بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره شانزدهم

دی ماه ۱۳۹۸

پایان عمر ویندوز ۷

و ماجراهای پس از آن!

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:
مرکز تخصصـــی آپـا دانشگـاه رازی

صفحه آرایی: **سید احسان حسینی**

سردبیران:
سیده مرضیه حسینی
صبا آزرمی

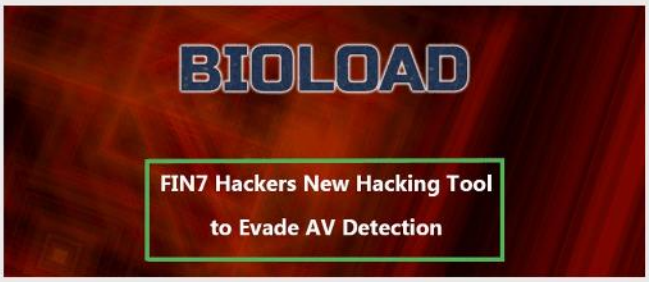
با همکاری
سیده آرزو حسنی

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

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

اخبار امنیتی

حمله هکرهای FIN7 به ویندوزهای 64 بیتی با ابزار جدید BIOLOAD



اخیـــراً محققان امنیتـــی ابزار هک جدیدی بـــه نام BIOLOAD کشـــف کرده اند که به گروه هکرهای FIN7 نسبت داده می‌شـــود. این ابزار با هدف به حداقل رساندن ردپای موجود در دســـتگاه قربانی و جلوگیری از شناســـایی، اقـــدام به فعالیت‌های مخرب می‌کند.

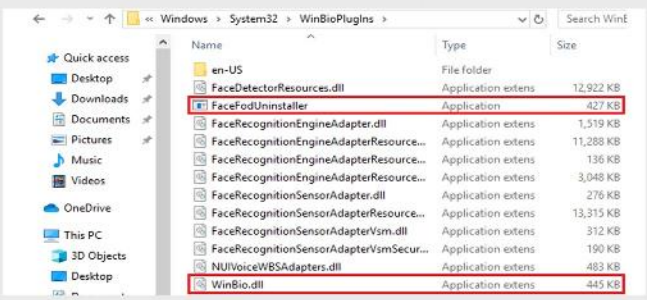
ابزار جدید شـــباهت‌هایی با ابـــزار BOOSTWRITE FIN7 دارد که از دســـتور جستجوی DLL برنامه‌ها سوءاستفاده می‌کند. BOOSTWRITE از سرویس‌های مجاز DirectX Typography مایکروسافت به نام "Dwrite.dll" در جهت اهداف خود استفاده می‌کند.

BIOLOAD در واقع نســـخه جدیدی از ابزار BOOSTWRITE است که هر دوی آنها دارای کدبندی یکسانی بوده و درب پشتی Carbanak را در سیستم‌های مورد هدف پایه‌گذاری می‌کنند. همچنین در سیستم‌عامل‌های ویندوز به دنبالDLL های مورد نیاز خود برای لود کردن در برنامه می باشند.

ابزار BIOLOAD از FaceFodUninstaller.exe در سیستم‌عامل ویندوز سوءاستفاده می‌کند و اجرای آن به("%WINDR%\System32") winbio.dll بستگی دارد. FaceFodUninstaller وظیفه داخلی برنامه‌ریزی شده ای دارد که مهاجمان علاقه خاصی به این فرآیند دارند. مسیر این فایـــل به صورت زیـــر است:

("%WINDR%\System32\WinBioPlugIns")

مهاجمان با قرار دادن نسخه جعلی WinBio.dll (حاوی حروف بزرگ) در همان فایلی که FaceFodUninstaller قرار دارد، DLL های پیش فرض را جستجو می‌کنند. برای قرار دادن این نسخه، مهاجم باید از امتیازات بالایی در دستگاه قربانی مانند مدیریت یا یک حساب کاربری SYSTEM برخوردار باشد.



DLL در پوشه اجرایی قرار داده شده است

BIOLOAD به زبان C ++ نوشته و در مارس و ژوئیه سال 2019 کامپایل شد و به طور خاص دستگاه‌های سیستم‌عامل 64 بیتی را مورد هدف قرار داده است. این برنامه دارای یک پیلود رمزگذاری شده مانند BOOSTWRITE است که برای رمزگشایی از الگوریتم XOR یا واکشی استفاده می‌کند. BIOLOAD نیز مانند BOOSTWRITE ، تنها از یک تک پیلود پشتیبانی می‌کند.

به نظر می رسد گروه هکرهای FIN7 از اواسط سال 2015 فعالیت خود را آغاز کرده‌اند و همچنان در حال افزودن ابزارهای جدیدی به فرآیندهای کاری خود برای شکست راه حل‌های امنیتی هستند.

منبع خبر :

https://gbhackers.com/fin7-bioload/

Scan Link

سرقت رمزهای عبور از طریق استقرار بدافزار Predator the Thief در اسناد ورد

نسخه جدید بدافزار Predator the Thief، که از طریق داکیومنت‌های جعلی گسترش می‌یابد، با هدف سرقت اطلاعات حساس کاربران منتشر شده است.

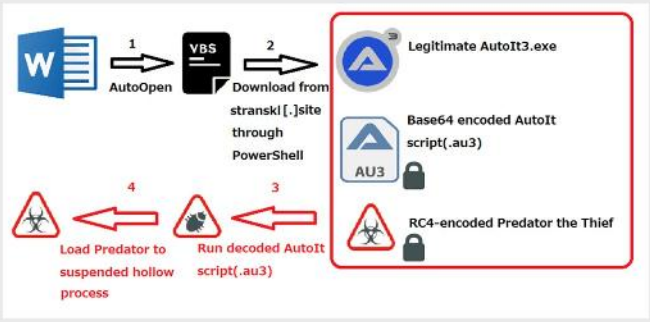
Predator the Thief بدافزاری است که به جمع‌آوری اطلاعات حساس مانند نام کاربری، رمزهای عبور، داده‌های مرورگر و اطلاعات حساب بانکی می‌پردازد و اولین بار در ژوئیه سال 2018، توسط Fortinet مورد شناسایی قرار گرفت. عاملان انتشار این بدافزار، در فاصله زمانی کوتاهی توانستند آن را ارتقاء دهند.

بدافزار مذکور تماماً به زبان C/C++ نوشته شده است و بدافزارهایی که در فروم‌های زیرزمینی فروخته می‌شوند بین 35 تا 80 دلار قیمت دارند.

آخرین نسخه Predator the Thief

Fortinet آخرین نسخه Predator the Thief یعنی 3.3.4 را با قابلیت‌های بیشتر مورد شناسایی قرار داده است. این نسخه از داکیومنت‌های جعلی استفاده می‌کند تا این بدافزار را به عنوان پی‌لود نهایی ارائه دهد.

هنگامی که کاربر فایل ورد را باز می‌کند، AutoOpen macro - macro یک الگوی قابل برنامه‌ریزی است که توالی خاصی از ورودی را به توالی از پیش تعیین شده خروجی ترجمه می‌کند- اسکریپت VBA بدافزار را به منظور دانلود سه فایل با استفاده از Powershell، اجرا می‌کند.



VjUea.dat – نسخه مجاز AutoIt3.exe

SevSS.dat – اسکریپت AutoIt رمزگذاری شده براساس Base64 که برای رمزگشایی certutil.exe استفاده می‌شود

apTz.dat – بدافزار Predator the Thief رمزگذاری شده براساس RC4

اسکریپت SevSS.dat با استفاده از ابزار certutil.exe رمزگشایی می‌شود و در اولین رمزگشایی از AutoIt3.exe مجاز برای اجرای اسکریپت AutoIt رمزگذاری شده، استفاده می‌کند. سپس اسکریپت AutoIt، apTz.dat را که در واقع پی‌لود نهایی بدافزار است، رمزگشایی می‌کند.

بدافزار مذکور، اطلاعات سرقت شده را به عنوان یک فایل zip ارسال می‌کند، این فایل در سیستم‌فایل تولید نمی‌شود ، در عوض، به صورت مستقیم از حافظه به داده‌های درخواست اضافه می‌شود.

ارتباطات سرور C2

ارتباط با سرورهای C2 از طریق API ایجاد و با استفاده از الگوریتم‌های base64 و RC4 پایه رمزگذاری می‌شوند.

لیست اطلاعاتی که جمع‌آوری و برای سرورهای C2 ارسال می‌شوند به صورت زیر است:

- رمز عبور
- کوکی‌ها
- اطلاعات کارت‌های بانکی
- اطلاعات حساب‌های کاربری Skype و Steam
- حساب‌های کاربری تلگرام
- پیکربندی روش اجرای ماژول
- و غیره

این بدافزار به توسعه خود ادامه می‌دهد و از ابزارهای مجاز برای اجرای این پی‌لود و جلوگیری از تشخیص، سوءاستفاده می‌کند.

منبع خبر :

https://gbhackers.com/predator-the-thief-malware/

Scan Link

ریسک امنیتی استخراج ارز دیجیتال در فایل‌های صوتی ویندوز 7

ویندوز 7 از تاریخ 14 ژانویه 2020رسماً به دلیل عدم پشتیبانی شرکت مایکروسافت، منقضی شده است و این در حالیست که میلیون‌ها کاربر رایانه‌ای همچنان از این سیستم عامل استفاده می‌کنند!

چرخه‌ی پشتیبانی ده ساله مایکروسافت از این سیستم‌عامل به پایان رسیده است و مایکروسافت پشتیبانی رسمی خود را از ویندوز 7، در زمینه‌ی فنی و بروزرسانی‌های امنیتی که از طریق آپدیت ویندوز صورت می‌پذیرفت متوقف می‌کند و این در حالی است که بسیاری از این سرویس‌ها بدون در نظر گرفتن ویندوز 7، برای سایر محصولات این شرکت ادامه خواهند داشت.

بر اساس گزارش‌ها، 32.74% از کاربران رایانه‌ای در سراسر جهان و بسیاری از کاربران کشور چین نیز از این سیستم‌عامل استفاده می‌کنند. و این مسئله موجب می‌شود بسیاری از رایانه‌ها در معرض تهدیدات امنیتی جدید قرار گیرند که در واقع برای رفع آن‌ها هیچ وصله‌ای وجود نخواهد داشت.

از آنجا که بروزرسانی‌های امنیتی منتشر شده در آینده، ویندوز 7 را پوشش نخواهد داد بنابراین آسیب‌پذیری امنیتی بحرانی استخراج ارز دیجیتال هم چنان در فایل‌های WAV صوتی این سیستم‌عامل باقی خواهد ماند.

خطر استخراج ارز در فایل‌های WAV ویندوز 7

Ophir Harpaz و Daniel Goldberg، دو محقق امنیتی آزمایشگاه Guardicore، فاش کردند که چگونه یک سکتور فنی پزشکی با اندازه متوسط، توسط استخراج کننده های ارز دیجیتال و با استفاده از فایل‌های صوتی WAV مورد حمله قرار گرفت.

مهاجمین از دسامبر سال 2019، در تلاش برای اکسپلویت آسیب‌پذیری EternalBlue در ویندوز 7 در حال اجرا بر روی کامپیوترها بودند. تصور می‌شود که این مسئله توسط آژانس امنیت ملی آمریکا (NSA) توسعه یافته است، حدود دو سال است که از اکسپلویت آسیب‌پذیری EternalBlue می‌گذرد. این حمله به حملات WannaCry که در سال 2017 به خدمات ملی بهداشت ایالات متحده (NHS) رسیده بود مربوط می‌شود. اخیراً اعلام شده است که حدود 4,700 دستگاه با سیستم‌عامل ویندوز 7 و سرور 2008 در معرض این حمله قرار دارند.

محققان به کاربرانی که همچنان قصد دارند از ویندوز 7 استفاده کنند توصیه می‌کنند که برای در امان ماندن از این حملات، از اتصال سیستم خود به اینترنت جلوگیری نمایند.

منبع خبر :

https://bit.ly/3anF8fF

Scan Link

اخبار کوتاه

خرید از سایت‌های فروشگاهی غیر معتبر

خرید کردن از فروشگاه‌های دارای مجوز نماد اعتماد الکترونیکی، زمینه افزایش امنیت کاربران در فضای مجازی را فراهم کرده و مانع از برداشت غیر مجاز از حساب آنان می‌شود.

همواره امنیت در خریدهای اینترنتی یکی از مهمترین دغدغه‌های هموطنان است. از آنجایی که علت بسیاری از کلاهبرداری‌های اینترنتی صورت گرفته، اعتماد بیش از حد قربانیان به افراد فعال در فضای مجازی می‌باشد لذا کاربران عزیز با در نظر گرفتن برخی از نکات کوچک می‌توانند دست مجرمین سایبری را در رسیدن به اهداف مجرمانه کوتاه نمایند. بنابراین لازم و ضروری است که هموطنان گرامی نسبت به خریدهای اینترنتی خود کمی دقت و حساسیت داشته و نسبت به برقراری روابط با افراد آنلاین در فضای مجازی توجه بیشتری داشته باشند. خرید از فروشگاه‌های اینترنتی دارای نماد اعتماد الکترونیکی از جمله راهکارهایی است که تا حدود زیادی می‌تواند امنیت کاربران در فضای مجازی را افزایش دهد.

پس:

- از فروشگاه‌های دارای نماد اعتماد الکترونیکی خرید کنید.
- اطلاعات بانکی خود را در اختیار دیگران قرار ندهید.
- لیست کسب و کارهای دارای اینماد را در سایت enamad.ir مشاهده نمایید.

خرید کردن از فروشگاه های دارای مجوز نماد اعتماد الکترونیکی، زمینه افزایش امنیت کاربران در فضای مجازی را فراهم کرده و مانع از برداشت غیر مجاز از حساب آنان می شود.

اپلیکیشن‌های نامعتبر را جهت دریافت رمز یکبار مصرف نصب نکنید

رئیس پلیس فتا کرمان، با توجه به اجرای طرح الزامی کردن دریافت رمز دوم یکبار مصرف پویا یا otp به شهروندان هشدار داد: برای دریافت اپلیکیشن رمز پویا حتما به فروشگاه‌های معتبر و یا شعب بانک مراجعه کنند، پایگاه اطلاع‌رسانی پلیس فتا: سرهنگ امین یادگارنژاد رئیس پلیس فتا استان کرمان در تشریح این خبرگفت: در کنار گسترش روز افزون بازار موبایل و فناوری های مرتبط با آن، استفاده از Application یا نرم‌افزارهای موبایلی این روزها زیاد شنیده می‌شود و این در حالی است که برخی افراد سودجو با ساخت یکسری نرم‌افزار، در پی سوءاستفاده از این فرصت بدست آمده هستند .

وی ادامه داد: این افراد سودجو، با توجه به اجرای طرح دریافت رمز دوم یکبار مصرف پویا اقدام به تبلیغ و ارائه خدمات به شهروندان با طراحی اپلیکیشن‌های جعلی سعی دارند اعتماد کاربران را در فضای مجازی جلب نمایند تا شهروندان را قربانی برخی اهداف شوم خود کنند.

سرهنگ یادگارنژاد افزود: با دانلود و نصب این اپلیکیشن‌ها سرقت اطلاعات ذخیره شده بر روی گوشی همراه یا سیستم‌ها صورت می‌گیرد، اطلاعاتی مانند عکس ذخیره شده بر روی دستگاه و یا اطلاعات بانکی به راحتی از سوی مجرمان سایبری به سرقت می‌رود.

آسیب پذیری

کشف چندین آسیب‌پذیری در نرم‌افزار مدیریت شبکه دیتاسنتر سیسکو (DCNM)!

به دنبال این آسیب‌پذیری‌ها مهاجمان می‌توانند از راه دور فرآیند احراز هویت را دور زده و اقدامات دلخواه خود را با سطح دسترسی مدیر بر روی یک دستگاه آسیب‌دیده اجرا نمایند.

با توجه به اینکه این آسیب‌پذیری‌ها به یکدیگر وابسته نیستند، بنابراین اکسپلویت یکی از آنها به دیگری وابسته نخواهد بود. علاوه بر این، یک نسخه نرم‌افزاری که تحت تأثیر یکی از آسیب‌پذیرها قرار دارد ممکن است تحت تأثیر دیگر آسیب‌پذیری‌ها قرار نگیرد.

محصولات آسیب‌پذیر

آسیب‌پذیری‌ها ذکر شده، نسخه 11.3(1) نرم‌افزار DCNM سیسکو برای سیستم‌عامل‌های ویندوز، لینوکس و دستگاه‌های مجازی را تحت تأثیر قرار می‌دهد.

آسیب‌پذیری دور زدن تأیید هویت در RESTAPI با شناسه "CVE-2019-15975"

این آسیب‌پذیری در RESTAPI نرم‌افزار DCNM سیسکو امکان دور زدن تأیید هویت را در یک دستگاه آسیب‌دیده برای مهاجم فراهم می‌کند. این آسیب‌پذیری ناشی از یک کلید رمزگذاری شده استاتیک مشترک بین برنامه‌های نصب شده است. مهاجم می‌تواند با اکسپلویت آن و با استفاده از این کلید استاتیک، یک توکن سشن ساختگی ایجاد کند. در نهایت پس از یک اکسپلویت موفق، مهاجم قادر خواهد بود از طریق RESTAPI و با سطح دسترسی مدیر، اقدامات دلخواه خود را انجام دهد.

آسیب‌پذیری دور زدن تأیید هویت در SOAPAPI با شناسه "CVE-2019-15976"

این آسیب‌پذیری در SOAPAPI نرم‌افزار DCNM سیسکو امکان دور زدن تأیید هویت را در یک دستگاه آسیب‌دیده برای مهاجم فراهم می‌کند. این آسیب‌پذیری ناشی از یک کلید رمزگذاری استاتیک مشترک بین برنامه‌های نصب شده است. مهاجم می‌تواند با اکسپلویت آسیب‌پذیری ذکر شده و با استفاده از این کلید استاتیک، یک توکن سشن ساختگی ایجاد کند و در نهایت پس از یک اکسپلویت موفق، قادر است از طریق SOAPAPI و با سطح دسترسی مدیر، اقدامات دلخواه خود را انجام دهد.

آسیب‌پذیری دور زدن تأیید هویت در مدیریت شبکه دیتاسنتر سیسکو با شناسه "CVE-2019-15977"

این آسیب‌پذیری که در رابط مدیریت مبتنی بر وب DCNM سیسکو وجود دارد موجب دور زدن فرآیند تأیید هویت توسط مهاجم از راه دور در دستگاه آسیب‌دیده می‌شود.

علت آسیب‌پذیری فوق، وجود اطلاعات ورود استاتیک است. یک مهاجم می‌تواند این آسیب‌پذیری را با استفاده از اطلاعات ورود استاتیک برای تأیید هویت در رابط کاربری، اکسپلویت نماید. یک اکسپلویت موفق، می‌تواند به مهاجم اجازه دهد تا به بخش خاصی از رابط وب دسترسی پیداکرده و اطلاعات محرمانه خاصی را از یک دستگاه آلوده بدست آورد و از این اطلاعات مهم برای انجام حملات بیشتر بر روی دستگاه استفاده کند.

نسخه‌های وصله شده

شرکت سیسکو، آسیب‌پذیری‌های مذکور را در نسخه 11.3(1) نرم‌افزار DCNM سیسکو رفع کرده است. جهت دانلود این نرم‌افزار از سایت سیسکو، مراحل زیر را دنبال کنید:

1. به لینک **https://software.cisco.com/download/home** مراجعه کنید.
2. بر روی بخش **Browse All** در این صفحه کلیک کنید.
3. **Cloud and Systems Management > Data Center Infrastructure Management >** **Data Center Network Manager** را انتخاب کنید.
4. **از بخش سمت چپ صفحه، نسخه مورد نظر خود را انتخاب کنید.**

منبع خبر :
https://bit.ly/3aqiTWu

Scan Link

لزوم بروزرسانی مرورگر فایرفاکس در پی آسیب‌پذیری بحرانی روز صفرم

اگر از مرورگر فایرفاکس در سیستم‌های ویندورز، لینوکس و یا مک استفاده می‌کنید، سریعاً مرورگر خود را از طریق وب‌سایت Mozilla به روزرسانی نمایید!

پیش از این نیز، موزیلا نسخه‌های Firefox 72.0.1 و Firefox ESR 68.4.1 را جهت رفع یک آسیب‌پذیری روز صفرم در این مرورگر منتشر کرده بود.

در واقع این نقص بحرانی با شناسه "CVE-2019-17026"، ناشی از نوعی آسیب‌پذیری 'type confusion vulnerability' در کامپایلر IonMonkey just-in-time (JIT) در SpiderMonkey موتور جاوااسکریپت است.

به طور کلی این نوع آسیب‌پذیری زمانی رخ می‌دهد که کد برنامه، از objectهای ارسالی، کورکورانه و بدون بررسی نوع آن‌ها استفاده کرده و به مهاجمان اجازه می‌دهد تا موجب از کار افتادن این برنامه یا اجرای کد موردنظر خود شوند.

موزیلا بدون آشکار ساختن جزئیات و نیز حملات احتمالی این نقص امنیتی اذعان داشت: "اطلاعات غلط در کامپایلر IonMonkey JIT جهت تنظیم عناصر آرایه، می‌تواند علت این نوع از آسیب‌پذیری باشد."

این بدان معناست که این مسئله در موتور آسیب‌پذیر جاوااسکریپت، می‌تواند توسط یک مهاجم از راه دور برای فریب کاربر به بازدید از یک صفحه وب مخرب و سپس اجرای کد دلخواه خود بر روی سیستم و در چارچوب برنامه، مورد اکسپلویت قرار گیرد.

این آسیب‌پذیری توسط محققان امنیت سایبریِ Qihoo 360ATA به موزیلا گزارش شده است و هنوز هیچ اطلاعاتی از آن‌ها درباره تحقیقات، یافته‌ها و اکسپلویت این آسیب‌پذیری منتشر نشده است.

اگرچه مرورگر فایرفاکس به طور پیش فرض و خودکار بروزرسانی‌ها را اعمال می‌کند و پس از راه‌اندازی مجدد آن، نسخه جدید در دسترس می‌باشد، اما می‌توانید از مسیر زیر نیز مرورگر خود را بروزرسانی نمایید:

Menu > Help > About Mozilla Firefox

منبع خبر :
https://thehackernews.com/2020/01/firefox-cyberattack.html

Scan Link

اکسپلویت آسیب‌پذیری اندورید و نصب بدافزار توسط مهاجمان

محققان امنیتی Trend Micro موفق به کشف سه برنامه مخرب در Google play شدند که هدف آن‌ها به خطر انداختن دستگاه قربانی و سرقت اطلاعات آن است.

این سه برنامه Camero، FileCryptManager و CallCam می‌باشند که در میان آن‌ها، Camero حاصل اکسپلویت آسیب‌پذیری CVE-2019-2215 است.

این نخستین حمله‌ای است که با اکسپلویت آسیب‌پذیری CVE-2019-2215 صورت گرفته است. و با این اکسپلویت، مهاجمان می‌توانند فایل‌ها را بدون تعامل کاربر، دانلود کنند.

استقرار بدافزار

برنامه‌های وابسته به گروه SideWinder APT، که از سال 2012 شروع به فعالیت کرده است، به دلیل حمله به سیستم‌های ویندوزی واحدهای نظامی، شناخته شده است.

این برنامه‌ها تحت عنوان اپلیکیشن‌های Camera و Filemanager خود را معرفی می‌کنند.

Camera – Dropper[1]

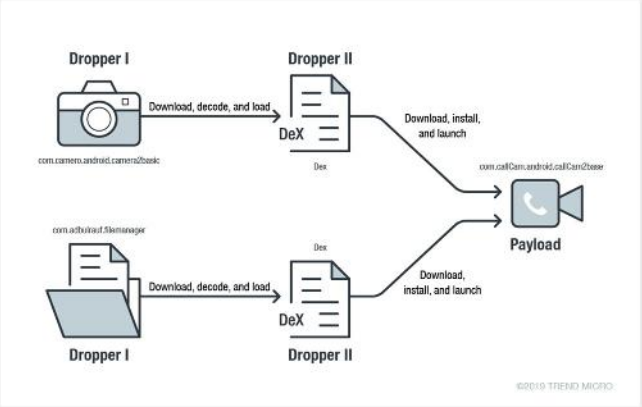
FileCryptManager – Dropper

CallCam – پی‌لود نهایی که اطلاعات را به سرقت می‌برد

SideWinder این پی‌لود را در دو مرحله مستقر می‌کند:

1. فایل DEX را از سرور C&C مهاجم دانلود می‌کند.

2. فایل DEX بارگیری شده، یک APK را که پس از اکسپلویت دستگاه یا بکارگیری قابلیت دسترسی نصب می‌شود، بارگیری می‌کند.



براساس پست منتشر شده از جانب Trend Micro: "همه‌ی این فعالیت‌ها بدون هیچگونه اطلاع و مداخله کاربر انجام شده و برای عدم شناسایی نیز از تکنیک‌های مختلفی مانند مبهم‌سازی[2]، رمزگذاری داده‌ها و استناد به کد پویا استفاده می‌شود."

پس از استقرار پی‌لود نهایی، این dropperها سعی می‌کنند تا دسترسی root و یا مجوز دسترسی به دستگاه مورد هدف را بدست آورند.

پی‌لود نهایی - CallCam

آیکن این برنامه مخرب پس از راه‌اندازی بر روی دستگاه قربانی مخفی شده و با اجرا در پس‌زمینه‌ی دستگاه مورد هدف، شروع به جمع‌آوری اطلاعات می‌کند. داده‌های به سرقت رفته، با استفاده از الگوریتم‌های RSA و AES رمزگذاری شده و به سرور C&C مهاجم فرستاده می‌شوند.

در ادامه اطلاعاتی که از طریق این برنامه‌های مخرب به سرقت برده می‌شوند آمده است:

1. موقعیت مکانی دستگاه
2. وضعیت باتری
3. فایل‌ها
4. لیست اپلیکیشن‌های نصب شده
5. اطلاعات دستگاه
6. اطلاعات سنسور
7. اطلاعات دوربین
8. اسکرین‌شات
9. حساب کاربری
10. اطلاعات وایفای
11. داده‌های جیمیل، فیسبوک، ایمیل یاهو، توییتر، کروم، WeChat و Outlook.

هر سه برنامه‌ی نام برده شده از ماه مارس 2019 فعال هستند و در حال حاضر از Google Play حذف شده‌اند.

منبع خبر :

https://gbhackers.com/sidewinder-apt-group/

Scan Link

کشف آسیب‌پذیری در پایگاه‌داده SQLite مرورگر کروم

چندین آسیب‌پذیری مهم به نام "Magellan 2.0" در پایگاه‌داده SQLite مرورگر گوگل کروم، که یکی از محبوب‌ترین مرورگرهای جهان محسوب می‌شود، کشف شده است. این آسیب‌پذیری‌ها مهاجمان را قادر می‌سازند تا با اکسپلویت فرآیند Chromium، کد دلخواه خود را از راه دور اجرا کنند.

SQLite یک پایگاه‌داده محبوب است که به طور گسترده برای ذخیره‌سازی به صورت local/client در نرم‌افزارهای کاربردی مانند مرورگرهای وب و سیستم‌عامل‌ها مورد استفاده قرار می‌گیرد.

این آسیب‌پذیری بر نسخه 79.0.3945.79 و نسخه‌های قبل‌تر مرورگر کروم دارای

[1] Dropper نوعی Trojan است که به منظور نصب یک نوع بدافزار (ویروس، backdoor و غیره) در سیستم قربانی طراحی شده است.

[2] obfuscation

WebSQL تأثیر می‌گذارد. محققان تأیید کرده‌اند که سایر دستگاه‌ها مانند IoT، تلفن همراه و کامپیوترهای شخصی نیز بسته به شدت حمله، ممکن است تحت تأثیر آسیب‌پذیری‌های مذکور قرار گیرند.

این آسیب‌پذیری در ابتدا توسط تیم Tencent Blade Team کشف شد و آنها توانستند با موفقیت آن را در مرورگر کروم آزمایش کرده و این آسیب‌پذیری را در فرآیند Chromium اکسپلویت نمایند.

جزئیات آسیب‌پذیری Magellan 2.0

این آسیب‌پذیری‌ها عمدتاً بر نرم‌افزاری که از SQLite به عنوان یک مؤلفه استفاده می‌کند تأثیر می‌گذارند و از کوئری‌های داخلی SQL نیز پشتیبانی می‌کند. مهاجمان از این آسیب‌پذیری‌ها برای اجرای از راه دور کدهای دلخواه خود که باعث نفوذ به حافظه و یا کرش شدن برنامه می‌شود استفاده می‌کنند.

به این آسیب‌پذیری‌ها شناسه‌های CVE-2019-13734 ، CVE-2019-13750 ، CVE-2019-13751، CVE-2019-13752، CVE-2019-13753 و اختصاص داده شده است.

به گزارش Tencent ، اگر مرورگرهای دارای WebSQL شرایط زیر را داشته باشند می توانند تحت تأثیر آسیب‌پذیری‌های "Magellan" قرار گیرند:

- Chrome / Chromium از نسخه 79.0.3945.79 و قبل‌تر (که از این پس تحت عنوان "نسخه قدیمی" نام برده می‌شوند).
- دستگاه‌های هوشمند که از نسخه قدیمی Chrome / Chromium استفاده می‌کنند.
- مرورگرهای ساخته شده با نسخه قدیمی Chromium / Webview.
- اپلیکیشن‌های اندرویدی که از نسخه قدیمی Webview استفاده می‌کنند.
- نرم‌افزاری که از نسخه قدیمی Chromium استفاده می‌کند.

منبع خبر :

https://gbhackers.com/magellan-2-0/

Scan Link

اخبار کوتاه

پنهان سازی بدافزار ارزکاوی در فایل‌های صوتی ویندوز

در حالی که هنوز چند روزی از پایان پشتیبانی مایکروسافت از ویندوز 7 سپری نشده محققان از کشف آسیب‌پذیری خطرناکی خبر داده‌اند که با هدف استخراج رمزارز صورت می‌گیرد.

Ophir Harpaz و Daniel Goldberg دو محقق امنیتی موسسه Guardicore Labs از حمله هکرها به کاربران ویندوز 7 با استفاده از فایل‌های صوتی خبر داده‌اند. مهاجمان در این حمله بدافزار را در قالب فایل صوتی پنهان کرده و شبکه‌های سازمانی را با استفاده از اکسپلویت EternalBlue هدف قرار می دهند. EternalBlue یکی از ابزارهای هک به سرقت رفته از آژانس امنیت ملی آمریکا است که در حملات مرگبار واناکرای هم بکار برده می‌شد.

علاوه بر این در هفته‌های آتی آسیب‌پذیری‌های دیگری هم در این سیستم‌عامل پیدا خواهد شد که از سوی مایکروسافت رفع نمی‌شوند. Goldberg به شرکت‌ها توصیه می‌کند اگر قصد به روزرسانی سیستمی را ندارند آنرا از اینترنت و دیگر اجزای شبکه ایزوله کنند. مایکروسافت قبلا به کاربران توصیه کرده بود برای در امان ماندن از حملات سایبری به استفاده از ویندوز 10 روی آورند.

فیشینگ در کمین کاربران تلفن همراه

رئیس پلیس فتا کرمان درخصوص کلاهبرداری با ارسال پیامک انبوه با عنوان قطع شدن تلفن همراه هشدار داد و گفت: شهروندان برای بررسی ریجیستری خود حتما از طریق سامانه همتا www.hamta.ntsw.ir اقدام نمایند. سرهنگ امین یادگارنژاد رئیس پلیس فتا کرمان در تشریح این خبر گفت: اخیراً پیامکی برای برخی افراد ارسال شده است، با متن، "مشترک گرامی دستگاه شما قانونی است ولی فعال نشده برای جلوگیری از قطع شدن شبکه موبایل تا 24 ساعت جهت فعال سازی اقدام نمائید "hamta.cc". سایت مذکور با نام سامانه همتا شبیه‌سازی شده و در هنگام وارد کردن اطلاعات مربوطه ابتدا با دریافت مبلغی به منظور کارمزد، اطلاعات کارت بانکی شهروندان را به سرقت می‌برد. سرهنگ امین یادگارنژاد افزود: کاربر از طریق لینک موجود در این پیامک‌ها به صفحه‌ای شبیه به سامانه اینترنتی گمرک همتا و سپس به صفحه‌ای هدایت می‌شود که ظاهر آن شبیه درگاه‌های پرداخت است و مشخصات کارت بانکی از کاربر دریافت و نهایتاً در دام فیشینگ گرفتار می‌شود. رئیس پلیس فتا کرمان به شهروندان توصیه کرد: از سه روش زیر می‌توانند با سامانه همتا ارتباط برقرار نموده و فرآیند فعال‌سازی دستگاه و یا انتقال مالکیت را انجام دهند: سایت اینترنتی به آدرس www.hamta.ntsw.ir، کد دستوری #7777* و اپلیکشین همتا.

مقالات آموزشی

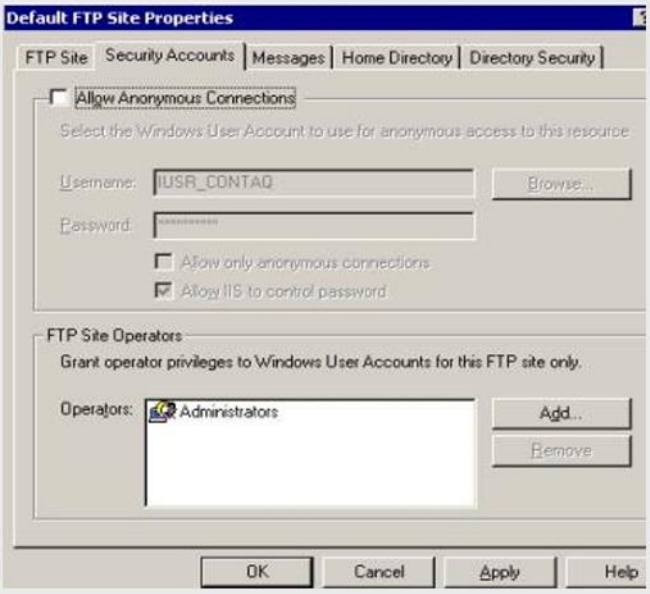
راهکارهای امن سازی FTP سرور

پروتکل FTP مخفف File Transfer Protocol ، یک پروتکل لایه Application است که منحصراً از استاندارد TCP/IP استفاده می‌کند و در عین حال ساده‌ترین و سریعترین راه برای تبادل فایل از مبدأ به مقصد می‌باشد. پورت پیش‌فرض برای دریافت داده TCP 21 و برای انتقال داده از درگاه TCP 20 استفاده می‌شود.

اما پروتکل FTP دارای معایب امنیتی از قبیل عدم پشتیبانی از رمزنگاری است که کلمات عبور را بصورت CLEAR و بدون رمزنگاری انتقال می‌دهد، در ادامه به راهکارهایی جهت امن‌سازی این سرویس اشاره می‌کنیم.

1- غیر فعال نمودن Anonymous Account

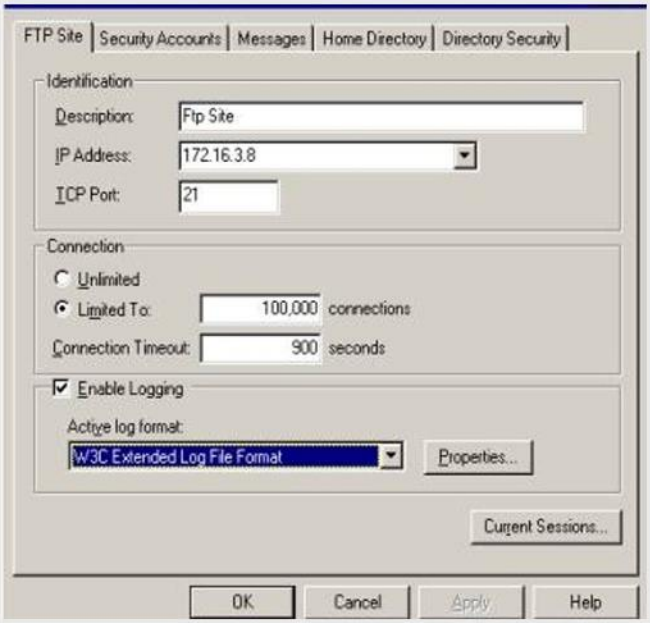
در ابتدا و پس از فعال ساختنFTP، دسترسی‌هایی ناشناس به صورت پیش‌فرض در سیستم به وجود می‌آیند. به عبارتی هر فردی بدون ثبت و Autentication قادر به استفاده از FTP Site خواهد بود. به غیر از موارد خاص، از این خاصیت در اکثر اوقات استفاده غیر مجاز می‌شود. با حذف دسترسی Anonymous که به معنای ناشناس است و استفاده از کلمه عبور و Password مختص کاربر، قادر به کنترل دسترسی‌ها خواهیم بود. این عمل با تنظیم ACL یا (Access Control List) روی FTP Home Directory که در سیستم NTFS وجود دارد قابل انجام است.



برای محدود کـــــردن دسترسی‌هـــــای ناشنـــــاس بهFTP ، گزینه مربوط بـــه Allow Anonymous Connection در پنجره Security Accounts واقـــع در FTP Property را بردارید.

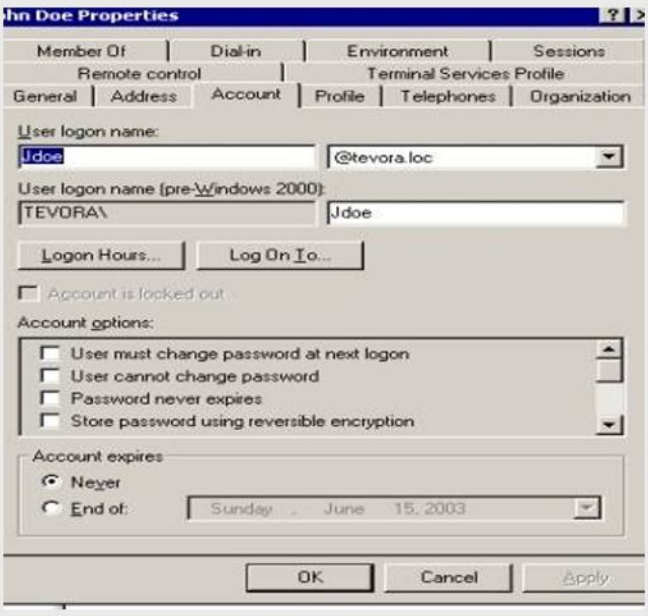
2 - فعال کردن گزارش‌گیری

با فعال شدن گزارش‌گیری، شما از اینکه چه کسانی با کدام آدرس شبکه (IP) به سایت شما دسترسی یافته‌اند آگاهی خواهید یافت. مرور گزارش‌ها شما را قادر می‌سازد ترافیک سایت را تشخیص داده و متوجه تهدیدهای امنیتی و مشکلات شوید. برای فعال ساختن گزارش‌گیری از FTP Site، Enable Logging را در صفحه Property فعال کنید. با این عمل فایل‌های گزارش با فرمت خاص قابل مرور شدن و تجزیه و تحلیل خواهند بود.



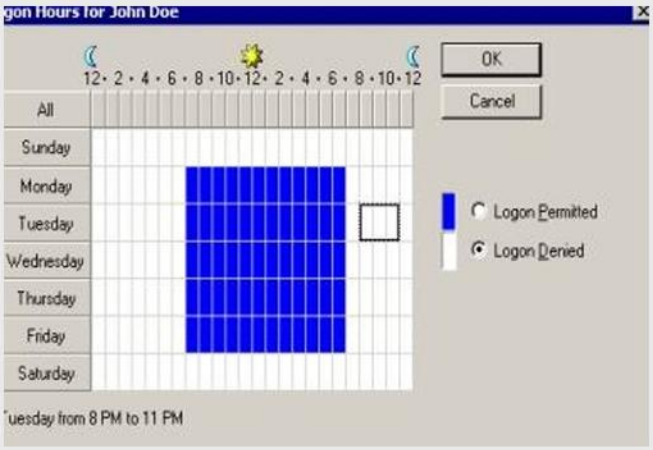
3- محدودسازي زمان Logon

اين خاصيت امكان دسترسي كاربران را تنها در ساعت‌هاي خاص فراهم مي‌آورد. در واقع با اين كار دسترسي‌هاي مجاز كاربران را محدود به زمان مي‌كنيم. به عنوان مثال اگر از FTP Site براي مقاصد كاري استفاده مي‌كنيد زمان دسترسي مي‌تواند به زمان شروع و پايان كار محدود شود. با Deny كردن Logon بعد از ساعات كاري شما بطور مؤثري FTP Site خود را ايمن ساخته‌ايد.



تنظیم مربـــوط به زمـــان Logon در صفحه User Property واقـــــع در Active Directory Users مي‌باشد.

Net user <username> /times :



Local user account براي زمان Login در Local Users و Group Console امكان‌پذير نيست لذا اين خاصيت در GUI در دسترس نمي‌باشد.

اخبار کوتاه

از حافظه تجهیزات هوشمند برای نگهداری اطلاعات شخصی استفاده نکنید

رئیس پلیس فتا استان گلستان از هموطنان خواست از ارسال تصاویر شخصی و خصوصی خود درمحیط شبکه‌های اجتماعی و پیام رسان‌ها خودداری کنند زیرا که این موضـــوع می‌تواند منجر به از دست رفتن اطلاعاتشان شود. پایگاه اطلاع‌رسانی پلیس فتا: سرهنگ ابراهیم پرسا، رئیس پلیس فتا استان گلستان در تشریح این خبر اظهار داشت: تاکنون تعداد زیادی مرجوعه قضایی مبنی بر سوء استفاده از اطلاعات شخصی کاربران به اداره پلیس واصل شده که نشان می‌دهد از اطلاعات شهروندان سوء استفاده شده است. سرهنگ پرسا گفت: برخی از شهروندان اطلاعات شخصی شامل تصاویر و فیلم‌های خانوادگی خود را درون حافظه گوشی هوشمند خود نگهداری می‌کنند که این موضوع می‌تواند منجر به از دست رفتن اطلاعاتشان شود؛ زیرا گوشی شما ممکن است مفقود یا سرقت شود یا اینکه ممکن است با آلوده شدن به نرم‌افزارها و بدافزارهای مختلف مورد دسترسی غیر مجاز توسط مجرمان سایبری قرار گیرد.

این مقام انتظامی یادآور شد: بهتر است برای حفظ اطلاعات مهم خود نسبت به تهیه یک دستگاه هارد اقدام کرده و همه اطلاعات مهم و خصوصی خود را درون این حافظه نگهداری کنند و ضمن رمزگذاری آن، در محل امن و مناسبی نگهداری کنند.

امنیت کاربر رایانه

امنیت شبکه

امروزه ارتباطات و شبکه‌های کامپیوتری مقوله‌ای اجتناب ناپذیر از مباحث حوزه فناوری اطلاعات است. هر زمان که صحبت از شبکه و ارتباطات آن است، امنیت شبکه نیز به همراه آن مطرح می شود. مزایای تأمین امنیت شبکه‌های کامپیوتری نه تنها از حملات سایبری سازمان یافته جلوگیری می کند، بلکه کارکردهای کسب وکار شما را در جهت پیشرفت سوق می دهد.

در این شماره از بولتن خبری، در فصل "امنیت شبکه" قصد داریم به راه‌های امن‌سازی ارتباطات و آداپتورهای شبکه بپردازیم. ادامه مبحث امنیت شبکه را در شماره‌های بعدی بولتن خبری دنبال کنید.

با ما همراه باشید ...

استفاده از فایروال

- فایروال بخشی از یک سیستم کامپیوتری/شبکه است که به منظور جلوگیری از دسترسی های غیرمجاز طراحی شده است
- فایروال ترافیک ورودی و خروجی سیستم را با مجوز دادن به ارتباطات مجاز کنترل می کند
- فایروال شبکه خانگی کاربر را از دید دنیای بیرون پنهان می کند
- فایروال می تواند نرم افزاری یا سخت افزاری باشد
- استفاده از فایروال های شخصی بر روی تمام کامپیوترها توصیه می گردد
- فایروال تمام درخواست های ورودی به سیستم را مانیتور نموده، به کاربر هشدار می دهد، و برای پذیرفتن/مسدود نمودن درخواست ها از کاربر سؤال می کند

نمونه هایی از فایروال های نرم افزاری:

- فایروال ویندو ز
- فایروال شخصی Norton
- فایروال شخصی McAfee
- فایروال شخصی Sunbelt
- ZoneAlarm
- فایروال شخصی Comodo

استفاده از آنتی ویروس

آنتی ویروس برای جلوگیری، تشخیص و حذف بدافزارهایی مانند ویروس های کامپیوتری، کرم ها و تروجان ها مورد استفاده قرار می گیرد

آنتی ویروس ها دارای قابلیت حفاظت "real-time"، به منظور اسکن بلادرنگ فایل ها و ایمیل ها در هنگام دریافت، می باشند

آنتی ویروس باید در سرور استفاده شود

آنتی ویروس باید برای اسکن موارد زیر پیکربندی گردد:

- تمام ایستگاه های کار ی
- اسکن کل شبکه به طور منظم
- ترافیک ورودی و خروجی
- پیوست های ایمیل
- دانلودها
- مرورها

AVG

McAfee Proven Security

Norton AntiVirus

KASPERSKY lab

نمایی از محیط چند آنتی ویروس مشهور

آنتی ویروس Kaspersky

آنتی ویروس AVG

آنتی ویروس Norton

رمزگذاری داده

- رمزگذاری، فرآیند تبدیل داده به یک فرم غیرقابل خواندن به نام **Cipher text** می باشد
- این عمل از اطلاعات حساسی که به صورت آنلاین انتقال می یابند محافظت می کند
- رمزگذاری یک روش مؤثر برای دستیابی به امنیت داده است
- مرورگرهای وب زمانی که به یک سرور امن متصل می شوند به طور خودکار متن را رمزگذاری می کنند

3

پشتیبان گیری های منظم

- پشتیبان گیری منظم از داده ها، به بازیابی داده به هنگام وقوع حوادث امنیتی کمک می کند
- از تنظیمات روتر و فایروال پشتیبان تهیه کنید
- قبل از وقوع یک رویداد امنیتی، یک دیسک بوت تهیه کنید. این دیسک به هنگام آسیب دیدن سیستم یا تسخیر شدن آن به بازیابی سیستم کمک می کند
- برای کسب اطلاعات بیشتر در رابطه با نحوه پشتیبان گیری، به فصل **پشتیبان گیری از داده و بازیابی** آن هنگام وقوع فاجعه مراجعه نمایید

2

استفاده از پسوردهای قوی

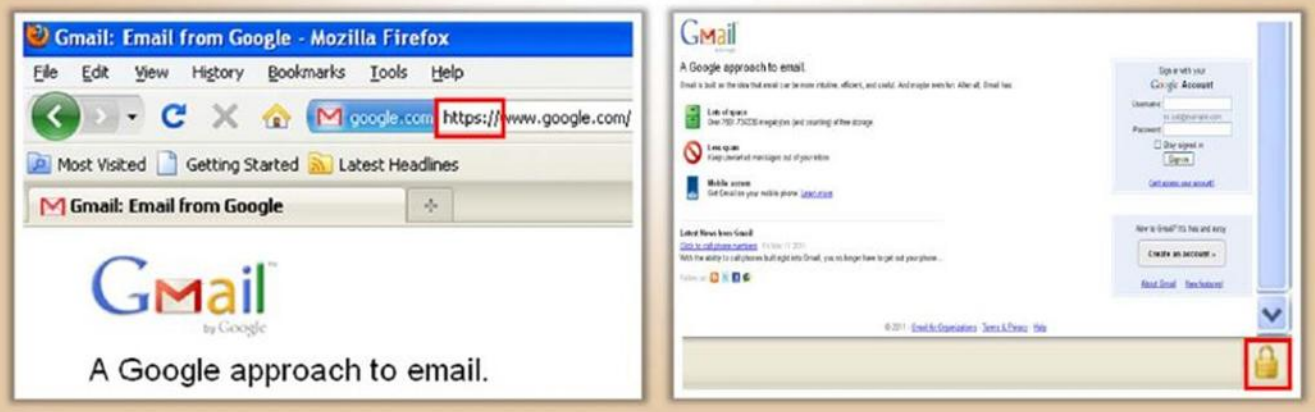
- پسورد باید به گونه ای انتخاب شود که کاربر بتواند آن را به خاطر بسپارد، اما مربوط به خود کاربر نباشد (مانند تاریخ تولد، نام فرزند، نام همسر و ...)
- یک پسورد قوی حداقل دارای 8-10 رقم، و شامل اعداد، حروف و کاراکترها می باشد (می توان از کاراکترهای خاص نیزاستفاده نمود اما باید بخاطر سپردن آن آسان باشد)
- برای دسترسی به تمام منابع از رمز عبورهای قوی استفاده کنید

1

نحوه شناسایی یک وب سایت امن

وب سایت های امن را می توان شناسایی نمود، اگر:

- URL شامل https:// باشد
- وجود علامت قفل در قسمت سمت چپ مرورگر (قبل از شروع URL)

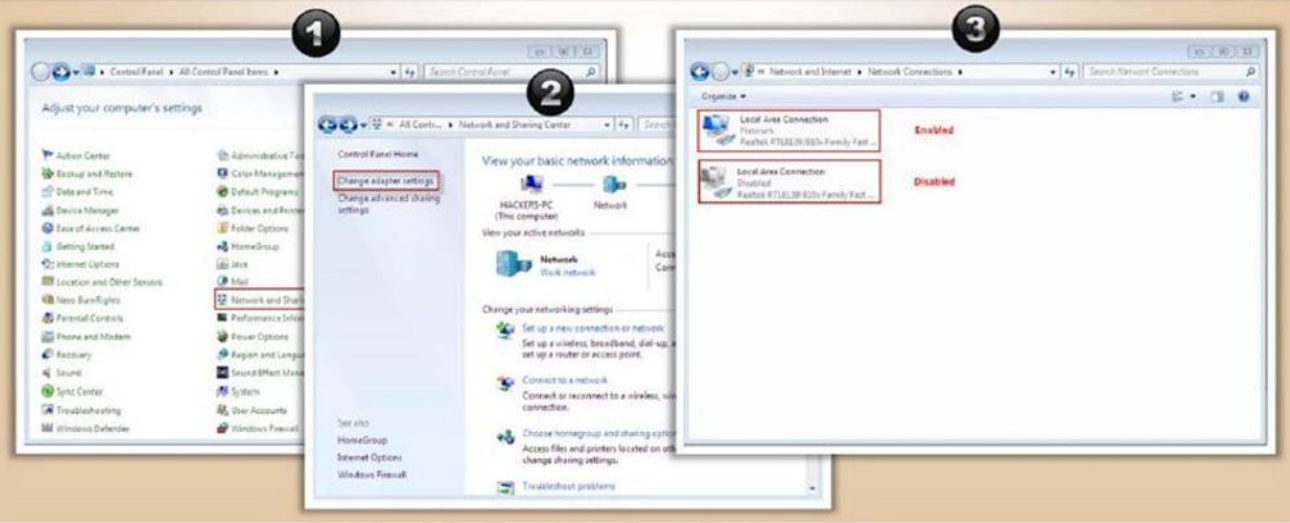


اقدامات امنیتی عمومی برای شبکه خانگی

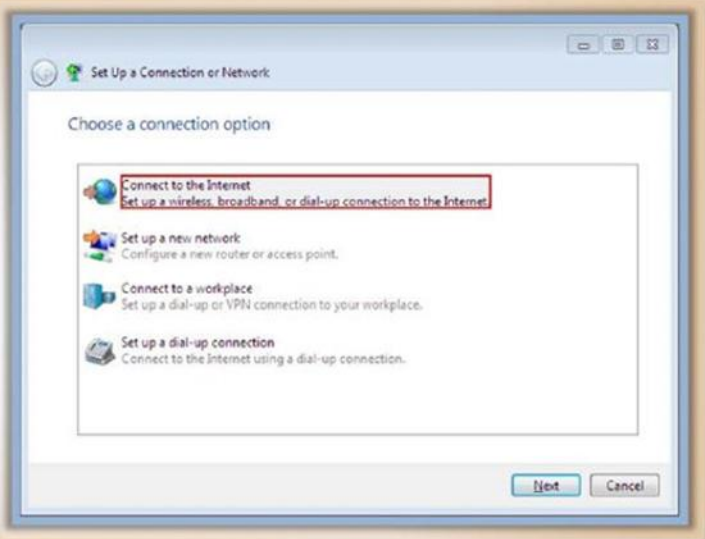
- بر روی تمام سیستم ها از آنتی ویروس استفاده کنید
- از بسته های نرم افزاری فایروال های شخصی استفاده نمایید
- به هیچ عنوان پیوست های ایمیل ارسال شده از جانب افراد ناشناس را باز نکنید و قابلیت اسکریپت را در برنامه های ایمیل غیرفعال نمایید
- هرگز یک برنامه را اجرا نکنید، مگر اینکه فرستنده/ شرکت یک منبع قابل اعتماد باشد
- تمام برنامه های کاربردی از جمله سیستم عامل را همیشه به روز نگه دارید، و در مواقع لزوم آن ها را وصله نمایید
- زمانی که از سیستم استفاده نمی شود آن را خاموش نموده یا رابط اترنت آن را قطع کنید
- غیرفعال کردن جاوا، جاوا اسکریپت و ActiveX موجب جلوگیری از آسیب پذیری کاربر در مقابل اسکریپت های مخرب خواهد شد
- به طور منظم از داده های مهم و حساس پشتیبان تهیه کنید
- سیستم عامل ویندوز دارای گزینه ای تحت عنوان "Hide file extensions for known file types" می باشد، برای نمایش پسوند فایل ها توسط ویندوز، این گزینه را غیرفعال نمایید
- برای بازیابی سیستم به هنگام آسیب دیدن یا تسخیر شدن، یک دیسک بوت تهیه کنید

بررسی آداپتور شبکه

- به مسیر Start →Control Panel →Network and Sharing Center بروید.
- بر روی Network and Sharing Center کلیک نمایید. در این قسمت اطلاعات پایه شبکه شما نشان داده خواهد شد.
- بر روی Change Adapter Settings کلیک نمایید.



ویزارد نصب شبکه



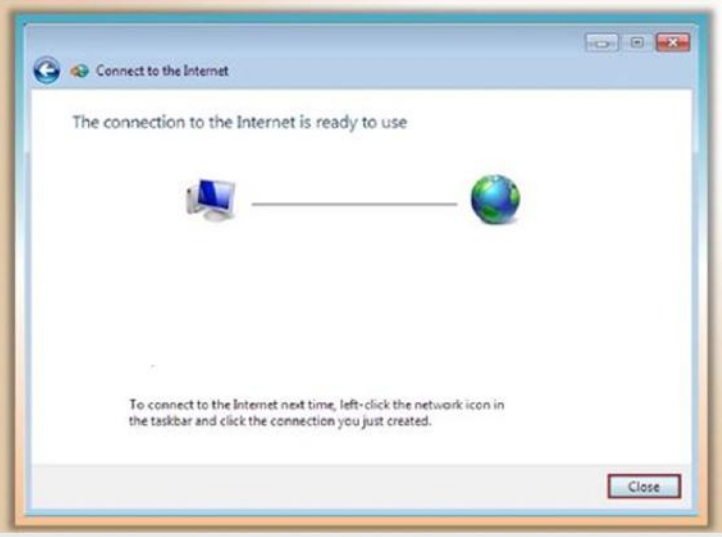
- به مسیرزیر بروید :

Start →Control Panel →Network and Sharing center →Set up a new connection or network →Connect to the Internet →Next

- بر روی Set up a new connection anyway کلیک نموده و سپس Next را بزنید
- در ویزارد How do you want to connect نوع ارتباط را انتخاب کنید و سپس Next را بزنید
- یوزرنیم، پسورد و نام ارائه دهنده خدمات اینترنت (ISP) خود را وارد نمایید
- نام کانکشن را وارد نموده و گزینه Allow other people to use this connection را تیک بزنید، سپس بر روی connect کلیک کنید

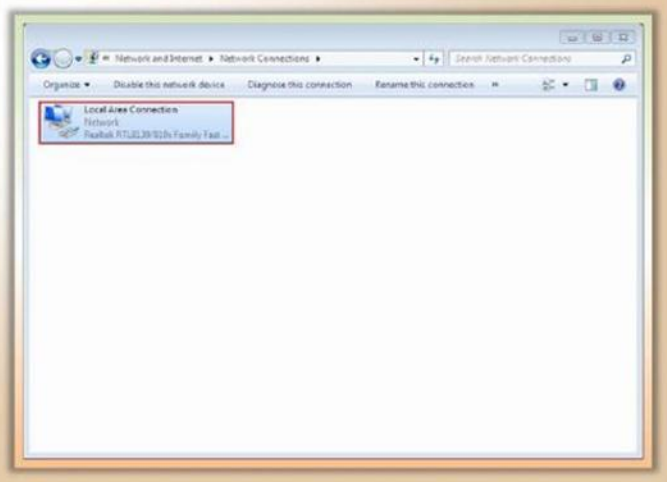
ویزارد نصب شبکه

- اگر با موفقیت متصل شوید، ویندوز پیغام The connection to the Internet is ready to use را به شما نشان خواهد داد-> بر روی close کلیک کنید
- بر روی Yes کلیک نمایید تا کامپیوتر ریستارت شود



چگونه مشکلات شبکه را رفع کنیم؟

- از منوی Start به Control panel بروید
- بر روی Network and Sharing Center کلیک نمایید
- بر روی Change Adapter Settings کلیک نمایید
- در پنجره Network Connections وضعیت آداپتور شبکه را بررسی کنید

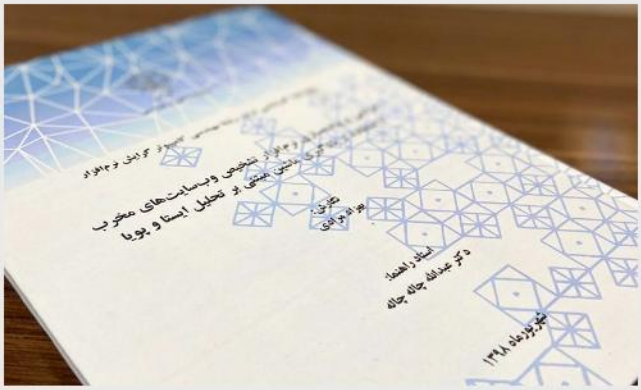


ادامه مبحث " امنیت شبکه" را در شماره های بعدی ما دنبال کنید...

اخبار داخلی

پایان اولین پروژه کارشناسی ارشد مورد حمایت مرکز آپا دانشگاه رازی

به دنبال حمایت مرکز تخصصی آپا دانشگاه رازی از پایان‌نامه‌های مقطع کارشناسی ارشد که موضوع آنها در راستای یکی از محورهای اصلی مرتبط با اهداف مرکز باشد، اولین پروژه کارشناسی ارشد مورد حمایت این مرکز با موضوع "طراحی و پیاده‌سازی نرم‌افزار تشخیص وب‌سایت‌های مخرب با استفاده از یادگیری ماشین مبتنی بر تحلیل ایستا و پویا" به پایان رسید. در این پروژه به طور خاص بر روی تشخیص وب‌سایت‌هایی که حمله Stored-XSS را انجام می‌دهند کار شده است و در نهایت یک برنامه اجرایی یا یک API برای تشخیص سلامت صفحات آماده شده است تا به راحتی به ابزارهای دیگر متصل شود.



در این پروژه، یک رویکرد براساس الگوریتم‌های یادگیری ماشین، برای طبقه‌بندی صفحات سالم از صفحاتی که حمله XSS بازتابی را با استفاده از URLها انجام می‌دهند، پیشنهاد شده است. الگوریتم‌های متعددی برای رده‌بندی صفحات وب ارائه شده‌اند. اغلب روش‌های ارائه شده، از ویژگی‌های ایستا و روش‌های متن کاوی صفحات وب استفاده می‌کنند که ویژگی‌های رفتاری (پویای) صفحـــات وب را به درستی استخراج نمی‌کنند. در عین حال برخی از روش‌های پیشنهادی با استفاده از ابزارهایی سعی کردند تا ویژگی‌های پنهان و پویا را استخراج کنند. هرکدام از این رویکردها دارای مشکلاتی هستند. در رویکرد پیشنهادی در این پروژه، با استفاده از ترکیب روش ایستایِ استخراج ویژگی و روش‌های پویای استخراج ویژگی، همچنین با حل چالش‌های رمزگشایی آدرس URL، عبور از مبهم‌سازی و هدایت وب‌سایت‌ها، در نهایت با مدل‌سازی مبتنی بر الگوریتم‌های یادگیری درختی و k-NN مدل طبقه‌بندی ارائه شده است که نتایج بهتری نسبت به سایر روش‌ها نشان می‌دهد. نقطه قوت این پژوهش، استفاده از روش استخراج ویژگی پویایی است که با استفاده از مکانیزم گزارش‌گیری رخدادهای صفحه، برخی از عیب‌های روش‌های پیشین مانند مبهم‌سازی را حل کرده است و به سادگی از پیچیدگی آنها عبور می‌کند.

در کارهای آینده می‌توان ویژگی‌های استخراج شده را برای سایر حملات، مانند فیشینگ و XSS ذخیره شده نیز استفاده کرد. به طور کلی، نرم‌افزار استخراج شده از پایان‌نامه، قابلیت ادغام با نرم‌افزارهای دیگر و یا بهینه شدن عملیات طبقه‌بندی را دارا می‌باشد که در آینده می‌توان آن را انجام داد.


Windows 7
R.I.P
JANUARY 14, 2020
مرکز تخصصی آپا دانشگاه رازی