بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره هجدهم

اسفند ماه ۱۳۹۸

شعله‌ور شدن آتش زیر خاکستر در وب‌سرورهای Apache-Tomcat!

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:
مرکز تخصصـــی آپـا دانشگـاه رازی

صفحه آرایی: **سید احسان حسینی**

سردبیران:
سیده مرضیه حسینی
صبا آزرمی

با همکاری
سیده آرزو حسنی

آدرس:
کرمانشـــاه، باغ ابریشـــم، دانشـــگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

۰۸۳۳۴۳۴۳۲۵۱
apa@razi.ac.ir
@APARazi
cert.razi.ac.ir

اخبار امنیتی

حملات جدید IMPersonation در شبکه‌های 4G

محققان شکل جدیدی از حملات IMPersonation را در شبکه‌های 4G LTE به نام IMP4GT کشف کرده‌اند که به مهاجمان اجازه می‌دهد تا با استفاده از فقدان حفاظت یکپارچگی برای داده‌های کاربر و تزریق پکت‌های مخرب دلخواه از طریق جعل هویت قربانیان، آن را اکسپلویت نمایند.

4G Long Term Evolution (LTE)، جدیدترین استاندارد ارتباطی تلفن همراه است که به طور گسترده و توسط صدها میلیون نفر در سراسر جهان برای دسترسی به اینترنت پر سرعت مورد استفاده قرار گرفته است.

حملات IMP4GT (حملات IMPersonation در شبکه‌های 4G)، در شبکه LTE می‌تواند از مکانیسم بازتاب پشته IP سیستم‌عامل تلفن همراه سوء استفاده کرده و پکت‌های دلخواه را تزریق نماید و نیز به پی‌لود[1] پکت‌های موجود دسترسی پیدا کند.

پروتکل IPV4 در سیستم‌عامل اندروید و IPV6 در هر دو سیستم‌عامل اندروید و iOS، در برابر حملات IMP4GT آسیب‌پذیر هستند و همچنین این حمله بر تمام دستگاه‌هایی که LTE در آنها فعال شده است، تأثیرگذار خواهد بود. از جمله: تلفن‌های همراه، لپ‌تاپ‌ها، تبلت‌ها و غیره.

انواع حملات جعل هویت

محققان از دو حمله متفاوت در یک شبکه تجاری LTE برای شکستن فرآیند احراز هویت دوطرفه و انجام حملات جعل هویت به کمک srsLTE پشته نرم‌افزار LTE توسط Software Radio System استفاده کردند:

- جعل هویت Uplink
- جعل هویت Uplink

در جعل هویت Uplink، این حمله به مهاجمان اجازه می‌دهد تا قربانیان را به سمت شبکه‌ها بکشانند و از سرویس‌های IP دلخواه مانند وب سایت ها با هویت قربانیان استفاده کنند.

در طی این حمله، تمام ترافیک ایجاد شده توسط مهاجم با آدرس IP قربانی در

[1] payload

در ارتباط است.

در جعل هویت Downlink مهاجم می‌تواند یک اتصال TCP/IP با تلفن همراه برقرار کند که از مکانیسم هر فایروال شبکه LTE عبور می‌کند. مهاجم قادر به شکستن هیچ مکانیسم امنیتی بالاتر از لایه IP نیست.

در نتیجه، مهاجم می‌تواند هر مجوز، accounting یا فایروال را دور بزند. محققان آزمایشاتی را برای اثبات فرضیه‌های خود و نشان دادن امکان حمله IMP4GT در دنیای واقعی در یک مجموعه واقعی انجام می‌دهند. در نتیجه، آنها می‌توانند به یک سایت سرویس دهنده که فقط باید توسط کاربر قابل دسترسی باشد، دسترسی پیدا کنند و یا فایروال را دور بزنند.

مهاجم می‌تواند قربانی یا شبکه را در لایه IP جعل هویت کند، بدین معنی که ارسال و دریافت پکت‌های IP با هویت سرقت شده امکان‌پذیر است. با این حال، مهاجم نمی‌تواند به حساب کاربری ایمیل یا پیام‌رسان‌های شخصی دسترسی پیدا کند، تماس تلفنی برقرار کند و یا رمزگذاری TLS را بشکند.

تمامی شبکه ها به یک اندازه در برابر این حمله آسیب‌پذیر هستند و انتظار می‌رود این آسیب پذیری در شبکه‌های 5G رفع گردد.

منبع خبر :

https://gbhackers.com/imp4gt-a-impersonation-attacks/

Scan Link

انتشار نسخه جدید بدافزار Android.Xiny اندروید

محققان موفق به کشف موج جدیدی از حملات WiFi Spreader از خانواده بدافزار Emotet شدند.

تروجان بانکی Emotet نخستین بار توسط محققان امنیتی در سال 2014 کشف و گزارش شد. Emotet در اصل یک بدافزار بانکی بود که با نفوذ به سیستم قربانی، اطلاعات شخصی و حساس قربانی را به سرقت می‌برد.

ماه گذشته نیز، خبر استفاده این بدافزار از یک روش جدید منتشر شد. روش جدید مورد استفاده Emotet به بدافزار اجازه می‌دهد تا شبکه‌های WiFi آسیب‌پذیر و ناامن محلی و دستگاه‌های متصل به آن را با استفاده از حلقه‌های brute-force آلوده کند. در این روش جدید، از رابط wlanAPI برای شمارش تمام شبکه‌های Wi-Fi در آن منطقه و انتشار بدافزار استفاده می‌شد. کتابخانه wlanAPI، یکی از کتابخانه‌های استفاده شده در رابط برنامه‌نویسی نرم‌افزار wifi محلی است (API) که مشخصات شبکه‌های بی‌سیم و اتصالات آن را مدیریت می‌کند.

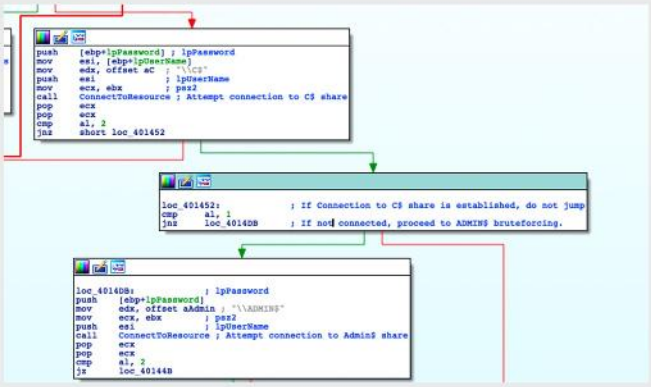
هم‌اکنون، محققان نسخه بروز شده WiFi Spreader را شناسایی کرده‌اند که این نسخه، از یک برنامه مستقل درون ماژولی تکامل یافته از بدافزار Emotet با برخی تغییرات عملکردی، برای بروزرسانی و تغییر نسخه پیش، استفاده کرده است.

تغییرات نسخه جدید

مهاجمان بدون تغییر در عملکردهای کلیدی این بدافزار، تغییرات جدیدی را در ماژول WiFi Spreader اعمال کرده‌اند. آنها همچنین قابلیت لاگین از طریق ماژول spreader را افزایش داده‌اند و به توسعه‌دهندگان این بدافزار این امکان را می‌دهند تا به صورت مرحله به مرحله لاگ‌های ماشین‌های آلوده شده را با استفاده از یک پروتکل ارتباطی جدید دیباگ کنند.

در طی این حمله، ماژول جدید Wifi spreader با شکست در بروت‌فورس بخش c$، در عوض، تلاش می‌کند تا بخش ADMIN$ را در شبکه مورد حمله قرار دهد.

قبل از بروت‌فورس C$/ADMIN$، یک سرویس باینری از یک آی‌پی کدگذاری شده دانلود و از راه دور نصب می‌شود.



کد بروت‌فورس spreader

این بدافزار برای آلوده کردن اولین سیستم از یک فایل فشرده که حاوی دو فایل باینری دیگر به نام‌های worm.exe و service.exe است برای انتشار از طریق WiFi استفاده می‌کند.

به دنبال آغاز به کار service.exe، این بدافزار به همان gate.php استفاده شده توسط spreader متصل می‌شود و رشته دیباگ را ارسال می‌کند. سپس، سرویس از راه دور دانلود payload را آغاز می‌کند. در مرحله بعد تلاش می‌کند تا به یک سرور C2 کدگذاری شده متصل شود و در آنجا فایل باینری Emotet را از بین برده و فایل firefox.exe را ذخیره کند.

سرانجام، بدافزار Emotet که از سرور C2 بارگیری شده است در پاسخ Service.exe تصدیق "payload downloaded ok" را قبل از اجرای فایل حذف شده، به سرور C2 ارسال می‌کند و همچنین این اطمینان را می‌دهد که لودکننده بارگیری شده دارای جدیدترین لودکننده Emotet است که یکی از روش‌های مؤثر برای جلوگیری از شناسایی توسط نرم‌افزارهای امنیتی است.

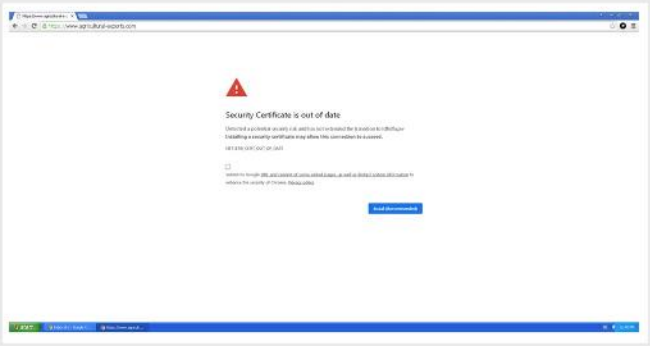
محققان معتقدند که این wifi spreader همچنان در مرحله توسعه قرار دارد.

منبع خبر :

https://gbhackers.com/wifi-spreader/

Scan Link

ایجاد Backdoor از طریق گواهی‌های جعلی امنیتی



اخیراً بدافزار جدیدی با ایجاد backdoor از طریق هشدارهای جعلی گواهی امنیتی منتشر می‌شود. این تکنیک جدید قربانیان را هنگام بازدید از سایت‌ها مجبور به نصب یک به‌روزرسانی گواهی امنیتی مخرب می‌کند. صادر کننده‌های گواهی امنیتی (CA)، گواهی نامه‌های امنیتی SSL/TLS را برای بهبود امنیت آنلاین با ایجاد رمزنگاری کانال‌های ارتباطی بین مرورگر و سرور - مخصوصاً برای دامنه‌های ارائه دهنده خدمات تجارت الکترونیکی- و تأیید هویت (برای ایجاد اعتماد در یک دامنه) منتشر می‌کند.

با وجود نمونه‌های سوءاستفاده از گواهی امنیتی، کلاهبرداری و جا زدن مجرمان سایبری به عنوان مدیران اجرایی برای به دست آوردن گواهی‌های امنیتی برای امضای دامنه‌های تقلبی یا بارگذاری بدافزار، رویکرد جدید فیشینگ در حال سوءاستفاده از مکانیزم گواهی های امنیتی است.

اخیراً محققان امنیتی از شرکت Kaspersky گزارش دادند این تکنیک جدید در انواع سایت‌ها مشاهده شده و اولین تاریخ سوءاستفاده آن در تاریخ 16 ژانویه 2020 گزارش شده است.

این پیغام ادعا می‌کند که تاریخ اعتبار گواهی امنیتی سایت به پایان رسیده است، و از قربانیان خواسته می‌شود یک به‌روزرسانی گواهی امنیتی را برای رفع این مشکل نصب کنند. این پیغام شامل یک iframe است و محتوای آن از طریق یک اسکریپت jquery.js از یک سرور کنترل و فرمان شخص ثالث بارگیری می‌شود؛ در حالی که نوار URL هنوز آدرس دامنه مجاز را نمایش می‌دهد.

طبق گفته محققان اسکریپت jquery.js، یک iframe که دقیقاً اندازه صفحه است را نمایش می‌دهد. در نتیجه کاربر به جای صفحه اصلی، یک صفحه ظاهراً واقعی را مشاهده می‌کند که خواستار نصب یک به‌روزرسانی گواهی امنیتی است.

اگر قربانی روی گزینه به‌روزرسانی کلیک کند، بارگیری فایل Certificate_Update_v02.2020.exe آغاز می‌شود. پس از نصب آن، مهاجم یکی از دو نوع نرم‌افزارهای مخرب Mokes یا Buerak را در سیستم قربانی اجرا می‌کند.

بدافزار Mokes یک backdoor برای macOS/Windows است، که توسط شرکت امنیت سایبری پیشرفته شناخته شده است، و قادر به اجرای کد، گرفتن screenshot، سرقت اطلاعات رایانه‌ای از جمله فایل‌ها، فایل‌های صوتی و فیلم‌ها، ایجاد یک backdoor و استفاده از رمزنگاری AES-256 برای پنهان کردن فعالیت‌های خود است. تروجان Buerak نیز یک تروجان تحت ویندوز است که قادر به اجرای کد، دستکاری فعالیت‌های در حال اجرا و سرقت محتوا است؛ این تروجان پایداری خود را از طریق کلیدهای رجیستری حفظ کرده و روش‌های مختلف آنالیز و تکنیک‌های sandboxing را تشخیص می‌دهد.

در هفته اخیر، سازمان صادر کننده گواهی امنیتی Let's Encrypt اعلام کرد که قصد ابطال بیش از سه میلیون گواهی امنیتی به دلیل باگ در کد پس زمینه که باعث می‌شود سیستم‌های کنترل از بررسی فیلدهای CAA چشم‌پوشی کنند، را دارد. اکنون خطای برنامه نویسی رفع شده است، اما صاحبان دامنه‌های قربانی باید درخواست دامنه‌های جدید بدهند.

منبع خبر :

https://cert.ir/news

Scan Link

اخبار کوتاه

باگ اپلیکیشن تأیید هویت دو مرحله‌ای گوگل اطلاعات میلیون‌ها کاربر را به خطر انداخته است

محققین شرکت امنیتی ThreatFabric باگی جدید در نرم‌افزار گوگل آتنتیکیتور پیدا کرده اند که به هکرها اجازه می‌دهد کدهای تولید شده توسط این اپلیکیشن را کپی کنند و وارد حساب‌های کاربری هدف خود شوند. گوگل آتنتیکیتور (Authenticator) برنامه‌ای است که به کاربران اجازه می‌دهد به جای استفاده از رمز عبور، از کدهای یک بار مصرفی استفاده کنند که توسط این برنامه تولید می‌شود؛ به نوعی می‌توان کارایی آن را مشابه رمز پویا دانست. با این حال باگی که در این برنامه پیدا شده، به هکرها اجازه می‌دهد به نمایشگر گوشی دسترسی داشته باشند و از کدهای تولید شده توسط این برنامه اسکرین شات بگیرند.

به نظر می‌رسد این باگ گریبان مایکروسافت را نیز گرفته باشند، چرا که همین باگ در برنامه مایکروسافت آتنتیکیتور نیز پیدا شده و با همین سطح از دسترسی به هکرها اجازه سرقت کدها را می‌دهد. البته هکرها برای دسترسی به کدهای تولید شده توسط این برنامه‌ها، ابتدا باید توسط برنامه تروجان خود وارد گوشی هوشمند کاربر شده و سپس به برنامه گوگل و مایکروسافت نفوذ کنند. پس از آن می‌توانند با وارد شدن به این برنامه، رمز عبور یکبار مصرف برای حساب‌های کاربری ذخیره شده در آن را تولید کنند و با استفاده از باگ، از صفحه و کد نمایش داده شده اسکرین شات بگیرند. سپس به کمک این کد و اطلاعات کاربری، می‌توانند وارد اکانت شخص هدف شوند. البته اندروید قابلیتی را در اختیار توسعه‌دهندگان قرار داده که به کمک آن می‌توان از اسکرین شات گرفتن از برخی صفحات ممانعت کرد.

آسیب پذیری

کشف نقص بحرانی در دو محصول شرکت ادوبی

شرکت ادوبی برای رفع دو آسیب‌پذیری بحرانی در برنامه‌های After Effects و Media Encoder، بروزرسانی‌های نرم‌افزاری را منتشر کرد.

این دو آسیب‌پذیری، ناشی از نقص بحرانی نوشتن در حافظه[1] است که با اجرای کد دلخواه بر روی سیستم قربانی و فریب وی از طریق باز کردن یک فایل مخرب با استفـــاده از نرم‌افزارهای مذکور، می‌توانند مورد اکسپلویت قرار گیرند.

Adobe After Effects، نرم‌افزاری جهت ایجاد جلوه‌های ویژه‌ی گرافیکی در ویدیوها می‌باشد که این نقص با شناسه‌ی "CVE-2020-3765" توسط یک محقق امنیتی به نام Matt Powell کشف و از طریق پروژه‌ی مقدماتی Trend Micro Zero Day به شرکت ادوبی گزارش داده شد.

Adobe Media Encoder نیز نرم‌افزاری جهت رمزگذاری و فشرده‌سازی فایل‌های صوتی یا تصویری می‌باشد که این نقص با شناسه‌ی "CVE-2020-3764" توسط یک محقق امنیتی کانادایی به نام Francis Provencher کشف شد.

هیچ یک از این آسیب‌پذیری‌های امنیتی، به طور علنی افشا و یا به طور گسترده اکسپلویت نشده‌اند، چرا که این شرکت هنوز مدرکی مبنی بر این موضوع پیدا نکرده است.

با این حال به کاربران ویندوز و مک توصیه می‌شود هر چه سریع‌تر آخرین نسخه‌ی ایـــن نرم‌افزارها را جهت محافظت از سیستمشان، بر روی آن نصب کنند.

در هفته سوم ماه فوریه 2020، شرکت ادوبی در Patch Tuesday، وصلـــه‌ی 42 آسیب‌پذیری را که به تازگی کشف شده بود، منتشر کرد که 35 مورد از آن‌ها دارای شدت بحرانی بودند.

گفتنی است کـــه Acrobat and Reader ,Flash Player ,Digital Edition, affecting Adobe Framemaker و Adobe Experience Manager از جمله نرم‌افزارهای تحت تأثیر این آسیب‌پذیری‌ها می‌باشند.

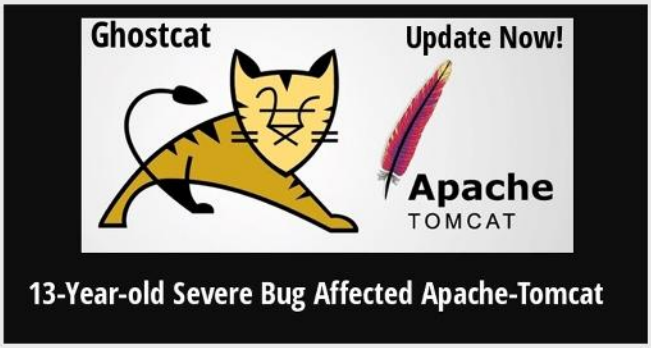
منبع خبر :

https://thehackernews.com/2020/02/adobe-software-updates.html

Scan Link

[1] write memory

Ghostcat ، باگ 13 ساله در Apache-Tomcat



Ghostcat، یک آسیب‌پذیری 13 ساله گنجاندن فایل (file inclusion) است که سرورهای Apache-Tomcat را تحت تأثیر قرار می‌دهد و مهاجمان را قادر می‌سازد تا از راه دور هر فایلی را در دایرکتوری‌های این وب سرور قرار دهند و یا از آن بخوانند.

Tomcat یکی از محبوب‌ترین سرورهای میان‌افزار[1] جاواست که برای استقرار Java Servlets و JSPs استفاده می‌شود، همچنین یک محیط وب سرور HTTP، "pure Java" ارائه می‌دهد که در آن، کدهای جاوا قابلیت اجرا شدن داشته باشند.

آسیب‌پذیری بحرانی Ghostcat، که در ابتدا توسط یکی از محققان Chaitin Tech کشف شد به طور خاص در پروتکل AJP مربوط به Tomcat وجود دارد.

پروتکل AJP، یک پروتکل باینری است که می‌تواند درخواست‌های ورودی از یک وب سرور را تماماً تا یک سرور اپلیکیشن که در پشت این وب سرور قرار دارد، پراکسی کند.

به این آسیب‌پذیری شناسه "CVE-2020-1938" اختصاص داده شده است و تمام نسخه‌های Tomcat 9/8/7/6 را تحت تأثیر قرار می‌دهد.

نسخه‌های آسیب‌پذیر Tomcat:

- Apache Tomcat 9.x < 9.0.31
- Apache Tomcat 8.x < 8.5.51
- Apache Tomcat 7.x < 7.0.100
- Apache Tomcat 6.x

Ghostcat، یک آسیب‌پذیری خواندن یا قراردادن فایل با ریسک بالا در Tomcat است و به موجب آن مهاجم می‌تواند با اکسپلویت نقص file inclusion (گنجاندن فایل)، کد مخرب خود را بر روی هاست مورد هدف اجرا نماید. به عبارت دیگر، آسیب‌پذیری مذکور به یک مهاجم اجازه می‌دهد تا فایل‌های پیکربندی و فایل‌های کد منبع[2] تمام وب‌اپلیکیشن‌های قرار گرفته در Tomcat را بخواند و در صورتیکه در این وب‌اپلیکیشن، به دلیل این نقص، امکان آپلود فایل وجود داشته باشد، مهاجم قادر است هر گونه فایل را در آن سرور آپلود کند.

امکان دیگری که برای مهاجم فراهم است این است که Java Server Pages (JSP) های مخرب که امکان اجرای کد از راه دور را در سرور دارند، آپلود نماید.

به گفته محقق Chaitin Tech، در شرایط زیر می‌توان این نقص موجود در Tomcat را مورد اکسپلویت قرار داد:

- اگر رابط AJP[3] فعال باشد و مهاجم بتواند به پورت سرویس AJP Connector دسترسی پیدا کند، خطر اکسپلویت آسیب‌پذیری Ghostcat وجود دارد.
- لازم به ذکر است که Tomcat AJP Connector به طور پیش‌فرض در 0.0.0.0:8009 فعال شده است.

محققان Chaitin Tech، این آسیب‌پذیری را در تاریخ 2020/01/03 به مقامات رسمی Apache Tomcat گزارش دادند و آنها نیز با رفع آسیب‌پذیری ذکر شده، نسخه‌های 9.0.31 و 8.5.51 را منتشر کردند.

کاربران می‌توانند اطلاعیه وصله آسیب‌پذیری Ghostcat را برای Tomcat 7.x، Tomcat 8.x و Tomcat 9.x مطالعه کنند. همچنین برای تشخیص و شناسایی این آسیب‌پذیری از اسکنر Utilize xray متعلق به محققان Chaitin Tech استفاده کنند.

منبع خبر :

https://gbhackers.com/ghostcat-tomcat-bug/

Scan Link

آسیب‌پذیری اعتبارسنجی مجوز SSL در Intelligent Proximity سیسکو

آسیب‌پذیری در اجرای SSL مربوط به Intelligent Proximity سیسکو، یک مهاجم غیر مجاز را قادر می‌سازد تا از راه دور اطلاعاتی را که در دستگاه‌های ویوئو کنفرانس Webex سیسکو به اشتراک گذاشته شده است را مشاهده کرده و یا تغییر دهد.

شناسه این آسیب‌پذیری "CVE-2020-3155" و با شدت بالا گزارش شده است.

آسیب‌پذیری فوق، ناشی از عدم اعتبارسنجی گواهی‌نامه (certificate) سرور SSL است که هنگام برقراری ارتباط با یک دستگاه ویدئو کنفرانس Webex سیسکو و یا collaboration endpoint سیسکو دریافت شده است. یک مهاجم می‌تواند با استفاده از تکنیک‌های man in the middle برای رهگیری ترافیک بین کلاینت آسیب‌دیده و یک نقطه پایانی (endpoint) و سپس با استفاده از یک certificate جعلی به منظور جعل هویت نقطه پایانی، این آسیب‌پذیری را مورد اکسپلویت قرار دهد. بسته به تنظیمات نقطه پایانی، یک اکسپلویت می‌تواند به مهاجمان اجازه دهد تا محتوای ارائه شده و به اشتراک گذاشته شده بر روی آن را مشاهده کنند، محتوایی که توسط قربانی ارائه شده

---

[1] middleware
[2] source code
[3] AJP Connector

است را تغییر دهند و یا به کنترل‌های تماس دسترسی داشته باشند.

محصولات آسیب‌پذیر

در صورتیکه محصولات سیسکو، یک نرم‌افزار آسیب‌پذیر در حال اجرا داشته باشند و قابلیت Proximity در آنها برای اتصال به دستگاه‌های داخلی فعال شده باشد تحت تأثیر این آسیب‌پذیری قرار دارند. محصولات آسیب‌پذیر عبارتند از:

- برنامه هوشمند Proximity سیسکو
- Jabber سیسکو
- Webex Meetings
- Webex Teams
- برنامه Meeting سیسکو

با توجه به اینکه تمام نسخه‌های این نرم‌افزارها تحت تأثیر آسیب‌پذیری ذکر شده قرار می‌گیرند، در حال حاضر سیسکو هیچ گونه بروزرسانی نرم‌فزاری را برای رفع این آسیب‌پذیری منتشر نکرده است.

تشخیص فعال بودن قابلیت Proximity بر روی کلاینت‌ها

درکلاینت‌هایی با نرم‌افزارهای ذکر شده در بالا، در صورتیکه در زمان پیکربندی، قابلیت Proximity در آنها فعال شده باشد، تحت تأثیر این آسیب‌پذیری قرار می‌گیرند. با این حال برای یک مهاجم که در صدد اکسپلویت این آسیب‌پذیری است، یک نقطه پایانی نیز باید قابلیت Proximity را فعال کرده باشد.

Jabber سیسکو

دو روش برای تعیین فعال بودن Proximity در Jabber سیسکو وجود دارد:

1. در فایل پیکربندی Jabber یعنی jabber-config.xml، اگر دستور زیر وجود نداشته باشد این قابلیت فعال است:

```
<EnableProximity>false</EnableProximity>
```

2. در تنظیمات این برنامه، به بخش Video Device بروید. اگر به صورت خودکار به نزدیکترین دستگاه متصل شد بدین معنی است که قابلیت مذکور در آن فعال است.

Cisco Webex Meetings

در تنظیمات پیشرفته این برنامه، به بخش Video Systems بروید. در صورت تشخیص خودکار دستگاه‌های مجاور، این ویژگی فعال است.

Cisco Webex Teams

از مرکز کنترل Webex سیسکو به بخش Settings و سپس Device Discovery مراجعه کنید. در صورتیکه برنامه Webex Teams، اجازه اتصال به دستگاه ثبت‌شده داخلی انتخاب شده را بدهد، نشان‌دهنده فعال بودن این قابلیت است.

برنامه Meeting سیسکو

قابلیت Proximity همواره فعال است و امکان غیرفعال کردن آن وجود ندارد.

راه‌حل

در حال حاضر هیچ راه‌حلی جهت رفع این آسیب‌پذیری ارائه نشده است. اما می‌توان توصیه‌های امنیتی زیر را اعمال کرد:

- غیرفعال کردن قابلیت Proximity Pairing
- غیرفعال کردن این قابلیت در دستگاه‌های ویدئویی Webex و Collaboration Endpoint سیسکو
- غیرفعال کردن تشخیص خودکار Collaboration Endpoint در کلاینت‌های Proximity
- انتقال از Collaboration به Cloud

منبع خبر :

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-proximity-ssl-cert-gBBu3RB

Scan Link

وصله آسیب‌پذیری بحرانی در تراشه‌های MediaTek rootkit

شرکت گوگل یک آسیب‌پذیری بحرانی را در تراشه‌های MediaTek rootkit وصله کرده است که میلیون‌ها دستگاه دارای این تراشه را تحت تأثیر قرار می‌دهد.

MediaTek یک شرکت بزرگ تولید کننده تراشه در تایوان است که تراشه‌هایی را برای ارتباطات بی‌سیم، تلویزیون‌های با وضوح بالا و دستگاه‌هایی مانند تلفن‌های هوشمند و تبلت‌ها تولید می‌کند.

آسیب‌پذیری MediaTek

این آسیب‌پذیری با شناسه "CVE-2020-0069" اولین بار توسط اعضای انجمن XDA کشف و شناسایی شد. این باگ از آوریل سال 2019 در اینترنت قرار گرفت و اکنون مهاجمان اکسپلویت آن را آغاز کرده‌اند.

سال گذشته شرکت MediaTek، وصله امنیتی را جهت رفع این آسیب‌پذیری منتشر کرد اما مهاجمان با نصب یک برنامه مخرب بر روی دستگاه، همچنان توانستند آن را مورد اکسپلویت قرار دهند. این اکسپلویت، تمام چیپست‌های 64 بیتی MediaTek شامل Motorola، OPPO، Sony، Alcatel، Amazon، ASUS، Blackview، Realme، Xiaomi و سایر دستگاه‌ها را تحت تأثیر قرار می‌دهد.

آسیب‌پذیری ذکر شده به هر کاربر اجازه می‌دهد تا دسترسی روت داشته باشد و به راحتی و تنها با کپی کردن این اسکریپت در یک پوشه موقت، ارائه مجوز اجرا و سپس اجرای آن،

ماژول امنیتی SELinux لینوکس را در دستگاه خود نصب کند.

آسیب‌پذیری دیگری کـــه توسط گوگـــل وصله شده است دارای شناسه اختصاصی "CVE-2020-0032" است که می‌تواند با استفاده از یک فایل ساختگی مخرب برای اجرای کد دلخواه در چارچوب یک فرآیند خاص، مورد اکسپلویت قرار گیرد.

منبع خبر :

https://gbhackers.com/mediatek-rootkit-vulnerability/

Scan Link

اخبار کوتاه

وقتی هکرها خود قربانی حمله سایبری هکرهای دیگر می‌شوند

هکرها به اهداف مختلفی حمله می‌کنند و اکثر مواقع افراد عادی و یا سازمان‌ها مورد حمله سایبری قرار می‌گیرند. با وجود چنین موضوعی، اطلاعات جدید از حمله هکرها به یکدیگر توسط بدافزار و آلوده کردن ابزارهای هک به تروجان njRat خبر می‌دهد.

به تازگی یک کمپین بدافزار شناسایی شده که نشان می‌دهد هکرها خود مورد حمله سایر هکرها قرار می‌گیرند. برای این کار ابزارهای معروف مورداستفاده در حمله سایبری، توسط بدافزار آلوده می‌شوند. یکی از اعضای Cybercason، (آمیت سرپر) به این موضوع پی برده که مهاجمان در این کمپین که قدمت بالایی دارد، ابزارهای موجود برای حمله سایبری که برخی از آن‌ها برای جداسازی اطلاعات از دیتابیس جهت کرک کردن و تولید کلید محصول برای دستیابی به نسخه‌های کامل یک نرم افزار Trial طراحی شده‌اند را به تروجان قدرتمند دسترسی از راه دور آلوده می‌کنند. زمانی که یک هکر این ابزارها را اجرا می‌کند، هکر دیگر به اطلاعات کامل سیستم وی دسترسی پیدا می‌کند.

پردازنده‌های تولیدی AMD در ۹ سال گذشته در برابر دو حمله جدید آسیب پذیرند

بر اساس گزارش محققان امنیتی، پردازنده‌های AMD که از 9 سال قبل تاکنون تولید شده اند، در برابر دو حمله جدید آسیبپذیر هستند. محققان امنیتی دانشگاه صنعتی گراتس اتریش (Graz University of Technology)، جزئیات دو حفره امنیتی تحـــت حمله ای به نام «Take A Way» را توضیح دادند که بوسیله آنها می‌توان داده‌هـــای پردازنده‌های AMD که بین سال‌های 2011 تا 2019 ساخته شده‌اند را سرقت کرد.

این دو اکسپلویت با هدف قرار دادن حافظه کش L1 پردازنده، سبب نشت محتواهای حافظه می‌شوند. حمله اول که «Collide+Probe» نام دارد، به هکر اجازه می‌دهد تا بدون داشتن آدرس‌های فیزیکی یا حافظه اشتراکی، به دسترسی حافظه نظارت کند. حمله «Load+Reload» نیز که روش مخفیانه‌تر محسوب می‌شود، از حافظه اشتراکـــی بهره برداری می‌کند.

این دو حمله ظاهراً در فضای ابری و ماشین‌های مجازی نیز قابل اجرا هستند. حملات Take A Way نسبت به حفره‌های امنیتی Meltdown و Spectre مقدار داده کمتری را فاش می‌کنند، ولی همین مقدار نیز برای محققان کافی بوده تا به کلیدهای رمزگذاری AES دسترسی پیدا کنند.

به گفته محققان، حفره‌های امنیتی یاد شده را می‌توان با اصلاحات نرم‌افزاری و سخت افزاری برطرف کرد، اما در مورد تأثیر آنها روی عملکرد پردازنده نمی‌توان نظـــری داد. پچ‌های برطرف کننده حفره‌های Meltdown و Spectre معمولاً منجر به کاهش سرعت می‌شدند، که البته میزان دقیق آن به وظایف پردازنده بستگی داشت.

محققان امنیتی می‌گویند AMD در رابطه با این حفره‌ها بسیار کند عمل کرده است. آنها اوت سال 2019 شرکت AMD را در جریان آسیب‌پذیری یاد شده قرار دادند، ولی این شرکت با وجود گذشت چندین ماه، هنوز واکنشی نشان نداده است.

کاهش ۷۶ درصدی اپلیکیشن های مخرب پلی استور گوگل در سال گذشته

در تحلیلی که RiskIQ روی 120 اپ استور موبایلی انجام داده مشخص شد که با وجود افزایش 18 درصدی اپلیکیشن‌ها در سراسر دنیا، مکانیزم‌های دفاعی علیه اپ‌های مخرب بهبودی قابل توجه پیدا کرده است. این اطلاعات از گزارش چشم‌انداز تهدید موبایل سال 2019 شرکت RiskIQ به دست آمده که در آن تعداد اپ‌های خطرناک یا فیلتر شده و همچنین تلاش‌های مختلف برای حفاظت در برابر آنها بررسی می‌شود.

براساس این گزارش پلی استور گوگل شاهد بیشترین کاهش اپ های مخرب در سال 2019 بوده و افت سال به سال 76 درصدی را در میزان اپ‌های لیست سیاه خود تجربه کرده است؛ به بیان دیگر شمار اپ‌های مخرب در این مارکت اندرویدی از رقم 108770 در سال 2018 به 25647 اپ در سال 2019 کاهش یافت.

طبق اعلام کارشناسان RiskIQ این غول تکنولوژی آمریکایی چندین طرح مختلف را برای کاهش شمار اپ‌های مخرب در سال گذشته کلید زد اما همچنان امکان آنکه به طور کامل از ورود آنها به پلی استور جلوگیری شود وجود ندارد. نکته مهم دیگر اینکه اپ‌های مخرب شناسایی شده در پلی استور غالبا به نحوی به چین ارتباط پیدا می‌کنند و چین همواره در کانون گزارش‌های RiskIQ قرار دارد؛ 40 درصد از کل هزینه‌های صرف شده در اپ استورهای سراسر دنیا از چین می‌آید و به همین خاطر این کشور بزرگترین مارکت اپلیکیشن در دنیا را دارد.

مقالات آموزشی

بدافزار و انواع آن

Malware یا به زبان ساده‌تر، بدافزار، به یک برنامه مخرب گفته می‌شود که برای کاربران اینترنت و دستگاه‌های دیجیتال از قبیل رایانه و گوشی هوشمند مضر می‌باشد. انواع بدافزارها عملکردهای متفاوتی را مثل سرقت اطلاعات، به اشتباه انداختن کاربر، تغییر یا حذف داده‌ها، کدگذاری (Data Encryption) ناخواسته روی‌داده‌ها و یا مانیتور کردن فعالیت‌های کاربر بدون مجوز او را انجام می‌دهند.

انواع بدافزارها

ویروس (Virus): بدافزارها انواع مختلفی دارند که هرکدام از آن‌ها دارای صفـــات و ویژگی‌های خاص خود می‌باشند. مثلاً یکی از انواع بدافزارها ویروس‌ها هستند و عملکرد اصلی آن‌ها تکثیر از خود و آلوده سازی دیگر برنامه‌ها می‌باشد.

کرم (Worms): از دیگر انواع بدافزارها می‌توان به کرم‌ها (Worms) اشاره نمود. عملکرد کرم‌ها تا حد زیادی شبیه به ویروس‌ها می‌باشد یعنی کرم‌ها هم می‌توانند خود را تکثیر کنند البته برای تکثیر از خود نیاز به آلوده سازی دیگر برنامه‌ها ندارند که به این عمل کرم‌ها، خود تکثیرکننده (SelfReplicate) گفته می‌شود.

تروجان (Trojan): تروجان یا اسب تروا، همان‌طور که از نام این بدافزار پیداست این بدافزار خود را در جلد یک برنامه سالم و قانونی مخفی می‌کند و هنگامی‌که برنامه به‌ظاهر سالم اجرا می‌شود اسب تروا شکسته شده و سربازان دشمن سیستم‌عامل را احاطه و منفجر می‌کنند.

جاسوس‌افزار (Spyware): جاسوس‌افزار یکی دیگر از انواع بدافزارها می‌باشد که کار آن جمع‌آوری اطلاعات از سیستم‌عامل کاربر است. جاسوس‌افزارها می‌توانند بدون اجازه کاربر فعالیت‌های کاربری را زیر نظر داشته باشند.

بات نت :(Botnet)این نوع از بدافزارها کنترل سیستم را از راه دور در اختیار گرفته و از آنجا اسپم یا جاسوس افزار را به دیگر قربانیان ارسال می‌کنند. بیشتر بات‌نت ها به صورت قربانی در اختیار هکر بوده و منتظر فرمان برای انجام اقدامات خود از سوی هکر هستند این بات‌نت ها به دو صورت ساده یا سلسله مراتبی هستند.

نحوه انتشار بدافزارها

- از طریق سیستم‌عامل
- از طریق شبکه‌های بیسیم
- از طریق اشتراک فایل
- از طریق شبکه‌های اجتماعی
- از طریق سامانه های مجازی
- از طریق سایت‌های اینترنتی و ایمیل

چگونه با بدافزارها مقابله کنیم؟

ازآنجاکه بدافزارها انواع زیادی دارند و هرکدام از آن‌ها نیز دارای انواع خود می‌باشند بهتر است همیشه نکات امنیتی مثل دانلود نکردن فایل از وب‌سایت‌های نامعتبر و یا بروز نگه داشتن سیستم‌عامل و ... را رعایت کنید. اما این گزینه کافی نمی‌باشد و ممکن است در بعضی از مواقع هکرها وب‌سایت‌های معتبر را نیز آلوده به انواع بدافزار کنند در این مورد بهتر است از نرم‌افزارهای امنیتی مناسب مثل انواع آنتی‌ویروس‌ها و یا نرم‌افزارهای امنیتی و دیوار آتش سیستم رایانه‌ای آپدیت شده استفاده کنید.

منبع خبر :

https://gbhackers.com/mediatek-rootkit-vulnerability/

Scan Link

اخبار کوتاه

صداوسیما مالکیت پیام رسان سروش را به مزایده گذاشت

سازمان صداوسیما با انتشار یک فراخوان اعلام کرده که مالکیت «پیام رسان سروش» را می‌فروشد. این احتمال مطرح است که قیمت پایه مورد نظر صداوسیما، حدود 38 میلیارد تومان برای پیام رسان سروش باشد. «سید جعفر خورشاد»، مدیرعامل سابق و رییس هیات مدیره کنونی پیام رسان سروش اعلام می‌کند که مالکیت 100 درصدی پیام رسان سروش متعلق به صداوسیما است و حالا این سازمان به دلایلی تصمیم گرفته است این پیام رسان را در مزایده‌ای به فروش برساند.

نکته اینجاست که هم‌اکنون پیام رسان سروش را می‌توان در قالب دو اپلیکیشن یافت. نسخه قدیمی‌تر، سروش نام دارد. اما از سال 98 نسخه دیگری تحت عنوان «سروش پلاس» معرفی شد که در آن زمان «مرتضی رحیمی»، مدیرعامل سابق سروش، گفته بود یک پیام رسان جداگانه است که در آینده نامش هم تغییر خواهد کرد. در حال حاضر پیام رسان سروش 500 هزار کاربر فعال و پیام رسان سروش پلاس، 2 میلیون کاربر فعال در کافه بازار دارد.

قابلیت ارسال پیام ناپدید شونده به نسخه بتا واتساپ اضافه شد

واتساپ به عنوان یکی از پرطرفدارترین برنامه‌های پیام‌رسان در جهان به شمار می‌رود، اما عموما ویژگی‌های جدید را به کندی به برنامه خود اضافه می‌کند. همین چند وقت پیش بود که بالاخره پس از یک سال دارک مود را در اختیار کاربران قرار داد. اکنون به نظر می‌رسد کاربران این پیام‌رسان به زودی می‌توانند از پیام‌های موقت استفاده کنند. پیام‌های موقت عملا پیام‌هایی هستند که تاریخ انقضا دارند؛ یعنی پس از مدتی که فرستنده تعیین می‌کند از بین می‌روند. این ویژگی اولین بار توسط اسنپ چت معروف شد و کم کم به اکثر پیام‌رسان‌ها نیز سرایت کرد. اکنون نوبت واتساپ است که این قابلیت را در اختیار کاربران قرار دهد. البته پیام‌های موقت فعلا در نسخه‌های بتا 2.20.83 و 2.20.84 سیستم‌عامل اندروید در دسترس هستند.

کاربرانی که از نسخه بتای این اپ استفاده می‌کنند می توانند پیام‌هایی ارسال کنند که پس از یک ساعت، یک روز، یک هفته، یک ماه یا یک سال از بین بروند. پس از این که پیامی با تاریخ انقضای مشخص برای مخاطب خود ارسال کردید، آیکن ساعتی کنار زمان ارسال پیام ظاهر می‌شود و نوع پیام ارسالی را هم برای شما و هم برای مخاطب مشخص می‌کند. اگر مبنا را ویژگی دارک مود بگذاریم، احتمالا چندین ماه با فرا رسیدن پیام‌های موقت به کاربران فاصله داریم.

شناسایی آسیب‌پذیری خطرناک در رم‌های جدید گوشی و کامپیوتر

بر اساس تحقیقاتی که روی رم کامپیوترها صورت گرفته، مشخص شده است که تمامی رم‌های ساخته شده از سال 2014 تاکنون نسبت به حملات Rowhammer آسیب‌پذیر هستند. تا پیش از این تصور می‌شد که رم‌های جدیدتر نسبت به این حملات مصونیت دارند ولی تلاش سازندگان به اندازه کافی خوب نبوده و ابزار TRRespass می‌تواند به رم کامپیوتر آسیب بزند.

راهکاری که شرکت‌های سازنده رم کامپیوتر ارائه داده‌اند، عموما با نام (TRR) با «همگام‌ساز ستون‌های هدف» شناخته می‌شود که از ترکیب نرم‌افزار و سخت‌افزار برای محافظت از حملات Rowhammer بهره می‌برد. این راه‌حل در تمامی رم‌های ساخته شده از سال 2014 تاکنون وجود دارد، ولی به نظر می‌رسد که راهکار فعلی آن‌ها، چندان هم جواب نداده است.

اما حملات Rowhammer چیست و چگونه به رم کامپیوتر آسیب می‌زند؟ در رم‌های مدرن، هرگاه که برنامه‌ای توسط کامپیوتر داخل رم بارگذاری می‌شود، داده‌های آن داخل سلول‌های حافظه‌ای ذخیره می‌شوند که به صورت یک شبکه در کنار هم قرار گرفته‌اند. این کار به مهندسین اجازه می‌دهد که تا جای ممکن از سلول‌های بیشتری استفاده کنند، اما در عین حال، تداخل الکتریکی بین سلول‌ها نیز بالا می‌رود.

حملات Rowhammer نیز عملا همین تداخلات الکتریکی هستند. این کار به کمک خواندن و نوشتن بسیار سریع (Hammer) داده روی یک ردیف از سلول‌های حافظه رم (Row) صورت می‌گیرد که باعث می‌شود تداخلات الکتریکی ایجاد شود و در نهایت داده‌ها را خراب کند یا تغییر دهد. در صورتی که به یک هکر زمان کافی برای انجام این حملات داده شود، آن‌ها می‌توانند داده‌های داخل یک کامپیوتر را دستکاری کنند یا برای مثال داده‌های یک مرکز داده ابری را به سرقت ببرند.

امنیت کاربر رایانه

امنیت ایمیل

ایمیل بشدت به هویت ما در فضای مجازی گره خورده؛ ما از ایمیل برای ایجاد حساب کاربری در پلتفرم‌های مختلف، تآیید لاگین، پیگیری‌های مختلف، دریافت هشدار از سرویس‌های مختلف، شکایت از موضوعات گوناگون و به اشتراک گذاشتن اطلاعات استفاده می‌کنیم. نه تنها ایمیل همچنان زنده و پابرجاست بلکه در حال حاضر به دلیل استفاده روزافزون از گوشی‌های هوشمند، استفاده از ایمیل هم شدت گرفته است.

حال با توجه به اهمیت این موضوع، در این شماره از بولتن خبری و در فصل "امنیت ایمیل" به روش‌های امنیتی ایمیل می‌پردازیم.

با ما همراه باشید ...


امنیت ایمیل
لایه های کنترل
گیرنده
فیلترهای اکتشافی
شناسایی زبان
فیلترهای URL
امضاها
سرویس اعتبار
لیست فرستندگان غیرمجاز
لیست فرستندگان مجاز
فیلترهای محتوا
Mail
فرستنده

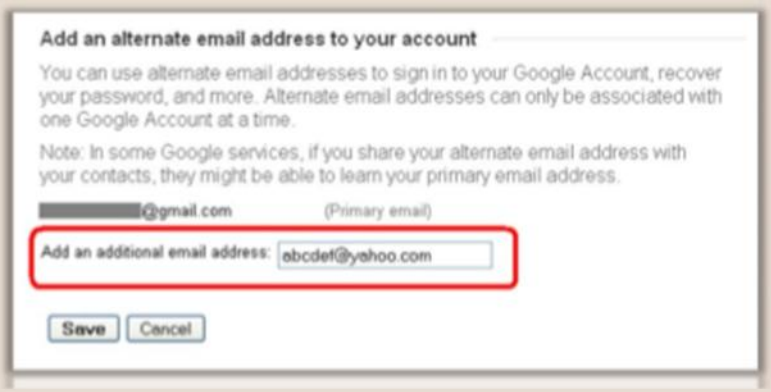

روش های امنیتی ایمیل
ایجاد و استفاده از پسورد قوی
تهیه آدرس ایمیل جایگزین برای بازیابی ایمیل
آخرین لاگین را بررسی کنید
از Https برای اتصال به مرورگر استفاده کنید
گزینه های Signed In/Remember Me,Keep Me را غیرفعال کنید و یا انتخاب نکنید
پیوست های ایمیل را جهت یافتن نرم افزارهای مخرب اسکن کنید
قابلیت پیش نمایش را خاموش کنید و تنظیمات دانلود را درکلاینت های ایمیل تغییر دهید
فیلتر ایمیل کم اهمیت را در کلاینت های ایمیل ایجاد کنید
پیام های ایمیل خود را به صورت دیجیتالی امضا کنید
با استفاده از فیلترها، از ایمیل های ناخواسته جلوگیری کنید

ایجاد پسوردهای قوی

- پسوردهای قوی برای کرک و حدس زدن دشوارهستند
- یک پسورد قوی، می تواند با ترکیبی از اعداد (0-9) ، حروف کوچک و بزرگ (A-Z و a-z) وکاراکترهای خاص (... %$#@!) ساخته شود
- یک پسورد قوی و آسان برای به یاد آوردن ایجاد کنید و آن را هرجایی یادداشت نکنید

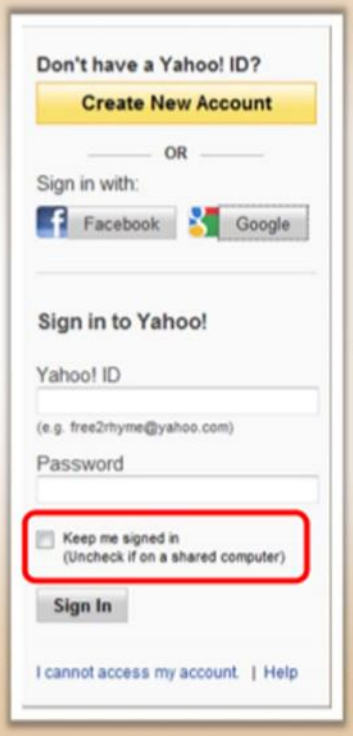
آدرس ایمیل جایگزین

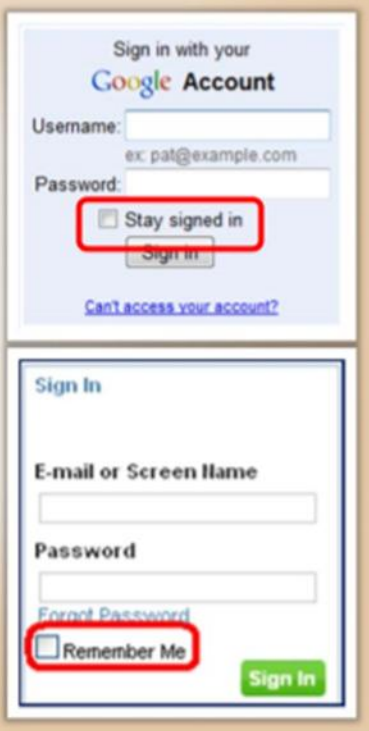
- آدرس ایمیل جایگزین، یک آدرس ایمیل اضافی و ضروری است برای ثبت نام در بسیاری از سرویس های ایمیل مانند Gmail و Yahoo
- توسط ارائه دهندگان سرویس برای تأیید تشخیص سازنده حساب، استفاده می شود
- آدرس های ایمیل جایگزین برای بازیابی پسورد در صورت فراموشی، مورد استفاده قرار می گیرند



Keep Me Signed In/Remember Me

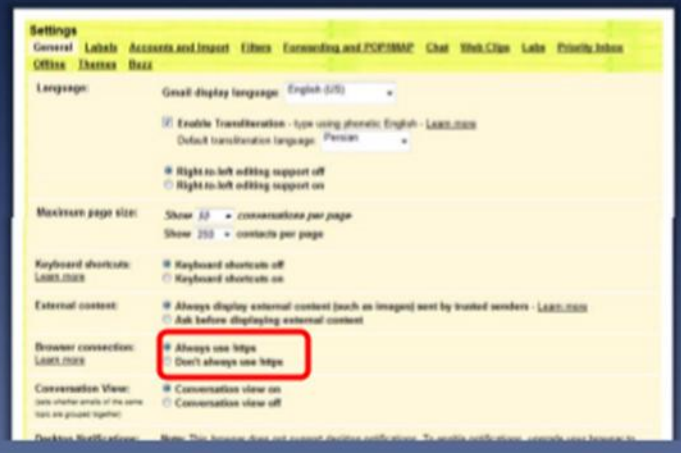
- بیشتر کلاینت های ایمیل محبوب، گزینه های Keep me signed in یا Remember Me را دارند
- بررسی این گزینه ها به کلاینت ایمیل اجازه می دهد تا صندوق پستی کاربر را بدون پرکردن مجدد اطلاعات لاگین، بازیابی کند
- این گزینه ها به کاربران دیگر اجازه می دهند تا به ایمیل کاربر دسترسی پیدا کنند
- کاربران باید این گزینه ها را هنگام دسترسی به ایمیل از یک کامپیوتر عمومی، انتخاب نکنند





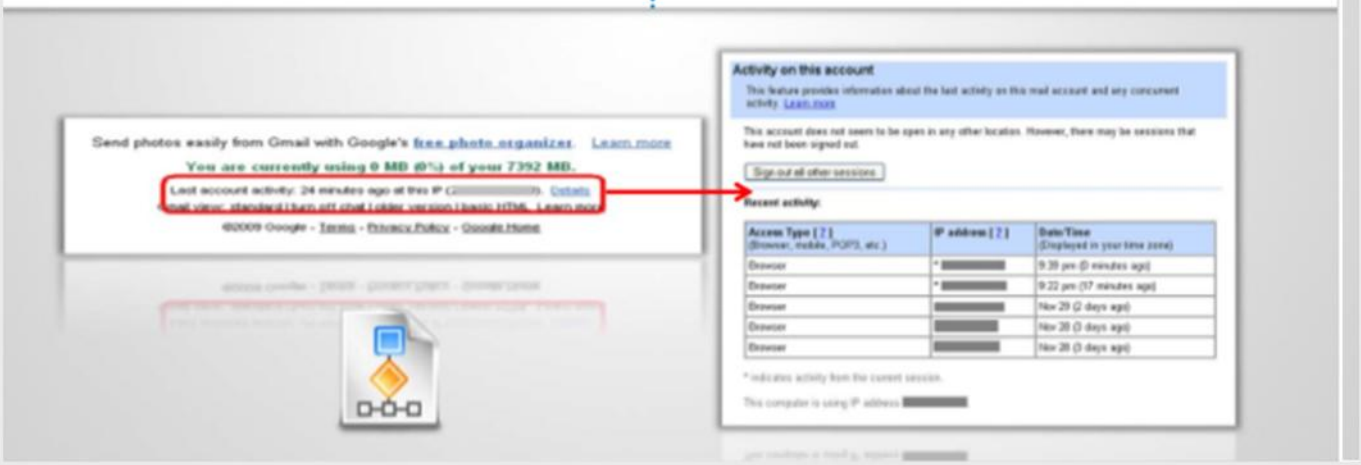
استفاده از HTTPS

- حساب های کاربری ایمیل تحت وب مانندGmail، Yahoomail، Hotmail، AOL Mail و غیره یک گزینه برای انتخاب پروتکل ارتباطی برای اتصال مرورگر دارند
- تنظیمات اتصال مرورگر را برای دریافت ایمیل با استفاده از پروتکل HTTPS (HTTPSecure) تغییر دهید



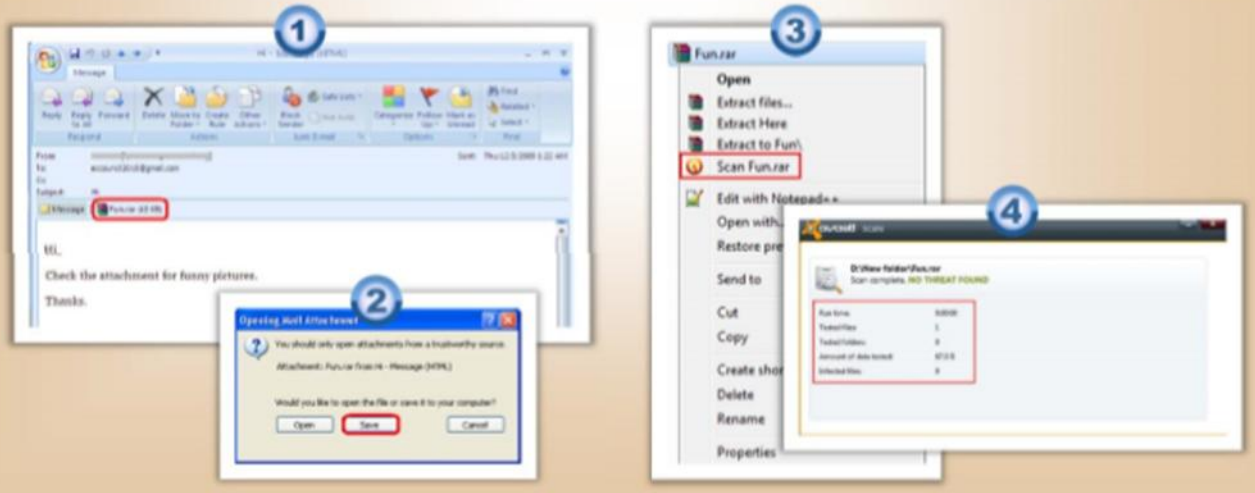
چک کردن آخرین فعالیت حساب کاربری

- در صورت در دسترس بودن این ویژگی در سرویس ایمیل، همیشه آخرین فعالیت حساب کاربری را بررسی کنید
- آخرین فعالیت حساب کاربری شامل اطلاعاتی مانند: نوع دسترسی (مرورگر، تلفن همراه و غیره) ، موقعیت(آدرس آی پی) و تاریخ و زمان فعالیت های حساب کاربری است
- برای بررسی فعالیت حساب کاربری در Gmail به پایین صفحه بروید و روی Details کلیک کنید
- درصورت مشاهده هر فعالیت مشکوک، بلافاصله پسورد و نشانه های آن را تغییر دهید



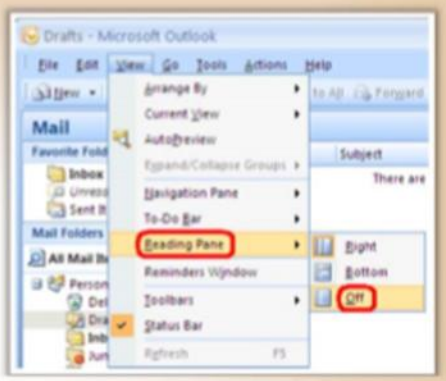
اسکن کردن پیوست های ایمیل

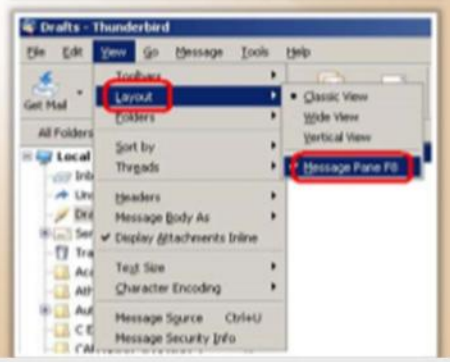
- هنگام باز کردن هر پیوست ایمیل احتیاط کنید
- همه فایل های پیوست را ذخیره کنید و آنها را قبل از باز کردن ، با استفاده از یک آنتی ویروس جهت یافتن بدافزارها اسکن کند
- فعال کردن آنتی ویروس، به طور خودکار همه ایمیل ها ودانلودها را اسکن می کند



خاموش کردن ویژگی پیش نمایش

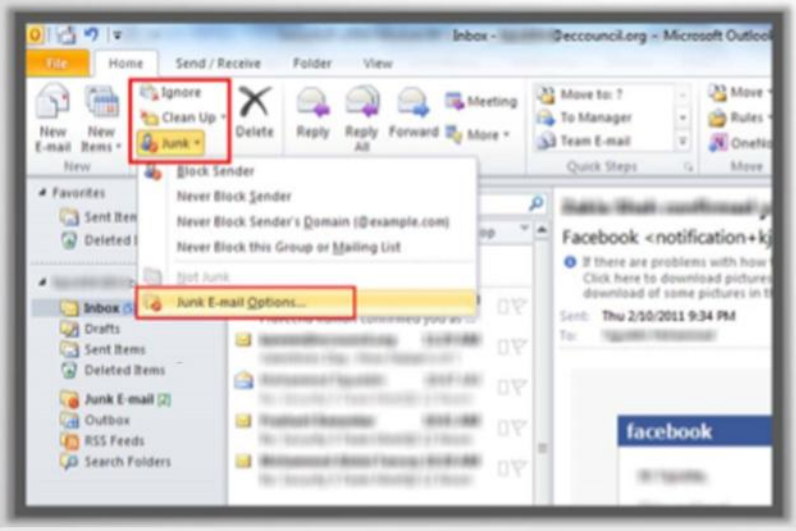
- کلاینت های ایمیل یک گزینه برای ارائه پیش نمایشی از ایمیل دارند
- این ویژگی را در کلاینت های ایمیل خاموش کنید
- با فعال کردن این ویژگی ممکن است بدون اینکه پیام را باز کنید یک کد اسکریپت اجرا شود
- برای خاموش کردن ویژگی پیش نمایش در Microsoft Outlook:
  - به منوی View بروید و Reading Pane را انتخاب کنید
  - بر روی گزینه Off کلیک کنید
- برای خاموش کردن این ویژگی در Mozilla Thunderbird:
  - به منوی View بروید و Layout را انتخاب کنید
  - گزینه Message Pane را غیرفعال کنید

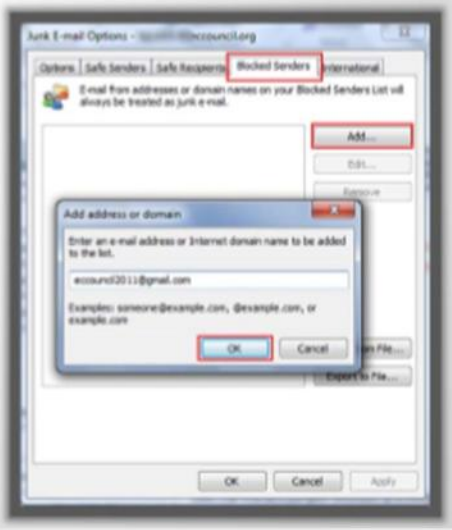




فیلترکردن ایمیل: اجتناب از ایمیل های ناخواسته

- فیلتر کردن ایمیل فرآیند سازماندهی ایمیل ها براساس یک معیار مشخص است
- فیلترهای ایمیل معمولا برای شناسایی و دسته بندی ایمیل های اسپم استفاده می شوند
- برای جلوگیری از ایمیل های ناخواسته در Outlook 2010، در منوی Home به قسمت Delete group بروید، روی گزینه Junk وسپس Junk E-mail Options کلیک کنید ، در منوی Blocked Sender، روی گزینه Add کلیک کنید
- یک آدرس ایمیل یا نام دامنه وارد کنید و روی گزینه OK کلیک کنید





سیستم آنلاین رمزگذاری ایمیل: Lockbin

- Lockbin یک سرویس رایگان برای ارسال ایمیل های محرمانه است
- این سیستم برای ارسال اطلاعات محرمانه مانند جزئیات کارت اعتباری و اطلاعات کسب و کار ، استفاده می شود

https://www.lockbin.com

ابزارهای امنیتی ایمیل

Comodo AntiSpam
http://www.comodoantispam.com

McAfee SpamKiller
http://us.mcafee.com

Netcraft Toolbar
http://toolbar.netcraft.com

Comodo Email Certificate
http://www.comodo.com

PhishTank SiteChecker
https://addons.mozilla.org

Mirramail Secure Email
http://www.mirrasoft.com

Spamihilator
http://www.spamihilator.com

Encryptomatic MessageLock
http://www.encryptomatic.com

خلاصه فصل

- Email(electronic mail) یک روش تبادل پیام های دیجیتال از یک فرستنده به یک یا چند گیرنده است
- فایل های ضمیمه(پیوست ها) می توانند حاوی برنامه های مخرب باشند، که باز کردن چنین پیوست هایی می تواند کامپیوتر را آلوده کند
- Spamming فرآیند اشغال کردن صندوق ورودی کاربر با ایمیل های ناخواسته و بی ارزش است
- Hoaxes هشدار های دروغین با ادعای گزارش های مربوط به یک ویروس غیرواقعی هستند
- پاک کردن cache ، پسوردها وhistory مرورگر را فراموش نکنید
- تنظیمات تلفن همراه را فقط برای دانلودheader ایمیل ها در نظربگیرید نه برای تمام ایمیل
- امضاهای دیجیتال برای تأیید هویت فرستنده یک پیام یا امضاکننده یک داکیومنت، استفاده می شوند
- ابزارهای امنیتی ایمیل از پسوردها و خروج خودکار از حساب های کاربری ایمیل، محافظت می کنند

ادامه مبحث " امنیت شبکه" را در شماره های بعدی ما دنبال کنید...


مرکز تخصصی آپا دانشگاه رازی