شماره چهارم - اردیبهشت ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

در این شماره خواهید خواند:

کنترل عابر بانک ها به دست هکرها

در این حمله مجرمان سایبری کنترل عابربانک را بدست می‌گیرند و بدافزاری بروی آن نصب می‌کنند - صفحه ۲

ROKRAT

یک ابزار مدیریت از راه دور (RAT) که جدیداً کشف شده از وبسایت های قانونی محبوب برای ارتباطات دستور و کنترلِ (C&C) خود و برای خروج داده ها (exfiltration of data) استفاده می‌کند.- صفحه ۴

- **شبکه‌ی رباتی Sathurbot**

Sathurbot، این تروجان مخفی، از لینک‌های تورنت بعنوان واسطه ی تحویل استفاده می‌کند. به محض شروع ، بدافزار به هدف اطلاع می‌دهد که دستگاه آن‌ها به یک ربات تبدیل شده است - صفحه ۸

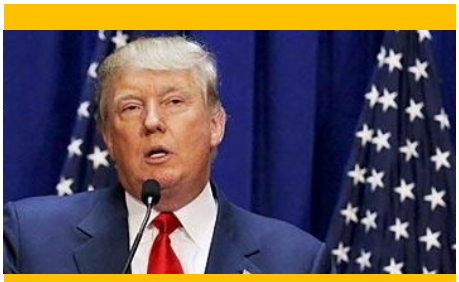
- **حمله PDoS**

پژوهشگران نوع جدیدی از حمله سایبری را شناسایی کردند که به جای به دام انداختن دستگاه های هوشمند در باتنت، موجب آسیب به آنها می شود. محرومیت دائم از سرویس حمله هایی بسیار آسیب زا هستند که در نتیجه ی آنها نیاز به تعویض یا جای گزینی سخت افزار به وجود می آید. - صفحه ۳

TRICKBOT

TrickBot

بررسی‌های بخش X-Force نشان می‌دهد که این بدافزار شباهت بسیار زیادی به بدافزار بانکی Dyre دارد و طیف گسترده‌ای از ویژگی‌ها و کدهایی که در هر دو پلتفرم استفاده شده‌اند.- صفحه ۵



پایان مهلت ۹۰ روزه ترامپ

پایان مهلت ۹۰ روزه ترامپ برای تهیه گزارش ضد هک (امنیت سایبری)، بدون هیچ نشانه‌ای از کار تیمی بر روی این طرح. - صفحه ۴

آسیب پذیری از راه دور بدون احراز هویت!

بیش از نیمی از این آسیب پذیری ها می توانند از راه دور بدون احراز هویت قابل استفاده باشند.- صفحه ۹

آپدیت آسیب پذیری وای فای iOS

نقص مورد نظر یک stack-based bufferoverflow است که به مهاجم اجازه می دهد هر کد دلخواهی را روی wifi chip اجرا کند.-صفحه ۹

بدافزاری که به هکرها اجازه‌ی کنترل عابربانک‌ها را می‌دهد.

این تهدید، بعد از اینکه بانکی روسی هدف حمله قرار گرفت، کشف شد. در این حمله مجرمان سایبری کنترل عابربانک را بدست گرفتند و بدافزاری روی آن فرستادند. با اینکه شاکی پرونده بعد از سرقت، این بدافزار را از بین برد و برای محققین امکان تجزیه و تحلیل را باقی نگذاشت، اما ردپای بدافزار و اسم بعضی از فایل‌ها، بعد از حمله بازیابی شد که امکان تجزیه و تحلیل را به محققان کسپرسکی داد.

فایل‌ها توسط محققان امنیتی ، بازیابی شد (در این جا: C:\Windows\Temp\kl.txtand C:\logfile.txt) و اسامی آن دو فایل قابل اجرا عبارت است از: C:\ATM\!A.EXE و C:\ATM\IJ.EXE البته کسپرسکی به این نکته اشاره کرد که محتوای درون فایلها را نتوانسته اند بازیابی کنند.

برطبق اطلاعات بدست آمده از فایلهای ردپا، محققین، قاعده ای را برای یافتن یک نمونه ساختند و سرانجام یک مورد هم به شکل "tv.dll" پیدا کردند. این به نوبه خود منجر به کشف ATMitch شد، قطعه بدافزاری که در اصل برای هکرها امکان اداره از راه دور عابربانک‌ها را بوجود می‌آورد. آنها بدافزار را نصب می‌کنند و از طریق اتصال از راه دور، آن را اجرا می‌کنند و به عابربانک مربوط به آن بانک دسترسی پیدا می‌کنند. یک مرتبه عامل تهدید در سیستم آلوده شده به دنبال فایل command.txt که در همان آدرس نصب خود بدافزار است، میگردد. چرا که این فایل شامل فهرستی از دستورات حروفی زیر است:

O- ناظر را باز کن.

D- نظارت کن.

I- فایل XFSاولیه.

U- قفل XFSرا باز کن.

S- نصب کن.

E- خارج شو.

G- شناسه ناظر را بگیر.

L- ناسه ناظر را تنظیم کن.

C- لغو کن.

سپس بدافزار، نتایج دستور را در فایل ردپا مینویسد و "command.txt" را از حافظه عابربانک پاک می‌کند. ATMitch که ظاهرا سعی در پنهان کردن خود در سیستم ندارد، از مخزن XFS استاندارد برای کنترل عابربانک استفاده می‌کند، به این معنی است که چنین کاری را می‌توان بر همه عابربانک هایی که از مخزن XFS پشتیبانی می‌کنند انجام داد.

فایل های اجراشدنی A.exe! و IJ.exe که باید نصب کننده و لغونصب کننده‌ی بدافزار باشند، بازیابی نشدند. محققان می‌گویند که "tv.dll" حاوی یک منبع روسی زبان است.

کسپرسکی خاطرنشان می‌کند که این حمله به یک حمله بدون فایل در فوریه ۲۰۱۷ مفصل شرح داده مرتبط است که سازمان‌های زیادی را در سراسر دنیا هدف قرار داد. همانطور که Cisco و FireEye بخوبی توضیح دادند، مورفیسِک ماه گذشته فاش کرد که این حمله به چارچوب حمله‌ایی که در حوادث سریالی دیگر نیز استفاده شده بود گره خورده است.

گردآورنده: حسین علیمرادی

حمله PDoS

پژوهشگران نوع جدیدی از حمله سایبری را شناسایی کردند که به جای به دام انداختن دستگاه های هوشمند در باتنت، موجب آسیب به آنها می شود. محرومیت دائم از سرویس (pdos) حمله هایی بسیار آسیب زا هستند که در نتیجه ی آنها نیاز به تعویض یا جای گزینی سخت افزار به وجود می آید.

محققان Radware دونوع را در ۲۰ مارس سال ۲۰۱۷ مشاهده کردند. یکی از آنها عمر کوتاهی داشت و غیر فعال باقی ماند، در حالی که نوع دیگر مدام کار می کند. اما هر دو هدف مشابهی داشتند: لطمه زدن به دستگاه های هوشمند و خراب کردن storage آنها.

هر دو ربات در تاریخ یکسانی شروع به تلاش های PDoS کردند و این مساله در عرض یک ساعت از هم دیگر کشف شد. با این وجود، در حالی که اولین نوع آن فعالیت شدید در سراسر عمر کوتاه خود نشان داد، دومین نوع آن شدت کمتری نشان داد ولی در حمله ها کامل تر بود و موقعیت خود را با استفاده از TOR مخفی میکند. به منظور لطمه زدن به دستگاه ها، BrickerBot از روش Telnet brute force که قبلا مرتبط به بات نت Maria بود استفاده می کند. این روشی است که از دستگاه های آلوده برای انجام حمله های DDoS سو استفاده می کنند.

درست زمانی که به دستگاه دسترسی پیدا کرد، ربات PDoS مجموعه ای از دستورات را به منظور تخریب sorage اجرا می کند.سپس، اقدام به ایجاد اختلالدر ارتباطات اینترنت وکارایی دستگاه میکند. و بعلاوه اقدام به پاک کردن همه فایل های موجود بر روی دستگاه می کند.

پژوهشگران Radware نشان دادند که: از جمله دستگاه های خاصی که مورد هدف قرار گرفته اند dev/mtd(Memory Technology Device) و dev/mtd (MultiMediaCard) هستند.

این حمله، به طور مشخص دستگاه های اینترنت اشیا مبتنی بر Linux/ BusyBox-based که Telnet port open دارند و به طور علنی در معرض اینترنت قرار گرفته اند را مورد هدف قرار داده است.

اینها یک نمونه از دستگاه هایی هستند که باتنت های اینترنت اشیا مرتبط و maria ورد هدف قرار می دهند.

اقدامات PDoS از تعداد محدودی آدرسهای IP در سراسر جهان آغاز می شود و با همه دستگاه هایی که پورت ۲۲ (SSH) را در معرض قرار می دهند و یک ورژن قدیمی تر از سرور Dropbear SSH را اجرا می کنند، سرو کار دارد. این دستگاهها به عنوان دستگاه های شبکه Ubiquiti شناسایی شده اند.

همچنین پژوهشگران ، نوع دومی از اقدامات PDoS را شناسایی کردند که این اقدامات آدرس های IP منبع خود را در پشت نود های Tor مخفی می کند.

بعلاوه، این حمله ها برای brute-force ورود تلنت با استفاده از نام کاربری و کلمه های عبور root/root and root/vizxv تلاش میکنند و طیف وسیعی از دستگاه های ذخیره سازی را هدف قرار می دهند.

پژوهشگران می گویند این حمله ها از busybox استفاده نمی کنند اما به هر دوی 'dd'و 'cat' دست می زنند ،هرکدام که در دسترس باشد.

همچنین این حمله ها اقدام به پاک کردن default gateway، پاک کردن دستگاه ها و از کار انداختن مهرهای زمانی tcp می‌کنند.

با کمک دستورات اضافی، حمله کننده ها تلاش می کنند تا همه ی قواعد NATو فایروال iptables را flush کنند و قاعده ای اضافه کنند تا همه ی بسته های خروجی را حذف کنند.

گردآورنده: حسین علمیرادی

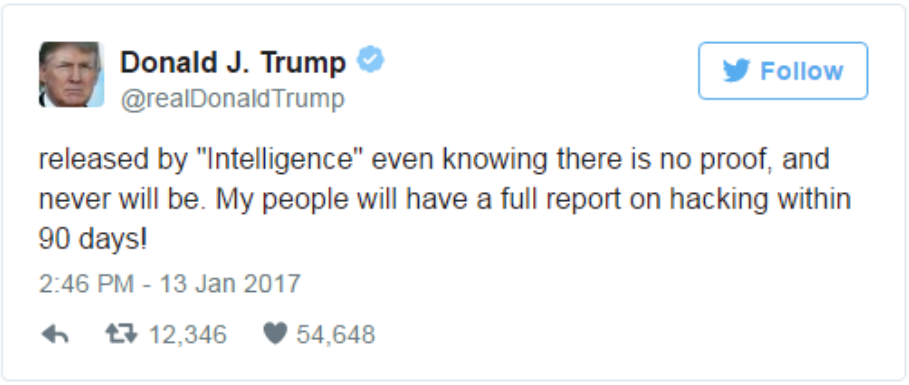
پایان مهلت ۹۰ روزه ترامپ

پایان مهلت ۹۰ روزه ترامپ برای تهیه گزارش ضد هک (امنیت سایبری)، بدون هیچ نشانه-ای از کار تیمی بر روی این طرح.

او ممکن است به دلیل نداشتن درک درست از تکنولوژی مشهور باشد اما در ماه ژانویه، به دنبال دخالت آشکار روسیه در جریان انتخابات آمریکا، دونالد ترامپ برای تعیین یک تیم از کارشناسان حرفه ای برای مقابله با تهدیدات امنیت سایبری ظرف ۹۰ روز وعده داده بود.در حال حاضر، مهلت مورد نظر پایان یافته و هنوزهیچ نشانه ای از برنامه های مرتبط با این وعده مشاهده نشده است.

ترامپ اظهار کرده بود: بهرحال دولت ،سازمان ها، انجمن ها و کسب و کار ما به شدت نیازمند مبارزه و جلوگیری از حملات

سایبری است. من یک تیم منصوب میکنم که ظرف ۹۰ روز طرحی را که در دفتر کارم در موردش صحبت کردم برنامه ریزی کنند .روش ها، ابزار و شیوه های مورد استفاده برای ایمن نگه داشتن امریکا نباید مانند یک بحث عمومی رسانه ای شود تا کسانی که به دنبال آسیب رساندن به ما هستند بهره مند نشوند، ایمنی و امنیت امریکا اولویت شماره یک من خواهد بود



پلیتیکو گزارش میدهد که با پایان یافتن این ۹۰ روز هیچ تیم، برنامه و پاسخ روشنی از کاخ سفید مبنی بر اقدامات انجام شده وجود ندارد.

ترامپ اوایل سال جاری رودی جولیانی را به سمت بالاترین پست امنیت سایبری منصوب کرده بود (با وجود فقدان تجربه لازم در این حوزه)، اما به گفته سخنگوی شهردار پیشین نیویورک او در ۹۰ روز گذشته درگیر تهیه گزارش مورد نظر نبوده است.

این که چه شخص یا سازمانی مسئول این برنامه است مارا دچارسردرگمی کرده است. شورای امنیت ملی آمریکا (NSC) به طور معمول در این گونه مسائل درگیر می شود، اما یک سخنگوی این شورا اظهار بی اطلاعی نموده از اینکه مسئول جمع آوری این گزارش شورای امنیت ملی باشد.

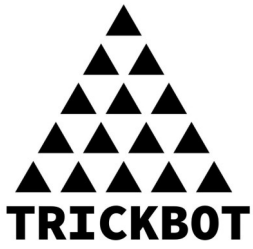
سخنگوی کاخ سفید طی مصاحبه ای با پلیتیکو هیچ توضیحی بابت پایان مهلت مقرر ۹۰ روزه نداد و گفت: رئیس جمهور مجموعه ای از مدیران بخشهای دولتی و خصوصی را منصوب کرده است و آنها قرار است طی یک پروژه مشارکتی بین شورای امنیت ملی و اداره نوآوری آمریکا روی طرح اولیه پروژه امنیت سایبری کار کنند.

از آنجایی که تا کنون هیچ خبری از پیشرفت این طرح منتشر نشده است، به نظر می آید کاخ سفید برای انتشار این گزارش به حداقل ۹۰ روز دیگر احتیاج دارد. ند پرایس که در دوارن ریاست جمهوری اوباما سخنگوی شورای امنیت ملی بوده است در این رابطه می گوید: اگر هنوز هیچ کاری در این رابطه انجام نشده باشد، نباید به این زودیها منتظر انتشار گزارشی دقیق و جامع باشیم.

گردآورنده: سمیه نیا خلیلی

TrickBot

لیمور کسام، مشاور بخش امنیت آی‌بی‌ام در بولتن امنیتی ماهانه آی بی ام نوشت: ‘‘ما انتظار داریم کمپین آلوده سازی و حملات کلاهبردارانه این بدافزار با قدرت زیادی اجرایی شوند؛ حملاتی که عمدتاً حساب های متعلق به کسب وکارها و شرکت ها را نشانه گرفته اند است. TrickBot در سه ماه گذشته و در طول فرایند آزمون و توسعه، مسیر پیشرفت خود را با سرعت زیادی پشت سر گذاشته است. این تروجان مجهز به دو تکنیک فوق پیشرفته است که به منظور دستکاری و ویرایش مرورگرها استفاده می شود. تروجان های بانکی در سال های گذشته به وفور از این تکنیک های ویرایشی استفاده کرده‌اند.“



بررسی‌های بخش X-Force نشان می‌دهد که این بدافزار شباهت بسیار زیادی به بدافزار بانکی Dyre دارد و طیف گسترده ای از ویژگی ها و کدهایی که در هر دو پلتفرم استفاده شده اند، با یکدیگر وجه اشتراک دارند. شواهد این گونه نشان می دهند که TrickBot با حملاتی که بانک های استرالیایی را تحت تأثیر خود قرار داده، در ارتباط است. در این حملات نیز همانند کدهایی که درون بدافزار Dyre استفاد شده اند، از طیف گسترده ای از تکنیک های تزریق کد استفاده شده بود. با این حال، طراحان بدافزار Dyre هم اکنون در زندان روسیه دوران محکومیت خود را پشت سر می‌گذارند

گروه امنیتی X-Force آی‌بی‌ام اعلام کرده است: TrickBot خود را با چند ویژگی جدید وفق داده و اهداف جدیدی برای خود پیدا کرده است. از جمله اهداف این بدافزار می‌توان به سایت‌های شخصی و سایت‌های بانکی تجاری مؤسسات مالی در کشورهای انگلستان، نیوزلند، استرالیا، کانادا و آلمان اشاره کرد. کسام در بخشی از یادداشت خود آورده است: ‘‘هکرهایی که در پس زمینه طراحی TrickBot بودند، در گام نخست تمرکزشان بر حملات تغییر مسیر و تزریق کد سمت سروری بود که تعدادی از سرورهای متعلق به بانک‌ها از آن‌ها استفاده می کردند. اما زمانی که بولتن امنیتی آی‌بی‌ام در ماه نوامبر منتشر شد، مشاهده کردیم که تعدادی از تاکتیک های این بدافزار نیز تغییر کرده است و توسعه دهندگان این بدافزار دو پیکربندی جدید را در اوایل ماه جاری میلادی برای بدافزار TrickBot پایه ریزی کردند.’’ این تغییر تاکتیکی، فراتر از اضافه کردن آدرس های اینترنتی به منظور پیکربندی بدافزار بود؛ روشی که علیه بانک های انگلیسی استفاده شد تا پیاده‌سازی حملات تغییر مسیر سفارشی را امکان‌پذیر سازد، در واقع پیشرفته ترین راهکار برای دستکاری فاکتورهایی به شمار می رود که کاربر در مرورگر خود قادر به مشاهده آن ها است. کسام در بخش دیگری از صحبت‌های خود گفته است: ‘‘تروجان TrickBot بر عکس مشابه خود Dyre، با راه اندازی تبلیغات مخرب، به کارگیری کیت نفوذی RIG، ضمیمه های مخرب ایمیلی و نیز ماکروهای آلوده آفیس، تقویت شده است. این ویژگی های منحصربه فرد نشان می دهند که گروه پشتیبانی کننده این بدافزار حساب های تجاری خاصی را هدف گرفته اند. این گروه هرزنامه‌هایی مشتمل بر بدافزارهای مختلف را برای کمپین ها ارسال می کنند و به ارسال ساده ایمیل های کم دردسر رضایت نمی دهند.

تحلیل های گروه امنیتی آی بی ام نشان می دهد که هکرها فرایند پیشرفت و به روز شدن این بدافزار را به طور مرتب دنبال می‌کنند و تکنیک‌های آلوده‌سازی این تروجان در هر زمانی متفاوت با زمان دیگر است. محتمل ترین نظریه ای که در زمینه تکامل مستمر این بدافزار می توان ارائه کرد، این است که طراحان این بدافزار، شبانه‌روزی در شبکه‌های توزیع‌کننده بدافزارها حضور دارند. این حضور پیوسته نه تنها باعث می‌شود آن‌ها از هرگونه تلاش شرکت های امنیتی باخبر باشند، بلکه به آن‌ها اجازه می‌دهد با هکرهای دیگر در تعامل باشند و سطح دانش خود را ارتقا دهند. نمونه ای از تروجان TrickBot که گروه امنیتی آی‌بی‌ام آن‌ها را بررسی کرده است، مشتمل بر یک دانلودکننده سفارشی موسوم به TrickLoader بوده است. این دانلودکننده پیش تر در روبات هرزنامه ای Cutwall هم استفاده شده بود. به عقیده کارشناسان آی بی ام این دانلودکننده همانند دانلودکننده‌ای است که پیش‌تر گروه Dyre در کمپین هرزنامه‌ای خود از آن استفاده کرده بود.

گردآورنده: حسین علیمرادی

ROKRAT

یک ابزار مدیریت از راه دور (RAT) که جدیداً کشف شده از وبسایت های قانونی محبوب برای ارتباطات دستور و کنترلِ (C&C) خود و برای خروج داده ها (exfiltration of data) استفاده می کند. یکی از محققین به نام Talos در این باره می‌گوید:

این RAT جدید، ملقب به ROKRAT، ابزاری است که از طریق ایمیل و توسط یک HWP توزیع شده است و قربانیان خود را از کره جنوبی انتخاب کرده است. محققان دریافته‌اند که یکی از این ایمیل‌های مخربِ فیشینگ (spear phishing) spear از سرورِ ایمیل Yonsei، دانشگاهی خصوصی در سئول، ارسال شده است. برای مشروعیت بخشی به این ایمیل، مهاجمان از ایمیل ارتباطیِ انجمن جهانی کره به عنوان آدرس فرستنده استفاده کرده‌اند.

این سندِ HWP مخرب شامل یک شیء EPS است که هدف آن اکسپولیت کردنِ یک آسیب پذیریِ شناخته شده (CVE-2013-0808) برای دانلود یک فایل باینری است که خود را در لباسِ مبدلِ یک فایل jpg. نشان می‌دهد. وقتی که فایل رمزگشایی (decoded) و اجرا شد، بدافزار ROKRAT بر روی دستگاه قربانی نصب می‌شود.

این RAT با استفاده از وبسایت هایی چون Twitter، Yandex و Mediafire به عنوان پلتفرم های ارتباطات C&C و خروج (exfiltration)، شناسایی خود را دشوار کرده زیرا نه تنها بلاک کردن این وبسایت‌ها از درون سازمان ها دشوار است، بلکه این سایت ها از اتصال HTTPS استفاده می‌کنند که شناسایی الگوهای خاص را نیز دشوار می‌کند.

Talos در جایی نوشته است: "یکی از نمونه‌های آنالیز شده تنها از Twitter برای تعامل با این RAT استفاده می کند، در حالی که نمونه ی دوم علاوه بر آن از پلتفورم های ابری مثل Yandex و Mediafire نیز استفاده می کند. Twitter tokens که ما قادر به استخراج آن بودیم در هر دوگونه یکسان بود. تلاش های آشکاری برای اضافه کردن امکانات جدیدی به این RAT وجود دارد تا مهاجمان بتوانند سطوح پیچیده تری از حمله به دستگاه های قربانیان را تجربه کنند"

با توجه به تحلیل ها، محققان امنیتی دریافتند که این RAT روی سیستم هایی که از ویندوز XP استفاده می کنند کار نمی کند، زیرا سیستمِ در معرض خطر را برای دنباله ای از ابزارهایی که برای تحلیل بدافزار استفاده می شوند یا در درونِ محیط‌های sandbox چک می‌کند.

برای ارتباطات با پلتفرم‌های C&C، بدافزار از ۱۲ hardcoded tokens (۷ API tokens متفاوت Twitter، ۴ Yandex tokens، و یک اکانت Mediafire) ستفاده می‌کند. این بدافزار آخرین پیام روی تایم‌لاین توییتر را چک می‌کند و همچنین می تواند که خود توییت کند؛ و می تواند فایل ها را دانلود و اجرا کند یا سندهای دزدیده شده را روی حافظه ی ابری Yandex یا Mediafire آپلود کند.

محققان می‌گویند در یکی از نمونه‌ها مشاهده شده که این بدافزار از سیستم ویروسی شده اسکرین‌شات می‌گیرد.

Talos نوشته است که بازیگر این تهاجم یک فرد با انگیزه است. این RAT خلاقانه است و از کانال‌های ارتباطی جدیدی استفاده می‌کند. علاوه بر آن، این بدافزار شامل یک سری قابلیت‌های عجیب و غریب است، مثلا اگر در sandbox اجرا شود این قابلیت را دارد که به سایت‌های قانونی (مثل Amazon و Hulu) درخواست دهد.

Talos این گونه نتیجه‌گیری می‌کند: "بازیگر این حمله یک آدرس ایمیل قانونی از یک انجمن بزرگ که توسط دانشگاهی در سئول اداره می شود، استفاده کرده است تا یک ایمیل spear phishing جعل کند و با این کار شانس موفقیت خود را بالا ببرد. "

گردآورنده: حسین علیمرادی

از همه جای دنیا!!!

شاید برای شمام افتاقا افتاده باشه که انقدر غرق در دنیای کامپیوتر باشید تا وقت رسیدن به ظاهر خودتون رو هم نداشته باشید، اما همه‌ی ما برای روز مصاحبه با ظاهری کاملا آراسته ظاهر میشیم. این اتفاق برای مهندس های کامپیوتر خیلی هم تازه نیست و به شرایط عادت کردن...

مهندسین کامپیوتر

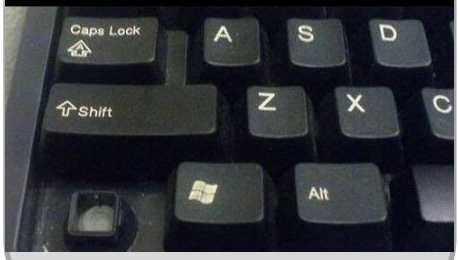
روز مصاحبه

روزهای عادی

یک ایده‌ی خوب برای پرده حمام

در صورت حمله سایبری شیشه را بشکنید و کابل ها را بکشید!!!

وقتی که کنترلمو از دست میدم...



بهترین جا برای پنهان کردن یک جسد، صفحه دوم گوگل است!!!

کیلومتر شمار ماشین یک مهندس شبکه...

گردآورنده: محمد مرتضوی

شبکه‌ی رباتی Sathurbot حسابهای وردپرس را هدف حمله قرار میدهد!

Sathurbot، این تروجان مخفی، از لینک‌های تورنت بعنوان واسطه ی تحویل استفاده می‌کند. وبسایت‌های درمعرض خطر تبدیل به میزبانی برای تورنت‌های تقلبی فیلم و نرم‌افزار می‌شود، هنگامی که یک کاربر برای دانلود فیلم یا نرم‌افزار جستجو می کند، لینک‌هایی که به این وبسایت‌ها متصلند، بجای تورنت‌های مجاز، به کار گرفته می‌شوند. به این دلیل که تورنت ها خوب پخش می‌شوند، احتمالا مجاز بنظر می‌آیند. به دلیل اینکه تورنت فیلم و نرم‌افزار، حاوی یک فایل اجراییست فایل DLL Sathurbot را بارگذاری می‌کند.

به محض شروع ، بدافزار به هدف اطلاع می‌دهد که دستگاه آنها به یک ربات در شبکه‌ی Sathurbot تبدیل شده است. همچنین Sathurbot کنترل و دستور (C&C) خود را در آغاز کار بازیابی می‌کند. ارتباط با سرور، شامل گزارش وضعیت، بازیابی وظایف، و دریافت لینک‌هایی برای دانلود بدافزارهای دیگر می‌شود.

محققان امنیتی ESET هشدار می‌دهند که: "Sathurbot می‌تواند خود را به روزرسانی کند و فایل اجرایی دیگری را آغاز کند. ما انواع Boaxxe، Kovter و Fleercivet را دیده‌ایم ولی این فهرست کاملی نیست".

بدافزار، نصب موفق خود را به سرور گزارش می‌دهد و همچنین حین انتظار برای وظایف اضافه، مرتبا گزارش ارسال می‌کند.

Sathurbot با مجموعه‌ای حاوی بیش از ۵۰۰۰ کلمه‌ی اصلی می‌آید تا بتواند با تلفیق تصادفی، عبارات دو سه کلمه‌ای بسازد تا از آنها بعنوان رشته‌های پرسیدنی از طریق موتورهای جستجوی محبوب، استفاده کند. سپس قطعه‌ای دو تا چهار کلمه‌ایِ تصادفی را از صفحه‌ی هرکدام از آدرس‌های منتج انتخاب می‌کند، و از آن برای چرخه‌ی بعدیِ جستجو استفاده می‌کند. مجموعه نتایج جستجوی بعدی، اسامی دامنه را بدست می‌دهد.

این تهدید، فقط دامنه‌هایی را انتخاب می‌کند که با استفاده از وردپرس ساخته شده‌اند، اما بنظر می‌رسد که این تهدید، به Drupal، Joomla، PHP-NUKE، phpFox و DedeCMS نیز علاقمند است. بدافزار، دامنه‌های حاصل شده را به C&C می‌فرستد.

سپس ربات، فهرستی از اعتبارات دسترسی به دامنه را - که به این شکل درآمده اند login:password@doamin - دریافت می‌کند که احتمالاتی برای دسترسی می‌دهند. رباتهای مختلف، از اعتبارات ورودی مختلفی برای یک سایت یکسان استفاده می‌کنند. بعلاوه، برای جلوگیری از قفل شدن، هر ربات فقط یک اطلاعات ورودی(لاگین) را برای هر سایت امتحان می‌کند و به دامنه ی بعدی می‌رود.

ESET فاش کرد: "حین آزمایش ما، فهرست ۱۰ هزار احتمال توسط C&C بازگردانده شد". آنها همچنین به این نکته اشاره کردند که رابط برنامه نویسی کاربردی XML-RPC از وردپرس - بخصوص رابط wp.getUsersBlogs - در این حمله استفاده شد.

این ربات همچنین دارای کتابخانه ی یکپارچه شده‌ی libtorrent است و برای تبدیل شدن به یک seederبا استفاده از دانلود یک جفت فایل و تولید تورنت، طراحی شده است. گرچه، ظاهرا همه ی ربات‌های موجود در شبکه، تمام این وظایف را انجام نمی‌دهند، چنانکه تعدادی از آنها بعنوان خزنده‌های وب استفاده می‌شوند، بقیه فقط به رابط‌های XML-RPC حمله می‌کنند، و بعضی نیز هردو را انجام می‌دهند. همه ی ربات‌ها نیز seeder نمی‌شوند.

محققان امنیتی توضیح می دهند که: " اقدامات مذکور روی wp-login.php/ از بسیاری از کاربران، حتی در سایت‌هایی که میزبان وردپرس نیستند، تأثیر مستقیم Sathurbot است. بسیاری از مدیران سایت‌ها چنین اتفاقاتی را مشاهده می‌کنند و تعجب می‌کنند که چرا رخ می‌دهد. بعلاوه، سایت‌های وردپرس می‌توانند پتانسیل حمله را بر wp.getUsersBlogs در لاگ‌هایشان ببینند"

با شمول بیش از ۲۰هزار رایانه‌ی آلوده، گفته می‌شود که Sathurbot از ژوئن ۲۰۱۶ فعال شده است.

گردآورنده: حسین علیمرادی

آسیب پذیری از راه دور بدون احراز هویت!

بیش از نیمی از این آسیب پذیری ها می توانند از راه دور بدون احراز هویت قابل استفاده باشند. ۴۰ مورد از این مسائل بسیار مهم محسوب می شدند و ۲۵ مورد از آنها نمره CVSS، ده داشتند.

برنامه های "سرویس های مالی" اوراکل تحت تاثیرترین محصول بود، اصلاحاتی برای ۴۷ امکان آسیب پذیری در این ماه دریافت کردند که ۱۹ تا از آنها با نمره CVS ده بسیار مهم محسوب می شدند. بعلاوه Advisory اوراکل فاش کرد ۲۵ مورد از این ۴۷ قابلیت آسیب پذیری بدون احراز هویت و از راه دور می توانستند قابل استفاده باشند.

آخرین CPU اوراکل که در این هفته منتشر شد قابلیت آسیب پذیری در۲۵ برنامه را مورد ملاحضه قرار داد:

MySQL و Retail Applications(هر یک ۳۹ اصلاح)، Fusion Middleware (31)، Sun Systems Products Suite (21)، PeopleSoft (16)، Virtualization (15)، Berkeley DB (14)، Support Tools (13)، E-Business Suite (11)، Communications Applications (11)، Java SE (8)، Utilities Applications (7)، Primavera Products Suite (7)، Hospitality Applications (6)، Commerce (3)، Database Server (2)، Enterprise Manager Grid Control (2)و Secure Backup، Hyperion، Supply Chain Products Suite، JD Edwards Products، Siebel CRM Health Sciences Applications، MySQL Enterprise Suite، Monitorاز Oracle MySQL (Struts 2)، Oracle FLEXCUBE Private Bankingاز Oracle Financial Services Applications (Struts 2)، Oracle Financial Services Asset Liability Managementاز Oracle Financial Services Applications (Struts 2)و Oracle Financial Services Data Integration Hub از Oracle Financial Services Applications (Struts 2) مورد توجه قرار داده است.

و Insurance Applications (هر کدام یک اصلاح).

مهمترین مسائل مورد ملاحظه قرار گرفته مربوط به نقص اجرای راه دور کد در Apache Struts 2 است که ماه گذشته پس از این که شخصی یک کد مخرب PoC را منتشر کرد، مشخص شد در دنیای واقعی مورد استفاده قرار گرفته بود. همچنین محصولات Cisco و VMWare تحت تاثیر قرار گرفته بودند.

الکساندر پلیاکف مدیر ارشد فناوری در ERPScan می گوید : جرایم رایانه‌ای همیشه یک کسب و کار سودآور بوده اند. این روزها ، هکرها بیشتر روی سازمان ها متمرکزند تا افراد زیرا انها دریافته اند که سازمان ها سودآورتر هستند. در نظر بگیرید که محصولات اوراکل در بزرگترین سازمان ها نصب شده اند، این برنامه ها می توانند هدف نهایی باشند. خبر خوب این است که فروشندگان قبل از این که نفوذ در داده جدی رخ دهد توجهشان را به این ناحیه حیاتی جلب کرده اند. خبر بد این است که ادمین های اوراکل مدت طولانی روی نصب پچ های فراوان کار خواهند کرد.

اوراکل باگ های مهمی را در Solaris از Oracle Sun Systems Products

CPU جولای ۲۰۱۶ با ۲۷۶ پچ نخستین CPU بود که شامل بیش از ۲۵۰ اصلاح بود، اما از آن زمان این روند هر فصل ادامه پیدا کرد با ۲۵۰ نقص مورد توجه قرار داده شده در اکتبر ۲۰۱۶ و ۲۷۰ نقص در ژانویه ۲۰۱۷.

همچنین انتظار می رود این روند در فصل پیش رو نیز ادامه پیدا کند. به هر حال چون این مساله با همه نرم افزار اتفاق می افتد، این به معنای این نیست که برنامه ها آسیب پذیرتر شده اند بلکه جامعه محققان در یافتن مسائل امنیتی بهتر شده اند.

گردآورنده: محمد مرتضوی

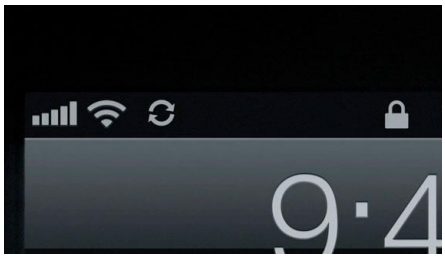
آپدیت آسیب پذیری وای فای iOS

با توجه به گزارش Tech giant، نقص مورد نظر یک stack-based bufferoverflow است که به مهاجم اجازه می دهد هر کد دلخواهی را روی wifi chip اجرا کند.

این باگ امنیتی، با شناسه CVE-2017-6975، از طریق اعتبارسنجیِ ورودیِ بهبودیافته - improved input validation - به همراه انتشار iOS 1.3.1 آمده است. این آپدیت برای آیفون ۵ و بعد از آن، آی پد لمسی نسل ۶ و بعد از آن، و آی پد نسل چهارم و بعد از آن در دسترس است.

to5mac ۹ گزارش کرد در حالی که iOS 10.3 پشتیبانی از دستگاه های۳۲ بیتی را قطع کرده است، آپدیتِ جدید پشتیبانی برای این سیستم ها را دوباره معرفی کرده است.

این آسیب پذیری توسط Gal Benamini از Google Project Zero شناخته و گزارش شده است. Google Project Zeroمعمولا جزییات نقص هایی که توسط محققانش پیدا می شود را بعد از ۹۰ روز افشا می کند.



در راهنمای امنیتی که اپل ارائه کرده است، به کاربران خود توصیه کرده است که در صورت امکان این آپدیت را فورا نصب کنند و همچنین اشاره کرده است که این آپدیت تنها از طریق iTunes و Software Update utility بر رو دستگاه های iOS در دسترس است؛ این آپدیت در سایت دانلودهای اپل - Apple Download Website - یا اپلیکیشن کامپیوتری Software Update نشان داده نمی شود.

iOS 10.3.1 تنها یک هفته پس از اینکه اپل دسترسی عمومی iOS 10.3 را اعلام کرد، منتشر شد. iOS 10.3 بسیاری از ویژگی ها و patchهای جدید برای حدود ۹۰ آسیب پذیری را در بر دارد که در حدود ۳۰ تا از این باگ های امنیتی توسط محققان Google Project zero به اپل گزارش شده است.

گردآورنده: محمد مرتضوی

Kharazmi CERT Coordinator Center

مرکز آپا دانشگاه خوارزمی

مدیر مسئول:

دکتر امید مهدی عبادتی

هیات علمی:

دکتر احسان ملکیان

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن یزدی نژاد

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

وب سایت:

http://cert.khu.ac.ir/