاربرانی را با نقش ادمین به گروه دعوت کرده بود و زمانی‌که می‌خواست دعوت‌نامه‌های در حالت انتظار را لغو کند، اشکال کوچکی را کشف کرد. او گفت: «در حالی‌که فیس‌بوک منتظر تأیید این دعوت باقی می‌ماند، کاربر به صفحه‌ی نقش‌ها هدایت می‌شود و می‌تواند این درخواست را لغو کند.»

او در ادامه به صفحه‌ی اعطای نقش در برنامه‌ی تلفن همراه فیس‌بوک مراجعه کرد و دید هنگامی‌که می‌خواهد دعوت به گروه کاربران را لغو کند، آدرس رایانامه‌ی کاربران برای او نمایش داده می‌شود.

دیُس گفت: «من متوجه شدم وقتی می‌خواهم دعوت کاربری به گروه به عنوان ادمین را لغو کنم، به صفحه‌ای هدایت می‌شود که در آن آدرس URL رایانامه‌ی کاربر قابل

مشاهده است. اینک شما می‌تواند از این آدرس URL که درخواست تأیید است، مستقیماً آدرس رایانامه را که به شکل متن ساده است، بردارید.»

او در یک پست وبلاگی دستاوردهای کشف خود را توضیح داد و عنوان کرد که این آسیب‌پذیری می‌تواند تأثیرات متنوعی داشته باشد. او گفت: «به دست آوردن آدرس رایانامه‌ی کاربران در تضاد با سیاست‌های حریم خصوصی فیس‌بوک است و این آدرس‌های رایانامه می‌تواند در حملات مخرب و فیشینگ مورد سوءاستفاده قرار بگیرد.»

فیس‌بوک این نفوذ را تأیید کرد و گفت که تاکنون مدرکی مبنی بر بهره‌برداری از این آسیب‌پذیری را مشاهده نکرده است. فیس‌بوک اعلام کرد برای جلوگیری از بهره‌برداری، وصله‌ای برای این آسیب‌پذیری پیاده‌سازی شده است.

دیُس که یک توسعه‌دهنده‌ی نرم‌افزار در ویرجینیا است گفت که تاکنون این بیشترین جایزه‌ای بوده که در یک برنامه‌ی پاداش در ازای اشکال دریافت کرده است. او گفت که در بسیاری از برنامه‌های پاداش در ازای اشکال شرکت کرده است از جمله برنامه‌های یاهو و نفوذ به پنتاگون.

فیس‌بوک در مهرماه گزارش داد که در طول 5 سال که برنامه‌ی پاداش در ازای اشکال را راه‌اندازی کرده، نزدیک به 5 میلیون دلار را به 900 محقق امنیتی به عنوان جایزه پرداخت کرده است. این شرکت اعلام کرد تنها در نیم‌سال اول سال 2016 مبلغ 611741 دلار به 149 محقق جایزه داده است.

فیس‌بوک جزو وب‌گاه‌هایی است که به دنبال شرکت موزیلا و گوگل در مرداد ماه سال 90 برنامه‌ی پاداش در ازای اشکال را راه‌اندازی کرد. بهمن ماه سال قبل بود که فیس‌بوک اعلام کرد بخاطر کشف یک آسیب‌پذیری در API اینستاگرام توسط یک پسربچه‌ی 10 ساله، 10 هزار دلار به او پاداش داده است. فیس‌بوک در سال 2012 اینستاگرام را به قیمت 1 میلیارد خرید. در فروردین ماه نیز فیس‌بوک به آناند پراکاش مبلغ 15 هزار دلار پاداش داد. او توانسته بود با استفاده از یک حمله‌ی جستجوی فراگیر گذرواژه‌ی 1.1 میلیارد کاربر فیس‌بوک را حدس زده و به حساب‌های کاربری دست یابد.

اخبار عمومی

موج جدیدی از هرزنامه‌های تگرگی، صندوق ورودی کاربران را فراگرفته است

ارسال‌کنندگان هرزنامه به تازگی به یک روش قدیمی با نام «تگرگ» برای دور زدن پالایش‌های ضدبدافزاری و ضدهرزنامه‌ای روی آورده‌اند. محققان امنیتی می‌گویند این روش اولین بار در سال 2008 مورد بررسی قرار گرفت. این شیوه بهبود داده شده و دوباره مورد استفاده قرار می‌گیرد. در حال حاضر این روش برای ارسال تروجان بانکی Dridex و باج‌افزار Locky مورد استفاده قرار می‌گیرد.

یکی از محققان امنیتی سیسکو تالوس اعلام کرد که استفاده از روش‌های هرزنامه‌ی تگرگی در سال 2016 مجدداً رایج شده است. این پویش در طول زمان بهبود داده شده و تلاش دارد سازمان‌های تجاری و سامانه‌ها را با تهدیدات جدیدی همچون آلوده کردن رایانامه‌ها، سرقت هویت و بارگیری بدافزارها هدف قرار دهد.

روش تگرگی شاخه‌ای از یک روش قدیمی برای ارسال هرزنامه است که «کفش اسکی» نام داشت. با استفاده از این روش حملات عظیم هرزنامه‌ای برای بازه‌های زمانی طولانی مدت و بر روی هزاران آدرس IP انجام می‌شد. به گفته‌ی محققان امنیتی سیسکو تالوس، در روش تگرگی، از چندین آدرس IP برای ارسال هرزنامه استفاده می‌شود اما برخلاف روش «کفش اسکی» در پویش تگرگی تعداد بسیار زیادی از هرزنامه‌ها در بازه‌های زمانی کوتاه ارسال می‌شود.

محققان امنیتی معتقدند حملات هرزنامه‌ی تگرگی زمانی پایان می‌یابد که راه‌کارهای ضدهرزنامه‌ی سنتی بتوانند به سرعت به روزرسانی شوند. تعداد درخواست‌های DNS در حملات «کفش اسکی» معمولاً 35 درخواست در هر ساعت بود. در پویش تگرگی، تعداد درخواست‌ها در ابتدای امر صفر است و به‌طور ناگهانی به 75 هزار درخواست در ساعت می‌رسد و مجدداً صفر می‌شود.

محقق امنیتی سیسکو می‌گوید: «واقعاً دشوار است بفهمیم چرا ارسال‌کنندگان هرزنامه از پویش‌های تگرگ تکامل‌یافته بیشتر استفاده می‌کنند. دلیل این موضوع این می‌تواند باشد که سامانه‌های ضدهرزنامه به نقطه‌ای از پیشرفت رسیده‌اند که مهاجمان نمی‌توانند این روش‌ها را دور بزنند. در نتیجه مهاجمان تصمیم گرفته‌اند با روش تگرگی به‌طور افراطی هزرنامه ارسال کنند.»

محققان حدس می‌زنند پویش تگرگ تکامل یافته است و در حال حاضر از طیف وسیع‌تری از آدرس‌های IP واقع در آمریکا، آلمان، هلند، بریتانیا و روسیه حمله انجام می‌دهد. خطرناک‌ترین بخش در پویش تگرگ، بار داده‌ی هرزنامه‌ها است. بات‌نت هرزنامه‌ی Necurs از پویش تگرگ برای ارسال تروجان بانکی Dridex و باج‌افزار Locky استفاده می‌کند. محققان اعلام کردند در برخی از روزها، تقریباً دو سوم از هرزنامه‌های روزانه متعلق به پویش تگرگ از بات‌نت Necurs بوده است.

در یک نمونه از رایانامه‌های فیشینگ ارسال شده، ادعا

شده که این رایانامه از طرف کاخ انگلستان ارسال شده است. از این طریق مهاجمان تلاش دارند قربانی را متقاعد کنند تا برنامه‌ی مخرب ورد با نام Complaint.doc را باز کند. این سند دارای ماکروهای مخرب است که اگر فعال شود باعث اجرا شدن Dyre و تروجان بانکی TrickBot خواهد شد.

فصل دوم

مدیریت امنیت

مدیریت امنیت

نفوذ به وب‌گاه روزنامه‌ی هنگ‌کنگ

نفوذگـری بـا شناسـه‌ی @Cryptolulz666 و همـکارش @EvoIsGod بـه وب‌گاه روزنامـه‌ی انگلیسـی هنگ‌کنـگ بـا نـام «هنگ‌کنـگ اسـتاندارد» نفـوذ کردنـد.

ایـن نفوذگـران بـه پایـگاه داده‌ی وب‌گاه دسـت یافتنـد و برخـی از داده‌هـای آن را بـر روی Pastebin بارگـذاری کردنـد. ایـن نفوذگـران عنـوان کردنـد کـه از یـک آسـیب‌پذیری تزریـق SQL بـر روی سـامانه‌ی مدیریـت وب‌گاه بهره‌بـرداری کردنـد. ایـن نفوذگـران تنهـا بخـش کوچکـی از اطلاعـات پایـگاه داده مربـوط بـه 12 هـزار کاربـر را منتـشر کردنـد. نفوذگـران در Pastebin عنـوان کردنـد کـه بـه دلایـل قانونـی تنهـا بخـش کوچکـی از پایـگاه داده را منتـشر کرده‌انـد و پایـگاه داده حـاوی اطلاعـات 12 هـزار نفـر اسـت. نفوذگـران داده‌هـای جدول‌هـای مشـتریان و کارمنـدان را افشـاء کرده‌انـد.

بـه گفتـه‌ی نفوذگـران بسـیاری از اطلاعـات ایـن پایـگاه داده محرمانـه اسـت و بخاطـر حفـظ حریـم خصوصـی کاربـران، نبایـد افشـاء شـود. هـدف ایـن نفوذگـران بـالا بـردن آگاهـی در خصـوص امنیـت در فضـای مجـازی اسـت.

ایـن نفوذگـران اعضـای سـابق گـروه نفـوذ «ارتـش قدرتمنـد یونـان» هسـتند کـه تعـدادی از وب‌گاه‌هـای دولتـی از جملـه سـفارت‌خانه‌ی روسـیه در ارمنسـتان را هـدف قـرار دادنـد. ایـن نفوذگـران همچنیـن حمـلات منـع سرویـس توزیع‌شـده را علیـه وب‌گاه دولـت ایتالیـا و وب‌گاه مبـارزه بـا مـواد مخـدر روسـیه انجـام داده‌انـد.

مدیریت امنیت

انجمن برنامه‌ی سلامت واشنگتن مورد نفوذ قرار گرفت

انجمن برنامه‌ی سلامت واشنگتن (CHPW) تأیید کرد که در تاریخ 17 آبان ماه تحت تأثیر یک نقض داده قرار گرفته و اطلاعات شخصی اعضای آن افشاء شده است.

این سازمان در مصاحبه‌ای به مطبوعات گفت به محض اطلاع از این نقض داده، دسترسی به کارگزارها را غیرفعال کرده و در حال حاضر با همکاری FBI بدنبال مسئولان این نفوذ است.

سازمان CHPW تأیید کرد اطلاعات افشاءشده حاوی نام، آدرس، تاریخ تولد، شماره‌ی امنیت اجتماعی و اطلاعات شناسایی مربوط به اعضای انجمن بوده است. هرچند در اطلاعات افشاءشده نشانی از داده‌های کارت‌های اعتباری و بانکی وجود ندارد.

در تاریخ 11 آذر این سازمان رایانامه‌هایی را به کاربران ارسال کرد تا آن‌ها را از این نقض داده مطلع سازد و همچنین به‌طور رایگان 12 ماه سرویس نظارت و شناسایی و گواهی‌نامه ارائه خواهد داد تا مطمئن شود هیچ یک از کاربران در معرض خطر قرار نگرفته‌اند.

در حال حاضر گروه نفوذ و مسبب این نقض داده شناسایی نشده و هیچ گروهی نیز مسئولیت آن را برعهده نگرفته است ولی مقامات این سازمان می‌گویند بررسی‌ها ادامه دارد و به محض شناسایی نفوذگران، نتایج را منتشر خواهند کرد.

در این بین، کاربرانی که تحت تأثیر قرار گرفته‌اند می‌توانند با شماره تلفن‌های اعلام شده و یا با نمایندگی‌های CHPW در ارتباط بوده و راهنمایی‌های لازم برای به حداقل رساندن خطرات را دریافت کنند.

در تاریخ 4 دی، خبرها حاکی از آن بود که CHPW دلیل این حادثه را پیدا کرده است. یک نفر در تماسی ناشناس عنوان کرده که یک آسیب‌پذیری در سامانه‌ی متعلق به شرکت NTT Data وجود دارد. این شرکت به سایر سازمان‌ها سرویس پشتیبانی فنی ارائه می‌دهد.

جاستین شافر می‌گوید او فردی است که این آسیب‌پذیری را کشف کرده و به CHPW گزارش داده است. او همچنین اشاره کرد که نفوذی رخ نداده و یک FTP به‌طور عمومی در معرض دید همگان قرار گرفته است.

مدیریت امنیت

شرکت Gogo برنامه‌ی پاداش در ازای اشکال برگزار می‌کند

شرکت Gogo که ارائه‌دهنده‌ی اینترنت در طول سفرهای هوایی است، اعلام کرد می‌خواهد برنامه‌ی پاداش در ازای اشکال برگزار کند. این برنامه وب‌گاه‌های اصلی این شرکت را پوشش خواهد داد.

این شرکت از محققان امنیتی دعوت کرد آسیب‌پذیری‌های موجود بر روی وب‌گاه‌های این شرکت به آدرس‌های gogoair.com و gogoinflight.com و دیگر زیردامنه‌ها را کشف کنند. وب‌گاه Gogoair.com وب‌گاهی است که کاربران بر روی آن حساب کاربری ایجاد می‌کنند و اطلاعات مربوط به هزینه‌ها را مشاهده می‌کنند. زیردامنه‌ی buy.gogoair.com فرآیندهای کارت پرداخت را مدیریت می‌کند و بیشترین تمرکز برنامه‌ی پاداش در ازای اشکال بر روی این زیردامنه است.

آدرس Gogoinflight.com وب‌گاهی است که کاربران در طول پرواز به آن دسترسی دارند. این وب‌گاه مانند یک دروازه‌ی اینترنت عمل می‌کند و مسئول ارائه‌ی محتوای ویدئویی در خطوط هوایی است. نفوذگران در طول سفرهای پروازی باید Gogoinflight.com را بر روی هواپیماهایی که از محصولات Gogo استفاده می‌کنند، مورد آزمایش قرار دهند.

شرکت Gogo در صفحه‌ی اشکالات خود می‌گوید: «بدلیل اینکه ما دنبال سناریوی‌های موجود در دنیای واقعی هستیم، اعتبار خیلی بالایی به محققان پرداخت نخواهد شد. تمامی محققان باید یک حساب کاربری رایگان ایجاد کرده و بخش‌های مشخص‌شده از وب‌گاه را مورد بررسی قرار دهند. هیچ کارت اعتباری یا داده‌ی آزمایشی وجود ندارد و تمامی آزمون‌ها بر روی وب‌گاه واقعی انجام می‌شود.»

این شرکت تصمیم دارد به هر محقق که آسیب‌پذیری بر روی وب‌گاه‌ها کشف می‌کند، مبلغی بین 100 تا 1500 دلار جایزه پرداخت کند. محققان اجازه ندارند جزئیات هیچ یک از آسیب‌پذیری‌ها را افشاء کنند.

محصولات شرکت Gogo بدنبال ضعف‌هایی که در سامانه‌ی وای‌فای هواپیماها وجود داشته، چندین بار مورد بررسی قرار گرفته است. سال گذشته، یکی از محققان امنیتی گوگل کشف کرد که سرویس‌های Gogo از گواهی‌نامه‌های جعلی گوگل استفاده می‌کند. این شرکت به‌طور آشکار با نهادهای قانونی همکاری می‌کند تا به عنوان نماد حفاظت از امنیت ملی و امنیت سرویس‌ها شناخته شود.

سامانه‌های خطوط هوایی، جزو صنایع قدیمی و سنتی هستند که نیاز است انجمن‌های مختلف با همکاری یکدیگر آسیب‌پذیری‌های موجود بر روی این سامانه‌ها را کشف کنند. سامانه‌های هواپیمایی پاناسونیک و ایالات جزو اولین‌ها بودند که چنین برنامه‌ای را راه‌اندازی کردند. در حالی که تحقیقات امنیتی نشان می‌دهد که

کارشناسان در حین طراحی سامانه‌های هوایی خیلی هم از امنیت غافل نبوده‌اند ولی با این حال ضروری است که متخصصان طراحی سامانه‌های هواپیمایی، همواره امنیت را در اولویت قرار دهند تا در آینده نفوذ وحشتناک و فجیعی رخ ندهد.

مدیریت امنیت

درخواست کمک پلیس از آمازون برای پیگیری یک پرونده‌ی قتل

پلیس آرکانزاس از آمازون درخواست کمک کرده تا داده‌های ثبت شده توسط دستگاه اکو را که متعلق به یک مظنون به قتل است، بدست آورد. این مسئله باعث بروز درگیری‌ها و بحث‌هایی در حوزه‌ی اینترنت اشیاء شده است.

دستگاه اکوی آمازون یک بلندگوی خانگی هوشمند است و قابلیت کنترل چندین دستگاه هوشمند خانگی که در در یک هاب ادغام شده‌اند را دارد. این دستگاه می‌تواند کارهایی از جمله پخش موسیقی، ایجاد لیست‌های کاری، تنظیم هشدار و ارائه‌ی اطلاعات بلادرنگ مانند اطلاعات ترافیکی و آب‌وهوایی را انجام دهد.

گزارش‌ها حاکی از آن است که مقامات بنتون ویل حکمی صادر کردند که در آن از آمازون درخواست شده اطلاعات و داده‌های ثبت شده بر روی دستگاه اکو متعلق به جیمز اندرو بیتس را در اختیار پلیس قرار دهد تا پلیس اطلاعاتی بیشتری برای پرونده‌ی قتل ویکتور کالینز داشته باشد.

دقیقاً مشابه اپل که از کمک به FBI در دور زدن قفل آیفون حادثه‌ی سان‌برنادیو سر باز زد، آمازون نیز از ارائه‌ی اطلاعات ثبت‌شده بر روی کارگزارهای اکو به پلیس خودداری کرد.

کالینز در 21 نوامبر سال قبل در حالی که از منزل دوست خود بیتس در بنتون ویل آرکانزاس دیدن می‌کرد به قتل رسیده است. فردای همان روز جسد کالینز در وان حمام منزل بیتس کشف شد و بیتس نیز به اتهام قتل دستگیر شده است. مقامات پلیس در تحقیقات خود از منزل بیتس، در کنار سایر تجهیزات متصل به اینترنت، یک دستگاه اکو آمازون متعلق به بیتس را نیز کشف کردند. دستگاه اکو پیش از ضبط صدا و ارسال آن به کارگزارهای آمازون در حالت بی‌کار باقی مانده و منتظر دریافت دستوراتی مانند «بیدار شو»، «الکسا» و «آمازون» باقی می‌ماند. با این حال با وجود ویژگی همیشه روشن بودن، این احتمال وجود دارد که دستگاه اکو به اشتباه دائماً فعال باشد و قطعه‌های صوتی را از کاربران در داخل منزل ضبط کرده باشد که افراد خودشان از آن بی‌خبر باشند.

برخی از این دستورات صوتی به‌طور محلی بر روی اکو ثبت نشده است ولی بر روی کارگزارهای خود آمازون وجود دارد. مقامات بر این باورند که احتمالاً در شب حادثه، دستگاه اکو صداهایی را ضبط و به سمت کارگزارهای آمازون ارسال کرده است. این اطلاعات ممکن است در روند بررسی پرونده به پلیس کمک کند.

با این حال آمازون ارائه‌ی هرگونه داده‌ای را که مقامات درخواست کرده‌اند، رد کرده است. در ادامه سخنگوی این شرکت گفت: «آمازون اطلاعات هیچ یک از مشتریان را بدون دریافت مجوزهای قانونی و الزام‌آور در اختیار هیچ نهادی قرار نخواهد داد.»

هرچند آمازون دوبار ارائه‌ی اطلاعات ثبت‌شده بر روی کارگزارهای آمازون را رد کرد ولی اطلاعات حساب و تاریخچه‌ی خرید بیتس را در اختیار مقامات قرار داد. پلیس گفت قادر است اطلاعات مورد نیاز را از دستگاه اکو استخراج کند ولی هنوز مطمئن نیست که آیا اطلاعات موجود در آن به روند بررسی پرونده کمک می‌کند یا خیر.

براساس گزارش دادگاه، کُنتور آب هوشمند خانه‌ی بیتس نشان می‌دهد همان شبی که جسد کالینز در وان حمام خانه‌ی او کشف شد، بین ساعت 1 تا 3 نیمه شب، بیش از 140 گالن آب مصرف شده است. دادستان ادعا می‌کند بیتس از این آب برای شستن شواهد پس از قتل کالینز استفاده کرده است.

در مورد بحثی که بین اپل و FBI پیش آمد، این شرکت مجبور می‌شد بر روی تلفن‌های همراه آیفون برای دور زدن سازوکارهای امنیتی یک دربِ پشتی قرار دهد. ولی این شرکت این دستور را اجرایی نکرد و در حال حاضر داده‌های رمزنگاری‌شده را بر روی کارگزارهای خود مدیریت می‌کند.

نکته‌ی خارج از بحثی که باید به کاربران یادآوری کرد این است که دستگاه‌های هوشمند و اینترنت اشیاء که در زندگی روزمره بسیار به شما کمک می‌کنند، ممکن است روزی علیه شما مورد استفاده قرار بگیرند. پرونده‌ی قتل کالینز اولین نمونه است که در آن دستگاه‌های هوشمند برای پیگیری پرونده مورد بررسی قرار می‌گیرند ولی مطمئناً در آینده بیشتر شاهد چنین اتفاقاتی خواهیم بود. خیلی جالب است که در آینده ببینیم شرکت‌های تولیدکننده دستگاه‌های هوشمند چگونه بین حریم خصوصی کاربران و کمک به نهادهای قانونی برای اجرای عدالت، تعادل برقرار می‌کنند.

مدیریت امنیت

نفوذگران OurMine حساب توییتر سونی را هدف قرار دادند

شرکت سونی آخرین هدف نفوذگران بوده است. حساب توییتر این شرکت روز دوشنبه مورد نفوذ قرار گرفت و توییتی جعلی مبنی بر مرگ بریتنی اسپیرز در آن منتشر شد. در پیامی که در حساب جهانی موسیقی سونی منتشر شد؛ آمده است: «بریتنی اسپیرز در یک تصادف کشته شد. ما جزئیات بیشتری از این حادثه را در ادامه به شما اطلاع خواهیم داد.»

چندی بعد حساب توییتر خواننده‌ی مشهور باب دیلن نیز مورد نفوذ قرار گرفت و توییتی با محتوای «در آرامش بخواب بریتنی اسپیرز» ارسال شد. به احتمال زیاد این نفوذ نیز کار همان گروه قبلی است.

در حال حاضر که این خبر را منتشر می‌کنیم هیچ‌یک از این توییت‌ها بر روی حساب‌های کاربری سونی و باب دیلن وجود ندارد. مدیران این حساب‌ها، کنترل را در دست گرفته و این توییت‌ها را حذف کرده‌اند. همچنین توییتی ارسال کرده و بقیه را از این نفوذ باخبر کرده‌اند. در پیام دیگر سونی می‌خوانیم: «ما دقایقی پیش شاهد بودیم که از آدرس IP دیگری به حساب توییتر ما وارد شدند و توییت‌هایی ارسال کردند. باید بگوییم که بریتنی اسپیرز زنده است.»

سخنگوی بریتنی اسپیرز توضیح داد که این خواننده زنده است و اخیراً نیز در توییتی عکس خود به همراه فرزندانش را منتشر کرده است. این سخنگو به CNN گفت: «در چند سال اخیر چندین مورد مشاهده شده که افراد ساده‌لوح چنین شایعه‌ای را منتشر کرده‌اند ولی از حساب جهانی موسیقی سونی این انتظار نمی‌رفت.»

سونی به این نفوذ اذعان کرده و از این خواننده و هوادارانش بخاطر توییت‌های جعلی عذرخواهی کرده است. در بیانیه‌ی سونی می‌خوانیم: «حساب توییتر موسیقی سونی در معرض خطر قرار گرفته و در حال حاضر این مسئله برطرف شده است. سونی از بریتنی اسپیرز و هوادارانش بخاطر این شایعات عذرخواهی می‌کند.»

نفوذگران پشت این توییت‌های جعلی گروه OurMine است. این گروه در چند هفته‌ی اخیر تلاش کرده حساب‌های توییتر شرکت‌های مهم دیگر مانند نت‌فلیکس را آلوده کند. در تمامی موارد OurMine توییت‌هایی را ارسال کرده تا به راه‌کارهای امنیتی این شرکت‌ها طعنه بزند. باید به این نکته نیز اشاره کرد که میلیون‌ها دنبال‌کننده‌ی این حساب‌ها در معرض هیچ خطر و آسیبی نیستند.

مدیریت امنیت

گزارش IBM: حملات علیه سامانه‌های کنترل صنعتی افزایش یافته است

باتوجه به گزارش سرویس‌های امنیتی IBM، در سال 2016 تعداد حملات علیه سامانه‌های کنترل صنعتی نسبت به سال قبل، 110 درصد افزایش یافته است. این افزایش قابل توجه به تعداد حملات جستجوی فراگیر بر روی سامانه‌های کنترلِ نظارتی و کسب داده (SCADA) نسبت داده شده است.به نظر می‌رسد مهاجمان در بهمن ماه سال قبل از چارچوب‌های تست نفوذ که بر روی گیت‌هاب قرار داشت، استفاده کرده‌اند. با استفاده از این ابزار که smod نام دارد، می‌توان ارزیابی امنیتی بر روی پروتکل ارتباط سریال Modbus انجام داد. این ابزار دارای قابلیت حمله‌ی جستجوی فراگیر نیز هست.

محقق ارشد امنیتی از IBM توضیح داد: «انتشار عمومی این ابزار بر روی گیت‌هاب و استفاده از آن توسط هر عامل ناشناس، موجب شده تا تعداد حملات بر روی سامانه های کنترل صنعتی در 12 ماه گذشته افزایش چشمگیری داشته باشد.» از آغاز سال 2016 تا اواخر ماه نوامبر، مشاهدات IBM حاکی از آن است که کشور آمریکا برترین کشور از لحاظ منشأ و مقصد حمله بوده است. محققان امنیتی عنوان کردند این موضوع به این خاطر است که آمریکا دارای بیشترین سامانه‌های کنترل صنعتی متصل به اینترنت است.

IBM در گزارش خود عنوان کرد، 60 درصد از این حملات از کشور آمریکا انجام شده و کشورهای دیگری مانند پاکستان (20 درصد)، چین (12 درصد)، هلند (5 درصد) و هند (4 درصد) در رتبه‌های بعدی عاملان حمله قرار دارند. نزدیک به 90 درصد از این حملات نیز سامانه‌های کنترل صنعتی آمریکا را هدف قرار داده‌اند. سامانه‌های کنترل صنعتی کشورهایی مانند چین، رژیم صهیونیستی، پاکستان و کانادا در ادامه‌ی فهرست اهداف مهاجمان قرار می‌گیرند.IBM سه مورد از حملات به سامانه‌های کنترل صنعتی را که خبرساز شده، عنوان کرده است. یکی از این حملات حمله به یک سد در نیویورک بود که در سال 2013 انجام شد و این موضوع در فروردین ماه توسط وزارت دادگستری آمریکا افشاء شد. مقامات آمریکایی مدعی بودند نفوذگران ایرانی سامانه‌ها را آلوده کرده‌اند تا کنترل این سد را در دست بگیرند.یکی دیگر از این اتفاقات، حمله به نیروگاه‌های برق اوکراین بود که در دی ماه سال 94 رخ داد. این حمله به دولت روسیه نسبت داده شد و موجب قطعی برق در اوکراین گردید. قطعی مشابهی امسال نیز اتفاق افتاد ولی اوکراین هنوز تأیید نکرده که این قطعی بخاطر حمله‌ی سایبری رخ داده است. IBM در ادامه نیز حمله‌ی بدافزار SFG را که در مرداد ماه اتفاق افتاد، توضیح داده است. در گزارش‌های اولیه عنوان شده بود این بدافزار که توسط نهادهای دولتی حمایت می‌شود، حداقل یکی از نیروگاه‌های برق اروپا را هدف قرار داده است. هرچند بعدها محققان امنیتی مشخص کردند که این بدافزار خیلی به سامانه‌های کنترل صنعتی علاقه‌ای ندارد و به احتمال زیاد توسط مهاجمان سایبری توسعه داده شده و مورد استفاده قرار گرفته است.

مدیریت امنیت

حمله‌ی منع سرویس توزیع‌شده علیه سرویس تامبلر

وب‌گاه تامبلر آخرین هدف نفوذگران برای انجام حمله‌ی منع سرویس توزیع‌شده بوده است. نفوذگران طی این حمله توانستند نزدیک به 2 ساعت باعث قطعی این وب‌گاه شوند.

این وب‌گاه دیروز ساعت 3:15 بعد از ظهر دقایقی قطع شد و کاربران در اتصال به این وب‌گاه تأخیر زیادی را شاهد بودند. سپس این وب‌گاه دقایقی به حالت برخط برگشت و در دسترس کاربران قرار گرفت ولی دوباره این حمله‌ی منع سرویس توزیع‌شده ادامه داشت و وب‌گاه مجدداً از حالت برخط خارج شد.

تامبلر در یک توییت کوتاه این مسئله را تأیید کرد ولی اعلام شد که این وب‌گاه با هیچ‌گونه حمله‌ی منع سرویس توزیع‌شده‌ای مواجه نبوده است. در توییت تامبلر ابتدا آمده بود: «برخی از کاربران در دسترسی به داشبورد وب‌گاه با کُندی سرعت مواجه هستند.» بعد از دو ساعت قطعی نیز توییت کرد: «بله! همه چیز برطرف شد و تامبلر به حالت عادی خود بازگشت. بخاطر تأخیر بوجود آمده از شما عذر می‌خواهیم و قدردان صبر و شکیبایی شما هستیم.»

گروه نفوذ استار پاترول مسئولیت این حمله را برعهده گرفته و عنوان کرد که این حمله را صرفاً بخاطر سرگرمی انجام داده و قصد نداشته اطلاعاتی را به سرقت ببرد و یا لینک مخربی را توییت کند. واقعیت این است که حمله‌ی منع سرویس هدف خاصی را دنبال نمی‌کند و می‌خواهد برای بازه‌ی زمانی مشخصی باعث قطعی یک سرویس و وب‌گاه شود.

مسئله‌ی عجیبی که وجود دارد این است که باوجود تأیید این مسئله و کندی سرعت در دسترسی به وب‌گاه توسط تامبلر، پس از بازیابی و راه‌اندازی مجدد این سرویس، تامبلر تمامی توییت‌ها را به دلایل نامشخصی حذف کرده است.

در حال حاضر بر روی سرویس تامبلر همه چیز به حالت عادی جریان دارد ولی این شرکت از اذعان به نفوذ امتناع می‌کند و می‌ترسد در آینده عواقبی برای این شرکت داشته باشد و این سرویس برای بازه‌های زمانی طولانی‌تری هدف حمله‌ی منع سرویس توزیع‌شده قرار بگیرد.

فصل سوم

امنیت سایبری

امنیت‌سایبری

مبارزات دولت ترکیه با فعالیت‌های تروریستی برخط

روز شنبه وزارت کشور ترکیه خبر داد که در حال بازجویی از 10 هزار نفر مظنون است. این افراد مرتبط با فعالیت‌های تروریسی در سطح اینترنت هستند و در شبکه‌های اجتماعی نظراتی با محتوای توهین‌آمیز به مقامات ارسال می‌کنند.

این وزارتخانه در بیانیه‌ای گفت: «این فعالیت‌ها بخشی از برنامه‌ی مبارزه با تروریسم است که با عزم و اراده در همه‌جا دنبال می‌شود از جمله در شبکه‌های اجتماعی»

پس از کودتایی که مرداد ماه در ترکیه انجام شد، این دولت در وضعیت اضطراری قرار گرفت و پاک‌سازی کشور از مخالفان را آغاز کرد. در پی این عملیات، گروه‌های حقوق بشر از این سرکوب‌ها توسط دولت ترکیه اظهار نگرانی کردند.

با توجه به گزارش‌های وزارت دادگستری ترکیه، در شش ماه گذشته 1600 نفر به اتهام شرکت در فعالیت‌های تروریستی یا توهین به مقامات دولتی دستگیر شده‌اند.

مقامات ترکیه در پی حوادث جدی که در این کشور رخ داد، دسترسی به شبکه‌های اجتماعی را محدود کردند تا از گردش اطلاعات جلوگیری کنند. گردش اطلاعات در شبکه‌های اجتماعی می‌تواند امنیت ملی ترکیه را تضعیف کند. دسترسی به شبکه‌های اجتماعی از روز دوشنبه هفته قبل، پس از ترور سفیر روسیه در ترکیه، به شدت مختل شده است.

دسترسی به شبکه‌های توییتر و یوتیوب نیز از روز پنج‌شنبه بسیار کُند شده است چرا که در این شبکه‌ها ویدئویی منتشر شده که گروه‌های داعشی دو سرباز تُرک را زنده‌زنده می‌سوزانند.

نهاد نظارت بر اینترنت ترکیه گزارش داده محدودیت‌هایی در دسترسی به شبکه‌های خصوصی مجازی (VPN) نیز ایجاد شده است. از این شبکه‌ها معمولاً برای دور زدن محدودیتِ دسترسی به شبکه‌های اجتماعی و وب‌گاه‌ها استفاده می‌شود.

امنیت‌سایبری

درخواست روسیه از اپل: باز کردن قفلِ آیفون قاتل سفیر روسیه

احتمالاً شما نیز ویدئوی مربوط به ترور سفیر روسیه در ترکیه را دیده‌اید که به سرعت در اینترنت منتشر شده است. سفیر روسیه، آندری کارلو توسط یک افسر پلیس خارج از وظیفه‌ی آنکارا در 29 آذر ماه مورد شلیک قرار گرفت و کشته شد. سفیر روسیه در حالی مورد اصابت قرار گرفت که در یک نمایشگاه هنری مشغول سخنرانی بود. این فرد موفق شد خود را به‌عنوان محافظ رسمی سفیر جا بزند و در ادامه به ضرب گلوله، سفیر روسیه را بکشد.

پس از این حادثه‌ی تکان‌هنده مقامات روسیه از اپل می‌خواهند قفل آیفون 4S این تیرانداز را باز کند و به احتمال زیاد بحثی شبیه به بحث اپل و FBI که اوایل امسال وجود داشت، مجدداً پیش بیاید.

مقامات ترکیه و روسیه از اپل می‌خواهند در دور زدن پین کد آیفون 4S به آن‌ها کمک کند و معتقدند با این کار اپل می‌تواند به بررسی روابط این قاتل با گروه‌های تروریستی دیگر کمک کند. انتظار می‌رود اپل این درخواست را رد کند ولی به گزارش MacReports و رسانه‌های محلی، مقامات روسی گروهی از کارشناسان را به ترکیه اعزام کرده‌اند تا در باز کردن قفلِ آیفون به مقامات کمک کنند.

در بحث بین اپل و FBI، اپل از کمک به باز کردن قفل آیفون تیرانداز سان‌برنادیو سر باز زد و گفت که هر درب پشتی که در داخل دستگاه وجود داشته باشد، روزی ممکن است به دست افزار نابکار بیفتد و از آن سوءاستفاده شود. زمانی‌که FBI از کمک اپل ناامید شد، با پرداخت 1.3 میلیون دلار به یک گروه نفوذ توانست قفلِ آیفون را باز کند اما اطلاعاتی در این تلفن همراه پیدا نکرد که در بررسی‌ها بتواند کمکی بکند.

مردی که سفیر روسیه را به قتل رسانده یک جوان 22 ساله به نام مولوت مرت آلتینتاس، یک افسر پلیس خارج از وظیفه‌ی آنکارا است که با استفاده از شناسه‌ی پلیس خود، زمانی که سفیر در حال سخنرانی بوده، توانسته به نمایشگاه هنری وارد شود.

در طول ترور، تیرانداز فریاد می‌زد: «حلب را فراموش نکنید!» مقامات روسیه و ترکیه معتقدند این ترور برای بی‌ثبات کردن روابط بین دو کشور طراحی شده است.

امنیت‌سایبری

قرار دادن دربِ پشتی در رمزنگاری‌ها در تضاد با منافع ملی است

کارگروه رمزنگاری در آمریکا، در جلسه‌ی پایان سال خود گزارشی را ارائه کرد که یک پیروزی برای فناوری و حریم خصوصی به حساب می‌آید. در این گزارش به 4 نکته‌ی اصلی اشاره شده که در ادامه مشاهده می‌کنید. در ضمن می‌توانید متن کامل گزارش را از اینجا مطالعه کنید.

• هر اقدامی که رمزنگاری را تضعیف کند، در تضاد با منافع ملی است.

• فناوری رمزنگاری یک فناوری جهانی است که به‌طور گسترده در سراسر دنیا در دسترس همگان قرار گرفته است.

• ذی‌نفعان، فناوری‌ها و عوامل مختلف در حوزه‌ی رمزنگاری، چالش‌های مختلفی را ایجاد می‌کنند؛ بنابراین راه‌حل یک شکل و یکسانی برای تمامی این چالش‌ها وجود ندارد.

• کنگره آمریکا باید همکاری بین شرکت‌های فناوری و مراجع اجرای قانون را تقویت کند.

نکته‌ی اول که در این گزارش به آن اشاره شده، اساس رمزنگاری و حریم خصوصی را مطرح می‌کند که برای مدت‌های طولانی موضوع بحثِ شرکت‌های فناوری و دولت‌ها و نهادهای قانونی بوده است.

این کمیته در بررسی‌های خود شاهد بوده بسیاری از نهادهای دولتی، شرکت‌های فناوری بخش خصوص را مجبور می‌کنند در رمزنگاری‌های خود از دربِ پشتی استفاده کنند. در گزارش این کارگروه آمده است: «کنگره نباید این فناوری حیاتی را تضعیف کند چرا که با این کار علیه منافع ملی عمل می‌کند. هرچند نباید نگرانی‌های نهادهای دولتی و اجرایی را نیز که گاهاً بجا نیز هست، نادیده بگیریم.»

گروه سیاست امنیت سایبری اتحادیه‌ی اروپا گفت قرار دادن دربِ پستی در رمزنگاری‌ها بیش از اینکه مزیت داشته باشد، خطرساز است. این کار باعث می‌شود تلاش‌های انجام شده برای حفظ محرمانگی و حریم خصوصی کاربران به هدر رفته و دربِ پشتی به سلاحی برای مهاجمان تبدیل شود تا بتوانند عملیات مخرب خود را اجرایی کنند.

مشابه همین گزارش، اوایل امسال لایحه‌ای در مجلس آمریکا به توصیب رسید مبنی بر اینکه دولت‌ها باید درخواست قرار دادن دربِ پشتی در رمزنگاری را متوقف کنند.

نکته‌ی دوم به این موضوع اشاره می‌کند اگر قرار باشد قرار دادن دربِ پشتی در رمزنگاری‌ها اجباری باشد، فقط باید در شرکت‌های آمریکایی اعمال شود و از آنجا که شرکت‌های تجاری بسیاری در کشورهای مختلف قرار دارند، چنین کاری نتیجه‌ای در پی نخواهد داشت.

در گزارش این کارگروه آمده است: «کنگره نمی‌تواند مهاجمان فضای مجازی را از استفاده‌ی رمزنگاری باز دارد. در نتیجه کمیته برای رسیدگی به نیازمندی‌های قانونی خود باید از استراتژی‌های دیگری استفاده کند.» به عبارت

دیگـر، بنـد دوم ایـن گـزارش بـه نهادهـای قانونـی پیشـنهاد می‌دهـد بجـای اسـتفاده از دربِ پشـتی در رمزنگاری‌هـا بـه دنبـال راه‌حـل دیگـری باشـند.

هرچنـد در گـزارش ایـن کارگـروه ذکـر نشـده چگونـه نهادهـای دولتـی بـدون دربِ پشـتی می‌تواننـد اطلاعـات مـورد نیـاز خـود از داده‌هـای رمزنگاری‌شـده را بدسـت بیاورنـد. نکتـه‌ی سـوم ایـن گـزارش نیـز اشـاره می‌کنـد بـرای چالش‌هـای مختلـف رمزنـگاری، راه‌حل‌هـای یکسـانی وجـود نـدارد.

امنیت‌سایبری

مقامات تایلند منتقدان دولت در فضای مجازی را دستگیر می‌کنند

یک مقام ارشد نظامی روز دوشنبه اعلام کرد مقامات تایلندی دست‌کم 9 نفر مظنون به نفوذ سایبری را دستگیر کردند. این دستگیری‌ها پس از آن رخ داد که تعدادی از نفوذگران به وب‌گاه نهادهای دولتی این کشور در اعتراض به قانون بحث‌برانگیز سانسور، نفوذ کردند.

در اوایل ماه جاری مجلس تایلند به اتفاق آرا قانونی را تصویب کرد. براساس این قانون تمامی مقامات ارشد نظامی می‌توانند وب‌گاه‌هایی که محتوایی بر ضد آن‌ها منتشر کرده را دست‌کاری کرده و از کار بیندازند.

در این لایحه که به‌طور گسترده عملیاتی شده است، کاربران از بارگذاری هرگونه محتوا که اخلاق خوب را نقض می‌کند، منع شده‌اند و کمیته‌ای نیز تشکیل شده تا وب‌گاه‌های دارای چنین محتواهایی را از کار بیندازد. به‌دنبال تصویب این لایحه، نفوذگران وب‌گاه‌های دولتی تایلند را هدف قرار دادند.

در حملات علیه وب‌گاه‌های دولتی تایلند، برخی از آن‌ها در اثر منع سرویس به‌طور موقت غیرفعال شده‌اند. در برخی موارد نیز نفوذگران عنوان کردند که توانستند به پایگاه داده‌ی وب‌گاه‌ها دست یافته و اطلاعات مهم کاربران آن را بدست آوردند.

شایعاتی مبنی بر بازداشت چندین نفر توسط ارتش این کشور در چند روز گذشته وجود داشت. اما مقامات این موضوع را روز دوشنبه به‌طور رسمی تأیید کردند. معاون نخست وزیر این کشور به خبرنگاران گفت: «ما تعدادی از نفوذگران را دستگیر کردیم. تعداد آن‌ها 9 نفر است و در چند روز آینده تعداد بیشتری از آن‌ها را بازداشت خواهیم کرد.»

روز دوشنبه پلیس بانکوک اعلام کرد یک جوان 19 ساله را به اتهام نفوذ سایبری دستگیر کرده و چند روز مورد بازجویی قرار داده است. مقامات پلیس اعلام کردند این جوان اعتراف کرده با جعل هویت توانسته است به سامانه‌های پلیس دسترسی پیدا کند. گروه‌های حقوقی و فعالان حوزه‌ی سایبری در تلاش هستند این قانون را در دادگاه به چالش بکشانند.

در حال حاضر در کشور تایلند مجموعه‌ای از قوانین به تصویب رسیده که مخالفان می‌گویند مناظرات را محدود می‌کند. در یکی از این قوانین عنوان شده که انتقاد از سلطنت و نظام حاکمیتی یک جرم محسوب می‌شود.

این قانون جدید به‌روزرسانی برای قانون جرائم رایانه‌ای است که در سال 2007 به تصویب رسیده بود. این قانون در ابتدا تلاش داشت فعالیت‌های مخرب و کلاه‌برداری مجرمان در فضای مجازی را هدف قرار دهد ولی اینک گریبان‌گیر منتقدان شده است. بسیاری از افرادی که در چند سال اخیر به جرم افترا به سلطنت بازداشت شده‌اند به ارتکاب جرائم سایبری نیز متهم گردیده‌اند.

حکومت نظامی تایلند بخاطر ممنوع کردن نشست‌های

سیاسی و دستگیری منتقدان با نارضایتی مردم مواجه شده است. در نتیجه اینترنت تنها جایی بود که منتقدان می‌توانستند حرف‌های خود را مطرح کنند که به لطف این قانون جدید، بحث در چنین فضاهایی نیز خطراتی به دنبال دارد.

معمولاً در نظراتی که در شبکه‌های اجتماعی ارسال می‌شود، افترا به سلطنت، فتنه و آشوب و جرائم سایبری سر به فلک کشیده است. منتقدان می‌گویند قانون سایبری جدید تاحدودی اهداف حکومت در تبدیل سلطنت به منطقه‌ی دیجیتال را پیش برده است.

امنیت‌سایبری

دو نفوذ جداگانه به وب‌گاه اتاق صنعت و بازرگانی ترکیه

وب‌گاه اتاق صنعت و بازرگانی ترکیه واقع در انگلستان در چند روز گذشته توسط دو گروه نفوذ جداگانه مورد حمله قرار گرفته است.

اولین و مهم‌ترین این نفوذها توسط یک گروه کردی با نام مزوپتامیا انجام شده است. در این نفوذ پیامی در وب‌گاه به نمایش گذاشته شده که نشان می‌دهد نفوذگران در اعتراض به حمله‌ی هوایی ترکیه که منجر به کشته شدن 34 کرد روستانشین شد، این وب‌گاه را هدف قرار داده‌اند.

باوجود اینکه انگیزه‌ی حمله‌ی این گروه کاملاً روشن است، هنوز مشخص نشده آیا این نفوذگران توانسته‌اند اطلاعاتی را به سرقت ببرند و یا سایر صفحات وب‌گاه را نیز آلوده کنند یا خیر.

در یک نفوذ جداگانه، کاپوست‌کی که روش نفوذ به وب‌گاه‌های اتاق صنعت و بازرگانی را یاد گرفته، تلاش کرد تا به این وب‌گاه نیز نفوذ کند. در این حمله کاپوست‌کی توانسته به اطلاعات کاربران از جمله نام، آدرس رایانامه، شماره تلفن و آدرس‌های تعدادی از اعضای وب‌گاه دست یابد.

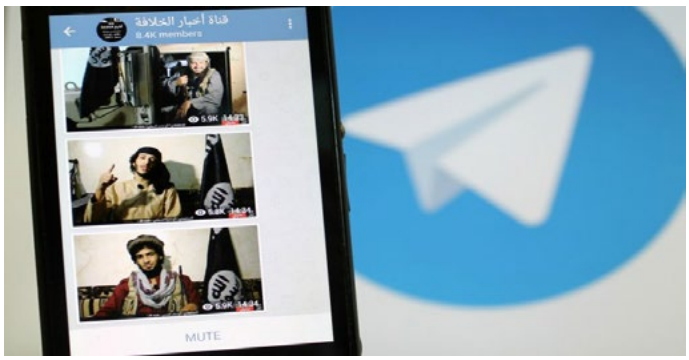
در نمونه داده‌هایی که بدست سافت‌پدیا رسیده، معلوم شده این پایگاه داده حاوی اطلاعات شخصی افراد از جمله نام، شماره تلفن و آدرس است. در این پایگاه داده یک حساب کاربری مدیریتی نیز به چشم می‌خورد که به نظر نمی‌رسد گذرواژه‌ی آن درهم‌سازی شده باشد.

کاپوست‌کی اعلام کرد با مدیران این وب‌گاه تماس گرفته و این مسئله را اطلاع داده ولی هنوز پاسخی از طرف آن‌ها دریافت نکرده است. به همین منظور بخشی از اطلاعات را افشاء کرده تا نشان دهد که واقعاً به پایگاه داده‌ی این وب‌گاه دست یافته است.

در زمان نگارش این خبر این وب‌گاه در حالت نفوذشده قرار دارد و پیغام گروه مزوپتامیا در آن در حال نمایش است. همچنین این احتمال نیز وجود دارد که آسیب‌پذیری کشف‌شده توسط کاپوست‌کی هنوز وصله نشده باشد. به عبارت دیگر اطلاعات صدها نفر در معرض خطر قرار دارد.

امنیت‌سایبری

تلگرام، اولین انتخاب داعش به‌عنوان بستر ارتباطی



برنامه‌ی پیام‌رسان تلگرام به اولین انتخاب اعضای داعش تبدیل شده و استفاده از آن به‌طور عجیبی از سایر رسانه‌های اجتماعی همچون توییتر پیشی گرفته است. اگر می‌خواهید از فعالیت‌های داعش باخبر باشید، باید بدانید که امروزه تلگرام کانال ارتباطی اصلی داعش برای تبلیغات است. در چند وقت اخیر استفاده از پیام‌رسان‌های مبتنی بر رمزنگاری در بین گروه‌های تروریستی افزایش یافته و اینک داعش نیز بیش از پیش از تلگرام استفاده می‌کند. این موضوع استفاده از سایر شبکه‌های اجتماعی مانند توییتر را تحت‌الشعاع قرار داده است.

شبکه‌های اجتماعی تلاش می‌کنند تا محتوای ارسال شده توسط گروه‌های داعشی را مسدود کنند و می‌خواهند تبلیغات برخط این گروه را متوقف نمایند.

توییتر بستن صدها هزار حساب کاربری به دلیل نقض سیاست های خشونت افراطی را ادامه می‌دهد. در شهریور ماه توییتر یک پست وبلاگی را منتشر کرد که نشان می‌داد از سال گذشته این شرکت نزدیک به 360 هزار حساب کاربری با محتوای تروریستی را مسدود کرده است.

در هفته‌های قبل از حادثه‌ی برلین، تحلیلگران اطلاعاتی مشاهده کردند در کانال‌های تلگرام منتسب به گروه‌های داعشی، پیام‌هایی برای جذب داوطلبان و دعوت به قانون‌شکنی و کشتار به اشتراک گذاشته شده است.

یکی از دلایل استفاده‌ی گسترده‌ی داعش از تلگرام این است که این شرکت اقدامات سرکوب‌گرانه‌ی جدی را علیه فعالیت‌های داعش انجام نمی‌دهد. گروه‌های داعشی و القاعده در شبه جزیره‌ی عربستان چندین کانال تلگرامی را راه‌اندازی کردند و اعضای این گروه‌های تروریستی می‌توانند به‌طور امن با هم در ارتباط باشند.

کانال «ناشر» یکی از کانال‌های مربوط به داعش است که به چند زبان خبرهایی را در تلگرام منتشر می‌کند. به گزارش محققان برنامه‌ی تلگرام به عنوان یک بستر ارتباطی برای گروه‌های تروریستی گوی سبقت را از توییتر ربوده است. استفاده از تلگرام برای تروریست‌های داعشی آسان بوده و این برنامه گزینه‌های مختلفی برای ارتباطات عادی و رمزنگاری‌شده را ارائه می‌دهد.

یک بار دیگر، داعش قابلیت‌های خود در تغییر روش‌ها را نشان داد و ثابت کرد چگونه با استفاده‌ی حداکثری از فناوری، نظارت بر فعالیت‌هایش را به حداقل رسانده است.

امنیت‌سایبری

نفوذ به توپخانه‌های اوکراین با استفاده از بدافزار اندرویدی

در تحقیقی که توسط محققان امنیتی شرکت CrowdStrike منتشر شد، نشان داده شده است که نفوذگران گروه Fancy Bear با استفاده از برنامه‌های اندرویدی مخرب، به سامانه‌های توپخانه‌ی اوکراین نفوذ کرده‌اند.

در این گزارش آمده است از این بدافزار برای ردیابی واحدهای مختلف توپخانه از جمله بخش خمپاره‌انداز D-30 ساخته‌شده توسط اتحادیه‌ی جماهیر شوروی در سال‌های 2014 تا 2016 استفاده شده است. این نفوذگران که با دولت روسیه مرتبط هستند، حدس زده می‌شود اطلاعات جمع‌آوری‌شده را برای ارتش نظامی روسیه ارسال کرده‌اند.

محققان امنیتی این شرکت کشف کردند که نفوذگران از یک برنامه‌ی اندرویدی آلوده به ابزار X-Agent برای دست یافتن به دستگاه‌های اندرویدی استفاده کرده‌اند. این دستگاه‌های اندرویدی در توپخانه‌های اوکراین برای عملیات خاصی مورد استفاده قرار می‌گرفت. این بدافزار در انجمن‌های نظامی اوکراین توزیع شده است و تقریباً 9 هزار نفر از افراد توپخانه، با استفاده از برنامه‌های قانونی به این انجمن دسترسی داشته‌اند.

بدافزار 9 هزار دستگاه را هدف قرار داده است

نفوذگران گروه Fancy Bear این برنامه را با یک بسته‌ی آلوده به نام Monp-M30.apk هدف قرار داده‌اند. این بسته‌ی مخرب اطلاعات مکانی و ارتباطی را از دستگاه آلوده بازیابی خواهد کرد.

این اطلاعات به ارتش روسیه کمک می‌کند تا مکان جغرافیایی دقیق توپخانه‌های اوکراین را پیدا کرده و آن را نشانه برود. در گزارش‌ها آمده است که ارتش اوکراین در طول 2 سال درگیری، 50 درصد از سلاح‌ها و نزدیک به 80 درصد از خمپاره‌اندازهای D-30 را از دست داده است.

این برنامه‌ی اندرویدی مخرب در بسیاری از انجمن‌های نظامی توزیع شده ولی هنوز شواهدی مبنی بر این وجود ندارد که در بازار گوگل پلی نیز منتشر شده باشد. کاربران باید این پرونده‌ی APK را به‌طور دستی نصب کنند.

این شرکت امنیتی اشاره کرده است: «استفاده از ابزار X-Agent نشان می‌دهد گروه Fancy Bear علاوه بر بستر iOS بدافزارهایی را در حوزه‌ی اندروید نیز توسعه داده و به یک مولفه‌ی جدید در جنگ روسیه علیه اوکراین تبدیل شده است.»

گروه Fancy Bear یکی از گروه‌های نفوذ روسیه است که قبلاً نیز حملاتی را از آن‌ها، از جمله حمله به آمریکا شاهد بوده‌ایم. اخیراً اف‌بی‌آی و سیا مدعی شدند که نفوذگران روسی به دونالد ترامپ کمک کردند تا در انتخابات ریاست جمهوری آمریکا، نامزد دیگر، هیلاری کلینتون را شکست دهد.

امنیت‌سایبری

لیتوانی دولت روسیه را به جاسوسی سایبری متهم کرد

روسیه مجدداً بخاطر نفوذ به رایانه‌های دولت‌های خارجی متهم شده است. این بار نیز لیتوانی جاسوس‌افزاری را کشف کرده و ادعا می‌کند این بدافزار توسط کرملین بر روی رایانه‌های دولتی این کشور نصب شده است.

در بیانیه‌ی رویترز، رئیس مرکز امنیت سایبری لیتوانی اعلام کرده نفوذگران روسی اولین بار در سال 2015 تلاش کردند تا رایانه‌های این کشور را با جاسوس‌افزار آلوده کنند ولی فقط همین امسال 20 تلاش مجدد دیگر توسط این نفوذگران به ثبت رسیده است.

قضیه زمانی بدتر می‌شود که این جاسوس‌افزار 6 ماه پس از نصب بر روی رایانه‌ها کشف شده است و رئیس این مرکز مدعی است که بدافزار اسناد و گذرواژه‌های دولت لیتوانی را برای آژانس‌های جاسوسی روسیه ارسال کرده است.

هنوز مشخص نیست که آیا اسناد محرمانه یا دولتی به سرقت رفته است یا خیر ولی مقامات لیتوانی می‌گویند برخی از این رایانه‌های آلوده توسط مقامات دولتی رده متوسط تا رده پایین مورد استفاده قرار می‌گرفت و این افراد بر روی پیش‌نویس تصمیمات دولت کار می‌کردند.

سخنگوی رئیس جمهور روسیه این اتهامات را رد کرده و این مسئله را خنده‌دار توصیف کرده است. او در ادامه گفت: «آیا درون این بدافزارها نوشته که توسط روسیه نوشته شده است؟ ما این اتهامات بی‌پایه و اساس را رد می‌کنیم.» او عنوان کرد که کشور روسیه هدف حملات و جاسوسی‌های سایبری قرار گرفته ولی دولت این کشور هیچ دولت خارجی را متهم نکرده است.

رئیس مرکز امنیت سایبری لیتوانی اشاره کرد که روسیه در حوزه‌ی امنیت سایبری به تهدیدی بزرگ تبدیل شده و همه‌ی دولت‌ها برای مقابله با نفوذهای نفوذگران وابسته به کرملین باید آماده شوند.

فصل چهارم

اخبار فنی

اخبار فنی

آسیب‌پذیری‌های روز-صفرم در مسیریاب‌های NETGEAR WNR2000

یک محقق امنیتی کشف کرد، آسیب‌پذیری‌هایی که در مسیریاب‌های NETGEAR WNR2000 وجود دارد به مهاجمان اجازه می‌دهد گذرواژه‌های مدیریتی را به سرقت برده و کنترل کامل دستگاه آسیب‌پذیر را در دست گیرند.

این آسیب پذیری‌ها به‌طور پیش‌فرض بر روی یک شبکه‌ی محلی (LAN) قابل بهره‌برداری است اما محقق امنیتی با نام پترو ریبریو، توضیح می‌دهد که اگر ویژگی مدیریت از راه دور فعال شده باشد، این آسیب‌پذیری‌ها در سطح اینترنت و از راه دور نیز قابل بهره‌برداری هستند. به گفته‌ی ریبریو تاکنون 10 هزار دستگاه آسیب‌پذیر شناسایی شده است و این‌ها فقط دستگاه‌هایی هستند که ویژگی مدیریت از راه دور بر روی آن‌ها فعال است. به عبارت دیگر ممکن است هزاران دستگاه دیگر نیز تحت تأثیر این آسیب‌پذیری قرار گرفته باشند.

این آسیب پذیری های امنیتی در مدل WNR2000v5 مسیریاب کشف شده است که در نسخه‌ی آخر ثابت‌افزار به‌طور پیش‌فرض مدیریت از راه دور در آن فعال نیست.

این موضوع نشان می‌دهد بهره‌برداری از راه دور زمانی امکان‌پذیر است که کاربران به‌طور دستی ویژگی مدیریت از راه دور را فعال کرده باشند. به نظر می‌رسد نسخه‌های 3 و 4 این مسیریاب‌ها نیز آسیب‌پذیر باشند هرچند محققان امنیتی هنوز این مسئله را آزمایش نکرده‌اند.

مسئله‌ی اصلی از جایی ناشی می‌شود که مسیریاب NETGEAR WNR2000 به یک ادمین اجازه می‌دهد از طریق اسکریپت CGI با نام apply.cgi توابع مختلفی را اجرا کند که موجب می‌شود زمانی که رشته‌ی مربوطه در قالب یک URL دریافت می‌شود، یک تابع بر روی کارگزار (HTTP (uhttpd فراخوانی شود. با مهندسی معکوس بر روی uhttpd محققان امنیتی کشف کردند که با فراخوانی apply_noauth.cgi به یک کاربر غیرمجاز نیز اجازه داده می‌شود توابع حساسی که ادمین اجرا می‌کند را بتواند اجرا کند.

در نتیجه مهاجم غیرمجاز می‌تواند بلافاصله از برخی از این توابع در دسترس بهره‌برداری کند مانند بوت مجدد مسیریاب. برای اجرای سایر توابع مانند تغییر تنظیمات WLAN، اینترنت و بازیابی گذرواژه‌های مدیریتی، مهاجم باید به انتهای URL متغیر «مهر زمان» را اضافه کند.

ریبریو توضیح می‌دهد: «این مهر زمانی هر بار که این صفحه مشاهده می‌شود، تولید شده و به عنوان توکن برای پیشگیری از حملات CSRF عمل می‌کند. تابعی که مهر زمانی را تولید می‌کند مهندسی معکوس شد و به دلیل استفاده‌ی نادرست از تولیدکننده‌ی عدد تصادفی، می‌توان در کمتر از 1000 تلاش، بدون هیچ دانش قبلی، توکن را شناسایی کرد.»

به شرطی که مهاجم نیز بر روی شبکه‌ی LAN باشد، با

بهره‌برداری از این اشکال پیاده‌سازی و آسیب‌پذیری‌های موجود بر روی مسیریاب، مهاجم می‌تواند گذرواژه‌های مدیریتی را بدست آورده و عملکرد telnet را بر روی مسیریاب فعال کند که یک شِل در اختیار او قرار بگیرد. علاوه بر این، ریبریو کشف کرد که یک آسیب‌پذیری سرریز بافر پشته نیز وجود دارد که با بهره‌برداری از آن یک مهاجم غیرمجاز می‌تواند کنترل مسیریاب را در دست گرفته و از راه دور کدهایی را بر روی آن اجرا کند. برای این منظور مهاجم باید از آسیب‌پذیری apply_noauth.cgi و حمله‌ی شناسایی مهر زمانی استفاده کند. کد مهاجم می‌تواند بر روی LAN و WAN قابل اجرا باشد.

به گفته‌ی ریبریو، به دلیل اینکه شرکت NETGEAR به رایانامه‌ی او پاسخ نداد، او نه تنها تصمیم گرفت که آسیب‌پذیری‌ها را به‌طور عمومی افشاء کند بلکه کدهایی برای بهره‌برداری از آن‌ها نیز منتشر کرد و به این ترتیب این آسیب‌پذیری‌ها به روز-صفرم تبدیل شدند. هنوز برای این آسیب‌پذیری‌ها شماره CVE اختصاص داده نشده است.

سکیوریتی‌ویک نیز برای بررسی این مسائل و اطلاع از زمان انتشار وصله، با NETGEAR تماس گرفته ولی تاکنون پاسخی دریافت نکرده است. اوایل این ماه مسیریاب‌های R6400، R7000 و R8000 و احتمالاً دیگر مسیریاب‌های این شرکت، تحت تأثیر آسیب‌پذیری‌های جدی قرار گرفتند و مهاجمان توانستند با بهره‌برداری از این آسیب‌پذیری‌ها، مسیریاب‌ها را به سرقت ببرند. با بازدید از یک وب‌گاه جعلی و مخرب توسط کاربر، مهاجم می‌توانست دستورات دلخواه خود را با امتیازات ویژه بر روی مسیریاب اجرا کند. بعد از اینکه این آسیب‌پذیری‌ها این شرکت را در سرفصل خبرهای حوزه‌ی امنیت قرار داد، این شرکت برنامه‌ی وصله‌ی خود را ارائه کرد.

اخبار فنی

بهره‌برداری از آسیب‌پذیری ارتقاء امتیاز در محصول CCO سیسکو

سیسکو از وجود یک آسیب‌پذیری جدی ارتقاء امتیاز در سامانه‌ی CloudCenter Orchestrator (CCO) به مشتریان خبر داد.

سامانه‌ی CloudCenter سیسکو یک بستر مدیریت اَبر ترکیبی است که از دو مؤلفه تشکیل شده است:

- مدیر CloudCenter، یک واسط که توسط مدیران و کاربران مورد استفاده قرار می‌گیرد.
- CloudCenter Orchestrator که توسعه‌ی برنامه‌های کاربردی را خودکار می‌سازد و زیرساختی برای تأمین و پیکربندی است.

این سامانه قبلاً بخشی از شرکت فناوری CliQr بود که سیسکو اوایل امسال آن را خریداری کرد.

به گفته‌ی سیسکو یک مهاجم غیرمجاز از راه دور می‌تواند کانتینرهای داکر مخرب را با امتیازات بالا نصب کند. در این عملیات از آسیب‌پذیری CVE-2016-9223 موجود در پیکربندی ماشین داکر بهره‌برداری می‌شود.

این حفره ی امنیتی در حین حل وفصل یک مشکل پشتیبانی کشف شد. این آسیب‌پذیری به دلیل اشتباه در پیکربندی ایجاد شده که باعث می‌شود درگاه مدیریت ماشین داکر، از خارج نیز قابل دسترسی باشد. یک مهاجم با بهره‌برداری از این آسیب‌پذیری می‌تواند کانتینرهای داکر با امتیازات دلخواه را بر روی سامانه‌ی CCO بارگذاری کند.

اگر درگاه TCP 2375 باز بوده و محدود به آدرس محلی 0.0.0.0 باشد، سامانه‌ی CCO آسیب‌پذیر است و معمولاً این تنظیمات جزو پیکربندی پیش‌فرض این سامانه است. کاربران با دستور زیر می‌توانند آسیب‌پذیری سامانه‌ی خود را بررسی کنند.

```
netstat -ant | grep 2375
```

گروه پاسخگویی به رخدادهای امنیتی سیسکو، گفت که از وجود تعداد محدودی از این دستگاه‌های آسیب‌پذیر آگاه است. سازمان‌ها می‌توانند با دستور تصویر داکر، آلوده شدن نصب‌های خود را بررسی کنند و برای موارد مشکوک فهرست کانتینرهای خود را مشاهده کنند.

سیسکو گفت: «از آنجا که این آسیب‌پذیری دسترسی ریشه به CCO می‌دهد، شاخصه‌های دیگری از آلودگی می‌توانند بسته به هدف مخرب مهاجم، متفاوت باشد.»

این آسیب‌پذیری با انتشار CCO 4.6.2 وصله شده است. به عنوان یک راه‌حل کاربران می‌توانند درگاه ماشین داکر خود را به آدرس محلی 172.0.0.1 محدود کنند. سیسکو راه‌کارهای دقیق‌تر را در مشاوره‌نامه‌ی امنیتی خود ارائه کرده است.

در حالی‌که اکثریت آسیب‌پذیری‌های کشف‌شده در محصولات سیسکو، در حملات واقعی مورد بهره‌برداری قرار نمی‌گیرند ولی بهره‌برداری از آن‌ها برای مهاجمان بسیار مفید خواهد بود. این شرکت اخیراً متوجه شده

یک گروه نفوذ وابسته به آژانس امنیت ملی آمریکا، با نام Equation از آسیب‌پذیری‌های ناشناخته‌ی محصولات سیسکو بهره‌برداری کرده و محصولات این شرکت را هدف قرار داده است.

اخبار فنی

کشف چند آسیب‌پذیری بر روی مسیریاب‌های زایکسل

محققان امنیتی از شرکت SecuriTeam هشدار دادند برخی از مسیریاب‌های ویژه‌ی زایکسل گرفتار چندین آسیب‌پذیری و گواهی‌نامه‌های ورود پیش‌فرض شده‌اند. این آسیب‌پذیری‌ها در تجهیزات توزیع‌شده توسط TrueOnline کشف شده است. این شرکت یک ارائه‌دهنده‌ی سرویس اینترنت در تایلند است.

این شرکت نسخه‌ی سفارشی از مسیریاب‌ها را به‌طور رایگان به مشتریان خود ارائه می‌دهد و تمامی این مسیریاب‌ها دارای حساب‌های کاربری و گذرواژه‌های پیش‌فرض هستند که کاربران را در معرض تهدیدات مختلف قرار می‌دهد.

بر روی مسیریاب‌های ساخت زایکسل نسخه‌ای از لینوکس با نام tclinux اجرا می‌شود و این مسیریاب‌ها در 3 مدل P660HN-T v2، P660HN-T v1 و Billion 5200W-T در کل جهان توزیع شده است. به گزارش Securi مدل P660HN-T v1 از سال 2103 توزیع شده و دیگر نسخه‌ها اخیراً بین کارخواه‌ها توزیع شده است.

این آسیب‌پذیری‌ها که توسط محققان امنیتیِ مستقل گزارش شده، عبارتند از:

- آسیب‌پذیری اجرای دستورات از راه دور به‌طور غیرمجاز بر روی P660HN-T v1
- آسیب پذیری‌های اجرای دستورات از راه‌دور به‌طور غیرمجاز و اجرای دستورات از راه دور به‌طور احراز هویت شده بر روی Billion 5200W-T
- آسیب‌پذیری اجرای دستورات از راه دور به‌طور غیرمجاز بر روی P660HN-T v2

علاوه بر این آسیب‌پذیری‌ها بر روی هر 3 مدل از مسیریاب‌ها از حساب‌ها و گ ذ ر واژه‌های پیش‌فرض استفاده شده که می‌تواند توسط مهاجمان برای دسترسی به حساب‌های کاربری مورد استفاده قرار بگیرد.

شرکت Securi در مشاوره‌نامه‌ی خود هشدار داد: «این مسیریاب‌های آسیب‌پذیر نسخه‌های سفارشی مسیریاب‌های زایکسل و Billion هستند. همه‌ی آن‌ها سامانه‌های MIPS هستند و تمامی آن‌ها کارگزار وب BOA را اجرا می‌کنند. این مسیریاب‌ها از طریق تزریق دستور در واسط وب دارای آسیب‌پذیری هستند که به مهاجم غیرمجاز یا احراز هویت شده امکان بهره‌برداری را می‌دهد.»

محققان امنیتی عنوان کردند که شرکت زایکسل مرداد ماه از این آسیب‌پذیری‌ها مطلع شده است. تاکنون چندین بار محققان امنیتی وضعیت ارائه‌ی وصله برای این آسیب‌پذیری‌ها را در تماس با این شرکت پیگیری کرده‌اند ولی پاسخی دریافت نشده است. در حال حاضر نیز برای این اشکالات راه‌حلی در دسترس نیست.

هفته‌ی قبل نیز در خبری عنوان کردیم که مسیریاب‌های NETGEAR WNR2000 تحت تأثیر یک آسیب‌پذیری

روز-صفـرم قـرار گرفته‌انـد کـه در نتیجـه‌ی آن مهاجـمان می‌تواننـد کنـترل کامـل دسـتگاه آسـیب‌پذیر را در دسـت بگیرنـد. پـس از اینکـه ایـن آسـیب‌پذیری به‌طـور عمومـی افشـاء شـد، NETGEAR بـه خبرگزاری‌هـا اعـلام کـرد، در تـلاش اسـت بـا به‌روزرسـانی ثابت‌افـزار ایـن آسـیب‌پذیری را وصلـه کنـد.

اخبار فنی

کشف 3 آسیب‌پذیری روز-صفرم در PHP 7

سه آسیب‌پذیری روز-صفرم در PHP 7 کشف شده و به مهاجمان اجازه می‌دهد کنترل نزدیک به 80 درصد از وب‌گاه‌ها را در دست بگیرند. این وب‌گاه‌ها از آخرین نسخه‌ی زبان برنامه‌نویسی PHP استفاده می‌کنند.

این آسیب‌پذیری‌ها در سازوکارِ غیرسریال این زبان برنامه‌نویسی کشف شده است و به نفوذگران اجازه می‌دهد با ارسال داده‌های جعلی و مخرب در کوکی‌های کارخواه، وب‌گاه‌های دروپال، جوملا، Magento و vBulletin را آلوده کنند.محققان امنیتی گروه چک‌پوینت چندین ماه سازوکار غیرسریال PHP 7 را مورد بررسی قرار داده و 3 آسیب‌پذیری جدید و ناشناخته را در آن پیدا کردند. هرچند در این سازوکار در PHP 5 نیز قبلاً آسیب‌پذیری‌هایی وجود داشت ولی محققان اشاره کردند که این آسیب‌پذیری‌ها با آسیب‌پذیری‌های قبلی متفاوت هستند.

این سه آسیب‌پذیری روز-صفرم با شناسه‌ی CVE CVE-2016-7480، 2016-7479 و CVE-2016-7478 مشابه آسیب‌پذیری که چک‌پوینت در شهریور ماه کشف کرد، قابل بهره‌برداری است.

آسیب پذیری CVE-2016-7479 یک اجرای کد و آسیب‌پذیری استفاده پس از آزادسازی است. آسیب‌پذیری دوم با شناسه‌ی CVE-2016-7480 اجرای کد با استفاده از یک متغیر است که مقداردهی اولیه نشده است. آسیب‌پذیری CVE-2016-7478 نیز یک منع سرویس از راه دور است.دو آسیب‌پذیری اول اگر مورد بهره‌برداری قرار بگیرند، به مهاجم اجازه می‌دهند کنترل کامل کارگزار را در دست گرفته و اجازه‌ی انجام هرکاری از جمله نصب بدافزار را داشته باشد. این بدافزارها می‌توانند داده‌های مشتریان را به سرقت برده و ظاهر وب‌گاه را تغییر دهند. محققان در گزارش خود توضیح دادند که آسیب‌پذیری سوم نیز برای اجرای یک حمله‌ی منع سرویس می‌تواند مورد بهره‌برداری قرار بگیرد. از این طریق مهاجمان می‌توانند باعث کُند شدن و مصرف بیش از حد حافظه‌ی این وب‌گاه شوند. محققان اشاره کردند هیچ یک از این آسیب‌پذیری‌ها در دنیای واقعی توسط نفوذگران مورد بهره‌برداری قرار نگرفته است.

محققان چک‌پوینت این آسیب‌پذیری‌های روز-صفرم را در تاریخ‌های 16 مرداد و 15 شهریور به گروه امنیتی PHP گزارش دادند. PHP نیز در تاریخ 22 مهر و 11 آذر برای 2 مورد از 3 آسیب‌پذیری، وصله‌هایی را منتشر کرد ولی هنوز یکی از این آسیب‌پذیری‌ها وصله‌نشده باقی مانده است.

علاوه بر ارائه‌ی این وصله‌ها، شرکت چک‌پوینت امضاهایی را نیز برای سامانه‌های پیشگیری از نفوذ (IPS) در تاریخ 2 مهر و 10 آبان ارائه کرد تا از کاربران در برابر این آسیب‌پذیری‌ها حفاظت بیشتری به عمل آید. به منظور اطمینان از امنیت کارگزارهای وب، به کاربران توصیه شده تا کارگزارهای خود را به آخرین نسخه‌ی PHP به‌روزرسانی کنند.

اخبار فنی

کشف آسیب‌پذیری در کتابخانه‌ی متن‌باز PHPMailer

یک آسیب‌پذیری جدی در PHPMailer کشف شد. PHPMailer یک کتابخانه‌ی متن‌باز معروف در PHP است که توسط 9 میلیون کاربر در کل دنیا برای ارسال رایانامه استفاده می‌شود.

میلیون‌ها وب‌گاه PHP و برنامه‌های متن‌باز تحت وب از جمله وردپرس، دروپال، Yii، SugarCRM، 1CRM و جوملا برای ارسال رایانامه از کتابخانه‌ی PHPMailer استفاده کرده و از روش‌های مختلف آن مانند SMTP بهره می‌برند.

این آسیب‌پذیری که توسط دیوید گلونسکی کشف شده دارای شناسه‌ی CVE-2016-10033 است و به مهاجمان اجازه می‌دهد بر روی کارگزار وب، کد دلخواه خود را اجرا کرده و برنامه‌ی تحت وب مورد نظر را آلوده کنند.

گلونسکی در مشاوره‌نامه‌ای که امروز منتشر کرد نوشت: «برای بهره‌برداری از این آسیب‌پذیری کافی است مهاجم از فرم‌های بخش تماس با ما، نظرات، فرم‌های ثبت‌نام، بازنشانی گذرواژه و سایر روش‌ها که با کمک رایانامه انجام می‌شود، استفاده کند. هنگام ارسال رایانامه از مؤلفه‌های این کتابخانه استفاده شده و آسیب‌پذیری مورد نظر قابل بهره‌برداری است.»

گلونسکی این آسیب‌پذیری را به توسعه‌دهندگان این کتابخانه گزارش داد و آن‌ها با انتشار PHPMailer 5.2.18 آسیب‌پذیری را وصله کردند. تمامی نسخه‌های PHPMailer بجز نسخه‌ی جدید تحت تأثیر این آسیب‌پذیری قرار گرفته‌اند و به مدیران و توسعه‌دهندگان وب قویاً توصیه می‌شود این کتابخانه را به نسخه‌ی وصله‌شده به‌روزرسانی کنند.

بخاطر اینکه این اولین گزارشی است که طی آن این آسیب‌پذیری به‌طور عمومی افشاء می‌شود، برای همین گلونسکی از ذکر جزئیات بهره‌برداری از آسیب‌پذیری امتناع کرده است.

با این حال، او وعده داده در چند روز آینده جزئیات فنی بیشتری از این آسیب‌پذیری را توضیح دهد. همچنین قرار است کد بهره‌برداری اثبات مفهومی و ویدئویی از انجام حمله را به نمایش بگذارد. ما نیز در طول چند روز آینده و به محض ارائه‌ی جزئیات توسط گلونسکی، خبر مربوط به این آسیب‌پذیری را به‌روزرسانی خواهیم کرد.

اخبار فنی

اپل به توسعه‌دهندگان iOS برای مهاجرت به سمت HTTPS مهلت بیشتری می‌دهد

اپل این هفته به توسعه‌هندگان iOS اطلاع داد که تصمیم گرفته به آن‌ها مهلت بیشتری بدهد تا ارتباطات برنامه‌های خود را بر روی کانال‌های امن HTTPS برقرار کنند.

در تیر ماه در کنفرانس توسعه‌دهندگان جهانی اپل، این شرکت اطلاع داد تمامی برنامه‌های کاربردی iOS بر روی فروشگاه اپل باید تا آخر سال از امنیت انتقال اپل (ATS) استفاده کنند.

قابلیت ATS به‌طور پیش‌فرض بر روی iOS 9.0 و 10.11 فعال شده است و در این ویژگی اجبار شده تا ارتباط بین برنامه‌ی کاربردی و کارگزار آن بر روی کانال HTTPS صورت گیرد.

اپل به این نتیجه رسید که بسیاری از توسعه‌دهندگان تا تاریخ 12 دی نمی‌توانند این کار را عملیاتی کنند و تصمیم گرفت این مهلت را به‌طور نامحدودی تمدید کند. برخی معتقدند که توسعه‌دهندگان می‌توانند بدون استفاده از HTTPS نیز بر روی فروشگاه اپل برنامه‌های خود را انتشار دهند اگر در طول فرآیند بررسی خود توجیه منطقی داشته باشند.

در مطالعات اخیر که توسط شرکت امنیتی تلفن همراه انجام شد، تنها 3 درصد از 200 برنامه‌ی برتر iOS در کل جهان با استفاده از ATS پیاده‌سازی شده است. یک مهندس از این شرکت امنیتی توضیح داد: «در طول 3 هفته‌ی گذشته در راستای سازگاری با ATS مشاهده کردیم که تنها 2 درصد افزایش در پیاده‌سازی ATS داشتیم. بنابراین بسیار عجیب نیست که بسیاری از توسعه‌دهندگان نمی‌توانند تا 12 دی ماه با ATS سازگار شوند. متأسفانه اپل تصمیم گرفته تا مدت زمان تعیین‌شده را تمدید کند. با این تصمیم داده‌های کاربران و برنامه‌ها در معرض خطر خواهد بود ولی توسعه‌دهندگان مهلت بیشتری برای سازگاری با ATS خواهند داشت. امیدواریم این مهلت کوتاه مدت باشد و تصمیم اپل برای سازگاری با ATS با شکست مواجه نشود.»

در یک پست وبلاگی این شرکت امنیتی توصیه‌های مختلفی را برای سازمان‌ها در راستای نظارت و اصلاح برنامه‌های فاقد ATS ارائه کرده است. محققان این شرکت توضیح دادند: «باتوجه به توسعه‌های جدید، به سازمان‌ها توصیه می‌کنیم سازگاری برنامه‌ها با ATS را ردیابی و دنبال کنند و برنامه‌ها را با نمونه‌های سازگار با ATS جایگزین کنند. همچنین به شرکت‌ها توصیه می‌کنیم برای جلوگیری از حملات مرد میانی، از برنامه‌هایی استفاده کنند که از پین‌گذاری گواهی‌نامه بهره می‌برند.»

فصل پنجم

اخبار تحـــلیلی

اخبار تحلیلی

ابزار رمزگشایی جدید برای نسخه‌ی 3 باج‌افزار CryptXXX منتشر شد

محققان امنیتی تهدیدات ناشی از نسخه‌ی 3 باج‌افزار CryptXXX را خنثی کردند و ابزاری برای رمزگشایی پرونده‌ها ارائه دادند. این ابزار رمزگشایی به پروژه‌ی No Ransom آزمایشگاه کسپرسکی اضافه شده است.

نسخه‌های قبلی ابزار رمزگشایی بر روی فهرست جزئی از پرونده‌های رمزنگاری‌شده با CryptXXX کار می‌کرد ولی نسخه‌ی جدیدِ این ابزار، تمامی پرونده‌ها را بازیابی می‌کند.

باج‌افزار CryptXXX امروزه یکی از فعال‌ترین خانواده‌ی باج‌افزاری است و این ابزار رمزگشایی با خنثی کردن تهدیدات آن، ضربه‌ی مهلکی را به نویسندگان این بدافزار وارد می‌کند. تقریباً یک چهارم از قربانیان باج‌افزار CryptXXX در آمریکا قرار دارند و کشورهایی مانند آلمان، روسیه و ژاپن در بین کشورهایی هستند که بیشتر هدف حمله‌ی این باج‌افزار قرار گرفته‌اند.

در اردیبهشت ماه محققان امنیتی برای رمزگشایی پرونده‌هایی که با نسخه‌ی اولیه‌ی باج‌افزار رمزنگاری شده بودند، ابزاری منتشر کردند. تا تیرماه نویسندگان قابلیت‌های CryptXXX را بهبود دادند تا بتوانند تأثیرات ابزار رمزگشایی را خنثی کنند و در این راستا یک ماژول سرقت گواهی‌نامه به این بدافزار اضافه کردند. در آن زمان محققان پروف‌پوینت می‌گفتند نویسندگان این باج‌افزار می‌خواهد با نرخ آلودگی و توزیع باج‌افزار Locky رقابت داشته باشند.

در اولین نسخه‌ی باج‌افزار CryptXXX یک اشکال در الگوریتم رمزنگاری وجود داشت و محققان امنیتی با بهره‌برداری از آن می‌توانستند ابزار رمزگشایی ارائه کنند. در نسخه‌ی دوم باج‌افزار، نویسندگان کد را به‌روزرسانی کردند ولی هنوز اشکالاتی در آن وجود داشت و محققان آزمایشگاه کسپرسکی مجدداً توانستند ابزاری برای رمزگشایی تهیه کنند. در ابزار رمزگشایی جدید، می‌توان پرونده‌هایی که با نسخه‌ی 2 یا 3 باج‌افزار رمزنگاری شده را رمزگشایی کرد.

به گفته‌ی محققان امنیتی آزمایشگاه کسپرسکی، باج‌افزار CryptXXX یک DLL است که به زبان دلفی نوشته شده و در حمله به پرونده‌ها از الگوریتم‌های رمزنگاری مختلفی استفاده می‌کند. آزمایشگاه کسپرسکی گزارش داد 3 مورد از روش‌های رمزنگاری که این باج‌افزار استفاده می‌کند از جمله RC4 از یک کلید یکسان برای رمزنگاری پرونده‌ها استفاده می‌کند. دو مورد دیگر از روش‌ها از RC4 و RSA برای رمزنگاری محتوای پرونده‌ها و کلیدهای RC4 استفاده می‌کنند. در مواردی نیز مشاهده شده که از ترکیبی از RC4 و RSA استفاده می‌شود. با استفاده از RC4 محتوای پرونده‌ها رمزنگاری شده و با RSA برخی پرونده‌های خاص و کلیدهای RC4 رمزنگاری می‌شود.

در نسخه‌ی 3 باج‌افزار CryptXXX به انتهای پرونده‌های رمزنگاری‌شده پسوند .cryp1، .crypt و .crypz اضافه

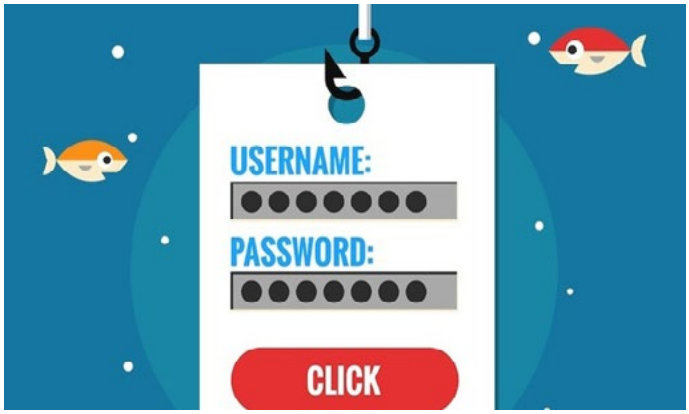
می‌شود. در بررسی‌های انجام‌شده، محققان اشاره کردند برخلاف باج‌افزار Locky که توسط پویش هرزنامه‌ای Dridex توزیع می‌شود، باج‌افزار CryptXXX به ترافیک مخرب URL ها که در کیت‌هایی مانند Angler و Neutrino مورد بهره‌برداری قرار می‌گیرد متکی است. باتوجه به برداشت‌های قبلی از باج‌افزار، نسخه‌ی 3 دارای ماژولی به نام stiller.dll است که بر روی رایانه‌های هدف بارگیری می‌شود. این ماژول می‌تواند اطلاعات 130 نوع کارت اعتباری مختلف را از روی رایانه‌ی قربانی به سرقت ببرد مانند اطلاعاتی که در کارخواه‌های رایانامه، برنامه‌های پیام‌رسان و مرورگرهای وب ذخیره می‌شود.

محققان امنیتی آزمایشگاه کسپرسکی می‌گویند: «پس از رمزنگاری پرونده‌ها و ارسال تمامی اطلاعات حساس به مهاجمان، این باج‌افزار در ادامه یک پیغام باج‌خواهی را نمایش می‌دهد.» در حال حاضر مشخص نیست در نسخه‌ی جدید CryptXXX چه مقدار باج از قربانی خواسته می‌شود. در تیرماه در نسخه‌ی 2 باج‌افزار، برای بازگرداندن پرونده‌ها مبلغی برابر با 1.3 بیت‌کوین معادل هزار دلار از قربانی خواسته شده بود.

آزمایشگاه کسپرسکی قبلاً نیز نزدیک به 12 ابزار رمزگشایی برای باج‌افزارهایی مانند TeslaCrypt، CoinVault، Wildfire و Crybola منتشر کرده است. فهرست کامل ابزارهای رمزگشایی در وب‌گاه No Ransom کسپرسکی قابل مشاهده است.

اخبار تحلیلی

استفاده از روش‌های توزیع بدافزار در پویش‌های فیشینگ



محققان امنیتی شرکت پروف‌پوینت پویش فیشینگ را کشف کردند که به سرقت اطلاعات بانکی کاربران می‌پردازد. این پویش از روش‌های مورد استفاده در توزیع بدافزار بهره می‌برد. محققان می‌گویند این پویش بسیار شبیه به پویش‌هایی است که باج‌افزار Cerber و تروجان بانکی Ursnif را توزیع می‌کند.

مهاجمان برای توزیع بدافزار از پرونده‌های .zip که با گذرواژه محافظت می‌شوند و حاوی اسناد مخرب هستند، استفاده می‌کنند. رایانامه‌ای که مهاجمان برای قربانی ارسال می‌کنند حاوی یک پرونده‌ی .zip است و در محتوای پیام نیز گذرواژه‌ای برای باز کردن این پرونده‌ی فشرده وجود دارد.

این پویش فیشینگ نیز تلاش دارد داده‌های کارت‌های اعتباری قربانیان را به سرقت ببرد. مهاجمان در این پویش رایانامه‌ای برای قربانی ارسال می‌کنند که حاوی یک سند HTML است که با گذرواژه محافظت می‌شود.

در این رایانامه اولین رقم از شماره کارت اعتباری قربانی نشان داده شده تا یک حس قانونی بودن رایانامه به قربانی القاء شود در حالی‌که مهاجمان به‌طور کامل شماره کارت اعتباری قربانی را نمی‌دانند. این رایانامه تلاش دارد تا به نحوی قربانی را فریب بدهد و اطلاعات کارت اعتباری را از او بگیرد. این رایانامه طوری وانمود می‌کند که یک عملیات ضروری به‌روزرسانی باید صورت گیرد و برای صدور تراشه‌ی جدید بر روی کارت اعتباری، اطلاعات کارت قربانی مورد نیاز است.

در گزارش پروف‌پوینت آمده است: «در نمونه رایانامه‌هایی که ما مورد تحلیل و بررسی قرار دادیم، پیام‌ها با استفاده از نام قربانی و رقم اول شماره کارت او، سفارشی‌سازی شده بود. وجود رقم اول کارت اعتباری قربانی باعث می‌شود این رایانامه در نظر قربانی، قانونی جلوه کند. این رایانامه‌ها از نام‌های تجاری به سرقت‌رفته و روش‌های مهندسی اجتماعی استفاده می‌کنند تا قربانی یک حس فوریت در به‌روزرسانی اطلاعات امنیتی کارت بانکی خود را احساس کند.»

پرونده‌ی HTML که در این رایانامه استفاده شده، از طریق XOR کدگذاری شده تا تحلیل پویای آن مشکل‌تر شود. محققان متوجه شدند در این سند HTML بجای استفاده از ویژگی محافظت با گذرواژه‌ی مایکروسافت، یک تابع جاوا اسکریپت استفاده شده است.

زمانی‌که کاربر گذرواژه را وارد می‌کند، سند HTML رمزگشایی شده و یک نمونه‌ی فیشینگ کارت‌های اعتباری با نام‌های تجاری به سرقت‌رفته نمایش داده می‌شود.

پروف‌پوینت توضیح داد: «از زمانی که مهاجمان در فضای مجازی وجود داشتند، سرقت اطلاعات کارت‌های اعتباری نیز وجود داشت. مهاجمان در عرصه‌ی نوآوری و آزمودن روش‌های جدید در حملات فیشینگ هیچ‌گاه متوقف نشدند. آن‌ها همواره تلاش دارند قربانی را متقاعد کنند

تـا اطلاعـات کارت‌هـای اعتبـاری و بانکـی خـود را وارد کنـد. در ایـن نمونـه نیـز شـاهد بودیـم در پویـش فیشـینگ از روش‌هـای توزیـع بدافـزار اسـتفاده شـده بـود. مهاجـمان از اسـناد محافظت‌شـده بـا گـذرواژه اسـتفاده می‌کننـد تـا روش‌هـای ضدبدافـزار را دور بزننـد و یـک حـسِ امنیـت کاذب را القـاء کننـد.»

اخبار تحلیلی

تبدیل بدافزار مخرب KillDisk به باج‌افزار

باج‌افزار جدید KillDisk که اخیراً کشف شده بود تمامی پرونده‌های دستگاه قربانی را رمزنگاری کرده و بجای حذف کردن، برای گرفتن باج آن‌ها را نگه می‌دارد. بخاطر اینکه این بدافزار سامانه‌های کنترل صنعتی را هدف قرار داده بود، متخصصان نگران هستند که این بدافزار، باج‌افزارها را وارد حوزه‌ی کنترل صنعتی کند.

نسخه‌های قبلی این بدافزار بر روی هارد درایو کار می‌کرد و سعی داشت آن را غیرقابل اجرا کند اما نسخه‌ی جدید که توسط متخصصان امنیتی مشاهده شده، پرونده‌ها را با ترکیبی از الگوریتم‌های RSA و AES رمزنگاری می‌کند. به‌طور ویژه هر پرونده با الگوریتم AES رمزنگاری شده و کلیدهای این رمزنگاری با کلید 1028 بیتی RSA که در بدنه‌ی بدافزار قرار دارد، رمز می‌شود.

محققان امنیتی گفتند نمونه‌ی جدید KillDisk که بررسی کردند، بخشی از یک باج‌افزار است و کد و عملکرد آن نیز بسیار نزدیک به بدافزار نسخه‌ی قبل است.

این باج‌افزار برای رمزنگاری پرونده‌های متنوعی مانند اسناد، پایگاه داده، کد منبع، تصویر دیسک، رایانامه و پرونده‌های رسانه‌ای طراحی شده است. این باج‌افزار پارتیشن‌های محلی و پوشه‌های به اشتراک گذاشته شده در سطح شبکه را هدف قرار می‌دهد.

از قربانیان برای بازگرداندن پرونده‌ها 222 بیت‌کوین باج درخواست شده است و محققان امنیتی بر این باورند که این باج‌افزار سازمان‌هایی که وضع مالی خوبی دارند، هدف قرار داده است. آدرس رایانامه‌ای که برای تماس در اختیار قربانیان قرار گرفته مربوط به یک ارائه‌دهنده‌ی سرویس رایانامه‌ی خصوصی با نام Lelantos بوده و دستیابی به آن تنها از طریق شبکه‌ی Tor امکان‌پذیر است. آدرس کیف پول بیت‌کوین که برای پرداخت باج در اختیار قربانی قرار گرفته، تاکنون هیچ تراکنشی را انجام نداده است.

محققان امنیتی اشاره کردند از یک کلید عمومی RSA یکسان در تمامی نمونه‌ها استفاده شده است. به عبارت دیگر قربانی با پرداخت باج و دریافت کلید رمزگشایی، می‌تواند پرونده‌های تمام قربانیان را رمزگشایی کند.

محققان امنیتی می‌گویند این بدافزار نیازمند امتیازات سطح بالا و ثبت خود به عنوان یک سرویس است. این بدافزار فرآیندهای زیادی را بر روی رایانه‌ی قربانی خاتمه می‌دهد ولی از خاتمه دادن به فرآیندهای سامانه‌ای و فرآیندهای مربوط به برنامه‌های ضدبدافزار خودداری می‌کند. دلیل این کار جلوگیری از خراب‌کاری در سامانه و تشخیص توسط محصولات امنیتی است.

محققان گفتند: «نکته‌ی مهمی که وجود دارد و باید به آن اشاره کنیم این است که نویسندگان این بدافزار به خوبی با API های رمزنگاری آشنا هستند و از برخی توابع به‌درستی برای تولید اعداد تصادفی استفاده می‌کنند. ولی

آن‌ها از تابع CryptDecrypt استفاده نکرده‌اند احتمالاً به این خاطر که این تابع به راحتی قلاب می‌شود. قابلیت قلاب کردن یک تابع به برنامه‌های ضدبدافزار این امکان را می‌دهد به پرونده‌های رمزنگاری‌شده دست یافته و کلیدهای رمزنگاری را بازیابی کنند.»

تکامل KillDisk به سمت باج‌افزار

اوایل این ماه شرکت امنیتی ESET گزارشی از جزئیات یک حمله که توسط گروه TeleBots انجام شده بود ارائه داد. محققان بر این باور بودند که این گروه، تکامل‌یافته‌ی گروه نفوذ روسی BlackEnergy است که در دی ماه سال گذشته نیز نیروگاه‌های برق اوکراین را هدف حمله قرار داده بود.

یکی از ابزارهایی که توسط گروه BlackEnergy مورد استفاده قرار می‌گرفت همین بدافزار KillDisk بود. این بدافزار برای حذف پرونده‌ها و غیرقابل اجرایی کردن سامانه طراحی شده بود. در حمله‌ای که باعث قطعی برق در اوکراین شد، بدافزار KillDisk بود که کار بازیابی سرویس برای نیروگاه‌های برق و انرژی را بسیار مشکل کرد.

در پویش‌های مخرب سایبری که اخیراً علیه اهداف با ارزش و مؤسسات مالی در اوکراین صورت گرفته، گروه TeleBots از ابزارهای مختلفی از جمله نسخه‌ی جدید KillDisk استفاده کرده است. این بدافزار معمولاً با امتیازات بالا در مراحل نهایی حمله مورد استفاده قرار گرفته است. در مراحل اولیه مهاجمان تلاش می‌کنند امتیازات سطح بالا و مدیریتی و گواهی‌نامه‌های لازم را بدست آوردند.

در این حملات بدافزار KillDisk به‌گونه‌ای پیکربندی شده تا در تاریخ و زمان مشخصی فعال شود. علاوه بر حذف پرونده‌های مهم سامانه‌ای، بدافزار طوری تنظیم شده که پرونده‌ها را با پسوند خاصی رونویسی می‌کند که تا حدی شبیه به کاری است که باج‌افزار با رمزنگاری پرونده انجام می‌دهد.

محققان امنیتی معتقدند مهاجمان بدافزار KillDisk را در داخل یک باج‌افزار قرار داده‌اند تا علاوه بر پویش‌های مخرب خود، بتوانند پولی نیز بدست آورند.

محققان اشاره کردند سامانه‌های صنعتی به دلایل مختلف می‌توانند هدف خوبی برای مهاجمان و باج‌افزارها باشند. این دلایل عبارتند از:

- پویش‌های مخرب به راحتی می‌تواند باعث خطرات و قطعی‌های فیزیکی قابل توجهی بشوند.
- عملکرد شبکه به راحتی قابل متوقف کردن نیست.
- پرونده‌های پشتیبان کافی برای بازیابی داده‌ها وجود ندارد.
- به احتمال زیاد کارمندان سامانه‌های صنعتی، خیلی از امنیت سایبری آگاه نیستند.

محققان می‌گویند: «بسیاری از شرکت‌ها به احتمال زیاد باج درخواستی از طرف مهاجمان را بی‌سروصدا پرداخت می‌کنند. دلیل پرداخت باج این است که شرکت‌ها از عمومی شدن این حملات سایبری و جریمه‌هایی که دریافت خواهند کرد، نگران هستند.»

اخبار تحلیلی

تروجان اندرویدی Switcher: نفوذ به مسیریاب‌ها و سرقت ترافیک

محققان آزمایشگاه کسپرسکی، تروجان اندرویدی جدیدی را مشاهده کردند. این تروجان به مسیریاب‌ها نفوذ کرده و تنظیمات DNS آن را بنحوی تغییر می‌دهد که ترافیک به سمت وب‌گاه‌های مخرب هدایت شود.

این بدافزار با نام Switcher به یک کارخواه اندرویدی برای موتور جستجوی چینی Baidu و یک برنامه‌ی چینی برای اشتراک جزئیات شبکه‌های وای‌فای تبدیل شده است. زمانی‌که کاربر یکی از این برنامه‌ها را نصب می‌کند، بدافزار تلاش می‌کند نام کاربری و گذرواژه‌ی مسیریابی که دستگاه آلوده به آن متصل شده را حدس بزند.

بدافزار Switcher فهرستی از نام کاربری و گذرواژه‌های ترکیبیِ پیشنهادی دارد که به مهاجم اجازه می‌دهد با استفاده از این ترکیب نام کاربری و گذرواژه، به رابط مدیریتی مسیریاب دست پیدا کند. این ترکیب‌ها عبارتند از admin:123456، admin:admin و admin:00000000.

یک محقق امنیتی در حوزه‌ی امنیت تلفن همراه از آزمایشگاه کسپرسکی، در یک پست وبلاگی نوشت: «این بدافزار با کمک جاوا اسکریپت تلاش دارد با استفاده از ترکیب‌های نام کاربری و گذرواژه، وارد حساب مدیریتی مسیریاب شود. باتوجه به نام‌های هارکدشده در فیلدهای ورودی و همچنین ساختار اسناد HTML که بدافزار تلاش می‌کند به آن‌ها دست یابد، می‌توان حدس زد که کد جاوا اسکریپت تلاش می‌کند بر روی رابط وب مسیریاب های وای‌فای TP-LINK کار کند.»

زمانی‌که مهاجم به رابط وب مدیریتی دست یافت، کارگزارهای DNS اصلی و ثانویه دستگاه را با آدرس‌های IP کارگزارهای مخرب جایگزین می‌کند. این آدرس‌های IP عبارتند از: 1.200.147.153 0 1، 112.33.13.11 و 120.76.249.59. یکی از این آدرس‌های IP به‌طور پیش‌فرض استفاده می‌شود و دو مورد دیگر برای ISP های خاص بکار می‌رود.

محققان امنیتی اشاره کردند: «کدی که این عملیات را اجرا می‌کند بسیار کامل است چرا که به‌گونه‌ای طراحی شده تا بر روی طیف وسیعی از مسیریاب‌ها عمل کرده و در حالت آسنکرون استفاده شود.»

با تغییر تنظیمات DNS مسیریاب، ترافیک بجای ارسال به سمت وب‌گاه قانونی، به سمت ماشین مخربی که تحت کنترل مهاجمان است، هدایت می‌شود. به گزارش کسپرسکی، مهاجمان نزدیک به 1300 وب‌گاه در چین را با این روش آلوده کرده‌اند.

محققان کسپرسکی گفتند: «این تروجان تمام شبکه و همه‌ی کاربران آن را هدف قرار می‌دهد. از افراد شخصی گرفته تا کسب‌وکارهای تجاری را با استفاده از فیشینگ تا آلودگی‌های ثانویه در معرض خطر قرار می‌دهد. اگر حمله‌ای با موفقیت انجام شود حتی شناسایی آن نیز سخت خواهد بود. تنها راه برای تنظیم مجدد کارگزارهای DNS نیز راه‌اندازی و بوت مجدد دستگاه است.»

اخبار تحلیلی

با دربِ پشتی Rakos کنترل کامل سامانه‌ی لینوکسی در دست مهاجمان خواهد بود

محققان امنیتی ESET بدافزار جدیدی را کشف کردند که دستگاه‌های لینوکسی تعبیه‌شده را هدف قرار داده و کنترل کامل دستگاه آسیب‌پذیر را در اختیار مهاجمان قرار می‌دهد. این دربِ پشتی راهی برای انجام عملیات مخرب مانند حملات منع سرویس توزیع‌شده نیز باز می‌کند.

این بدافزار با نام Rakos در دستگاه‌ها و کارگزارهای تعبیه‌شده بر روی درگاهِ باز SSH حمله‌ی جستجوی فراگیر انجام می‌دهد تا بتواند گذرواژه‌ی ورود را بشکند. محققان ESET معتقد هستند نویسنده‌ی این بدافزار می‌خواهد تا جایی که می‌تواند دستگاه‌های تعبیه‌شده را آلوده کرده و به باتنت خود اضافه کند و در ادامه از این باتها در حملات منع سرویس توزیع‌شده بهره ببرد.

در مرحله‌ی اول این بدافزار با استفاده از آدرس‌های IP از پیش تعیین‌شده، دستگاه‌های آسیب‌پذیر را پویش می‌کند. از آنجایی که این بدافزار برای حمله از جستجوی فراگیر استفاده می‌کند، تنها سامانه‌های دارای گذرواژه‌ی ضعیف در معرض خطر قرار دارند.

زمانی‌که بدافزار توانست گذرواژه را بشکند و به سامانه دسترسی یابد، بر روی آدرس http://127.0.0.1:61314 با دو هدف، یک سرویس http محلی را راه‌اندازی می‌کند. محققان امنیتی ESET می‌گویند: «دلیل اول برای ایجاد این سرویس، داشتن روش حیله برای آینده است. مهاجمان در آینده می‌توانند در نسخه‌ی جدید بات، نمونه‌های قبلی در حال اجرا را بدون توجه به نام بات، تنها با ارسال درخواست به آدرس http://127.0.0.1:61314/et متوقف کنند.

دلیل دوم نیز این است که این بدافزار می‌تواند پرس‌وجو URL با پارامترهای ip، u و p را با ارسال درخواست به آدرس http://127.0.0.1:61314/ex تجزیه و تحلیل کند. هنوز دلیل منبع ex/ مشخص نیست و در جای دیگری از کد نیز به آن اشاره نشده است.»

این بدافزار به‌طور خودکار سامانه را پویش کرده و اطلاعات را جمع‌آوری و به سمت کارگزار دستور و کنترل ارسال می‌کند. اطلاعات جمع‌آوری‌شده حاوی آدرس IP، نام کاربری و گذرواژه‌ها است. یک پرونده‌ی پیکربندی نیز به‌طور محلی بر روی سامانه‌ی آسیب‌پذیر ذخیره شده و بدافزار می‌تواند با دستورات و وظایف جدیدی، خود را به‌روزرسانی کند. اما برای به‌روزرسانی پرونده‌های بدافزار، نویسندگان باید در آینده نسخه‌ی پیچیده‌تری را توسعه دهند.

چگونه آلودگی به بدافزار Rakos را حذف کنیم؟

اگر به هر دلیلی دستگاه تعبیه‌شده‌ی لینوکسی شما آلوده به این بدافزار شد، شما باید با استفاده از SSH/ Telnet به آن متصل شده و به دنبال فرآیندی به نام javaxxx. باشید. مطمئن شوید که این فرآیند برای برقراری

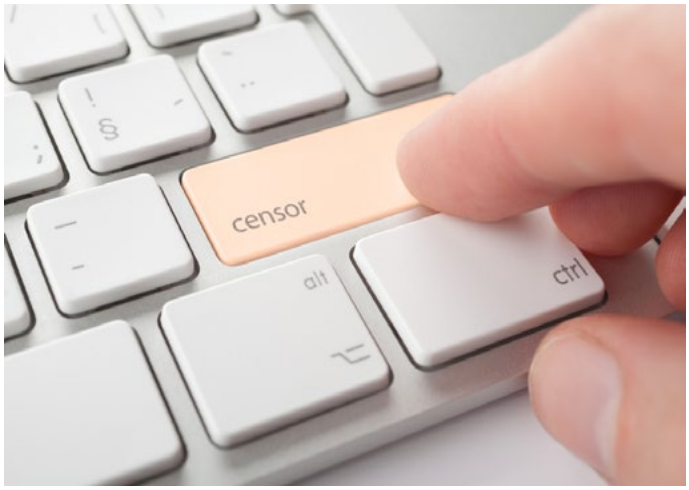
ارتباطات ناخواسته مورد استفاده قرار می‌گیرد و در ادامه این فرآیند را بکُشید.

بوت مجدد سامانه نیز باعث می‌شود این فرآیند کُشته شود و بدافزار هنوز طوری پیکربندی نشده که مجدداً راه‌اندازی شود. اما معمولاً پس از چند وقت، ممکن است این دستگاه دوباره به بدافزار آلوده شود.

برای جلوگیری از آلوده شدن به بدافزار Rakos استفاده از گذرواژه‌های امن برای SSH ضروری است. شرکت ESET اعلام کرده است در چند روز اخیر تعداد آلودگی به این بدافزار افزایش یافته است.

اخبار تحلیلی

پیام‌رسان سیگنال برای دور زدن سانسور از روش «نمای دامنه» استفاده می‌کند



گروه نرم‌افزاری OWS روز چهارشنبه به کاربران اطلاع داد که آخرین نسخه‌ی اندروید پیام‌رسان سیگنال دارای ویژگی است که سانسورهای صورت گرفته در برخی کشورها را دور می‌زند.

این شرکت اخیراً متوجه شده که ISP ها در برخی کشورها از جمله مصر و امارات متحده‌ی عربی سرویس سیگنال و وب‌گاه آن را مسدود می‌کنند. این مسدودسازی توسط مقامات این کشورها در راستای جلوگیری ارتباط کاربران در کانال‌های محرمانه صورت گرفته است.

به منظور دور زدن این سانسورها، در آخرین نسخه‌ی اندرویدی برنامه‌ی سیگنال از روشی با نام «نمای دامنه» استفاده شده است. در این روش ترافیک به شکلی مخفی می‌شود و این‌گونه به نظر می‌رسد که ترافیک از سمت وب‌گاهی ارسال شده که شامل سانسور نمی‌شود.

روش «نمای دامنه» سال گذشته در مقاله‌ای توسط محققان دانشگاه کالیفرنیا ارائه شد. محققان توضیح دادند: «ایده‌ی اصلی در این روش این است که در لایه‌های مختلف ارتباطی از دامنه‌های متفاوتی استفاده شود. یک دامنه وقتی خارج از درخواست HTTPS ظاهر می‌شود قابل مشاهده است ولی داخل درخواست که قرار بگیرد به دلیل رمزنگاری HTTPS قابل سانسور نخواهد بود.» به دلیل اینکه این روش از طریق شرکت‌های مهمی مانند گوگل، آمازون، Fastly، CloudFlare و Akamai مورد استفاده قرار می‌گیرد، سانسور تنها در صورتی امکان‌پذیر است که کل سرویس مسدود شود و این مسدودسازی برای یک کشور می‌تواند عواقب جدی به دنبال داشته باشد.

در مورد برنامه‌ی سیگنال، پیام‌ها شبیه به درخواست‌های HTTPS به آدرس وب‌گاه گوگل به نظر می‌رسد و مسدود کردن این درخواست‌ها مستلزم این است که ISP ها گوگل را مسدود کنند. روش «نمای دامنه» برای کاربرانی با پیش شماره‌ی مصر و امارات فعال شده است.

روش «نمای دامنه» از طریق گوگل در یک طرح با نام GoAgent در چین برای دور زدن سانسور مورد استفاده قرار گرفت ولی تا تیر ماه سال 93 کار کرد چرا که دولت چین تصمیم گرفت سرویس گوگل را به‌طور کامل مسدود کند.

ویژگی دور زدن سانسور در نسخه‌ی بتای سیگنال برای iOS نیز وجود دارد و به زودی برای کاربران آیفون و آی‌پاد در دسترس قرار خواهد گرفت.

بنیان‌گذار شرکت OWS گفت: «ما سانسور شدن برنامه‌ی سیگنال را شناسایی کرده و زمانی‌که نیاز باشد، این سانسورها را دور خواهیم زد و در سرویس سیگنال روش «نمای دامنه» را گسترش خواهیم داد.»

اخبار تحلیلی

بدافزار آلیس: سرقت تمام پول‌های نقد دستگاه‌های خودپرداز

محققان امنیتی ترندمیکرو هشدار دادند، خانواده‌ی جدیدی از بدافزارهای ATM کشف شده که پول نقد موجود در صندوق ماشین‌های خودپرداز را خالی می‌کند. بدافزار آلیس ساده‌ترین بدافزار ATM است که تاکنون مشاهده شده است. این بدافزار هیچ‌گونه قابلیت سرقت اطلاعاتی ندارد و از طریق صفحه کلید عددی ATM قابل کنترل نیست. این بدافزار اولین بار در نوامبر 2016 کشف شد و حدس زده می‌شود بدافزار آلیس از سال 2014 وجود داشته است. محققان ترندمیکرو معتقدند این هشتمین بدافزار ATM است که مشاده شده ولی به‌هرحال 9 سال است که بدافزارها دستگاه‌های ATM را هدف قرار می‌دهند.

استفاده از این بدافزار نیازمند این است که به دستگاه ATM دسترسی فیزیکی وجود داشته باشد. ترندمیکرو حدس می‌زند هدف اصلی این بدافزار به سرقت بردن تمام پول نقد موجود در صندوق دستگاه ATM است. مشابه چنین حمله‌ای سال قبل توسط بدافزار GreenDispenser انجام شد.

این بدافزار به پد پین دستگاه ATM متصل نمی‌شود و می‌تواند از طریق پروتکل رومیزی راه دور (RDP) مورد استفاده قرار بگیرد هرچند ترندمیکرو می‌گوید تاکنون شواهدی مبنی بر چنین استفاده‌ای را مشاهده نکرده است.

تحلیل‌های بدافزار نشان می‌دهد که آلیس با استفاده از یک بسته‌بندی‌کننده و مبهم‌ساز تجاری با نام VMProtect بسته‌بندی شده است. این کار باعث می‌شود از اجرای بدافزار در محیط‌های اشکال‌یابی جلوگیری شود. علاوه بر این، بدافزار پیش از اجرا شدن، محیط خود را مورد بررسی قرار می‌دهد و اگر محیط اجرایی دستگاه ATM نبود به فرآیند خود خاتمه می‌دهد.

در هنگام اجرای بدافزار در ماشین ATM، بدافزار آلیس دو پرونده را در دایرکتوری ریشه می‌نویسد، یک پرونده‌ی خالی با اندازه‌ی 5 مگابایت با نام xfs_supp.sys و یک پرونده‌ی ثبت خطا با نام TRCERR.LOG. بعد از آن بدافزار به محیط CurrencyDispenser1 متصل می‌شود. این محیط یک دستگاه تلگراف در محیط XFS است. در ادامه اگر پین درستی ارائه شود، این محیط اطلاعات موجود بر روی نوار کاست و پول‌های بارگذاری‌شده در ماشین را نمایش می‌دهد.

به دلیل اینکه بدافزار تنها به محیط CurrencyDispenser1 متصل می‌شود و برای استفاده از پد پین ماشین تلاش نمی‌کند، محققان معتقدند، مهاجمان می‌توانند از طریق USB و یا CD-ROM دستگاه ATM را باز کرده و آن را آلوده کنند. علاوه بر این، محققان حدس می‌زنند مهاجمان صفحه کلیدی را به مادربرد دستگاه متصل کرده و بدافزار را راه می‌اندازند.

محققان امنیتی کشف کردند که بدافزار آلیس از 3 دستور پشتیبانی می‌کند که هر کدام با یک پین مشخص صادر می‌شود. یکی برای نصب پرونده‌ای برای حذف کردن بدافزار، یکی برای خروج از برنامه و اجرای روال پاک‌سازی و خاتمه و سومی برای باز کردن پنل عملیاتی. این پنل مکانی است که اطلاعات مربوط به مبلغ موجود در ماشین، در آن برای مهاجمان نمایش داده می‌شود.

مهاجم تنها نیاز دارد تا شناسه‌ی کاست را در ماشین ATM وارد کرده و ماشین تمام پول‌ها را توزیع کند. دستور توزیع پول از طریق API WFSExecute برای محیط CurrencyDispenser1 ارسال می‌شود. به‌خاطر اینکه اکثر بانک‌ها محدودیت ارائه‌ی 40 اسکناس را دارند، مهاجمان باید عملیات یکسانی را چندین بار انجام دهند تا کل پول‌های موجود در صندوق خالی شود. به‌طور پویا اطلاعات مربوط به پول‌های برداشت‌شده در ATM نمایش داده شده و مهاجم خواهد فهمید چه زمانی صندوق ماشین خالی شده است.

محققان ترندمیکرو معتقدند مهاجمان به‌طور دستی با استفاده از بدافزار در ماشین ATM هدف، مدیر وظایف ویندوز را جابجا می‌کنند چرا که بدافزار در سامانه‌های آلوده در قالب taskmgr.exe یافت شده است. این بدافزار هیچ‌گونه سازوکار ماندگاری ندارد اما به‌عنوان مدیر وظایف اجرا می‌شود، به‌عبارت دیگر هر وقت دستور اجرای مدیر وظایف صادر شود، بدافزار آلیس فراخوانی خواهد شد.

سامانه‌ی احراز هویت پین مشابه روشی است که در سایر خانواده‌های بدافزاری ATM مورد استفاده قرار گرفته است ولی در بدافزار آلیس، سامانه‌ی احراز هویت این امکان را به نویسنده می‌دهد که بر روی کسانی که به آلیس دسترسی داشته‌اند، کنترل داشته باشد. با تغییر دادن کد دسترسی در نمونه‌های مختلف بدافزار، نویسندگان از اشتراک‌گذاری کد و ردیابی افراد جلوگیری می‌کنند.

در نمونه‌های تحلیل‌شده از 4 رقم برای کلمه‌ی عبور استفاده شده است اما نمونه‌های دیگر می‌توانند از پین طولانی‌تری استفاده کنند. بر روی پین نمی‌توان جستجوی فراگیر انجام داد چرا که این بدافزار قبل از خاتمه دادن به فرآیند خود، تعداد محدودی پین را قبول می‌کند و در انتها یک پیام خطا را نمایش می‌دهد. محققان معتقدند آلیس می‌تواند بر روی هر سخت‌افزاری که دارای میان‌افزار سرویس مالی توسعه‌یافته‌ی مایکروسافت (XFS) باشد، اجرا شود.

محققان ترندمیکرو می‌گویند: «بدافزارهای ATM تا همین اواخر در دسته‌ی بسیار کوچکی از دنیای بدافزاری قرار داشتند و تنها توسط گروه‌های انگشت‌شماری در حملات هدف‌مند مورد استفاده قرار می‌گرفتند. ولی در حال حاضر شاهد هستیم که بدافزارهای ATM در جریان اصلی تهدیدات قرار دارند.»

اخبار تحلیلی

حمله‌ی منع سرویس توزیع‌شده با شدت ۶۵۰ گیگابیت بر ثانیه توسط باتنت Leet

د رست قبل از کریسمس، شرکت Imperva بر روی شبکه‌ی خود یک حمله‌ی عظیم منع سرویس توزیع‌شده را شناسایی کرد که شدت آن به ۶۵۰ گیگابیت بر ثانیه می‌رسید و در نوع خود بی‌نظیر بود. تاکنون حمله‌ای با این شدت ثبت نشده است. به گزارش Imperva این حمله توسط باتنتی با نام Leet در تاریخ ۱ دی ماه انجام شده و شبکه‌ی این شرکت را تحت تأثیر قرار داده است. هرچند در حال حاضر نمی‌توان انتساب دقیقی برای دستگاه‌های مهاجم انجام دارد ولی این‌طور به نظر می‌رسد که شبیه به باتنت Mirai، این باتنت نیز از هزاران دستگاه اینترنت اشیاء آلوده تشکیل شده است. محققان امنیتی شرکت Imperva در گفتگویی عنوان کردند: «به دلیل جعل آدرس IP، شناسایی دستگاه‌های استفاده شده در این حمله بسیار سخت است. با این حال ما سرنخ‌های قابل توجهی را در بار داده‌ی بسته‌ها کشف کردیم. بررسی‌های انجام شده بر روی بار داده نشان داد که این حمله توسط دستگاه‌های لینوکس انجام شده است. به عنوان مثال در برخی از این دستگاه‌ها پوشه‌ی proc/ مشاهده شده که مربوط به سامانه‌های یونیکس است.»

در تحلیل و بررسی‌های انجام شده، این شرکت گفت که مهاجمان نمی‌توانستند اهدافی که پشت پروکسی این شرکت قرار داشت را مکان‌یابی کنند و به همین دلیل سرویس‌های مبتنی بر ابر این شرکت را هدف قرار دادند. این حمله در دو موج مشاهده شد. در دور اول حمله که ۲۰ دقیقه طول کشید، شدت حمله به ۴۰۰ گیگابیت بر ثانیه می‌رسید. این حمله در رسیدن به اهداف خود شکست خورد. در دور دوم حملات، باتنت قوی‌تر شده و شدت حمله به ۶۵۰ گیگابیت بر ثانیه رسید و در هر ثانیه نزدیک به ۱۵۰ میلیون بسته به سمت شبکه‌ی این شرکت گسیل می‌شد. دور دوم حمله ۱۷ دقیقه به طول انجامید و این حمله نیز با شکست مواجه شد.

بدلیل جعل آدرس IP شناسایی منطقه ی جغرافیایی دستگاه‌های مهاجم غیرممکن است ولی محققان این شرکت بار داده‌ی بسته‌های دریافتی را مورد تحلیل و بررسی قرار دادند. اگرچه این حمله از نظر اندازه مشابه حمله‌ی Mirai است ولی کاملاً مشخص است که باتنت دیگری عامل این حمله بوده است.

نام باتنت Leet نیز از یک امضا در داخل بسته‌های دریافتی گرفته شده است. در این حمله از دو نوع متفاوت بار داده در بسته‌ها استفاده شده است. در نوع اول بسته‌های SYN با اندازه‌ی معمولی ۴۴ تا ۶۰ بایت ارسال شده است. در نوع دوم بسته‌های SYN با اندازه‌ی غیرعادی ۷۹۹ تا ۹۳۶ بایت مشاهده شده است. محتوای بسته‌های بزرگ از دستگاه آلوده برداشته شده و درهم شده است. در نتیجه حجم انبوهی از بار داده‌ی مبهم و تصادفی به سمت شبکه ارسال شده که می‌تواند هرگونه

تشخیص مبتنی بر امضاء را دور بزنند.

این شرکت اشاره کرده که باتنت Leet در حال رقابت با Mirai بر سر اندازه‌ی باتنت است و در آینده شاید شاهد رخدادهای بدتری باشیم. باتوجه به تعداد زیاد دستگاه‌های ناامن اینترنت اشیاء به احتمال زیاد حملات شدیدتری رخ خواهد داد.

محقق امنیتی از شرکت F-Secure گفت: «سازمان‌ها باید آمادگی مقابله و کاهش اثرات حمله‌ی منع سرویس توزیع‌شده را داشته باشند و با یک سامانه‌ی پشتیبان بتوانند سرویس‌دهی خود را از سر بگیرند. به‌طور کلی نمی‌توان از حملات منع سرویس توزیع‌شده جلوگیری کرد ولی باید آماده بود و مدت زمان قطعی ناشی از این حمله را کاهش داد. مهاجمان همواره اهداف ضعیف را که آمادگی مقابله با این نوع از حملات را ندارند، انتخاب می‌کنند.»

در طولانی مدت باید راه‌حلی برای باتنت‌های اینترنت اشیاء تنظیم شود. دولت‌ها به دلیل محدود شدن نوآوری‌ها از تنظیم چنین مقرراتی می‌ترسند ولی این تنها راه‌حل ممکن است. چندین سال است که محققان امنیتی در خصوص امنیت دستگاه‌های اینترنت اشیاء هشدار می‌دهند ولی سازندگان این تجهیزات به آن توجهی نکرده و برای بدست آوردن سهم بازار، همچنان محصولات ناامن را روانه‌ی بازار می‌کنند.

این مقررات و تنظیمات در حوزه‌های دیگر مانند سلامت و مهندسی وجود دارد. اینکه شرکت‌های سازنده‌ی تجهیزات اینترنت اشیاء را مسئول ناامنی تجهیزات بدانیم گامی بسیار سخت است. استفاده از گواهی‌نامه‌های امنیتی نیز ممکن است کمک‌کننده باشد ولی به هر حال کافی نیست. اما ممکن است چند جریمه‌ی سنگین برای سازندگان ناامن باعث شود سایر تولیدکنندگان به امنیت تجهیزات خود بیشتر توجه کنند.

در کوتاه مدت خیلی نمی‌توان امیدوار بود که امنیت دستگاه‌های اینترنت اشیاء و تجهیزات شبکه بهبود یابد ولی ارائه‌دهندگان سرویس اینترنت می‌توانند گروه‌های امنیتی خود را برای داشتن شبکه‌ای امن، تقویت کنند.

Expert Bulletin News

Information Communication Technology

2th year 2016 | Weekly bulletin

اخبار فناوری اطلاعات و ارتباطات

هفته نامه | شماره نود و سه | سال دوم | ۶۰ صفحه

خبرنامه هفتگی کارشناسی

مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج