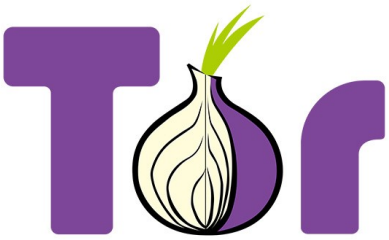
شماره بیست و نهم - خرداد ۱۳۹۸

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:



حملات DDOS به سایت‌های Onion

چندی پیش سرویس تور در برخی از مناطق با مشکل مواجه شده بود. آسیب پذیری تور سال ها مورد سواستفاده، خرابکاری و اخاذی از سایت‌های Onion قرار گرفته است. - صفحه ۲

ردیابی گوشی‌ها با بلوتوث متصل!

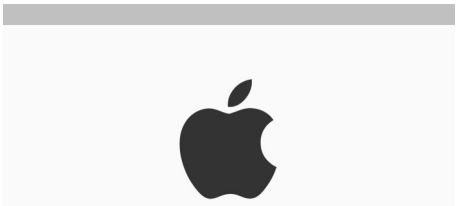
بلوتوث امواج نامرئی است که میلیون‌ها وسیله با یکدیگر را متصل می‌کند. بنابراین آسیب پذیری و یا حضور یک باگ برروی شمار زیادی از مشتریان نا آگاه تاثیر می‌گذارد و باعث می‌شود تا هکرها اطلاعات افراد آسیب پذیر را به راحتی به سرقت ببرند. - صفحه ۵

Godlua، اولین بدافزار شناخته شده DNS

یک Backdoor در Lua نوشته شده است که از DoH پروتکل برای ترویج DNS خود استفاده می‌کند. محققان در آزمایشگاه تحقیقات امنیت شبکه اولین بدافزار شناخته شده را که از پروتکل DNS توسط پروتکل HTTPS استفاده می کنند، را کشف کردند. که نام این بدافزار Dubbed Godlua، می باشد - صفحه ۳

نرم افزار SupportAssist دارای نقص امنیتی "شدید" است!

مشتریان Dell ممکن است در معرض خطر باشند. بر اساس تحقیقات امنیتی شرکت SafeBreach Labs، یک نقص در نرم افزار SupportAssist کشف شده است، که یک چک کننده سلامت برای سیستم-های Dell می‌باشد که از پیش نصب شده است - صفحه ۶



اپل برنامه‌های Walkie Talkie را غیرفعال می‌کند!

مثل اینکه مشکلات شنود و استرق سمع کاربران در سال ۲۰۱۹ برای اپل کم کم به یک مشکل جدی تبدیل شذده است. این دومین اشکال استعماری است که اپل در سال جاری با آن روبرو شده است. اپل بعد از متوجه شدن این آسیب پذیری برنامه Walkie Talkie را برای ساعت اپل غیر فعال کرد این آسیب پذیری می‌تواند برای استراق سمع دستگاه مورد نظر اجازه استفاده و دسترسی از راه دور دهد. - صفحه ۴

پرداخت هزینه‌ی شهر فلوریدا به هکرها!

شهر فلوریدا موافقت خود را برای پرداخت هزینهٔ به هکرها به مبلغ ۶۰۰۰۰۰ دلار برای باز کردن داده های خود اعلام کرد. - صفحه ۷

حملات DDOS به سایت‌های Onion.

چندی پیش سرویس تور در برخی از مناطق با مشکل مواجه شده بود. آسیب پذیری تور سال ها مورد سواستفاده، خرابکاری و اخاذی از سایت‌های Onion قرار گرفته است.

پروژه Tor آماده اصلاح یک اشکال است که برای سال های گذشته مورد سوء استفاده قرار گرفته است تا حملات انکار سرویس توزیع شده (DDoS) را علیه سایت های Darkweb انجام دهد.

اما چگونه حمله DOS بر روی سایت های دارک وب کار می کند؟

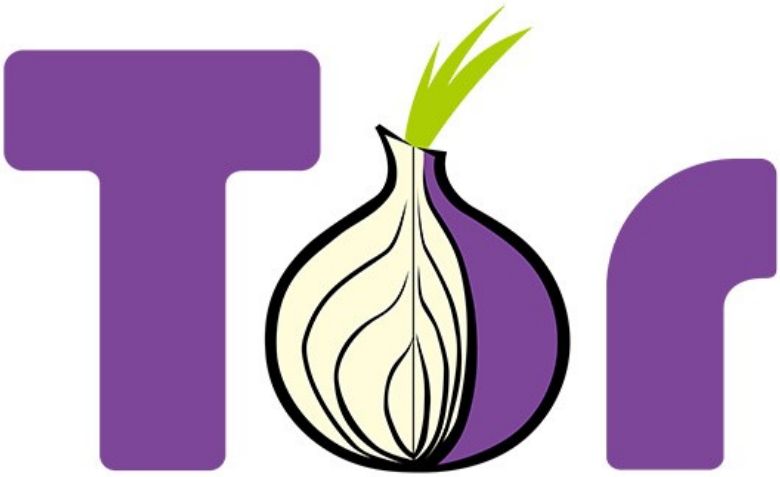
به طور خلاصه در یک توضیح ساده که در طی این اشکال، مهاجم می تواند هزاران اتصال به یک وب سایت هدفمند میزبانی شده Onion در DarkWeb را آغاز کند، و اتصالات به وب سرور را متوقف کند.

برای هر ارتباط، سرویس پیگیری از راه دور بایستی یک مسیر پیچیده از طریق شبکه Tor را در نظر بگیرد و بسته ها را به مقصد برساند و این سرویس ارتباط بین کاربر و سرور آن را تأمین می کند

حالا با علم به این عمیل می توان در خواست جعلی در شبکه تور ساخت و به سمت سایت مقصد فرستاد. این فرآیند CPU را شدیدا درگیر میکند و با اتصالات کافی، پردازشگر سرور در ۱۰۰ حداکثر توان قرار میگیرد و نمی تواند اتصالات جدید را بپذیرد.

این یک اشکال قدیمی است که به مدت طولانی برای توسعه دهندگان Tor شناخته شده است، اما به دلیل کمبود نیروی انسانی مرتفع نشده است، زیرا این اشکال فرآیند مشابهی را که ، برای ایجاد یک اتصال کاربر مشروع باید اتفاق افتد را دارد.

هیچ روش قابل قبولی برای شناسایی اینکه آیا درخواست های اتصال ورودی از یک مهاجم است یا یک کاربر قانونی است وجود ندارد تا زمانی که ارتباط برقرار شود که در آن لحظه،دیگر خیلی دیر است.



گردآورنده: امیرحسین ضرغامی

Godlua، اولین بدافزار شناخته شده DNS

یک Backdoor در Lua نوشته شده است که از DoH پروتکل برای ترویج DNS خود استفاده می‌کند.

محققان در آزمایشگاه تحقیقات امنیت شبکه اولین بدافزار شناخته شده را که از پروتکل DNS توسط پروتکل HTTPS استفاده می کنند، را کشف کردند. که نام این بدافزار Dubbed Godlua، می باشد

اواخر ماه اکتبر، نیروی کاری مهندسی اینترنت به طور رسمی پروتکل DoH را به تصویب رساند، که به عنوان RCF 8484 منتشر شد

محققان Netlabیک فایل ELF مشکوک را کشف کردند، که در ابتدا به نظر می رسید یک تروجان cryptocurrency است.

در حالی که محققان هر گونه معادله ی cryptocurrency را تایید یا رد نکرده اند،بلکه آنها تأیید کرده اند که شبیه یک ربات DDoS است.

محققان متوجه شده اند که این فایل به عنوان یک Backdoor مبتنی بر Lua در سیستم های آلوده عمل می کند و حداقل یک حمله DDoS علیه آن اعمال می کند

تا به حال، محققان حداقل دو نسخه از ویتنام کشف کرده اند،که هر دو با استفاده از سواستفاده DNS جعلی بیش از درخواست

HTTPS به جای یک درخواست ازDNS سنتی استفاده می‌کنند.

سوء استفاده از تروجان می تواند ترافیک DNS خود را از طریق یک اتصال HTTPS رمزگذاری شده را مخفی کند، به این ترتیب اجازه می دهد Godlua از نظارت DNS منفعل جلوگیری کند

هر دو گوگل و موزیلا از پروتکل DoH حمایت کرده اند. موزیلا در حال حاضر DoH را آزمایش می کند، و گوگل هم اکنون بخشی از سرویس DNS عمومی خود را ارائه می دهد. شبکه های تحویل محتوا مانند Cloudflare همچنین DNS resolution over HTTPS را ارائه می دهند.

گردآورنده: امیرحسین ضرغامی

اپل برنامه‌های Walkie Talkie را غیرفعال می‌کند!

مثل اینکه مشکلات شنود و استرق سمع کاربران در سال ۲۰۱۹ برای اپل کم کم به یک مشکل جدی تبدیل شذده است. این دومین اشکال استعماری است که اپل در سال جاری با آن روبرو شده است.

اپل بعد از متوجه شدن این آسیب پذیری برنامه Walkie Talkie را برای ساعت اپل غیر فعال کرد این آسیب پذیری می‌تواند برای استراق سمع دستگاه مورد نظر اجازه استفاده و دسترسی از راه دور دهد.

برنامه Walkie Talkie سال گذشته با عرضه WatchOS 5 معرفی شد. این نرم افزار قابلیت ارتباط و گفتار را ارائه می‌دهد.

در اظهاراتی که به TechCrunch ارائه شده، اپل اعلام کرد که در شرایط خاص به دنبال رویدادهایی ممکن است موجب شود کسی بدون آگاهی از طریق آیفون دیگری مورد شنود قرار گیرد.

اپل برای این مشکل عذرخواهی کرد و گفت که در حال کار برای حل این مشکل می باشد.

اپل برنامه Walkie-Talkie را از روی دستگاه‌ها حذف کرد، تا زمانی که آسیب پذیری را رفع و دوباره این برنامه را فعال کند.

این مورد شبیه آسیب پذیری face time نیز بود که در ماه ژانویه، یک اشکال FaceTime کشف شد که کاربران قبل از پاسخ به تماس میتوانستند شخص را در یک تماس ببینند و صدای وی را شنود کنند.

باگ Face Time مربوط به ویژگی تماس گروهی که در سال ۲۰۱۸ توسط اپل رو نمایی شد بود که قابلیت سوء استفاده از آن از طریق مخاطبین iOS بود. برای سوء استفاده از این باگ تنها کافی بود تا صفحه از پایین به بالا بدهید و برروی دکمه‌ی Add Person بزنید، سپس در صفحه‌ی باز شده شماره‌ی خود را وارد نمایید. با اینکار تماس Face Time آغاز می گردید و میکرفون دریافت کنندگان تماس را پیش از پاسخ دادن آنان بتوانید شنود کنید.

تا لحظه‌ی نشر این خبر هنوز از فعال شدن این برنامه خبری نشده است.

گردآورنده: امیرحسین ضرغامی

ردیابی گوشی‌ها با بلوتوث متصل!

بلوتوث امواج نامرئی است که میلیون‌ها وسیله با یکدیگر را متصل می‌کند. بنابراین آسیب پذیری و یا حضور یک باگ برروی شمار زیادی از مشتریان نا آگاه تاثیر می‌گذارد و باعث می‌شود تا هکرها اطلاعات افراد آسیب پذیر را به راحتی به سرقت ببرند.

مهندسین دانشگاه بوستون به تازگی با یک بررسی گسترده در پیاده سازی بلوتوث متوجه شده‌اند که هرکسی امکان ردیابی و شناسایی دیگران را از طریق بلوتوث دارا می‌باشد.

تمامی محصولات شرکت‌هایی همچون اپل و مایکروسافت شامل این نقص امنیتی می‌باشند. همچنین وسایل و گجت‌ها پوشیدنی نیز مانند بند Fitbit از این قاعده مستثنی نیستند.

این آسیب پذیری در خلال بررسی پروتکل‌های وسایل IoT برای تحلیل خطرات نقص حریم خصوصی توسط تیم امنیتی David Starobinski کشف گردیده است. یکی از یافته‌های آنان مربوط به نحوه جفت شدن دستگاه های بلوتوثی با یکدیگر است. برای انجام این کار، آنها باید یک سلسله مراتب را ایجاد کنند که در آن یکی نقش اصلی را بازی کند و دیگری محیطی است تا بتوانند مبادله اطلاعات را شروع کند.

محیط - مثلا یک جفت هدفون - باید هویت خود را (یک آدرس منحصر به فرد) بفرستد تا دستگاه مرکزی - تلفن شما - بتواند در مورد حضور و موجود بودن آن برای یک اتصال، که همراه با برخی اطلاعات دیگر است تصمیم گیری نماید.

بیشتر وسیله‌ها به گونه‌ای تنظیم شده‌اند که در هر بار آدرسی تصادفی ارسال کنند که برای ارتقای امنیت و حریم خصوصی این آدرس به صورت دوره‌ای تغییر می‌کند. اما محققان امنیتی متوجه شده‌اند که Payload موجود همچنان کارایی خود را دارد و یک الگوریتم شنود ساده نیز می‌تواند این اطلاعات را به عنوان یک شناسه منحصر به فرد مورد استفاده قرار دهد.

جالب توجه است که دستگاه‌های اندرویدی از این اکسپلویت تحت تاثیر قرار نمی گیرند، زیرا هیچ نشانه شناسایی را پخش نمی‌کنند.

در هر حال، محققان در خصوص این آسیب پذیری در ماه نوامبر سال گذشته به اپل و مایکروسافت هشدار داده‌اند اما نمیدانیم که در حال حاضر این آسیب پذیری رفع گردیده است یا خیر. در هر صورت شما می‌توانید با یکبار خاموش و روش کردن بلوتوث دستگاه خود از این مشکل جلوگیری کنید.

با اینکه از سال ۲۰۱۹ تا ۲۰۲۲ تعداد دستگاه‌های بلوتوث دار از ۴.۲ به ۵.۲ میلیون خواهد رسید اما در هر صورت نیاز نیست تا در خصوص این آسیب پذیری خیلی نگران باشید زیرا تولید کنندگان تلاش می‌کنند تا در نسل‌های جدیدتر همواره موارد امنیتی را در نظر بگیرند از طرفی هم برای ردیابی افراد راه‌های بیشتری از بلوتوث وجود دارد.

گردآورنده: محمد مرتضوی

نرم افزار SupportAssist دارای نقص امنیتی "شدید" است!

مشتریان Dell ممکن است در معرض خطر باشند. بر اساس تحقیقات امنیتی شرکت SafeBreach Labs، یک نقص "شدید" در نرم افزار SupportAssist کشف شده است ، که یک چک کننده سلامت برای سیستم های Dell می باشد که از پیش نصب شده است، این نرم افزار دستگاه شما را برای مشکلات نرم افزاری یا سخت افزاری اسکن می‌کند و اطلاعات را برای رفع عیب به Dell منتقل می‌کند.

SupportAssist نیاز به سطوح بالای مجوز برای کار کردن دارد، به این معنی که هر آسیب پذیری که از طریق این شکاف که ایجاد می شود خطرناک‌تر می‌شود.

این نقص امنیتی در این هفته با شناسه CVE-2019-12280 در دسترس می‌باشد. این نقص به بد افزار امکان ورود به سیستم قربانی و افزایش سطح دسترسی خود را به Admin می‌دهد.

نقص امنیتی چیست؟ ظاهرا، الزامات اجازه پشتیبانی SupportAssist به خوبی با شیوه اساسی عملکرد نرم افزارها ارتباطی ندارد: فایل‌های DLL آن از یک پوشه محافظت نشده بارگیری می‌شود. یعنی هکر ها می‌توانند DLL های واقعی SupportAssist را با بدافزارها مبادله کنند و با استفاده از مجوزهای بالا موجب خرابکاری در دستگاه قربانی می‌شوند.

خوشبختانه تلاش‌های این سازمان بیهوده نبود. Dell قبلا پچ‌های این آسیب پذیری را صادر کرده است که اکنون در دریافت های پشتیبانی OfficialAssist موجود است.

این نقص امنیتی شامل ورژن ۲.۰ و ورژن ۳.۲.۱ این نرم افزار می‌باشد. شرکت Dell همواره کاربران خود را تشویق می‌کند تا به محض امکان نرم افزارهای خود را به روز رسانی نمایند و همواره از آخرین ورژن آن استفاده نمایند.

آپدیت خودکار به صورت پیش فرض همیشه فعال می‌باشد اما اگر در هر صورتی به مشکلی در به روز رسانی برخورد کردید بهتر است به سایت زیر مراجعه نمایید و به صورت دستی آپدیت‌ها را دریافت و به روز رسانی را انجام دهید تا از خطر تهدیدات این چنینی در امان باشند.

https://www.dell.com/support

گردآورنده: امیرحسین ضرغامی

پرداخت هزینه‌ی شهر فلوریدا به هکرها!

شهر فلوریدا موافقت خود را برای پرداخت هزینهٔ به هکرها به مبلغ ۶۰۰۰۰۰ دلار برای باز کردن داده های خود اعلام کرد.

اغلب توصیه می شود که برای باز کردن فایل های قفل شده توسط باج افزارها پرداختی انجام ندهید، معمولا هکرها مجبور نیستند تضمین کنند که به قربانیان کلید قفل را ارسال کنند. اما شورای شهر فلوریدا قرار است بیش از ۶۰۰،۰۰۰ دلار را در امید بازگشت داده‌ها که بیش از سه هفته است که رمزگذاری شده است به هکر ها پرداخت کند. این در حالی است که بررسی‌های صورت گرفته از سوی آنان نشان می‌دهد که این بار پرداخت این هزینه برای آنان بسیار به صرفه-تر از دست رفتن اطلاعاتشان می‌باشد.

حمله به Riviera Beach، فلوریدا، یک شهر کوچک در شمال غرب پالم بیچ، در ۲۹ ماه مه آغاز شد، زمانی که یک کارمند اداره پلیس یک پیوست ایمیل را که حاوی ransomware بود باز کرد. آن را به سایر سیستم‌های فناوری اطلاعات گسترش داد و وب سایت شهر، سرور ایمیل، سیستم صدور صورت حساب و غیره قفل شد و تمامی اطلاعات داخل آن رمز شد.

در ۳ ژوئن، مقامات شهر موافقت کردند که ۹۴۱،۰۰۰ دلار صرف بازسازی سیستم‌های IT خود صرف کنند حدود ۳۱۰ کامپیوتر جدید و ۹۰ لپ تاپ.

یک رایزنی در شورا انجام گرفت که در آن شرکای بیمه به پرداخت ۶۵ بیت کوین، حدود ۵۹۲،۰۰۰ دلار به هکرها موافقت کردند.

گردآورنده: امیرحسین ضرغامی

KHARAZMI CERT COORDINATOR CENTER

مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

امیرحسین ضرغامی

محسن یزدی‌نژاد

فاطمه الهی

نشانی:

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

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

https://cert.khu.ac.ir/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.