بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیست و پنجم

مهرماه ۱۳۹۹

این بار آسیب‌پذیری در McAfee

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:
مرکز تخصصـــی آپـا دانشگـاه رازی

صفحه آرایی: **سید احسان حسینی، سهیلا مرادی**

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

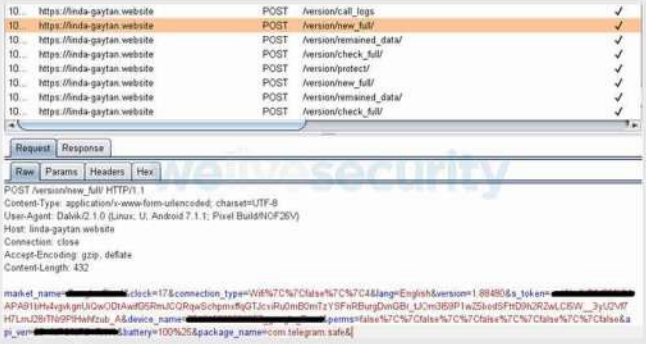
اخبار امنیتی

کشف نرم‌افزار جاسوسی جدید اندروید در قالب پیام‌رسان‌های تلگرام و Threema

اخیراً گروهی از هکرها، جاسوس‌افزاری کشف کرده‌اند که در ظاهر پیام‌رسان‌هایی همچون تلگرام و Threema به آلوده کردن دستگاه اندروید می‌پردازد.

طبق تحلیل شرکت سایبریِ ESET: "جاسوس‌افزار Android/SpyC23.A نسبت به نسخه سال 2017، قابلیت‌های جاسوسی خود را افزایش داده است، از جمله خواندنِ اعلان[1] پیام‌رسان‌ها، ضبط تماس‌ها و ضبط صفحه گوشی و ویژگی‌های پنهان دیگری از جمله نادیده گرفتن اعلان‌های نرم‌افزارهای امنیتی اندورید."

این بدافزار اولین بار در سال 2017 با عنوان Two-tailed Scorpion منتشر شد و به دلیل توانایی جاسوسی در دستگاه قربانی، دسترسی به اطلاعات تماس، دفترتلفن، مکان‌یابی، پیام‌ها، تصاویر و دیگر مستندات حساس، شناخته شده است. در اوایل سال جاری نیز محققان Check Point، شواهد جدیدی از فعالیت گروه APT-C-23 مشاهده کردند.



آخرین نسخه این نرم‌افزار جاسوسی که جزئیات آن توسط شرکت ESET منتشر شد، دارای قابلیت جمع‌آوری اطلاعات از رسانه‌های اجتماعی و برنامه‌های پیام‌رسان از طریق ضبط صفحه و گرفتن عکس از صفحه و حتی ضبط تماس‌های ورودی و خروجی در WhatsApp و خواندن متن اعلان‌های نرم‌افزارهایی همچون Skype، Facebook، Viber، WhatsApp و Messenger می‌باشد.

فعالیت این جاسوس‌ابزار زمانی آغاز می‌شود که فرد قربانی از یک اپلیکیشن جعلی اندروید به نام "DigitalApps" بازدید کند

[1] Notification

و اپلیکیشن‌هایی مانند Threema ، Telegram و weMessage را دانلود نماید. این جاسوس‌ابزار علاوه بر درخواست مجوزهایی جهت خواندن اعلان‌ها، خاموش کردن Google Play Protect، ضبط صفحه، با سرور کنترل و فرمان (C2[1]) جهت ثبت قربانی جدید و انتقال اطلاعات دستگاه وی، ارتباط برقرار می‌کند. سرورهای C2، وظیفه انتقال مجدد دستورات مخرب به تلفن آسیب‌دیده را دارند که آن دستورات جهت ضبط صدا، راه‌اندازی مجدد Wi-Fi، حذف تمامی برنامه‌های نصب شده روی دستگاه و غیره استفاده می‌شوند.

در سال‌های اخیر، برنامه‌هایی که از طریق اپلیکیشن‌های جعلی شخص ثالث دانلود می‌شوند، منشاء بدافزارهای اندرویدی بوده‌اند. بنابراین به کاربران توصیه می‌شود برای محدود کردن خطرات احتمالی سعی کنند از منابع معتبر و قابل اعتماد برنامه‌های خود را دریافت کرده و نیز قبل از نصب آنها، مجوزهای درخواست شده توسط برنامه‌ها را به طور دقیق‌تر بررسی کنند.

منبع خبر :

Scan Link

انتشار بدافزار بوت‌کیت جدید به نام MosaicRegressor

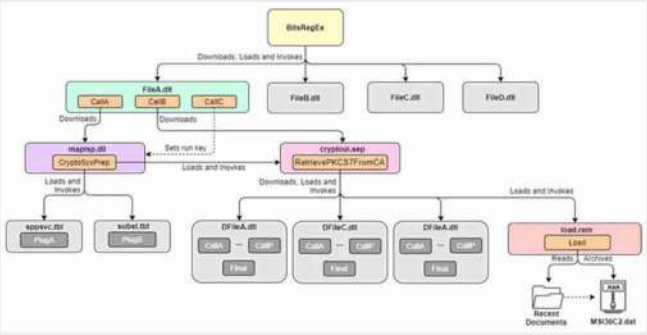
محققان امنیت سایبری نوع نادری از یک بدافزار بالقوه و خطرناک را شناسایی کرده‌اند که فرآیند بوت شدن دستگاه را به منظور استقرار دائمی بدافزارها مورد هدف قرار می‌دهد. این کمپین از میان‌افزار UEFI[2] آلوده که حاوی یک بخش مخرب است استفاده می‌کند، این دومین حمله عمومی شناخته شده است که در آن از روت‌کیت[3] UEFI استفاده شده است.

طبق بررسی‌های Kaspersky، imageهای میان‌افزار آلوده UEFI به گونه‌ای تغییر یافته که چندین ماژول مخرب را در خود جای داده است که از آن‌ها برای انتقال بدافزار بر روی دستگاه قربانی در یک سری حملات سایبری هدفمند در آفریقا، آسیا و اروپا استفاده می‌شود.

UEFI یک رابط میان‌افزار و جایگزین BIOS است که امنیت را بهبود می‌بخشد و این اطمینان را می‌دهد که هیچ بدافزاری در فرآیند بوت شدن اختلال ایجاد نکرده است. از آنجا که UEFI به بارگذاری سیستم‌عامل خود کمک می‌کند، چنین حملاتی در برابر نصب مجدد سیستم‌عامل یا جایگزینی هارد درایو مقاوم هستند.

طبق گفته Kaspersky: "میان‌افزار UEFI مکانیسم کاملی برای ذخیره‌سازی دائم بدافزار ایجاد می‌کند. یک مهاجم حرفه‌ای می‌تواند میان‌افزار را به گونه‌ای تغییر دهد که بتواند کد مخربی را که پس از بارگذاری سیستم‌عامل اجرا می‌شود، مستقر سازد".

این دقیقاً همان کاری است که به نظر می‌رسد مهاجم انجام داده است. اگرچه جزییات دقیق استفاده شده برای بازنویسی میان‌افزار اصلی در این مرحله ناشناخته مانده است، اما یک بررسی انجام شده نشان می‌دهد که ممکن است این بدافزار از طریق دسترسی فیزیکی به دستگاه قربانی، استقرار یافته باشد.



این بدافزار جدید، نسخه سفارشی‌سازی‌شده بوت‌کیت VectorEDK تیم Hacking است که در سال 2015 منتشر شد و از آن زمان به صورت آنلاین در دسترس می‌باشد.

MosaicRegressor یک چارچوب چند مرحله‌ای و ساختار یافته با هدف جاسوسی و جمع‌آوری داده‌هاست که شامل downloaderهای دیگری برای واکشی و اجرای مؤلفه‌های ثانویه است. این downloaderها به نوبه خود به سرور فرمان و کنترل (C2) برای گرفتن DLLهای مرحله بعدی جهت اجرای دستورات خاص متصل می‌شوند، و نتایج آن نیز به همان سرور C2 یا به یک آدرس ایمیل "feedback" فرستاده می‌شود.

پی‌لودها به روش‌های مختلفی از جمله از طریق پیام‌های الکترونیکی از صندوق‌های پستی ("mail.ru") که در باینری بدافزار کدگذاری شده‌اند ارسال می‌شوند.

منبع خبر :

Scan Link

انتشار بدافزار PoetRat با استفاده از اسناد مخرب Microsoft Word

محققان امنیتی نوع جدیدی از بدافزار Rat به نام PoetRat را شناسایی کرده‌اند. در این حملات، مهاجم جهت فریب قربانیان برای دانلود اسناد مخرب word از ارائه‌دهندگان

[1] command-and-control
[2] Unified Extensible Firmware Interface
[3] روت‌کیت‌ها گونه‌ای از بدافزارها هستند که برای آلوده کردن یک رایانه مورد استفاده قرار می‌گیرند و به مهاجم اجازه می‌دهند تا مجموعه‌ای از ابزارها که به آن‌ها امکان دسترسی از راه دور را می‌دهد نصب کنند.

هاست موقت، از اسناد مخرب word استفاده می‌کند.

بدافزار RAT دارای ابزارهایی برای مانیتور کردن هارد دیسک و استخراج خودکار داده‌ها است، همچنین سرقت رمزهای عبور موجود در مرورگرها، keylogger، برنامه‌های کنترل دوربین و سرقت سایر رمزهای عبور از ویژگی‌های دیگر این بدافزار است.

عاملان تهدید از اسناد word برای انتقال بدافزار استفاده می‌کنند، این بدافزار همچنین حاوی ماکروهای[1] مخرب دیگری است که به نوبه خود پی‌لودهای دیگر را دانلود می‌کنند. نسخه‌های قدیمی بدافزار PoetRat از مفسر[2] پایتون برای اجرای کد منبع استفاده می‌کردند اما این نسخه جدید از اسکریپت Lua برای این کار استفاده می‌کند.

هنگامی که کاربر اسناد مخرب را باز می‌کند، مفسر Python و بدافزار PoetRAT به سیستم قربانی منتقل می‌شوند. این نسخه جدید همچنین از پروتکل HTTP برای ارتباطات با سرور C2 استفاده می‌کند.

در تمامی این حملات، مهاجم به طور مداوم مراکز و بخش‌های مهم و عمومی را هدف قرار داده و سعی می‌کند اسناد حساس را از سیستم‌هایی آسیب‌پذیر، استخراج کند.

منبع خبر :

Scan Link

اخبار کوتاه

سوءاستفاده هکرها از سرویس گزارش خطای ویندوز در حمله fileless جدید

محققان امنیتی تکنیک حمله بدون فایل (Fileless) جدیدی کشف کرده‌اند که با سوءاستفاده از سرویس گزارش خطا ویندوز (WER) سیستم قربانی را آلوده می‌کند. به گزارش«ZDNet»، یک گروه هک ناشناخته تکنیک جدیدی برای هک ابداع کرده است که در آن بدافزار در فایل‌های اجرایی مبتنی بر سرویس گزارش خطای مایکروسافت ویندوز (Microsoft Windows Error Reporting) پنهان می‌شود.

محققان امنیتی، یک فایل ZIP حاوی فایل ورد با عنوان Compensation manual پیدا کرده‌اند که در ظاهر در رابطه با حقوق و دستمزد کارمندان است، اما به محض باز شدن، یک ماکرو مخرب اجرا می‌کند.

این ماکرو از نسخه سفارشی ماژول CactusTorch VBA برای اجرای حمله بدون فایل از طریق shellcode استفاده می‌کند. CactusTorch قادر به بارگذاری یکی از فایل‌های Net. به نام Kraken.dll در حافظه بوده و آن را از طریق VBScript اجرا می‌کند. این پی‌لود سپس shellcode را به درون فایل WerFault.exe تزریق می‌کند. این فایل اجرایی به سرویس WER متصل بوده و مایکروسافت از آن برای ردیابی و رفع خطاهای ویندوز استفاده می‌کند.

به گفته محققان، shellcode پس از آلوده کردن فایل اجرایی، یک درخواست HTTP به یک دامنه به منظور دانلود بدافزارهای دیگر می‌فرستد.

کشف یک آسیب‌پذیری در چیپ امنیتی T2 اپل که احتمالاً غیرقابل رفع است!

در سال‌های اخیر برای افزایش امنیت کامپیوترها شاهد استفاده از چیپ‌های امنیتی هستیم. حالا به نظر می‌رسد در چیپ امنیتی T2 اپل آسیب‌پذیری وجود دارد که نمی‌توان آن را با بروزرسانی نرم‌افزاری برطرف کرد.

این چیپ مبتنی بر پردازنده اپل A10 بوده که در برخی محصولات اپل مورد استفاده قرار گرفته و به نظر می‌رسد در معرض خطر اکسپلویت جیلبریک «checkm 8» قرار دارد. این آسیب‌پذیری می‌تواند منجر به نفوذ به فرآیند بوت سیستم‌عامل «SepOS» شود که نتیجه آن، دسترسی به سخت‌افزار خواهد بود.

با دسترسی به این سخت افزار، مهاجمان هرکاری به جز رمزگشایی مستقیم فایل‌هایی که با استفاده از رمزنگاری «FileVault 2» ذخیره شده‌اند، می‌توانند انجام دهند. آن‌ها می توانند با تزریق کی‌لاگر به پسورد سیستم دسترسی پیدا کرده و این فایل‌ها را رمزگشایی کنند. با وجود چنین مواردی، برای انجام چنین حمله‌ای باید به کابل مخصوص و همچنین کامپیوتر مک دسترسی داشت. اپل در حال حاضر درباره این مشکل اظهارنظری نکرده، بنابراین تا زمان رفع این مشکل از مک و مک‌بوک خود از نظر فیزیکی محافظت کنید.

جاسوسی از گوشی کاربران از طریق آسیب‌پذیری اینستاگرام

محققان امنیتی یک آسیب‌پذیری را در اینستاگرام شناسایی کرده‌اند که به هکرها امکان جاسوسی از گوشی کاربران از طریق دوربین و میکروفون را می‌دهد.

این باگ مهم توسط موسسه امنیتی «Check Point» شناسایی شد اما برای جلوگیری از سوءاستفاده هکرها به صورت محرمانه به فیسبوک گزارش شد. مشکل مذکور که حالا برطرف شده به عنوان آسیب‌پذیری حیاتی در پردازش تصویر اینستاگرام توصیف شده است. به گفته این شبکه اجتماعی حفره امنیتی ناشی از سرریز پشته بوده است: "زمانی که کاربر بخواهد تصویری خاص را آپلود کند در نسخه اندروید یک سرریز پشته رخ می‌دهد".

به گفته Check Point، برای به دست گرفتن کنترل اینستاگرام در گوشی کاربران کافی است هکر تصویری مخرب را از طریق ایمیل، واتس‌اپ، پیامک یا دیگر روش‌ها ارسال کند. به محض باز کردن اینستاگرام و فارغ از اینکه کاربر عکس را ذخیره کرده یا خیر دستگاه مقصد هک شده است.

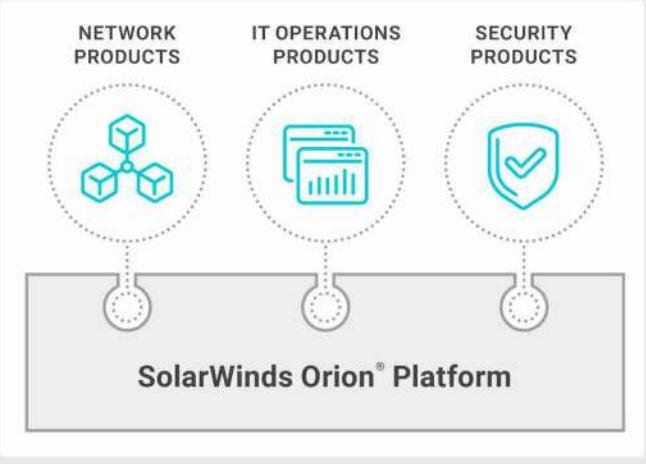
مشکل اصلی به نحوه مدیریت کتابخانه‌های شخص ثالث برای پردازش تصویر برمی‌گردد. برای مثال می‌توان به دکودر متن باز Mozjpeg اشاره کرد که توسط موزیلا توسعه یافته و شبکه اجتماعی مذکور از آن برای مدیریت آپلود تصاویر استفاده می‌کند. پیکربندی اشتباه باعث شده تصویری با محتوای خاص بتواند تمام مجوزهای اینستاگرام را در اختیار بگیرد. این مجوزها شامل دسترسی به مخاطبان، اطلاعات مکانی، دوربین و حتی فایل‌های ذخیره شده می‌شود. در خود اپ هم می‌توان به پیام‌های دایرکت دسترسی پیدا کرد، پست ها را حذف کرده یا تصاویر جدیدی منتشر کرد.

---

[1] ماکروها ابزارهای کوچک اما کارآمدی هستند که سرعت کار کاربران را افزایش می‌دهند.
[2] interpreter

آسیب پذیری

آسیب‌پذیری XSS ذخیره شده در پلتفرم Orion نرم‌افزار مانیتورینگ SolarWinds



این آسیب‌پذیری با شناسه "CVE-2020-13169"، یک آسیب‌پذیری XSS ذخیره شده یا (Stored XSS (Cross-Site Scripting است که در چندین فرم و صفحه در پلتفرم Orion نرم‌افزار مانیتورینگ SolarWinds قبل از نسخه 2020.2.1 وجود دارد. آسیب‌پذیری مذکور، بر برخی عملکردهای نامشخص حساب کاربری administrator تاثیر گذاشته و ممکن است منجر به افشای اطلاعات و نیز افزایش امتیازات دسترسی حتی دستیابی به امتیازات حساب کاربری administrator شود. دستکاری یک ورودی نامشخص منجر به ظهور این آسیب‌پذیری گردیده و یکپارچگی[1] این نرم‌افزار را تحت تأثیر قرار داده است.

مهاجم ممکن است بتواند کد HTML و اسکریپت دلخواه خود را درون وب‌سایت آسیب‌پذیر تزریق کرده و بدین ترتیب موجب تغییر ظاهر و نیز گشودن راهی برای شروع حملات بیشتر علیه بازدیدکنندگان وب‌سایت گردد.

این حمله می‌تواند از راه دور انجام شود. در حال حاضر جزئیات فنی بیشتری از این آسیب‌پذیری شناسایی نشده است و اکسپلویت آن نیز در دسترس نمی‌باشد.

توصیه امنیتی

به کاربران توصیه می‌شود نرم‌افزار خود را به نسخه 2020.2.1 ارتقاء دهند. این نسخه در مقایسه با نسخه‌های پیشین، ویژگی‌ها و عملکردهای جدیدی از جمله بهبود مقیاس‌پذیری یا Scalability، بروزرسانی متمرکز برای محیط‌های آفلاین و همچنین رفع آسیب‌پذیری CVE-2020-13169 را ارائه می‌دهد.

اگر در حال ارتقاء نسخه 2015.1.3 یا بالاتر پلتفرم Orion هستید، از SolarWinds Orion Installer استفاده کنید.

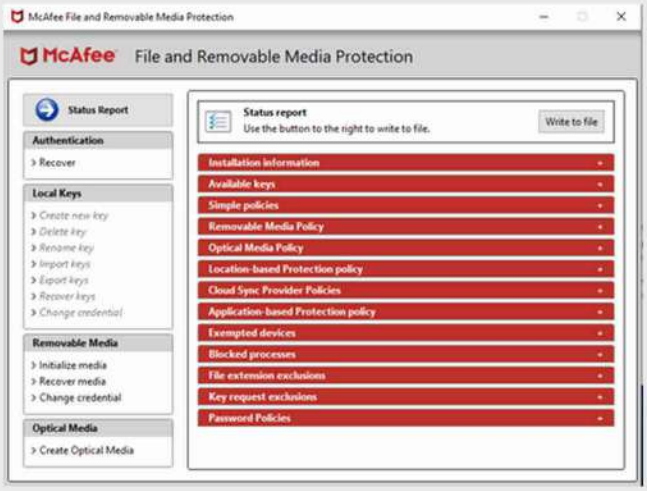
اگر در حال ارتقاء نسخه 2019.2 هستید، می‌توانید از صفحه My Orion Deployment جهت بروزرسانی استفاده کنید. بدین صورت که روی Settings > My Orion Deployment > Updates & Evaluations کلیک کنید. دانلود Orion Installer لازم نیست.

[1] Integrity

منبع خبر :

Scan Link

آسیب‌پذیری مسیر سرویس محافظت نشده در McAfee FRP



این نقص یک آسیب‌پذیری مسیر سرویس محافظت نشده[1] در نسخه‌های قبل از نسخه 5.3.0 نرم‌افزار FRP[2] است که مهاجمان را قادر می‌سازد تا به صورت محلی یا local از طریق اجرای یک فایل آلوده و دارای نقص، کد دلخواه خود را با امتیازات بالاتر اجرا و به بسیاری از منابع دسترسی قابل توجهی پیدا کنند. شایان ذکر است که این مسئله ممکن است منجر به رمزگذاری فایل‌ها هنگام اجرای یک policy[3] شود.

File and Removable Media Protection یک نرم‌افزار رمزنگاری است که به محافظت از داده‌های ذخیره شده بر روی file shares، رسانه‌های قابل جابجایی[4] مانند درایوهای USB، CD یا DVD، فایل‌های ISO و سرویس‌های ذخیره‌سازی ابری مانند Google Drive، Dropbox، Box و Microsoft OneDrive کمک می‌کند. این نرم‌افزار برای تبلت، لپ‌تاپ، رایانه‌های شخصی و workstationهای سیستم‌عامل ویندوز و همچنین مک در دسترس می‌باشد.

FRP یک نقطه مدیریت مرکزی ایجاد و اطمینان حاصل می‌کند که داده‌ها در هر کجا که باشند ایمن هستند. موارد معمول استفاده از FRP عبارت است از رمزگذاری فایل‌هایی مانند صفحات گسترده[5] و اسناد مهم و حساس، امکان دسترسی به یک پوشه خاص در یک شبکه مشترک، رمزگذاری فایل‌های همگام‌سازی شده با سرویس‌های ذخیره‌سازی ابری، رمزگذاری رسانه‌های قابل جابجایی یا ممانعت از کپی کردن فایل‌های رمزگذاری نشده، و ارسال فایل‌های موجود در پیوست‌های ایمیل که به صورت خودکار extract می‌شوند.

آسیب‌پذیری مسیر سرویس محافظت نشده یک نقص شناخته شده در نرم‌افزارهاست و زمانی به وجود می‌آید که در مسیر یک فایل اجرایی و در نام آن یک کاراکتر فاصله وجود دارد و در تگ کوتیشن قرار داده نشده است. این آسیب‌پذیری با قرار دادن یک فایل اجرایی مخرب در مسیر اصلی و واداشتن یک برنامه‌ی امن و قابل اطمینان برای اجرای آن، قابلیت پایداری و دور زدن روش‌های شناسایی را فراهم می‌آورد. علاوه بر اینکه بهره‌برداری از این آسیب‌پذیری می‌تواند راه‌کارهای امنیتی را دور بزند، امکان ارتقاء امتیاز را نیز برای مهاجم فراهم می‌کند و این در صورتی است که برنامه‌ی اجرا شده و آسیب‌پذیر، دارای امتیازات بالایی باشد.

برای اطلاع از آسیب‌پذیر بودن نرم‌افزار مورد استفاده خود، برای FRP از دستورالعمل زیر استفاده کنید:

۱. Administrator's User Interface (UI) را باز کنید.

۲. نسخه محصول را مشاهده کنید. اگر نسخه آن پایین‌تر از نسخه 5.3.0 باشد آسیب‌پذیر بوده و باید بروزرسانی شود.

باتوجه به اهمیت آسیب‌پذیری مذکور، به کاربران توصیه می‌شود جهت رفع آن به لینک https://www.mcafee.com/enterprise/en-us/downloads.html مراجعه کرده و هر چه سریع‌تر فایل مربوط به بروزرسانی محصول را دانلود و نصب نمایند.

منبع خبر :

Scan Link

افشای چندین آسیب‌پذیری در کنترل‌پنل Webmin

سه آسیب‌پذیری در کنترل‌پنل Webmin گزارش شده که اطلاعات مربوط به هر یک از آنها در ادامه آورده شده است.

اولین آسیب‌پذیری با شناسه "CVE-2020-8820"، یک نقص XSS در نسخه Webmin 1.941 و نسخه‌های قبل‌تر از آن است که مؤلفه Cluster Shell Commands Endpoint این کنترل‌پنل را تحت تأثیر قرار می‌دهد.

آسیب‌پذیری بعدی که شناسه "CVE-2020-8821" به آن اختصاص داده شده است یک نقص اعتبارسنجی نامناسب داده‌ها یا Improper Data Validation در Webmin 1.941 است که در مؤلفه Command Shell Endpoint وجود دارد.

سومین آسیب‌پذیری با شناسه "CVE-2020-12670" نیز در Webmin 1.941 و نسخه‌های قبل‌تر از آن وجود دارد و عملکرد Save یا ذخیره‌سازی در مؤلفه Read User Email Module/mailboxes Endpoint این کنترل‌پنل را در زمان ذخیره کردن ایمیل‌های HTML تحت تأثیر قرار می‌دهد. این ماژول، بدون پاکسازی عناصر اسکریپت، هر خروجی را تجزیه می‌کند، درست در مقابل عملکرد View

[1] Unquoted service path
[2] McAfee File and Removable Media Protection
[3] Policy امکانی است که باعث می‌شود مدیرشبکه بتواند سیاست‌های مدنظر خود را بر روی Kasperskyهای Endpoint Security اعمال کند.
[4] removable media
[5] spreadsheet

که ورودی‌ها را به درستی پاکسازی می‌کند.

webmin (وبمین) یک رابط گرافیکی برای مدیریت سیستم‌های لینوکسی است که مدیر سرور به وسیله مرورگر وب می‌تواند کاربران، سرویس‌ها، تنظیماتDNS ، آپاچی، ویرایش فایل‌های سرور و سایر عملیات سرور خود را به صورت گرافیکی تحت وب (به جای وارد کردن دستورالعمل در ترمینال ssh) مدیریت کند.

سامانه و مؤلفه‌های تحت تأثیر آسیب‌پذیری‌های کشف شده عبارتند از:

سامانه تحت تأثیر	نسخه	شناسه آسیب‌پذیری	مؤلفه آسیب‌پذیر
کنترل‌پنل Webmin	1.941 و قبل‌تر	CVE-2020-8820	Cluster Shell Commands Endpoint
		CVE-2020-8821	Command Shell Endpoint
		CVE-2020-12670	Read User Email Module / mailboxes Endpoint

روش‌های بهره‌برداری از آسیب‌پذیرهای کنترل‌پنل Webmin در جدول زیر قابل مشاهده است.

شناسه آسیب‌پذیری	روش بهره‌برداری	شرط بهره‌برداری
CVE-2020-8820	یک کاربر ممکن است هر پیلود[1] XSS را در قسمت Command وارد کرده و آن را اجرا کند. سپس، پس از بازدید مجدد از منوی Cluster Shell Commands، این پیلود اجرا می‌شود.	این حمله ممکن است از راه دور انجام شود. بهره‌برداری موفق این آسیب‌پذیری نیازمند یک احراز هویت ساده است.
CVE-2020-8821	یک کاربر ممکن است کد HTML را در قسمت Command وارد کرده و آن را ارسال کند. سپس پس از بازدید از منوی Action Logs و مشاهده لاگ‌ها[2]، کد HTML مذکور فرستاده می‌شود (با این حال، JavaScript اجرا نمی‌شود). تغییرات ایجاد شده برای کاربران هم وجود خواهد داشت.	این حمله فقط از طریق شبکه محلی امکان‌پذیر بوده و بهره‌برداری از آن نیازمند احراز هویت است.
CVE-2020-12670	یک کاربر مخرب می‌تواند هر پیلود JavaScript را در قالب پیام ارسال کرده و در صورت تصمیم کاربر برای ذخیره آن ایمیل، پیلود را اجرا کند.	بهره‌برداری از این آسیب‌پذیری بسیار ساده است و به احراز هویت نیازی نیست. شروع حمله از راه دور امکان‌پذیر است.

توصیه امنیتی

با توجه به اینکه در حال حاضر روشی جهت رفع آسیب‌پذیری‌های مذکور ارئه نشده است، به کاربرانی که از کنترل‌پنل Webmin و نسخه‌های آسیب‌پذیر آن -که در بخش‌های قبلی به آنها اشاره شد- استفاده می‌کنند توصیه می‌شود با انتشار بروزرسانی‌های نرم‌افزاری و وصله‌های امنیتی آن، نسبت به نصب بروزرسانی‌ها و پچ‌های امنیتی اقدام نمایند.

منبع خبر :

Scan Link

کشف آسیب‌پذیری‌های متعدد در سیستم‌عامل SonicOS

اخیرا چندین آسیب‌پذیری در سیستم‌عامل SonicOS کشف و شناسایی شده است که سرویس SSLVPN فایروال این سیستم‌عامل را تحت تأثیر قرار می‌دهد. SonicOS سیستم‌عاملی برای تجهیزات امنیتی شبکه SonicWall است. SonicWall یک شرکت خصوصی است که محصولات امنیتی شبکه و محافظت از داده تولید می‌کند. این شرکت فایروال، کلاس سازمانی، بی‌سیم ایمن، امنیت ابر و تجهیزات عملکردی را طراحی می‌کند و توسعه می‌دهد.

در ادامه اطلاعات مربوط به هر یک از آسیب‌پذیری‌ها به تفکیک ذکر شده است.

"CVE-2020-5143": این آسیب‌پذیری مربوط به صفحه ورود SonicOS SSLVPN است و به یک مهاجم احراز هویت نشده اجازه می‌دهد تا از راه دور شمارش نام کاربری administrator مدیریت فایروال را براساس پاسخ‌های سرور انجام دهد. در این نقص، دستکاری یک ورودی ناشناخته منجر به آسیب‌پذیری افشای اطلاعات یا in-formation disclosure می‌شود.

"CVE-2020-5141": در این آسیب‌پذیری یک مهاجم احراز هویت نشده قادر است از راه دور بر روی ID بلیط Virtual Assist در سرویس SSLVPN فایروال Brute force انجام دهد.

" CVE-2020-5140": با وجود این آسیب‌پذیری یک مهاجم غیرمجاز و احراز هویت نشده می‌تواند از راه دور با ارسال یک درخواست مخرب HTTP که منجر به افشای آدرس‌های حافظه می‌شود، موجب حمله انکار سرویس یا Denial of Service (DoS) بر روی سرویس SSLVPN فایروال شود.

" CVE-2020-5142": این نقص یک آسیب‌پذیری XSS ذخیره‌شده[3] در رابط وب SonicOS SSLVPN است و از طریق آن یک مهاجم احراز هویت نشده می‌تواند از راه دور کد جاوااسکریپت دلخواه خود را در پورتال SSLVPN فایروال، ذخیره و اجرا کند.

" CVE-2020-5133": به دنبال این آسیب‌پذیری یک مهاجم احراز هویت نشده قادر خواهد بود تا از راه دور با سرریز کردن بافر منجر به حمله انکار سرویس و در نهایت از کار افتادن[4] فایروال شود.

"CVE-2020-5138": این نقص مربوط به یک آسیب‌پذیری سرریز پشته است که در پی آن مهاجم احراز هویت نشده قادر است از راه دور منجر به حمله انکار سرویس در سرویس SSLVPN فایروال و سپس از کار افتادن سیستم‌عامل SonicOS شود.

" CVE-2020-5137": یک نقص سرریز بافر است که به واسطه آن مهاجم می‌تواند با سرریز کردن بافر منجر به حمله انکار سرویس در سرویس SSLVPN فایروال و در

---

[1] Payload
[2] logs
[3] stored cross-site scripting
[4] crash

در نهایت از کار افتادن فایروال شود.

"CVE-2020-5139": به دنبال این آسیب‌پذیری مهاجم می‌تواند به دلیل انتشار اشاره‌گر[1] نامعتبر منجر به انکار سرویس و از کار افتادن فایروال شود.

"CVE-2020-5134": این آسیب‌پذیری به مهاجم احراز هویت شده اجازه می‌دهد تا با ارجاع فایل نامعتبر خارج از محدود[2] منجر به از کار افتادن فایروال شود.

"CVE-2020-5135": این نقص مربوط به آسیب‌پذیری سرریز بافر است که به دنبال آن مهاجم می‌تواند با ارسال یک درخواست مخرب به فایروال، منجر به حمله انکار سرویس شده و کد دلخواه خود را اجرا نماید.

"CVE-2020-5136": یک نقص سرریز بافر است و به مهاجم احراز هویت شده اجازه می‌دهد تا منجر به حمله انکار سرویس در SSL-VPN و پورتال virtual assist و در نهایت از کار افتادن فایروال شود.

نسخه‌های آسیب‌پذیر این سیستم‌عامل عبارتند از:

شناسه آسیب‌پذیری	سامانه تحت تأثیر	نسخه‌های آسیب‌پذیر
CVE-2020-5143 CVE-2020-5141 CVE-2020-5140 CVE-2020-5140 CVE-2020-5138 CVE-2020-5137 CVE-2020-5139 CVE-2020-5136	SonicOS Gen 5	۵،۹،۱،۷ و ۵،۹،۱،۱۳
	SonicOS Gen 6	۶،۵،۴،۷ و ۶،۵،۱،۱۲ و ۶،۰،۵،۳
	SonicOSv 6.5.4.v	-
	SonicOS Gen 7	۷،۰،۰،۰
CVE-2020-5133 CVE-2020-5134 CVE-2020-5135	SonicOS Gen 6	۶،۵،۱،۱۲ و ۶،۰،۵،۳
	SonicOSv 6.5.4.v	-
	SonicOS Gen 7	۷،۰،۰،۰

توصیه امنیتی

کاربران جهت رفع آسیب‌پذیری‌های مذکور باید نسبت به بروزرسانی نسخه‌های آسیب‌پذیر و نصب نسخه‌های وصله شده اقدام نمایند. نسخه‌های وصله شده عبارتند از:

- SonicOS 6.5.4.7-83n
- SonicOS 5.9.2.7-5n
- SonicOS 5.9.2.13-7n
- SonicOS 6.5.1.12-1n
- SonicOS 6.0.5.3-94o
- SonicOS 6.5.4.v-21s-987
- Gen 7 7.0.0.0-2 and onwards

منبع خبر:

Scan Link

[1] pointer
[2] out-of-bound invalid file reference

اخبار کوتاه

بروزرسانی ویندوز اجرای برنامه‌های مخرب را برای هکرها ممکن می‌کند

سرویس بروزرسانی ویندوز به تازگی به لیست باینری‌های «LoLBins» اضافه شده که به هکرها اجازه می‌دهد کدهای مخرب را روی سیستم‌های ویندوزی اجرا کنند.

LoLBins فایل‌های اجرایی مایکروسافت هستند که به صورت پیش‌فرض روی سیستم نصب می‌شوند یا قابل دانلود هستند که هکرها می‌توانند از آن سوءاستفاده کنند. مهاجمان می‌توانند با دور زدن مرحله شناسایی، کدهای مخرب را روی سیستم‌ها دانلود، نصب و اجرا کنند. علاوه بر امکان اجرای کدهای مخرب، هکرها می‌توانند از آن برای دور زدن کنترل حساب کاربری ویندوز (UAC) یا کنترل ویندوز دیفندر (WDAC) استفاده کنند و به سیستم‌ها دسترسی پایدار پیدا کنند.

در این حمله، مهاجمان چنین کاری را با اجرای کد مخرب از طریق DLL انجام می‌دهند. مایکروسافت به تازگی آنتی‌ویروس مایکروسافت دیفندر را بروزرسانی کرده که روشی برای دانلود فایل‌ها را روی دستگاه‌های ویندوزی فراهم می‌کند. پس از مدتی این کمپانی این قابلیت را از MpCmdRun.exe حذف کرد.

ابزار جدید مایکروسافت آنتی ویروس دیفندر را از طریق ایمیج ویندوز آپدیت می‌کند

مایکروسافت از ابزار جدیدی رونمایی کرده است که به کاربران اجازه می‌دهد پکیج امنیتی آنتی‌ویروس پیش‌فرض ویندوز 10 یا همان «مایکروسافت دیفندر» را از طریق ایمیج‌های نصبی ویندوز (شامل WIM یا VHD) آپدیت کنند.

مایکروسافت می‌گوید این ابزار جدید برای سازمان‌هایی مناسب است که ویندوز را روی تعداد بالایی از workstationها و سرورها نصب می‌کنند. برخی از شرکت‌ها از یک ایمیج ویندوز به مدت چندین ماه استفاده می‌کنند و بنابراین نرم‌افزار مایکروسافت دیفندر به شکل آپدیت نشده روی سیستم نصب خواهد شد که می‌تواند سیستم را در معرض انواع خطرات امنیتی قرار دهد.

کاربران به کمک ابزار جدید می‌توانند ایمیج‌های ویندوز در فرمت‌های WIM یا VHD را بروز کرده و پس از دریافت آخرین نسخه‌ی فایل‌های امنیتی مایکروسافت دیفندر، سیستم‌عامل را روی سیستم‌ها نصب کنند.

پس از دانلود نسخه مناسب این ابزار از سایت مایکروسافت، فایل را استخراج کرده تا پکیج آپدیت مایکروسافت دیفندر (defender-dism-[x86|x64].cab) و ابزار پچ (de-fenderupdatewinimage.ps1) را دریافت کنید. برای اجرای ابزار کافیست اسکریپت DefenderUpdateWinImage.ps1 را اجرا کنید. این اسکریپت برای اجرا شدن به سطح Administrator و نسخه 5.1 به بعد PowerShell نیاز دارد.

مقالات آموزشی

۱۰ نکته برای امن‌سازی ویندوز در سازمان‌ها (بخش اول)

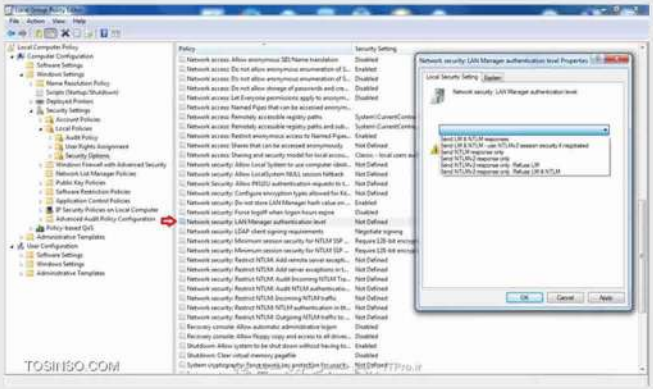
در سازمان‌ها، یکی از راه‌های معمول اعمال قوانین واجازه سطح دسترسی‌های مختلف در کامپیوترهای ویندوزی مایکروسافت، Group Policyها می‌باشد. در اکثر موارد Group Policyها تنظیماتی به منظور پیکربندی تنظیمات امنیتی و دیگر رفتارهای عملیاتی هستند که بر روی رجیستری کامپیوترها می‌نشینند.

Group Policyها می‌توانند توسط اکتیودایرکتوری یا Local group policy پیکربندی و اعمال شوند. این قابلیت تنظیم و پیکربندی تنظیمات امنیتی با استفاده از Group Policy، یکی از بزرگترین مزیت‌های کار کردن با کامپیوترهایی است که سیستم‌عامل‌های آن‌ها ویندوزی است. در بخش اول این آموزش، در این شماره از بولتن خبری می‌خواهیم به ۵ نکته بپردازیم که در صورت در نظر گرفتن آن‌ها تا حد قابل قبولی امنیت سازمان شما حفظ می‌شود، اکثر این تنظیمات به پیکربندی Group Policy مربوط می‌شوند. بخش دوم این آموزش در بولتن شماره بعدی منتشر خواهد شد.

۱. LM و NTLM v1 را غیر فعال کنید.

LM (LAN Manager) و پروتکل‌های احراز هویت NTLM v1 پروتکل‌های احراز هویتی می‌باشند که دارای نقاط آسیب‌پذیری هستند و ترجیحاً پیشنهاد می‌شود از پروتکل‌های NTLM v2 و Kerberos استفاده شود که دارای امنیت قابل قبولی هستند. به صورت پیش‌فرض، اغلب سیستم‌های ویندوزی هر ۴ پروتکل ذکر شده را پشتیبانی می‌کنند، مگر اینکه سیستم‌عامل مورد استفاده شما خیلی قدیمی باشد.

نکته: این Policy به صورت پیش‌فرض پیکربندی نشده است، برای پیکربندی و اعمال تغییرات می‌توانید به مسیر مشخص شده در شکل زیر رجوع کنید.

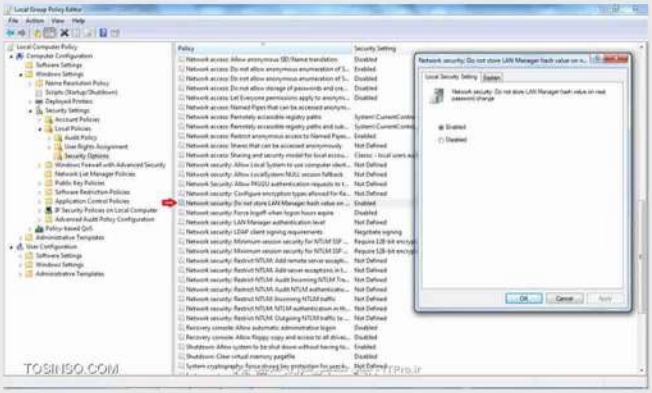


۲. LM Hash Storage را غیرفعال کنید.

LM قبلا در ویندوز برای سازگاری با کلاینت‌های قدیمی مورد استفاده قرار می‌گرفت، به ویژه برای ویندوز ۹۸ به پایین، زمانیکه شما این گزینه را فعال کنید ویندوز به صورت خودکار LAN Manager hash (LM hash) و Windows NT hash(NT hash) مربوط به پسوردها را تولید می‌کند

که این LM password Hashها به آسانی به رمزهای عبور متنی قابل تبدیل هستند و از این رو هکرها با ابزار hash dump می‌تواند پسوردها را بدست آورند. وقتی شما LM Hash Storage را غیرفعال می‌کنید با این کار از ذخیره شدن پسوردها بر روی هارد دیسک کامپیوتر خود جلوگیری می‌کنید. اما مشکلاتی که در صورت فعال کردن این گزینه به وجود خواهد آمد عبارت است از:

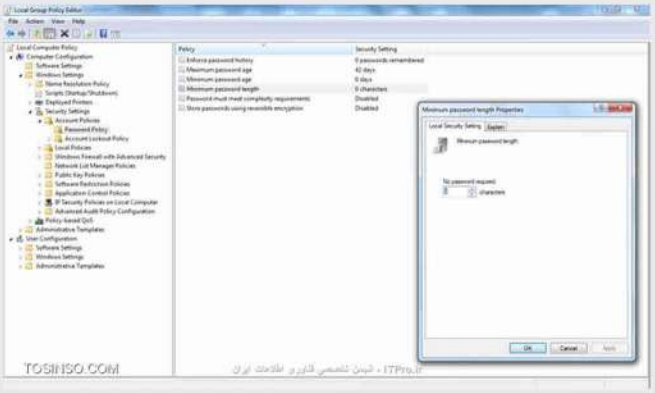
- پسوردها دیگر case sensitive نیستند یعنی PASSWORD با password تفاوتی ندارد، و این بدان معناست که پیچیدگی پسورد شما کاهش می‌یابد.
- پسوردها به کاراکترهای ۷ تایی تقسیم می‌شوند و به صورت جداگانه Hash می‌شوند، (در این صورت ممکن است مورد حمله Brute force قرار بگیرید).
- پسوردها حداکثر به ۱۴ کاراکتر ختم می‌شوند یعنی شما نمی‌توانید پسوردی بیشتر از ۱۴ کاراکتر داشته باشید.



- **نکته۱:** در ویندوز این تنظیمات به صورت پیش‌فرض غیر فعال می‌باشد.
- **نکته۲:** دامین کنترلر پسورد مربوط به کاربرانی که در Event طولشان از 15 کاراکتر بیشتر است، LM hash مربوط به آن کاربران را ذخیره نمی‌کند.

۳. کوتاه نبودن طول پسورد (Minimum password length)

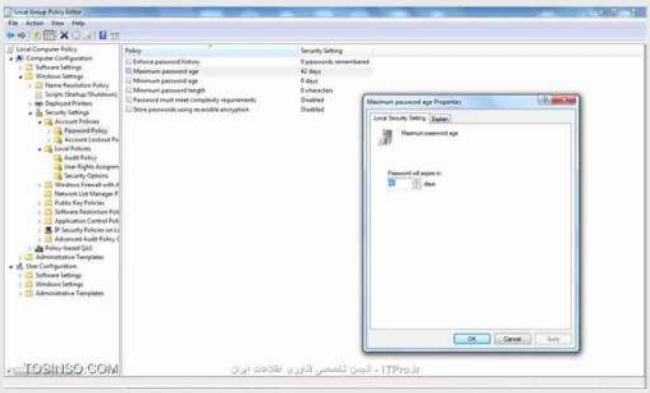
حداقل تعداد پسورد شما باید ۱۲ کاراکتر یا بیشتر باشد. البته در برخی موارد ۸ کاراکتر و در برخی موارد ۱۵ کاراکتر به عنوان یک پسورد قوی عنوان شده است که در دنیای احراز هویت کامپیوترها از آن به عنوان یک پسورد جادویی یاد می‌شود و پیشنهاد می‌شود از پسوردهای ۱۵ کاراکتری استفاده کنید.



۴. بیشترین دوره پسورد (Maximum password age)

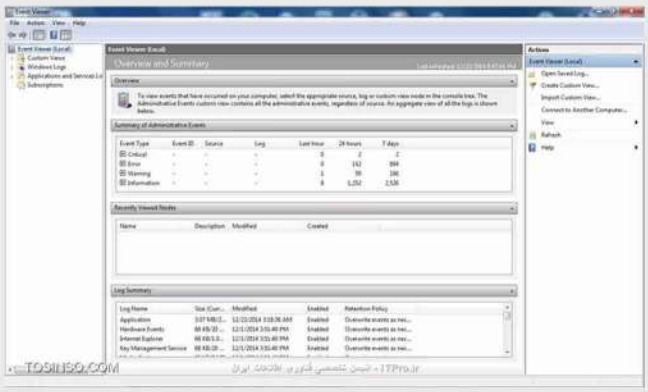
به این معنی که برخی از پسوردها نباید بیشتر از ۹۰ روز مورد استفاده قرار بگیرند و بهتر است که هر ۹۰ روز یکبار تغییر کنند. البته این به نوع سازمان برمی‌گردد که چقدر امنیت در آنجا مهم است، در برخی از سازمان‌هایی که امنیت در آن‌ها بسیار مهم است حتی از پسوردهای یکبار مصرف استفاده می‌شود.

یعنی به عنوان مثال، اگر مدیر شبکه از این پسورد برای ورود به سیستم استفاده کند دیگر آن پسورد Expire می‌شود و بعد از آن حتی شخص مدیر شبکه هم نمی‌تواند از آن استفاده کند و باید از پسورد جدیدی که تولید شده است استفاده کند (این مورد در برابر حملات Sniffing شگرد خوبی می‌باشد). البته در ویندوز این مدت ۴۲ است که می‌توانید طبق شکل زیر به مسیر آن دست پیدا کنید و بسته به سطح امنیتی که می‌خواهید آن را تغییر دهید.



۵. رویداد ثبت وقایع (Event Logs)

به منظور ثبت لاگ رویدادها، Evnet Logs را فعال کنید. Event Logs فایل‌های ویژه‌ای هستند که رویدادهای مهم کامپیوتر شما را ثبت می‌کنند، به عنوان مثال، زمانی که یک کاربر وارد کامپیوتر می‌شود یا برنامه‌ای با Error مواجه می‌شود. هرگاه این مورد از حوادث رخ می‌دهد ویندوز این وقایع را در Event Log ذخیره می‌کند که شما می‌توانید با استفاده از Event Viewer آن‌ها را بخوانید. کاربران حرفه‌ای زمانی‌که اشکال‌زدایی می‌کنند با استفاده از این روش می‌توانند جزئیات سودمندی را بدست آورند.



اخبار داخلی

برگزاری نشست خبری سومین دوره مسابقات فتح پرچم دانشگاه رازی

سه‌شنبه ۱۵ مهرماه ۱۳۹۹، نشست خبری با موضوع "سومین دوره مسابقات فتح پرچم دانشگاه رازی" با حضور اصحاب رسانه استان کرمانشاه در سالن جلسات معاونت پژوهشی دانشگاه رازی برگزار شد.

این مسابقه برای اولین بار به صورت بین‌المللی برگزار خواهد شد. دکتر منکرسی بیان کرد در رده‌بندی جهانی CTFTime تیم مرکز آپای دانشگاه رازی حائز رتبه سوم کشوری و 337 جهانی می‌باشد.

اختتامیه مسابقات نیز با توجه به شرایط کنونی کشور و شیوع ویروس کرونا به صورت آنلاین، صبح روز هشتم آبان ماه ۱۳۹۹، با شرکت علاقمندان برگزار و به ۳ تیم برتر جوایزی اهدا می‌شود، جوایز برای تیم اول ۲۵ میلیون ریال، تیم دوم ۲۰ میلیون ریال و تیم سوم ۱۵ میلیون ریال است.

همزمان با سومین دوره مسابقات فتح پرچم، مسابقه شکارچیان تهدیدات سایبری نیز به عنوان برنامه جانبی برگزار می‌گردد. این مسابقه رقابتی بین بهترین تجربیات شناسایی، پیشگیری و مقابله با تهدیدات سایبری است و به ایده‌های برتر این مسابقه در روز اختتامیه جوایزی اهداء می گردد که برای ایده اول مبلغ ۱۵ میلیون ریال، ایده دوم ۱۰ میلیون ریال و ایده سوم ۵ میلیون ریال در نظر گرفته شده است.

وی مسابقات فتح پرچم را یک مسابقه در حوزه امنیت کامپیوتر دانست و بیان کرد: یکی از اهداف برگزاری این مسابقات، شناسایی افراد متخصص و دارای استعداد جهت معرفی برای رفع نیاز سازمان‌ها و ادارات است.

دکترمنکرسی در پایان گفت: علاقه‌مندان می‌توانند جهت کسب اطلاعات بیشتر و زمان آغاز ثبت‌نام در خصوص مسابقه بین‌المللی فتح پرچم به آدرس اینترنتی ctf.razi.ac.ir مراجعه کنند.

اخبار کوتاه

ربودن حساب بانکی از راه دور ترفند بدافزار جدید Vizom

محققان نوع جدیدی از بدافزار را که از حملات همپوشانی از راه دور برای حمله به دارندگان حساب بانکی استفاده می‌کند را کشف کرده‌اند.نوعی بدافزار جدید که شرکت IBM آن را Vizom نام‌گذاری کرده است ، در یک کمپین فعال مورد استفاده قرار گرفته است. محققان امنیتی IBM، اظهار داشتند که این بدافزار از روش‌های جالبی برای پنهان ماندن و به خطر انداختن دستگاه‌های کاربر در زمان واقعی - یعنی تکنیک‌های پوشش از راه دور و سرقت DLL- استفاده می‌کند.

Vizom از طریق کمپین‌های فیشینگ مبتنی بر spam گسترش می‌یابد و خود را به عنوان نرم‌افزار محبوب ویدئو کنفرانس تبدیل می‌کند، ابزاری که به دلیل شیوع ویروس کرونا در تجارت و رویدادهای اجتماعی بسیار مهم شده است.

هنگامی که بدافزار بر روی یک کامپیوتر آسیب‌پذیر ویندوز قرار گرفت، Vizom ابتدا برای شروع زنجیره آلودگی به فهرست AppData حمله می‌کند. با کنترل سرقت DLL، بدافزار سعی خواهد کرد DLLهای مخرب را با نامگذاری انواع مبتنی بر Delphi با نام‌هایی که در فهرست نرم‌افزار قانونی قرار دارد ، مجبور به دانلود کند.

با ربودن"inherent logic"، سیستم‌عامل برای دانلود بدافزارvizom فریب داده می‌شود . DLL با نام Cmmlib.dll، فایلی است که با zoom مرتبط است.

برای اطمینان از اینکه کد مخرب از" Cmmlib.dll "اجرا شده، نویسنده بدافزار لیست استخراج واقعی DLL قانونی را کپی کرده است اما برای اصلاح آن مطمئن شده و همه functionها را به همان آدرس هدایت می‌کند.

یک dropper سپس zTscoder.exe را از طریق خط فرمان راه اندازی می‌کند و -pay load دوم ،- با همان ترفند سرقت در مرورگر اینترنت Vivaldi، Trojan Access Remote (RAT)، از یک سرور راه دور استخراج می‌شود.

برای ایجاد ماندگاری، shortcutهای مرورگر دستکاری می شوند و مهم نیست که کاربر چه مرورگری را اجرا می کند، کد مخرب Vivaldi / Vizom در پس زمینه اجرا می‌شود.

در این مرحله بدافزار، بی سر و صدا منتظر هرگونه نشانه دسترسی به خدمات بانکی آنلاین خواهد ماند. اگر نام عنوان یک صفحه وب با لیست هدف Vizom مطابقت داشته باشد ،به اپراتورها هشدار داده می شود و می‌توانند از راه دور به کامپیوتر آسیب‌دیده متصل شوند.

از آنجا که Vizom قبلاً قابلیت‌های RAT را به کار گرفته است ، مهاجمان می‌توانند جلسه ای که به خطر افتاده را در دست بگیرند و محتوای آن‌ها را بپوشانند تا قربانیان را برای ارسال اطلاعات دسترسی و اعتبار حساب های بانکی خود فریب دهند.

قابلیت‌های کنترل از راه دور همچنین از عملکردهای Windows API، مانند حرکت دادن نشانگر ماوس، وارد کردن input صفحه کلید و کلیک‌ها، سوءاستفاده می‌کند. Vizom همچنین می‌تواند اسکرین شات ها را از طریق ویندوز پرینت و ذره بین (magni- fier) بدست بیاورد.

هم‌اکنون، Vizom بر روی بانک‌های بزرگ برزیل تمرکز دارد ، با این حال، معلوم شده است که همان شیوه‌ها علیه کاربران در سراسر آمریکای جنوبی استفاده می شود و قبلاً نیز مشاهده شده که بانک های اروپا را نیز هدف قرار داده است.

مرکز تخصصی آپا دانشگاه رازی