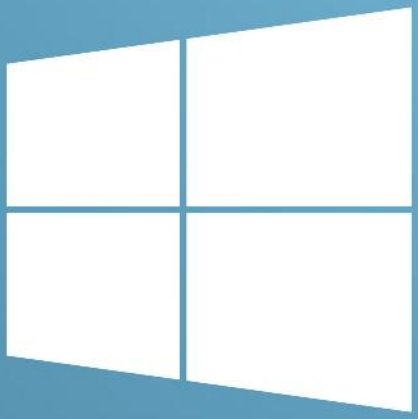
بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره هفتم دی ماه ۱۳۹۷

افشاء آسیب پذیری های روز صفرم ویندوز یکی پس از دیگری!



ZERO DAY

در این شماره می‌خوانید :

فهرست

مرکز تخصصی آپا دانشگاه رازی

پیشرو در ارائه خدمات امنیت فناوری و اطلاعات

صاحب امتیاز :
مرکز تخصصی آپا دانشگاه رازی

سردبیر :
سهیلا مرادی

همکاران این شماره :
سهیلا مرادی
آتوسا خدامرادی
پویان مسعودی‌نیا
سیده مرضیه حسینی
سیده آرزو حسنی

صفحه آرایی و چاپ :
سید احسان حسینی
آژانس تبلیغاتی تمام خدمت باروک

آدرس :
کرمانشاه، بلوار طاق بستان، دانشگاه رازی، ساختمان کتابخانه مرکزی، طبقه دوم، مرکز تخصصی آپا

۰۸۳۳۴۲۷۳۳۹۰

cert.razi.ac.ir

apa@razi.ac.ir

اخبار امنیتی

سرقت شماره‌های تلفن از طریق پیوست‌های pdf آلوده در گوشی‌های اندرویدی

گردآورنده: سهیلا مرادی

هوشیار باشید!

یکی از کمپین‌های ارائه کننده فایل‌های PDF، فایل‌های PDF مخربی تولید نموده است که کاربران اندرویدی را به دانلود فایل‌های APK مخرب ترغیب می‌کند.

محققان شرکت امنیتی Quick heal فایل‌های PDF مخرب ارسال شده برای کاربران را بررسی نموده و دریافتند که این فایل‌ها از طریق ایمیل‌های فیشینگ برای کاربران ارسال شده و آنان را برای باز کردن ایمیل وسوسه نموده است.

فایل PDF مذکور حاوی لینکی است که فایل APK مخرب را بر روی دستگاه کاربر دانلود می‌کند. فایل APK مخرب از آیکونی متفاوت با آیکون Adobe reader اصلی استفاده می‌کند و هنگام نصب نیز مجوزهای حساسی مانند دسترسی به مخاطبان، SMSها و تاریخچه تماس‌ها را از کاربر تقاضا می‌کند که این با عملکرد اپلیکیشن اصلی Adobe reader کاملاً مغایر است.

زمانی که کاربر برنامه را باز می‌کند صفحه نمایش نصب نرم‌افزار Adobe Acrobat به وی نشان داده می‌شود و کاربر باور می‌کند که در حال نصب برنامه Acrobat است. این در حالی است که وقتی کاربر برای بروزرسانی نرم‌افزار کلیک می‌نماید آیکون برنامه مخفی شده و اقدامات مخرب خود را در پس‌زمینه آغاز می‌کند.

بدافزار مذکور دارای قابلیت‌های جاسوسی است که SMSهای کاربر را ردیابی نموده و شماره آن‌ها را به سرورهای تحت کنترل مهاجم ارسال می‌کند.

این بدافزار همچنین مختصات جغرافیایی محل تماس را دریافت کرده و سپس به سرورهایی که توسط مهاجمان کنترل می‌شوند ارسال می‌نماید.

از دیگر قابلیت‌های این بدافزار می‌توان به دسترسی به مخاطبین، دسترسی به صفحات مورد علاقه کاربر در مرورگر، ثبت کلیدهای فشرده شده و خاتمه دادن به فرآیندهای پس زمینه گوشی اشاره نمود.

Scan Link

منبع خبر :

https://gbhackers.com/android-malware-malicious-pdf/

امکان رمزگشایی رایگان باج‌افزار Aurora!

گردآورنده: پویان مسعودی نیا

یک خبر خوب!

قربانیان باج‌افزار Aurora می‌توانند از یک ابزار رمزگشایی که توسط Michael Gillespie، کارشناس حوزه باج‌افزار توسعه داده شده است، به صورت رایگان برای رمزگشایی داده‌های رمز شده‌ی خود استفاده نمایند.

خبر خوب برای قربانیان باج‌افزار Aurora این است که، با وجود اینکه انواع مختلفی از این باج‌افزار مخرب وجود دارد، اما سیستم‌های اکثر قربانیان با نسخه‌ای که با پسوند Nano. فایل‌ها را رمز می‌نماید آلوده شده‌اند، که می‌توان آن‌ها را به آسانی رمزگشایی نمود.

مهاجمان سیستم‌ها را از طریق سرویس‌های دسترسی از راه دور دسکتاپ (RDP) آلوده می‌نمایند. زمانی که باج‌افزار نصب، و در سیستم هدف اجرا می‌شود، هر فایلی که در دسترس باشد را رمز نموده، به نام هر فایل یک پسوند اضافه می‌کند و سپس پیغام باج‌خواهی بر روی دسکتاپ قرار می‌گیرد.

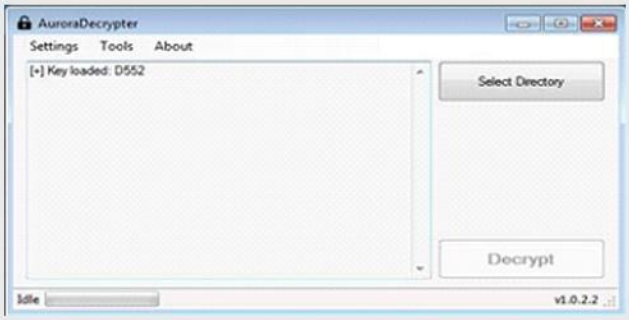
این رمزگشا فقط فایل‌هایی با پسوندهای زیر را پشتیبانی می‌کند:

- .Nano
- .Animus
- .Aurora
- .desu
- .ONI
- .aurora

قربانیان برای رمزگشایی فایل‌های رمز شده‌ی خود می‌توانند رمزگشای Aurora Decryptor را از لینک زیر دانلود و نصب نمایند. مراحل انجام کار نیز در این **لینک** موجود است:

Scan Link

https://www.bleepingcomputer.com/news/security/how-to-decrypt-the-aurora-ransomware-with-auroradecrypter



برای شروع حمله‌ی brute-force و کشف کلید رمزگشایی، به دو فایل رمز شده با پسوندهای یکسان نیاز داریم که می‌توانند یکی از پسوندهای زیر باشند :

.png, .gif, .pdf, .docx, .xlsx, .pptx, .doc, .xls, .ppt, .vsd, .psd, .mp3, .wmv, .zip, .rar, .pst, .rtf, .mdb, .ico, .lnk, .fdb, .jar, and .idx

پس از انتخاب دو فایل رمزگذاری شده، قربانی می‌تواند حمله Brute Force را آغاز نماید، این فرآیند ممکن است زمان‌بر باشد. فرآیند با کشف کلید رمزگشایی پایان خواهد یافت که در مرحله آخر پس از اتمام رمزگشایی، یک کلید پیدا خواهد شد. اکنون کاربر می‌تواند با مشخص نمودن مسیرهای مختلف، موفق به رمزگشایی یک پوشه یا کل یک درایو شود.

پس از اتمام مراحل فوق، رمزگشا خلاصه‌ای از فایل‌های رمزگشایی شده را به کاربر نمایش می‌دهد، اگر برخی از فایل‌ها رمزگشایی نشده‌اند، ممکن است به علت مجوزهای مربوط به آن فایل‌ها باشد. توجه داشته باشید که فایل‌های اصلی رمزگذاری شده بر روی کامپیوتر قربانی باقی می‌مانند تا زمانی که تأیید شود تمام فایل‌ها به درستی رمزگشایی شده‌اند.

Scan Link

منبع خبر :

https://securityaffairs.co/wordpress/79525/malware/aurora-ransomware-decryptor.html

آلودگی کاربران بـــه نرم‌افزار جاسوســـی موجود در گوگل پلی، در ۱۹۶ کشور دنیا

گردآورنده: سیده مرضیه حسینی

نرم‌افزارهای جاسوســـی خطرناکی در فروشگـــاه گوگل پـــلی کشـــف شـــده‌اند که از مجموعه برنامه‌هـــای معتبر بـــوده و تقریباً ۱۰۰,۰۰۰ کاربـــر آن‌هـــا را دانلـــود نموده‌اند. ایـــن برنامه‌های مخرب کاربران را در ۱۹۶ کشور جهان تحت تأثیر قرار داده‌اند.

طبق بررســـی‌های صـــورت گرفته از حمـــلات مبتنی بـــر تلفن همراه، سیســـتم اندروید یکی از بزرگتریـــن اهداف مجرمان ســـایبری برای جاسوسی و سرقت اطلاعات شخصی کاربران است.

۶ برنامه‌ی مخرب کشـــف شـــده از فروشگاه گوگل پلی، شامـــــل بازی‌های معـــروف و برنامه‌های دیگر هســـتند که لیســـت آن‌ها در زیر آورده شده است:

- FlashLight
- HZPermis Pro Arabe
- WinYLauncher
- Flappy Bird
- Flappy Birr Dog

محققان این نرم‌افـــــزارهای جاسوســـــی را به عنـــوان ANDROIDOS_MOBSTSPY شناســـایی نموده‌انـــد کـــه قـــادر به سرقت اطلاعات حســـاس مانند موقعیت کاربر، مکالمات، SMS و سایر اطلاعات مربوط به تماس هستند.

این نرم‌افزارهای جاسوســـی کاربـــران را در بیش از ۱۹۰ کشـــور جهان از جمله: موزامبیک، لهســـتان، ایران، ویتنام، الجزایـــر، تایلند، رومانی، ایتالیـــا، مراکـــش، مکزیک، مالزی، آلمـــان، عراق، آفریقـــای جنوبی، ســـریلانکا، عربســـتان ســـعودی، فیلیپین، آرژانتین، کامبوج، بلاروس، قزاقستان، تانزانیا، مجارستان و غیره تحت تأثیر قرار داده‌اند.

فرآیند ســـرقت اطلاعـــات توســـط نرم‌افزارهای جاسوسی مذکور

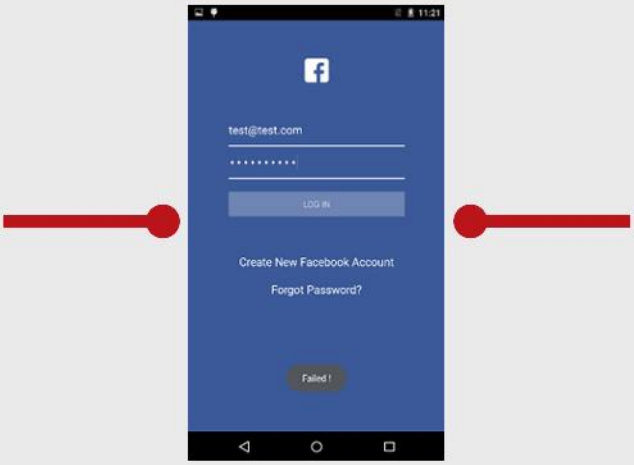
پس از راه‌اندازی بدافزار در دستگاه مربوطـــــه، بدافزار دستـــــگاه را از نظر در دســـترس بودن شـــبکه بررســـی نموده و پس از آن یـــک فایل پیکربندی XML را با کمک سرور C&C تجزیه می‌نماید.

در مرحلـــه بعد، بدافزار شـــروع به جمـــع‌آوری اطلاعات دستـــگاه مانند زبان، کشور ثبت شده آن، سازنده دستگاه و غیره می‌نماید.

پـــس از انجام فرآینـــد جمع‌آوری اطـــلاعات، بدافزار شـــروع به برقـــراری‌ارتباط‌باسرورفرماندهـــی‌وکنتـــرل(Command&control) و به اشتراک گذاشتن اطلاعات جمع‌آوری شده می‌نماید.

مهاجم به بدافـــزار فرمان می‌دهد که اطلاعات حساســـی مانند SMS، لیست تماس‌ها، فایل‌ها و غیره را جمع‌آوری نماید.

ایـــن بـــدافزار هم‌چنین قادر به انجام حملات فیشـــینگ اســـت تا بتواند از این طریـــق، اطلاعـــات ورود را از طـــریق نمایـــش صفحه ورود جعلی فیسبوک و pop-upهای گوگل سرقت نماید.



هنگامی‌که کاربران اطلاعات خود را در صفحه فیشینگ جعلی فیسبوک وارد می‌کنند، اطلاعات آن‌ها به مهاجم ارسال می‌گردد.

طبق گفته محققان Trend Micro، نکته جالب توجه این است که چگونه برنامه‌های مذکور توانسته‌اند این‌گونه به صورت گسترده توزیع گردند!

منبع خبر :

https://gbhackers.com/spyware-google-play

اخبار کوتاه

پشتیبانی از ویندوز 7، سال آینده به پایان می‌رسد

مایکروسافت در بیانیه‌ای اعلام کرد که از 14 ژانویه 2020 (24 دی 1398) پشتیبانی رایگان از ویندوز 7 به اتمام می‌رسد. در واقع اگر کاربری بعد از این زمان بخواهد آپدیت‌های امنیتی ویندوز 7 را دریافت کند، باید هزینه‌ای بپردازد و نکته اینجاست هر سال نیز این هزینه افزایش خواهد یافت، مایکروسافت برنامه دارد تا سال 2023 این آپدیت‌های امنیتی پولی را منتشر کند.

مرکز ماهر: 300 بازی مخرب از فروشگاه‌های اندرویدی حذف شدند

یکی از مهم‌ترین اهداف هکرها برای دسترسی به اطلاعات شخصی کاربران، مارکت‌های اپلیکیشن‌ها هستند. گوگل‌پلی و اپ‌استور مدت‌هاست که با این مشکل دست و پنجه نرم می‌کنند و حالا با توجه به گزارش "مرکز ماهر"، ظاهراً فروشگاه‌های اندرویدی داخلی، به خصوص کافه‌بازار نیز با این دسته از اپلیکیشن‌ها غریبه نیستند. در این گزارش مرکز ماهر به بررسی رفتار 300 بازی حذف شده از کافه‌بازار پرداخته که همگی جزء اپلیکیشن‌های دارای شبیه‌ساز بوده‌اند.

افزایش حملات سایبری به تجارت الکترونیک و خطرناک‌ترین حملات سایبری در سال 2019

تهدیدات اینترنتی مختلفی وجود دارد که باعث می‌شود تا کسب وکار تجارت الکترونیک آسیب‌پذیرتر شود زیرا برخی عملیات حساس در زمینه فناوری اطلاعات در پشت این مسئله وجود دارد. در یک سال پیش، بیش از 150 میلیون حمله توسط مجرمان اینترنتی توسط تهدیدهای جدی نظیر تلاش‌های ورود به سیستم، تقلب در کارت بانکی، بات‌نت، فیشینگ و بسیاری دیگر از حملات تجارت الکترونیک گزارش شد.

خطرناک‌ترین حملات سایبری به تجارت الکترونیک در سال 2019

- حملات فیشینگ
- حمله DDOS
- کلاهبرداری کارت‌بانکی
- سرقت هویت

بدافزار WhatsApp Gold بازگشته است!

WhatsApp Gold در واقع یک پیام کلاهبردارانه است که کاربران را تشویق به دانلود و نصب به‌روزرسانی جعلی واتس‌اپ می‌کند. این ترفند که در سال 2016 میلادی فراگیر شده بود اکنون دوباره ظهور کرده است.

WhatsApp Gold که توسط کلاهبرداران سایبری طراحی شده، کاربران را تشویق به نصب یک به‌روزرسانی ویژه از واتس‌اپ نموده و ادعا می‌کند می‌تواند ویژگی‌های پیشرفته را به برنامه بدهد، ادعایی که دروغی بیش نبوده و پیشتر توسط شرکت واتس‌اپ رد شده است.

این شرکت در این مورد اظهار داشت:

"این برنامه هیچ ارتباطی با WhatsApp ندارد و این شرکت WhatsApp Plus را پشتیبانی نمی‌کند."

آسیب پذیری

کشف آسیب‌پذیری در پکیج wget لینوکس

گردآورنده: سهیلا مرادی

توسعه‌دهندگانی که پکیج wget گنو را در برنامه‌های خود دارند، باید از نسخه جدیدی که در Boxing Day منتشر شده است استفاده کنند!

GNU Wget یک پکیج نرم‌افزاری رایگان برای بازیابی فایل‌ها با استفاده از رایج‌ترین پروتکل‌های اینترنت مانند HTTP، HTTPS، FTP و FTPS می‌باشد. ابزار مذکور یک ابزار خط فرمان غیرتعاملی است، بنابراین می‌تواند به راحتی توسط اسکریپت‌ها، کرون جاب‌ها، ترمینال‌های بدون پشتیبانی X-Windows و غیره فراخوانی گردد. GNU Wget دارای امکانات فراوانی برای بازیابی آسان فایل‌های بزرگ و یا ایجاد mirror برای وب‌سایت‌ها یا FTP می‌باشد.

آسیب‌پذیری یافت شده با شناسه CVE-2018-20483، به کاربران محلی اجازه می‌دهد با خواندن attributeها، اطلاعات حساسی مانند اطلاعات محرمانه موجود در URL را به دست آورند.

یک محقق امنیتی به نام Gynvael Coldwind، دریافت که attributeهای ذخیره شده می‌توانند حاوی نام کاربری و رمز عبور کاربر باشند.

محقق امنیتی دیگری به نام Hanno Böck، تأکید نمود که URLها گاهی می‌توانند حاوی "secret tokens" برای سرویس‌های خارجی، مانند میزبانی فایل باشند و با استفاده از دستور getfattr تمام attributeهای موجود در هر دستگاه لاگین شده‌ای می‌تواند قابل دسترسی باشد.

Böck نوشت: "در سیستم‌هایی که attributeهای توسعه یافته یونیکس را پشتیبانی می‌کنند URL مربوط به دانلودها ازطریق attributeهای فایل سیستم ذخیره می‌گردند."

شما می‌توانید با اجرای دستور زیر این attributeها را بر روی سیستم لینوکسی خود مشاهده فرمایید:

```
getfattr -d [filename] (The download URL is stored in a variable "user.xdg.origin.url")"
```

این موضوع به صورت محرمانه و خصوصی به کروم گزارش شده و امید است که به زودی مرتفع گردد.

به گفته تیم توسعه‌دهنده Wget، با استفاده از xattrs، این قابلیت به طور پیش‌فرض از نسخه 1.20.1 متوقف شده است.

Scan Link

منبع خبر :

https://securityaffairs.co/wordpress/79413/security/wget-flaw.html

کشف نقص ارتقا سطح دسترسی در محصولات ASA سیسکو

گردآورنده: پویان مسعودی نیا

شدت آسیب‌پذیری

با توجه به گزارشات منتشر شده، شدت این آسیب‌پذیری High می‌باشد.

خلاصه آسیب‌پذیری

یک آسیب‌پذیری ارتقاء سطح دسترسی در محصول ASA سیسکو کشف شده است، که برای کاربری با سطح دسترسی پایین، امکان ایجاد کاربر جدید، تغییر firmware و نیز تغییر فایل حاوی تنظیمات را فراهم می‌آورد.

این آسیب‌پذیری توسط Tenable شناسایی شده و شناسه CVE-2018-15465 به آن اختصاص داده شده است. به واسطه این آسیب‌پذیری برای یک مهاجم از راه دور امکان اجرای دستورات مدیریتی در رابط وب فراهم می‌گردد.

به منظور بهره‌برداری از این آسیب‌پذیری، مهاجم به فعال کردن رابط کاربری HTTP برای IOS نیاز دارد، و باید احراز هویت "AAA"را تنظیم کند، که این تنظیم بخشی از پیکربندی پیش‌فرض ASAv نیست.

آسیب‌پذیری مذکور به دلیل اعتبارسنجی نامناسب مدیریت کاربران در سیستم مدیریت وب اتفاق می‌افتد، مهاجم می‌تواند با ارسال یک درخواست ساختگی HTTP از طریق HTTPS به عنوان یک کاربر غیرمجاز این آسیب‌پذیری را اکسپلویت نماید.

مهاجم می‌تواند از این آسیب‌پذیری برای بازیابی فایل‌ها از دستگاه، یا آپلود و جایگزینی ایمیج نرم‌افزارها در دستگاه آسیب‌پذیر استفاده کند.

این آسیب‌پذیری تمامی تجهیزات ASA سیسکو با دسترسی مدیریت وب فعال را تحت تاثیر قرار می‌دهد.

در حال حاضر شرکت سیسکو راهکارها و وصله‌هایی را منتشر کرده است، که با فعال کردن دستورات Authorization ، از اکسپلویت کردن این آسیب‌پذیری جلوگیری می‌کند.

راهکارهای امنیتی ارائه شده تا کنون

سیسکو توصیه می‌کند: "مدیرانی که از ASDM (Adaptive Security Device Manager) برای مدیریت ASA استفاده می‌کنند، دستورات Authorization را با استفاده از ASDM فعال کنند، زیرا انجام این کار به ASDM اجازه می‌دهد تا دستورات از پیش تعیین شده را برای سطح دسترسی‌های مختلف به ASA اجرا نماید."

Scan Link

منبع خبر :

https://gbhackers.com/privilege-escalation-asa/

افشای آسیب‌پذیری روز صفرم دیگری در ویندوز

گردآورنده: آتوسا خدامرادی

خانم SandboxEscaper (نام مستعار وی در توئیتر) آسیب‌پذیری روز صفرم جدیدی برای ویندوز منتشر نمود که به هکر اجازه می‌دهد داده دلخواه خود را در فایل هدف بازنویسی کند.

این محقق کد اثبات مفهومی آسیب‌پذیری مذکور را در Github منتشر نمود. این چهارمین باگ روز صفرم ویندوز است که وی در یک سال گذشته کشف و افشاء نموده است. وی به تازگی کد اثبات مفهومی این آسیب‌پذیری روز صفرم را به صورت آنلاین منتشر نمود. این کد شامل اکسپلویتی است که به هکر اجازه می‌دهد هر فایلی را در سیستم ویندوزی آسیب‌پذیر بخواند.

آسیب‌پذیری روز صفرم ویندوز

این آسیب‌پذیری توسط محقق امنیتی بلژیکی با نام مستعار SandboxEscaper در توئیتر، کشف و منتشر شد این محقق به طور مداوم از اواخر سال 2018 باگ‌های 1، 2 و 3 ویندوز را افشاء نمود.

اکسپلویت روزصفرم جدید که توسط این محقق در گیت‌هاب منتشر شد اجازه بازنویسی فایل pci.sys را می‌دهد. وی این آسیب‌پذیری را angrypolarbearbug نام نهاد.

Bleeping computer[1] بیان می‌کند که: "اکسپلویت منتشر شده با برخی محدودیت‌ها کار می‌کند و روی برخی CPUها تأثیرگذار نخواهد بود، به عنوان مثال در ماشین‌هایی که CPU یک هسته‌ای دارند امکان استفاده از این باگ وجود ندارد."

تجزیه و تحلیل های بیشتر توسط تحلیلگر CERT/CC انجام شده و گزارش می‌دهد که بازنویسی به طور مداوم رخ نمی‌دهد. وی در توئیت خود افزود آسیب‌پذیری روز صفرم کشف شده توسط خانم SandboxEscaper نیاز به زمان زیادی برای بهره‌برداری دارد. علاوه بر این تنها گاهی اوقات امکان بازنویسی داده‌هایی که توسط هکر وارد شده‌اند وجود دارد. معمولاً داده‌های WER از این قاعده مستثنی هستند.

از آنجا که این آسیب‌پذیری از Pci.sys بهره‌برداری می‌کند، حتی برای کاربرانی که دسترسی admin هم ندارند ممکن است موجب حملات DDoS شود. هم‌چنین می‌تواند موجب از کار افتادن آنتی ویروس گردد.

این محقق معمولاً باگ‌ها را به مایکروسافت گزارش نمی‌دهد، اما این بار آسیب‌پذیری مذکور را به مرکز پاسخگوی امنیتی مایکروسافت (MSRC) گزارش نمود و متأسفانه پیامد آن مسدود شدن حساب کاربری وی در توئیتر بود.

این دومین آسیب‌پذیری روزصفرم ماه دسامبر در سال ۲۰۱۸ و اولین آسیب‌پذیری است که ReadFile.exe را تحت تأثیر قرار می‌دهد (یکی از توابع ویندوز که به خواندن داده‌ها از فایل مشخص شده یا دستگاه‌های ورودی/خروجی کمک می‌کند).

Scan Link

منبع خبر :

https://gbhackers.com/hacker-windows-zero-day-flaw/

کشف آسیب‌پذیری اجرای کد از راه دور در MicrosoftEdge

گردآورنده: آتوسا خدامرادی

شدت آسیب‌پذیری

با توجه به گزارشات، شدت این آسیب‌پذیری critical (حیاتی) گزارش شده است.

خلاصه آسیب‌پذیری

این آسیب‌پذیری با شناسه CVE-2018-8629، موتور جاوا اسکریپت Chakra را که در مرورگر وب مایکروسافت Edge اجرا می‌شود تحت تأثیر قرار می‌دهد. هکر می‌تواند با اکسپلویت این آسیب‌پذیری، کدهای دلخواه خود را توسط کاربری که قبلاً وارد شده است در سیستم هدف اجرا کند. این آسیب‌پذیری می‌تواند حافظه را به گونه‌ای تخریب کند که هکر بتواند کد دلخواه خود را با مجوز کاربر جاری سیستم اجرا کند. پس از این عمل هکر می‌تواند در سیستم قربانی برنامه نصب کند، داده‌ها را ببیند، تغییر دهد یا حذف کند و یا یک حساب کاربری جدید ایجاد نماید. این آسیب‌پذیری در تمامی نسخه‌های

[1] Bleeping computer یک سایت کمک به کامپیوتر است که توسط Lawrence Abrams در سال 2004 تأسیس شد. این یک سایت منبع برای پاسخ به کامپیوتر، امنیت، و سؤالات فنی است. تمام خدمات به عموم مردم رایگان هستند، از جمله نرم‌افزارهای مخرب و پاکسازی روت کیت از کامپیوترهای آلوده و دستورالعمل‌های حذف برنامه‌های جاسوسی.

ویندوز به عنوان آسیب‌پذیری حیاتی شناسایی شده است، اما در ویندوز سرورهای نسخه 2016 و 2019 شدت آن متوسط اعلام شده است.

راهکارهای امنیتی ارائه شده تا کنون

مایکروسافت در به‌روز رسانی امنیتی دسامبر، این آسیب‌پذیری را تحت پوشش قرار داده است اما هم‌چنان سیستم‌های بسیاری در معرض خطر هستند.

Scan Link

منبع خبر :

https://securityaffairs.co/wordpress/79264/hacking/microsoft-edge-poc-exploit.html

انتشار وصله‌های اضطراری Adobe برای دو آسیب‌پذیری بحرانی در محصولات Acrobat و Reader

گردآورنده: سیده مرضیه حسینی

Adobe به‌روزرسانی امنیتی بی سابقه‌ای را برای رفع دو آسیب‌پذیری مهم در محصولات Acrobat و Reader برای سیستم‌عامل‌های ویندوز و macOS منتشر نموده است.

هر دو آسیب‌پذیری توسط دو محقق امنیتی به نام‌های Abdul-Aziz Hariri و Sebastian Apelt از Trend Micro's Zero Day Initiative(ZDI)، گزارش شده‌اند.

آسیب‌پذیری‌های بحرانی Adobe Acrobat و Reader

آسیب‌پذیری اول که با شناسه CVE-2018-16011 توسط Apelt گزارش شده است، باگ use-after-free می‌باشد که می‌تواند منجر به اجرای کد دلخواه گردد.

مهاجمان می‌توانند با فریب دادن کاربر برای کلیک بر روی یک فایل PDF ساختگی، از این نقص بهره برداری نمایند و در نهایت کد انتخابی خود را با امتیازات کاربری که در حال حاضر وارد شده است، اجرا نمایند. این آسیب‌پذیری مهاجم را قادر می‌سازد تا هر نرم‌افزار مخربی را در کامپیوتر قربانی و بدون آگاهی وی، اجرا نماید.

دومین آسیب‌پذیری با شناسه CVE-2018-19725، که توسط Hariri کشف شده است یک نقص امنیتی می‌باشد که می‌تواند منجر به ارتقاء سطح دسترسی گردد.

هر دو آسیب‌پذیری امنیتی در گروه آسیب‌پذیری‌های حیاتی رتبه‌بندی شده‌اند، اما در اولویت 2 قرار گرفته‌اند و این بدان معناست که شرکت هیچ گزارشی از اکسپلویت نمودن آسیب‌پذیری‌های مذکور دریافت ننموده است.

نسخه‌های آسیب‌پذیر و وصله‌های امنیتی

Acrobat و Reader DC 2015 نسخه 2015.006.30461 و قبل از آن، Reader DC 2015 نسخه 2017.011.30110 و قبل از آن، Continuous نسخه 2019.010.20064 و قبل از آن، برای سیستم‌عامل‌های ویندوز و macOS تحت تأثیر این آسیب‌پذیری‌ها قرار گرفته‌اند.

Adobe این آسیب‌پذیری‌ها را با انتشار آخرین نسخه‌های Acrobat DC 2015 و Acrobat Reader DC 2015 (نسخه 2015.006.30464)، Acrobat 2017 و Acrobat Reader DC 2017 (نسخه 2017.011.30113) و Acrobat DC Continuous و Acrobat Reader DC Continuous (نسخه 2019.010.20069) برای ویندوز و macOS برطرف نمود.

از آنجا که این آسیب‌پذیری‌ها در حال حاضر عمومی هستند، به کاربران سیستم‌های مک و ویندوز اکیداً توصیه می‌گردد که در اسرع وقت وصله‌ها را برای این دو آسیب‌پذیری نصب نمایند.

انتشار اکسپلویت آسیب‌پذیری روزصفرم وصله نشده در ویندوز

گردآورنده: پویان مسعودی نیا

یک محقق امنیتی با نام مستعار SandboxEscaper در توییتر، هفته گذشته اکسپلویت کد اثبات مفهومی مربوط به یک آسیب‌پذیری روزصفرم، که سیستم‌عامل‌های مایکروسافتی را تحت تأثیر قرار می‌دهد منتشر نمود.

SandboxEscaper همان محققی است که چندی پیش با انتشار اکسپلویت‌هایی برای دو آسیب‌پذیری روزصفرم وصله نشده در ویندوز، کاربران این سیستم‌عامل را در معرض خطر قرارداده بود.

این آسیب‌پذیری روزصفرم وصله نشده، در واقع باگ مربوط به خواندن فایل است که اجازه خواندن محتویات فایل‌های مهم ویندوز که به دسترسی مدیر نیاز دارند را به یک کاربر با کمترین حق دسترسی، یا یک برنامه مخرب می‌دهد.

آسیب‌پذیری مذکور مربوط به عملکرد تابع "MsiAdvertiseProduct" در ویندوز است که به گفته این محقق، به دلیل اعتبارسنجی نامناسب، تابع مذکور می‌تواند به منظور وادار ساختن سرویس نصب‌کننده برای ایجاد یک فایل کپی از تمامی فایل‌ها به عنوان مجوز SYSTEM و خواندن محتوای آن‌ها مورد سوء استفاده قرار گیرد.

با توجه به اظهارات این محقق، آسیب‌پذیری مذکور از این رو حائز اهمیت است که، بسیاری از نرم‌افزارهای ایجاد سند، مانند Office، در واقع فایل‌ها را در مکان‌های ثابتی نگه می‌دارند که حاوی نام و آدرس کامل مسیر اسنادی است که اخیراً باز شده‌اند. بنابراین با خواندن فایل‌های مشابه این اسناد، می‌توان نام اسناد ایجاد شده توسط سایر کاربران را بدست آورد، و باتوجه به ساختار سیستم‌فایل، می‌توان به فایل‌های ایجاد شده توسط کاربر در هرجایی دسترسی پیدا کرد.

SandboxEscaper علاوه بر به اشتراک‌گذاری ویدئوی نشان‌دهنده این آسیب‌پذیری، لینک حاوی اکسپلویت کد اثبات مفهومی (PoC) آن را نیز در Github قرار داده است. لازم به ذکر است که این کد برای سومین آسیب‌پذیری روزصفرم ویندوز بوده که توسط این محقق در Github قرار داده شده است و نکته قابل توجه این است که حساب کاربری محقق نامبرده در GitHub از آن تاریخ به بعد غیرفعال شده است!

این برای سومین بار در چند ماه اخیر است که SandboxEscaper آسیب‌پذیری روزصفرم ویندوز را فاش می‌کند. در ماه اکتبر،SandboxEscaper اکسپلویت کد اثبات مفهومی را برای آسیب‌پذیری ارتقاء سطح دسترسی در Data Sharing مایکروسافت منتشر نمود که به کاربری با سطح دسترسی پایین اجازه می‌داد بتواند فایل‌های سیستمی مهم و حیاتی را از سیستم ویندوزی قربانی حذف نماید. یا در اواخر ماه آگوست، این محقق جزئیات و اکسپلویت کد اثبات مفهومی را برای نقص ارتقاء سطح دسترسی محلی در Microsoft Task Scheduler افشا نمود که به علت خطا در کنترل سرویس Advanced Local Procedure Call (ALPC) رخ می‌داد.

مدت کوتاهی پس از انتشار اکسپلویت PoC، و پیش از آنکه مایکروسافت آسیب‌پذیری‌های مذکور را در به‌روزرسانی سپتامبر 2018 مرتفع نماید، این آسیب‌پذیری‌ها به طور چشمگیری مورد سوءاستفاده قرار گرفتند.

منبع خبر :

https://thehackernews.com/2018/12/windows-zero-day-exploit.html

منبع خبر :

https://thehackernews.com/2019/01/adobe-reader-vulnerabilities.html?m=1

مقالات آموزشی

آموزش نحوه استفاده از قابلیت "Controlled Folder Access" در ویندوز ۱۰

گردآورنده: سهیلا مرادی

در این آموزش قصد داریم یکی از ویژگی‌های جدید ویندوز 10 که بخشی از ابزار «ویندوز دیفندر» محسوب می‌شود را معرفی نماییم. این قابلیت یک لایه‌ی محافظتی اضافه در مقابل برنامه‌هایی به وجود می‌آورد که ممکن است به هر علتی تلاش نمایند سطح دسترسی کاربر به پوشه‌های شخصی مانند Documents، Pictures، Desktop و... را تغییر دهند. این ویژگی جدید که «Controlled Folder Access» نام گرفته، به صورت پیش‌فرض غیر فعال بوده و برای استفاده از آن باید به صورت دستی فعال گردد.

به طور معمول هر برنامه‌ای که بر روی سیستم در حال اجرا است می‌تواند سعی کند سطح دسترسی کاربر به پوشه‌ها را تغییر داده و در اصل کاربر را از باز کردن فایل‌هایی که در آنها ذخیره دارد محروم نماید. با قابلیت جدیدی که در ویندوز 10 مورد اشاره قرار گرفت، و فعال کردن آن، تنها برنامه‌هایی که توسط مایکروسافت مجاز تشخیص داده شده‌اند یا اپلیکیشن‌هایی که شما آنها را مجاز می‌سازید اجازه خواهند داشت سطح دسترسی کاربر را به فایل‌ها و پوشه‌های شخصی تغییر دهند.

به زبان ساده‌تر، باج‌افزارها دیگر نمی‌توانند در تنظیمات پوشه‌ها و فایل‌هایی که تحت نظارت قابلیت یاد شده قرار دارند تغییری به وجود آورده، یا آنها را رمزنگاری نمایند.

قابلیت Controlled Folder Access به شما کمک می کند که از اطلاعات ارزشمند خود در برابر برنامه‌های مخرب و تهدیداتی مانند باج‌افزارها محافظت نمایید. این قابلیت در ویندوز سرور 2019 و همچنین در ویندوز 10 پشتیبانی می‌شود.

فعال کردن قابلیت Controlled Folder Access

شما می‌توانید قابلیت Controlled Folder Access را با برنامه PowerShell، Group Policy، Security Center یا MDM CSPs فعال کنید. همچنین می توانید این ویژگی را بر روی مُد Audit تنظیم نمایید. مُد Audit امکان تست نحوه عملکرد این قابلیت را بدون تأثیر بر عملکرد عادی سیستم فراهم می‌آورد (رویدادها را چک می‌کند).

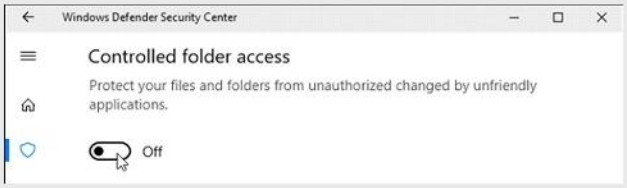
قابلیت Controlled folder access در قسمت Windows Security و تحت تنظیمات Virus & threat protection قرار داشته و وضعیت را نشان خواهد داد. اگر این قابلیت با Group Policy، PowerShell یا MDM CSPs فعال گردد پس از ریستارت شدن سیستم، وضعیت در برنامه Windows Security تغییر خواهد کرد. اگر قابلیت مذکور با هریک از ابزارهای فوق بر روی حالت Audit تنظیم گردد وضعیت برنامه Windows Security به صورت OFF نشان داده خواهد شد.

فعال کردن قابلیت Controlled folder access با استفاده از برنامه Windows Defender Security

- با کلیک بر روی آیکون سپر در نوار وظیفه، یا جستجوی کلمه Defender در منوی start، برنامه Windows Security باز کنید.

- بر روی Virus & threat protection، یا آیکون سپر در منوی سمت چپ کلیک نموده و سپس Ransomware protection را انتخاب کنید.

حال قدری به سمت پائین اسکرول کرده تا به گزینه‌ی Controlled folder access برسید و دکمه‌ی مربوط به آن را با کلیک کردن، در وضعیت On قرار دهید.



* لازم است اشاره کنیم که اگر گزینه‌ی مذکور را نمی‌یابید، احتمالاً ویندوز 10 شما هنوز به نسخه جدید به‌روزرسانی نشده است.

استفاده از Group Policy برای فعال‌سازی قابلیت Controlled folder access

• در قسمت مدیریت Group Policy سیستم خود، کنسول مدیریت Group Policy را باز کنید، بر روی Group Policy Objectی که قصد پیکربندی آن را دارید کلیک راست نموده و Edit را انتخاب کنید.

• در ویرایشگر مدیریت Group Policy بر روی قسمت Computer configuration کلیک نموده و Administrative templates را انتخاب نمایید.

• در منوی درختی سمت چپ، Windows components را بازکرده و سپس مسیر زیر را دنبال کنید:

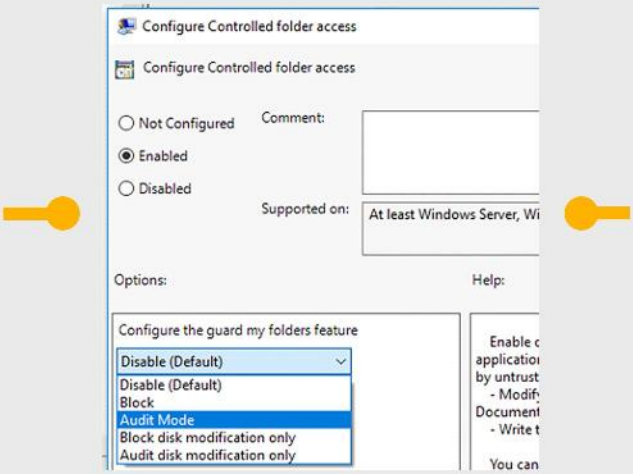
Windows Defender Antivirus > Windows Defender Exploit Guard > Controlled folder access

• بر روی تنظیمات Configure Controlled folder access دابل کلیک نموده و از میان گزینه‌ها Enabled را انتخاب نمایید. در قسمت انتخاب گزینه‌ها باید یکی از موارد زیر را انتخاب کنید:

Enable: برنامه‌های مشکوک و مخرب اجازه ایجاد تغییر در فایل‌های موجود در پوشه‌های محافظت شده را نخواهند داشت. اگر برنامه‌ای سعی کند فایل‌ها را تغییر دهد لاگ آن در قسمت Windows event log ثبت خواهد شد.

Disable (حالت پیش‌فرض): قابلیت Controlled folder access کار نخواهد کرد و تمام برنامه‌ها قادر خواهند بود فایل‌ها را در پوشه‌های محافظت شده تغییر دهند.

Audit Mode: اگر برنامه‌ی مخرب یا مشکوکی سعی کند فایل‌ها را در پوشه‌ی محافظت شده تغییر دهد، این امکان وجود خواهد داشت، اما لاگ آن در قسمت Windows event log ثبت خواهد شد. این به شما اجازه می‌دهد تأثیر قابلیت مذکور را در سازمان خود ارزیابی کنید.



استفاده از PowerShell برای فعال‌سازی قابلیت Controlled folder access

• در منوی start، عبارت powershell را جستجو کنید، بر روی آن کلیک راست نموده و گزینه Run as administrator را انتخاب نمایید.

• دستور زیر را در آن وارد نمایید:

Set-MpPreference -EnableControlledFolderAccess Enabled

به منظور فعال کردن این قابلیت در مُد Audit، باید در بخش نهایی دستور، به جای Enabled از AuditMode استفاده نمایید.

استفاده از MDM CSPs برای فعال‌سازی قابلیت Controlled folder access

از CSP (configuration service provider) به منظور ارائه مجوز برای تغییر فایل در پوشه محافظت شده توسط برنامه‌ها استفاده نمایید.

./Vendor/MSFT/Policy/Config/Defender/GuardedFoldersList

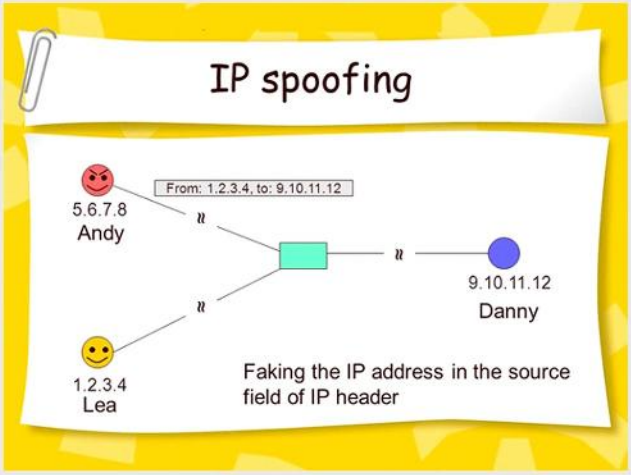
Scan Link

منبع خبر:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/enable-controlled-folders-exploit-guard

راهکارهای مقابله با حملات IP Spoofing

گردآورنده: سیده آرزو حسنی



1. اجتناب ازTrust Relationship ها

در حملات جعل، هکرها برای اینکه خودشان را از دید شما پنهان نمایند هویت خودشان را با هویت کامپیوترها و دستگاه‌هایی که در شبکه شما قابل اعتماد هستند جعل یا Spoof می‌کنند و بسته‌های مخرب خود را به سمت شما هدایت می‌نمایند. اگر شما این بسته‌های آلوده را که به نظر از منابع قابل اعتمادی هستند، بپذیرید به احتمال زیاد شبکه و سیستم‌های شما نیز آلوده خواهند شد. بنابراین پیشنهاد می‌گردد که حتی اگر شبکه‌هایی دارید که برای شبکه شما قابل اعتماد تعریف شده‌اند بسته‌های آن‌ها را نیز واکاوی نمایید. به عنوان مثال اگر دو شبکه در ساختار اکتیودایرکتوری دو شرکت مختلف Trust متقابل ایجاد کرده‌اند بسته‌های آن‌ها نیز باید بررسی گردند. یکی از مهم‌ترین مکانیزم‌های امنیتی که برای جلوگیری از ورود بسته‌های مخرب از شبکه‌های قابل اعتماد پیشنهاد می‌گردد راه‌اندازی مکانیزم احراز هویت با پسورد، برای کامپیوترهایی است که از شبکه‌های Trusted به شبکه شما بسته ارسال می‌کنند. بدیهی است که با این مکانیزم، تا کامپیوتری برای شبکه شما احراز هویت نشود قابلیت ارسال بسته‌های جعل شده را نیز نخواهد داشت. به این کار در اصطلاح فنی Password Authentication در میان Trust Relationship گفته می‌شود.

2. استفاده از فایروال و مکانیزم‌های فیلترینگ Packet

در روش فوق شبکه‌های Trusted را بررسی و معرفی کردیم اما در روش بعدی شما باید کلیه ترافیک‌های ورودی و خروجی به شبکه را با استفاده از فایروال ها و تجهیزات Packet Filtering مناسب مانیتور کنید. ترافیک ورودی به شبکه ممکن است ترافیک آلوده‌ای باشد که هکر به سمت شبکه شما ارسال نموده است، اگر شما هیچگونه مکانیزم فیلترینگ بسته‌ای برای ورود ترافیک به شبکه داخلی ندارید باید بگوییم احتمال زیادی وجود دارد که به IP Spoof دچار شوید. شما می‌توانید در فایروال‌ها و تجهیزات امنیتی خود با استفاده از Access Control List ها یا ACL هایی که می‌نویسید دسترسی‌های غیرمجاز به شبکه داخلی را مسدود نمایید. اما در همین شرایط امکان حمله دیگری نیز وجود دارد و آن، وجود مهاجم از داخل شبکه است، این‌گونه افراد ممکن است از طریق شبکه داخلی، اطلاعات حساس سازمان یا شرکت شما را از شبکه خارج کنند. این کار هم می‌تواند از نظر غیرفنی اعتبار و آبروی سازمان شما را خدشه‌دار کند وهم امکان ارسال و هدایت Packet آلوده توسط هکر به داخل شبکه را فراهم نماید. یعنی ممکن است هکر بتواند با استفاده از یک ابزار آلوده ترافیک شبکه داخلی شما را شنود، و ریسک افشاء اطلاعات محرمانه سازمانی شما را بسیار بالا ببرد. به همین دلیل پیشنهاد می‌گردد که شما حتی برای ترافیک‌های خروجی از شبکه نیز Access Control List طراحی کنید و به هر فرد و هر ترافیکی اجازه عبور غیرمجاز از شبکه داخلی به سمت بیرون را ندهید. این مکانیزم امنیتی معمول‌ترین مکانیزمی است که در خصوص جلوگیری از حملات IP Spoof در اکثر سازمان‌ها در حال حاضر در حال اجرا می‌باشد.

3. استفاده از Random Initial Sequence Number

بسیاری از تجهیزات، ISN یا Initial Sequence Number بسته‌های اطلاعاتی خود را بر اساس وهله‌های زمانی تعیین می‌کنند. این روش باعث می‌شود که مهاجمین به راحتی بتوانند نحوه تولید کردنISN ها را پیدا کنند و از آن‌ها برای تولیدISN های جعلی در TCP Connection بعدی استفاده نمایند و خود را درون Session قرار دهند. اگر هکر بتواند الگوریتم ایجاد ISN شما را بیابد می‌تواند

وارد شبکه شده و یک ارتباط مخرب ایجاد نماید و ترافیک سرور و شبکه شما را شنود کند. برای جلوگیری از این مشکل شما می‌توانید از مکانیزم صدور تصادفی ISN ها در ارسال و دریافت بسته‌ها استفاده نمایید.

4. تعریف فوانین ترافیک‌های معین ورودی و خروجی

شما می‌توانید در فایروال‌های خود چه برای ترافیک ورودی و چه برای ترافیک خروجی مقاصد معین تعیین کنید. به عنوان مثال، مشخص کردن آدرس وب سایت‌هایی که کاربران شما صرفاً می‌توانند به آن‌ها متصل شوند یا اینکه مشخص کردن آدرس‌های داخلی که از بیرون، درخواست‌ها باید به آن‌ها ارسال شود. با این روش اگر هکر بخواهد ترافیکی را از شبکه داخلی شما به آدرس دلخواه خود ارسال نماید این امکان برای وی وجود نخواهد داشت. این شیوه با استفاده از تعریف ACL در روترها و فایروال‌ها قابل اجرا می‌باشد.

5. رمزنگاری یا Encryption

برای رسیدن به بالاترین درجه امنیت در شبکه بایستی برای کلیه ترافیک شبکه خود از یک مکانیزم رمزنگاری قوی استفاده نمایید. هکرها همیشه به دنبال راه‌هایی هستند که به سادگی بتوانند ورود کنند، اگر هکر بتواند وارد یک شبکه رمزنگاری شده شود، متوجه می‌شود که کل ترافیک به صورت رمزنگاری شده رد و بدل می‌شود و کار هکر به شدت در این موارد سخت می‌شود، و به همین دلیل هکر به دنبال تکنیک‌های دیگری برای نفوذ خواهد بود، یا نقطه آسیب پذیر دیگری را می‌یابد که الگوریتم ضعیف‌تری داشته باشد. اکثر تکنیک‌های جلوگیری از حملات SYN Flood در مقابل IP Spoofing نیز می‌توانند مؤثر باشند.

منبع خبر:

Scan Link

https://bit.ly/2D1dTZn

اخبار کوتاه

با سه نشانه مهم از آلودگی مک به ویروس آشنا شوید

متأسفانه سیستم‌عامل مکینتاش دیگر مثل گذشته جزء امن‌ترین سیستم‌عامل‌ها به شمار نمی‌رود و با اینکه وجود ویروس‌ها در آن نسبت به ویندوز کمترند، اما همچنان وجود دارند. اگر مک شما رفتارهای ناهنجاری از خود نشان می‌دهد یا به طور مکرر در آن تبلیغ‌های نامربوط مشاهده می‌کنید، شاید سیستم شما به بدافزار آلوده شده است.

اما آیا مک شما آلوده شده است؟ نگاهی به نشانه‌های مک آلوده داشته باشید:

1. تبلیغات ناخواسته و پاپ آپ‌ها
2. کند شدن بی دلیل سیستم‌عامل
3. اسکنرها وجود آنتی‌ویروس را تأیید کنند

درآمد سرشار توسعه‌دهندگان باج افزار Ryuk طی 5 ماه

بر اساس برآورد محققان مؤسسات CrowdStrike و FireEye ، باج‌افزار Ryuk تنها در 5 ماه درآمدی 3.7 میلیون دلاری را طی 52 تراکنش بیت‌کوین عاید هکرها کرده است. به گفته این تحلیلگران نکته اصلی در دستیابی به این مبلغ بردباری هکرها و تمرکز روی اهداف بزرگ بوده است.

حملات معمولاً با آلوده کردن سیستم به باج‌افزار TrickBot از طریق روش‌هایی نظیر ایمیل اسپم شروع می‌شد که هدف از آن تنها دسترسی به سیستم قربانی و برآورد پتانسیل درآمد و بودجه آنها بود.

امنیت کاربر رایانه

با توجه به خطـــرات امنیتـــی روزافزون اینترنت بـــرای کاربران، دســـت‌اندرکاران ویـنـــدوز ابزارهای متنوعـــی را در نظـــر گرفته‌اند که به کمـــک آن بتوانید از بروز مشـــکلات پیش‌بینی شـــده جلوگیری کنید. مشـــکلاتی همچون برنامه‌های جاسوســـی، کی‌لاگرها، تروجان‌ها و غـــــــیره، که بســـیار می‌توانند خطرناک باشـــند و خســـارات جبران‌ناپذیـــری را به بار آورند. آشـــنایی با ایـــن ابزارها و روش‌هـــای مقابله با مشـــکلات احتمالی، مخصوصـــاً برای شـــرکت‌هایی که کارکنانشـــان از ویندوز استفاده می‌کنند به شدت ضروری است.

در ایـــــن شماره از بولتـــــن خبری قصد داریم در ادامـــــه مبحث امـــــنیت سیستم‌عامل‌ها، ابزارهای امنیتی ویندوز را معرفی نماییم.

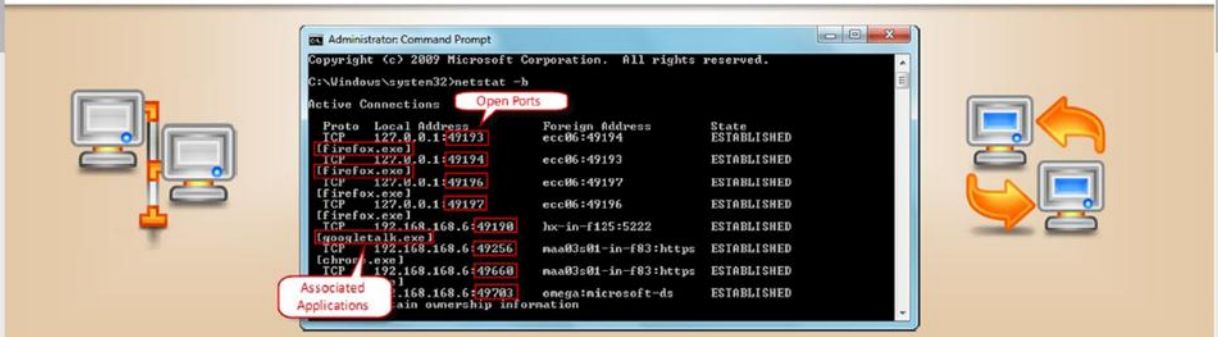
با ما همراه باشید...

یافتن پورت های باز با استفاده از ابزار Netstat

- آگاهی از پورت های باز، سرویس ها و برنامه های مرتبط با پورت ها در تشخیص وجود بدافزار در سیستم، مانند ویروس، کرم، تروجان و غیره کمک می کند
- بدافزار معمولاً پورت ها را برای دریافت یا ارسال بسته های داده به مهاجم باز می کند
- Netstat یک قابلیت درون ساخت در ویندوز است که می تواند برای تعیین پورت های باز در سیستم و برنامه های مرتبط با آن ها درسیستم مورد استفاده قرار گیرد
- از مسیر زیر Command Prompt را باز کنید :

Start-> type cmd in search bar-> Right click on cmd-> Run as administrator

- دستور netstat -b را در cmd وارد نمایید تا لیست پورت های باز و برنامه های مرتبط با آن ها نشان داده شود

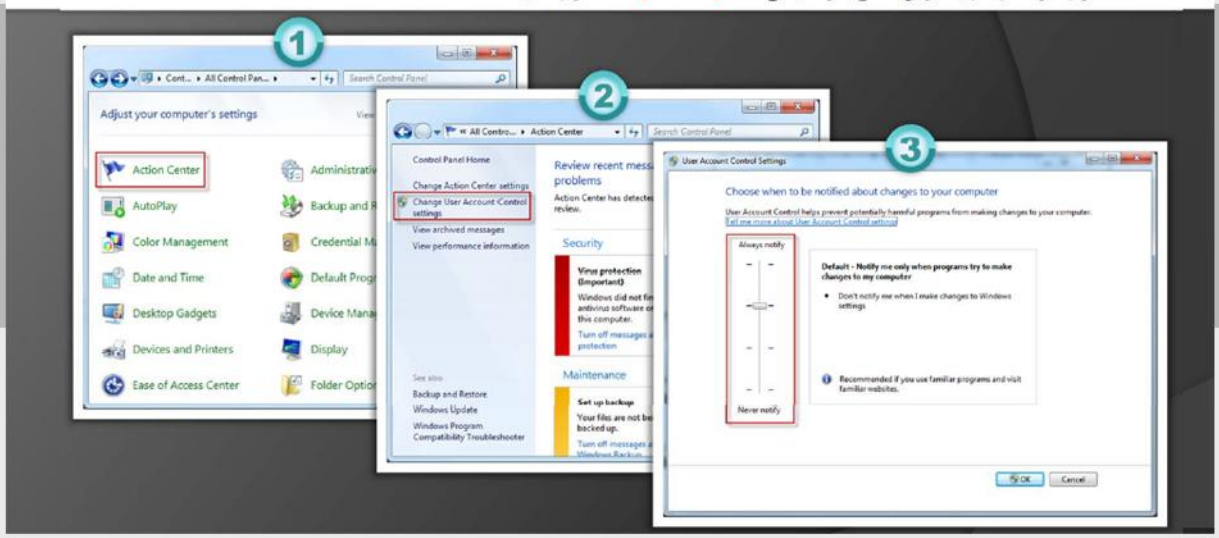


استفاده از کنترل حساب کاربری در ویندوز (UAC)

- کنترل حساب کاربری (UAC) به کاربر کمک می کند تا در هنگام نصب نرم افزار تصمیمات مهمی را اتخاذ نماید
- در مسیر زیر:

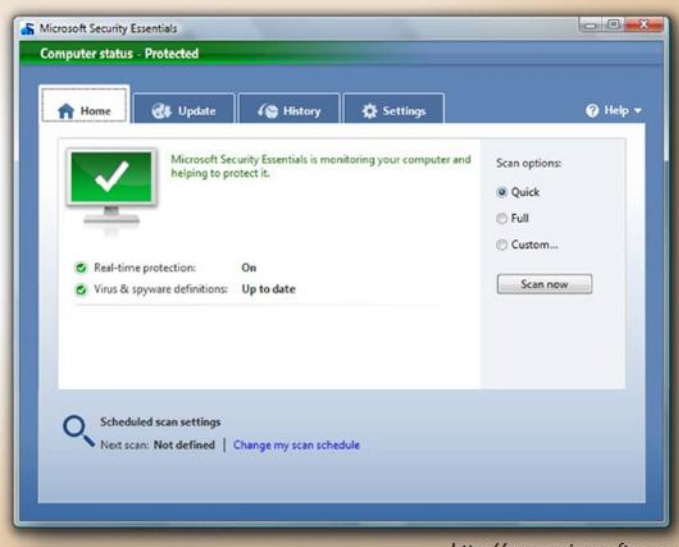
Start-> Control Panel-> User Account Control-> Change User Account Control Settings

نوار لغزنده را در بالاترین سطح خود، یعنی Always notify me قرار دهید



ابزارهای امنیتی ویندوز: Microsoft Security Essentials

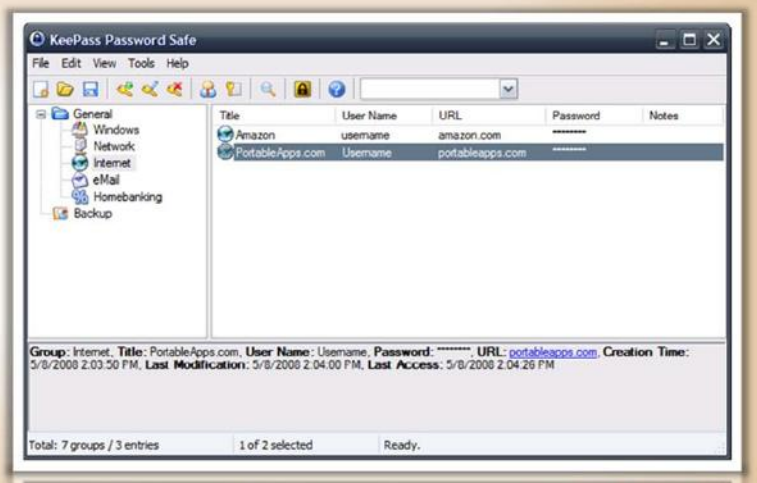
Microsoft Security Essentials
امکان محافظت بلادرنگ را برای یک سیستم خانگی فراهم می آورد، که آن را در مقابل ویروس ها، جاسوس افزارها و سایر نرم افزارهای مخرب محافظت می کند



http://www.microsoft.com

ابزارهای امنیتی ویندوز: KeePass Password Safe Portable

- KeePass یک ابزار مدیریت پسورد است که رمزهای عبور را به شیوه ای ایمن مدیریت نموده و تمام پسوردها را در یک پایگاه داده نگهداری می کند، که با یک masterkey یا key_disk قفل می شود
- این پایگاه داده، با استفاده از الگوریتم های رمزنگاری شناخته شده فعلی مانند(AES_256) و (Twofish) رمزگذاری می شود



http://portableapps.com

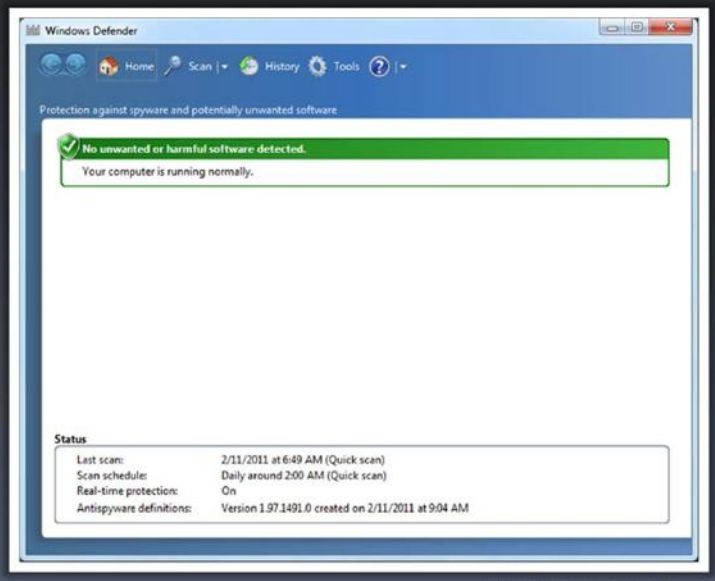
ابزارهای امنیتی ویندوز : Registry Mechanic

1. Registry Mechanic ابزارهایی را جهت افزایش سرعت و بهبود عملکرد ویندوزهای 7، ویستا وXP ارائه می دهد
2. Registry Mechanic به صورت کاملاً امن، رجیستری را پاکسازی، تعمیر و بهینه سازی نموده و به صورت اتوماتیک از تغییرات صورت گرفته برای بازیابی های آتی پشتیبان گیری می نماید
3. به طور مداوم فعالیت های اینترنتی، فایل های شخصی و فضای آزاد را پاک می کند تا اطلاعات را به دور از چشم جاسوسان نگه دارد

http://www.pctools.com

ابزارهای امنیتی ویندوز: Windows Defender

Windows Defender با شناسایی و حذف جاسوس افزارهای شناخته شده از یک سیستم، آن را از شر پاپ آپ ها، عملکرد کند و تهدیدات امنیتی ناشی ازجاسوس افزارها و سایرنرم افزارهای مخرب مصون می دارد



http://www.microsoft.com

منابع موجود در اینترنت برای امنیت کامپیوتر

خلاصه مباحث مطرح شده در فصل "امنیت سیستم‌عامل‌ها"

- مهاجمان برای‌اکسپلویت نمودن نرم افزارهای کامپیوتری مدام در پی یافتن آسیب پذیری ها و باگ های جدید هستند
- عرضه کنندگان نرم افزار، معمولاً برای رفع مشکلات امنیتی وصله هایی را ارائه می کنند
- رمزگذاری، فرآیند تبدیل داده ها به یک کد مخفی است
- به طور منظم سیستم عامل و برنامه های خود را بروز رسانی کنید
- در صورت خرابی سیستم یا به وجود آمدن مشکلات عمده در آن، Windows System Restore به منظور بازگردانی کامپیوتر به وضعیت قبلی مورد استفاده قرار می گیرد
- Microsoft Security Essentials امکان محافظت بلادرنگ را برای یک سیستم خانگی فراهم می آورد، که آن را در مقابل ویروس ها، جاسوس افزارها وسایر نرم افزارهای مخرب محافظت می نماید
- Windows Defender به محافظت از سیستم در مقابل پاپ آپ ها، عملکرد کُند و سایر تهدیدات امنیتی کمک می کند

اخبار داخلی

نشست و هم‌اندیشی دومین دوره مسابقات فتح پرچم آپا با حضور مسئولین سازمان‌ها و دانشگاه‌های سطح استان

روز سه‌شنبه مورخ ۱۱ دی ماه ۱۳۹۷، جلسه‌ای با محوریت همکاری و همفکری به منظور برگزاری دومین دوره مسابقات فتح پرچم در غرب کشور با حضور مسئولین و نمایندگان سازمان‌ها، بخش خصوصی و دانشگاه‌های سطح استان در دانشکده فنی مهندسی دانشگاه رازی برگزار گردید.

دکتر منکرسی مدیر مرکز تخصصی آپا ضمن معرفی فعالیت های مرکز، گزارشی از نحوه برگزاری و نتایج اولین دوره مسابقات فتح پرچم (CTF) که سال گذشته در دانشگاه رازی برگزار شد ارائه نمودند. ایشان هدف از برگزاری این جلسه را گسترش همکاری و ارتباط با فعالان حوزه فناوری اطلاعات استان به منظور برگزاری هرچه بهتر این مسابقه مطرح کردند.

در ادامه جلسه، کمبود نیروی متخصص امنیت سایبری به عنوان یکی از مشکلات حال حاضر استان توسط مهندس سپیده‌دم نماینده اداره کل ارتباطات و فناوری اطلاعات استان مطرح گردید. ایشان خاطر نشان نمودند که برگزاری چنین رویدادهایی می تواند در جهت ترغیب دانشجویان به این موضوع و تربیت نیروی متخصص گامی مثبت قلمداد گردد.

در ادامه، شرکت‌کنندگان حاضر در جلسه در مورد مسائلی همچون تعیین اعضاء کمیته‌های علمی، فنی، تبلیغات، زمان برگزاری مسابقه، نحوه برگزاری، کانال‌های اطلاع رسانی و حامیان مسابقه به بحث و تبادل نظر پرداختند.

در پایان، جمع حاضر در جلسه با برگزاری دومین دوره مسابقه فتح پرچم غرب کشور در اردیبهشت ماه سال ۹۸ به توافق رسیدند. همچنین مقرر گردید تصمیم‌گیری در خصوص محورهای اصلی مسابقه و جزئیات برگزاری در جلسات آتی در کمیته‌های تخصصی انجام پذیرد.

کلاهبرداری میلیونی از طریق اپلیکیشن‌های جعلی

رئیس پلیس فتا مازندران از شناسایی افرادی که با تبلیغ برنامه‌های غیرمجاز در شبکه‌های اجتماعی، مردم را فریب داده و اقدام به کلاهبرداری میلیونی از طعمه‌های خود کرده بودند، خبر داد.

پایگاه اطلاع‌رسانی پلیس فتا: سرهنگ حسن محمدنژاد رئیس پلیس فتا استان مازندران در تشریح این خبر اعلام کرد: یکی از شهروندان با ارائه مرجوعه قضایی به این پلیس مراجعه و اظهار داشت چندی پیش در یک کانال تلگرامی که آدرس آن را به خاطر ندارم عضو شدم و سپس به منظور پرداخت مبلغ 5 هزار تومان، لینک نرم‌افزار درگاه پرداخت موجود در کانال را دانلود کرده و سپس بعد از درج اطلاعات حساب بانکی‌ام، در مدت کوتاهی مبلغ 430 میلیون ریال از حسابم به صورت اینترنتی برداشت شد، از این‌رو پیگیر موضوع شدم.

سرهنگ محمد نژاد در ادامه عنوان کرد: با توجه به شکایت صورت‌گرفته و با هماهنگی مقام قضایی، مراتب در دستور کار کارشناسان این پلیس قرار گرفت که با تحقیقات تخصصی و اطلاعاتی صورت‌گرفته مشخص شد متهم علاوه بر فرد مذکور، اقدام به سرقت از حساب بانکی افراد دیگری نیز نموده است.

این مقام انتظامی افزود: به همین منظور با بررسی‌های به عمل آمده مشخص گردید برداشت از حساب مالباختگان با استفاده از چندین خط تلفن همراه صورت گرفته و وجوه سرقتی نیز از طریق سامانه‌های پرداخت موبایلی انتقال یافته است که سرانجام با بررسی‌های فنی و تخصصی انجام شده، متهم به هویت معلوم ساکن یکی از شهرستان‌های استان خوزستان شناسایی گشت.

سرهنگ محمدنژاد اشاره کرد: مأموران این پلیس با اخذ نیابت قضایی به شهرستان موردنظر مراجعه کرده و متهم را دستگیر کردند که وی در تحقیقات به عمل آمده ضمن اقرار به جرم خود گفت چندی پیش از طریق تلگرام با شخصی آشنا شدم و در ادامه او به من پیشنهاد پولشوئی از حساب اشخاصی که هک می‌کرد را داد، من نیز با استفاده از اطلاعات حساب بانکی افرادی که او برایم می‌فرستاد اقدام به انتقال وجوه از طریق سامانه‌های پرداخت موبایلی می‌نمودم و در نهایت مبالغ را تبدیل به ارز دیجیتال کرده و سهم 20 درصدی خود را دریافت و بقیه مبلغ را به صورت ارز دیجیتال برایش ارسال می‌کردم.

وی گفت: در ادامه رسیدگی پرونده، کارشناسان این پلیس متهم اصلی پرونده را که ساکن یکی از شهرهای اطراف شهرستان موردنظر بود شناسائی و دستگیر کردند و در بازرسی از منزل او تعدادی سیمکارت، گوشی تلفن همراه و وسایل دیگر بدست آمد.

این مقام مسئول خاطرنشان کرد: متهم در تحقیقات انجام شده ضمن اقرار به جرم خود عنوان داشت که از اواخر تابستان سال جاری با طراحی نرم‌افزارهای صیغه‌یاب، ماهواره جیبی و ایجاد درگاه جعلی بر روی آن‌ها و انتشار آن در گروه‌ها و کانال‌های تلگرامی، اقدام به اخذ اطلاعات حساب بانکی اشخاص کرده و در فرصتی مناسب اقدام به برداشت از حساب‌ها می‌کردم.

این مقام انتظامی با بیان اینکه متهمان جهت سیر مراحل قانونی به دادسرا تحویل داده شدند،عنوان کرد: در بازبینی از سیستم‌های رایانه‌ای و گوشی تلفن همراه متهمان، نرم‌افزارهای صیغه‌یاب و ماهواره جیبی به همراه فایل‌های تکست شامل اطلاعات حساب بانکی تعداد یک هزار و 769 نفر نیز شناسایی شد.

رئیس پلیس فتا مازندران در پایان با بیان اینکه امروزه بسیاری از برنامه‌های غیرمجاز که در فضای مجازی وجود دارند، در واقع طعمه‌ای از سوی کلاهبرداران می‌باشند، گفت: کاربران مراقب باشند تا به هر برنامه‌ای که در فضای مجازی تبلیغ می‌شود اعتماد نکنند، زیرا افراد سودجو از طریق این نرم‌افزارها کاربران را به درگاه‌های جعلی کشانده و اقدام به کلاهبرداری از آن‌ها می‌کنند.

سرهنگ محمدنژاد در خاتمه به خانواده‌ها توصیه کرد : همواره به دنبال این باشید تا سواد رسانه‌ای خود را افزایش دهید و به طور جدی مراقب فعالیت‌های فرزندان خود در فضای مجازی باشید تا اینکه ندانسته و از روی کنجکاوی گرفتار خطرات آن نشوند.

منبع خبر : پایگاه اطلاع‌رسانی پلیس فتا

ثبت نام

دوره های مرکز تخصصی آپا دانشگاه رازی

همراه با ارائه مدرک معتبر

با اسانیدی مجرب دارای مدارک بین المللی

MikroTik MTCNA

دوره آموزشی میکروتیک MTCNA
مدرس:مهندس سعید نادری
طول دوره: 40 ساعت

C|EH Certified Ethical Hacker V10

دوره هکر قانونمند CEH
مدرس: مهندس مهدی اسفندیاری
طول دوره:50 ساعت

CompTIA Security+

دوره مقدماتی Security+
مدرس : مهندس مهدی فرهمند
طول دوره: 40 ساعت

سرفصل های این دوره ها منطبق با سرفصل مدارک MTCNA,CEHv10,Security+ تدریس می شود

با توجه به محدودیت ظرفیت اولویت با افرادی است که زودتر ثبت نام کنند

مهلت ثبت نام تا ۲۰ بهمن ماه ۹۷

جهت ثبت نام به آدرس cert.razi.ac.ir مراجعه نمایید

مرکز تخصصی آپا دانشگاه رازی
دانشگاه رازی
اداره کل ارتباطات و فناوری اطلاعات استان کرمانشاه
Edu_APARazi
@Edu_APARazi
083-34273390


مرکز تخصصی آپا دانشگاه رازی