بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره هشتم بهمن ماه ۱۳۹۷

خلق ابتکاری دیگر در حملات سایبری

"شراکت باج‌افزار و استخراج کننده ارز دیجیتال!"

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

خلق ابتکاری دیگر در حملات سایبری
"شراکت باج‌افزار و استخراج‌کننده ارز دیجیتال!"

گردآورنده: آتوسا خدامرادی

به زودی در ژانویه 2019، بدترین ائتلاف باج‌افزار و خانواده استخراج‌گر ارزهای دیجیتال گسترش خواهد یافت. Malware Spam یا MalSpam اصطلاحی است که به بدافزارهایی اطلاق می‌شود که از طریق ایمیل گسترش می‌یابند.

هرزنامه‌های مخرب یا MalSpam از فایل‌های فشرده شده جاوا اسکریپت (.js) استفاده می‌کنند که به ایمیل‌ها پیوست شده‌اند. این یک تاکتیک مؤثر است که توسط مجرمان سایبری برای توزیع بدافزارها استفاده می‌شود.

ترافیک آلوده شامل باج‌افزار GandCrab، استخراج‌گر ارز دیجیتال Monero (XMRig) و ربات هرزنامه Phorpiex می‌باشد.

ابتدا ایمیل با فایل جاوا اسکریپت تحویل داده شده، و سپس فایل "exe" از آن استخراج می‌گردد. سپس این فایل، [1] dropper را دانلود نموده و dropper سایر دستورات را از سرور C&C (Command and Control) دریافت می‌نماید.

در روزهای اخیر نمونه‌های زیادی یافت شده، و نمونه‌های جدیدی نیز در سندباکس‌های عمومی بارگذاری شده‌اند. در "app.any.run" که یک سندباکس عمومی است، نزدیک به 1200 نمونه بارگذاری شده و در حال گسترش می‌باشند.

به نظر می‌رسد باج‌افزار GandCrab به همراه استخراج‌گر ارز دیجیتال، بحران جدید سال 2019 خواهد بود. هدف GandCrab به عنوان یک باج‌افزار، رمز نمودن تمام یا بیشتر فایل‌های سیستم آسیب‌پذیر، و درخواست مبلغی برای رمزگشایی آن‌ها می‌باشد. توسعه دهنده، مبلغ درخواستی خود را در قالب ارز دیجیتال DASH [2] درخواست می‌کند چرا که پیگیری آن پیچیده می‌باشد.

سیر تکامل باج‌افزار GandCrab

GandCrab v1: در سال 2018 کشف شد. در یک ماه اخیر بیش از 50000 کاربر به آن گرفتار شده و فایل‌های آن‌ها رمز شده است. این باج‌افزار درخواست پرداخت باج خود را در فرمت ارز دیجیتال "DASH" عنوان می‌کند.

GandCrab v2: در ماه می 2018 کشف شد. از پسوند رمزگذاری جدید ".CRAB" استفاده می‌کند.

GandCrab v3 and v3.1: در اواخر سال 2018 و با تکنیک‌های دور زدن آنتی ویروس کشف شد.

GandCrab v4: تغییرات زیادی در جریان کار و الگوهای ارتباطی آن به وجود آمده است. در الگوریتم رمزگذاری آن از پسوند جدید ".KRAB" استفاده می‌شود. به طور شگفت‌انگیزی این نوع به CnC [3] متصل نمی‌شود.

GandCrab v5 & v5.0.4: تغییرات زیادی در الگوهای ارتباطی ایجاد نموده است و از استانداردهای رمزنگاری پیشرفته استفاده می‌نماید. در اواخر سال 2018 قربانیان آن بیشتر شده‌اند.

بدافزارهای استخراج ارز دیجیتال چه هستند؟

بدافزارهای استخراج ارز دیجیتال، بدافزارهایی هستند که مجرمان سایبری از طریق آن‌ها و با استفاده از قدرت پردازش تعداد زیادی از کامپیوترها، گوشی‌های هوشمند و دیگر دستگاه‌های الکترونیکی، اقدام به تولید و استخراج ارز دیجیتال می‌نمایند. به این ترتیب آن‌ها با آلوده نمودن ماشین‌ها، استفاده از دستگاه‌ها، رمزگذاری با استفاده از بدافزار و از بین بردن ردپا، اقدامات خود را تکمیل می‌نمایند. مهاجمان سایبری در حال یافتن راه‌های بیشتری برای ایجاد یک ائتلاف از بدافزارهای مخرب و ترکیب آن‌ها با یکدیگر، به منظور رسیدن به اهداف خود هستند.

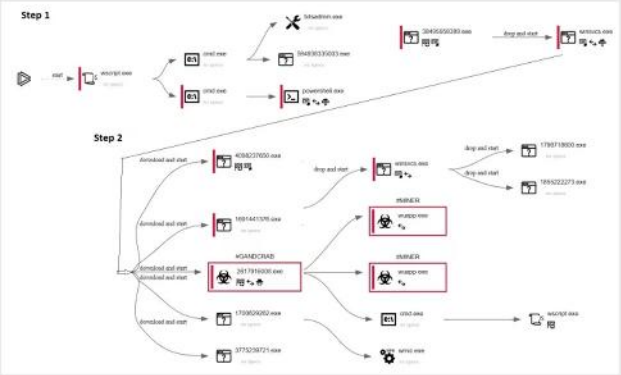
---

[1] نوعی تروجان است که نرم‌افزارهای مخرب را به سیستم هدف متصل می‌کند. کد مخرب به گونه‌ای در داخل Dropper قرار می‌گیرد که توسط اسکنرهای ویروس قابل شناسایی نباشد و یا در زمان اولین فعالیت Dropper در ماشین هدف، بدافزار بارگیری می‌شود.

[2] یک نوع ارز دیجیتال open source می‌باشد و یک نوع سازمان غیرانتفاعی و مستقل است که توسط مجموعه‌ای از کاربران اجرا می‌شود که "masternodes" نامیده می‌شوند.

[3] Computer Numerical Control

فرآیند MalSpam



توصیه‌هایی جهت مقابله با MalSpam

1- مسدودسازی پیوست‌های ایمیل با نام‌هایی شبیه Love_You_ , Luv_You , Love_You , Love و غیره.

2- در صورتی که به فایل‌های با پسوند js. نیاز ندارید، مطمئن شوید که آن‌ها را در ایمیل خود مسدود نموده‌اید.

3- تمامی URLها و IoCsهای مبتنی بر آی‌پی را در فایروال، IDS، دروازه‌های وب (مثل وب‌سایت‌ها) و مسیریاب‌ها مسدود نمایید.

4- اطمینان حاصل نمایید که تیم SOC شما مسیرهای فعالیت باج‌افزارها را به درستی نظارت می‌کنند.

5- اطمینان حاصل نمایید که تیم SOC شما به درستی متوجه فعالیت‌های غیرعادی اجرا شده در Powershell می‌باشند.

منبع خبر :

https://gbhackers.com/malspam/

دور زدن فیلترهای گوگل توسط هکرها به منظور انتشار بدافزار CSV از طریق گوگل‌شیت

گردآورنده: سیده مرضیه حسینی

اخیراً مجرمان سایبری به جای استفاده از گوگل شیت مایکروسافت که اغلب توسط هکرهای بدخواه مورد استفاده قرار می‌گیرد، از تکنیک‌های پیچیده و جدیدی برای انتشار بدافزار CSV از طریق گوگل شیت‌ها استفاده می‌کنند. فایل‌های CSV می‌توانند در MS Excel باز شوند. در این حالت، مهاجم برای آلوده نمودن سیستم کاربران و ارسال بدافزار به آن، بدافزار را از طریق ایمیل‌های اسپم در spreadsheet گوگل قرار می‌دهد.

با گسترش این بدافزار از طریق Spread Sheet گوگل، و سوءاستفاده از اعتماد مردم نسبت به گوگل، قربانیان این ماجرا، صرف‌نظر از اینکه چه کسی پیام را برایشان ارسال نموده است راحت‌تر فریب خواهند خورد. البته کسانی که امنیت را در نظر می‌گیرند محتاط‌تر عمل نموده و هرگز به آن اطمینان نمی‌کنند.

گوگل تکنیک‌های پیچیده gMail و gDrive ضدبدافزار را اجرایی نموده، تا از گسترش یافتن این بدافزار در قالب فایل‌های خاص (.zip, .dll, .exe و غیره) در gMail جلوگیری نماید.

خبر بد اینجاست که متأسفانه مهاجمان این فیلتر گوگل را نیز دور زده و به راحتی از گوگل شیت‌ها به‌عنوان حامل بدافزار استفاده می‌کنند، که گوگل در مورد این مسئله هشدار داده است.

به گفته محققان، در نهایت مهاجم می‌تواند لینکی را از طریق یک پیام و یا ایمیل ارسال نموده و از قربانی درخواست نماید که

برای باز نمودن spreadsheet گوگل شیت، به صورت محلی از "MSExcel compatibility issues" استفاده کند. به محض دانلود گوگل شیت و باز نمودن آن از طریق مایکروسافت، مهاجم به هدف خود دست یافته و سیستم کاربر آلوده می‌گردد.

کاربران باید از این نوع حملات آگاه باشند و در صورت دریافت لینکی مبنی بر کار نکردن گوگل شیت‌ها، از دانلود آن اجتناب نمایند.

Scan Link

منبع خبر :

https://gbhackers.com/csv-malware-via-google-sheets

کشف آسیب‌پذیری‌های خطرناک در پروتکل محبوب RDP

گردآورنده: پویان مسعودی نیا

همان‌طور که بارها و بارها در مطالب آموزشی و اخبار امنیتی هشدار داده شده است، هیچ‌گاه نباید به افراد غیرقابل اعتمادی که می‌خواهند از راه دور به سیستم شما دسترسی داشته باشند، و یا می‌خواهند از راه دور به شما امکان دسترسی به سیستم خودشان را بدهند اعتماد نمود.

محققان شرکت امنیتی Check Point، چندین آسیب‌پذیری را در کلاینت‌های متن‌باز RDP و کلاینت اختصاصی مایکروسافت کشف نموده‌اند، که این آسیب‌پذیری‌ها به یک سرور RDP مخرب امکان دسترسی کامل و تسخیر یک کلاینت را به صورت معکوس فراهم می‌آورد.

پروتکل Remote Desktop Protocol_ RDP_ به کاربران این امکان را می‌دهد تا به کامپیوترها از راه دور متصل شوند. می‌توان گفت که این پروتکل معمولاً توسط کاربران فنی و مدیران IT جهت برقراری ارتباط از راه دور به دیگر دستگاه‌های شبکه مورد استفاده قرار می‌گیرد.

این پروتکل ابتدا توسط شرکت مایکروسافت صرفاً برای سیستم‌عامل‌های ویندوز توسعه داده شد، اما چندین کلاینت متن‌باز نیز برای این پروتکل وجود دارند که سبب می‌شوند RDP در لینوکس و همچنین سیستم‌عامل‌های یونیکس نیز مورد استفاده قرار گیرد.

محققان شرکت امنیتی Check Point، به‌تازگی با تجزیه و تحلیلی که بر روی سه کلاینت معروف و پراستفاده FreeRDP_RDP, rdesktop و کلاینت RDP ویندوز_ انجام داده‌اند، 25 آسیب‌پذیری امنیتی را شناسایی نموده‌اند. برخی از این آسیب‌پذیری‌ها برای سرورهای مخرب RDP با دسترسی از راه دور، امکان در دست گرفتن کنترل کامل کامپیوتری که کلاینت RDP بر روی آن قرار دارد را فراهم می‌آورند.

FreeRDP، که می‌توان آن را محبوب‌ترین کلاینت متن‌باز RDP بر روی گیت‌هاب دانست، تحت تأثیر 6 آسیب‌پذیری قرار گرفته است که 5 مورد از این آسیب‌پذیری‌ها سبب خرابی حافظه و حتی امکان اجرای کد از راه دور بر روی کامپیوتر کلاینت می‌گردند.

Rdesktop، که میتوان از آن به عنوان یک کلاینت RDP متن‌باز قدیمی که به صورت پیش‌فرض بر روی کالی لینوکس وجود دارد یاد کرد، این کلاینت آسیب‌پذیرترین کلاینتی است که تحت تأثیر 19 آسیب‌پذیری قرار دارد. که 11 مورد از این آسیب‌پذیری‌ها، به یک سرور مخرب RDP امکان اجرای کد دلخواه بر روی کامپیوتر کلاینت را می‌دهد.

کلاینت RDP ویندوز، حاوی هیچ آسیب‌پذیری اجرای کد از راه دور نیست، اما محققان چندین سناریوی حمله‌ی جذاب را برای آن کشف نموده‌اند. همانطور که می‌دانید سرور و کلاینت داده‌های

clipboard را به‌اشتراک می‌گذارند، که این موضوع به کلاینت امکان دسترسی و تغییر داده‌های clipboard بر روی سرور و بالعکس را می‌دهد.

محققان آسیب‌پذیری‌های کشف شده را در اکتبر 2018 به توسعه‌دهندگان گزارش نموده‌اند.

آسیب‌پذیری‌های موجود در کلاینت FreeRDP، به عنوان بخشی از نسخه‌ی v2.0.0-rc4 وصله شده، و در کمتر از یک ماه از تاریخ انتشار آسیب‌پذیری، بر روی repository گیت‌هاب منتشر گردید.

Rdesktop نیز آسیب‌پذیری‌های مربوطه را در نسخه‌ی v1.8.4 وصله نموده، و این نسخه را در اواسط ماه ژانویه منتشر کرد.

کاربران کلاینت RDP ویندوز نیز می‌توانند با غیرفعال نمودن قابلیت clipboard-sharing، از سیستم‌های خود در برابر حملات محافظت نمایند. البته باید خاطر نشان کرد که قابلیت clipboard-sharing به صورت پیش‌فرض هنگام اتصال به دستگاه‌ها از راه دور فعال است، که باید آن را به صورت دستی غیرفعال نمود.

Scan Link

منبع خبر :

https://thehackernews.com/2019/02/remote-desktop-hacking.html?m=1

باز هم یک آسیب‌پذیری وصله نشده در سیستم‌عامل مک!

گردآورنده: پویان مسعودی نیا

آسیب‌پذیری امنیتی جدیدی در آخرین نسخه سیستم‌عامل MacOS Mojave اپل کشف شده است که به سبب آن یک برنامه مخرب می‌تواند به پوشه‌های حیاتی_restricted_ که سایر برنامه‌ها اجازه دسترسی به آن را ندارند، دسترسی داشته باشد.

این آسیب‌پذیری در تاریخ 8 فوریه توسط eff Johnson _توسعه دهنده نرم افزار_ کشف شده است، و از زمان انتشار آن تا به حال هیچ وصله‌ی امنیتی برای آن منتشر نشده است. نکته قابل توجه این است که این آسیب‌پذیری تمامی نسخه‌های macOS Mojave حتی نسخه "10.14.3"، که در بروزرسانی 7 فوریه منتشر شد را نیز تحت تاثیر قرار می‌دهد.

برخی از پوشه‌ها در سیستم‌عامل مک به دلایل امنیتی دسترسی محدودی دارند که به طور پیش فرض دسترسی به آن‌ها ممنوع است، مانند پوشه "~/Library/Safari"، که فقط توسط چند برنامه کاربردی ازجمله Finder قابل دسترسی است. با این‌حال این محقق، راهی برای دور زدن این محدودیت‌ها در سیستم‌عامل Mojave کشف کرد که به برنامه‌های کاربردی، بدون داشتن مجوز از کاربر یا سیستم اجازه دسترسی به پوشه "~/Library/Safari" و خواندن سابقه مرورگر وب کاربران را می‌دهد.

از آنجا که از زمان گزارش این آسیب‌پذیری به شرکت اپل، تاکنون هیچ وصله‌ای برای آن ارائه نشده است، Johnson تصمیم دارد تا زمانی که رفع این آسیب‌پذیری صورت نپذیرفته است، جزئیات فنی آن را منتشر نکند.

Johnson همچنین اظهار داشت که این آسیب‌پذیری برای دور زدن حریم خصوصی کشف شده هیچ ارتباطی با افزونه‌های _extensions_ سافاری ندارد، چرا که این مسئله بر روی پوشه‌های محدود شده تاثیر می‌گذارد، و به طور بالقوه می‌تواند بر همه پوشه‌های محدود شده در

سیستم macOS، از جمله "~/Library / Safari" تاثیرگذار باشد.

از آنجا که این مشکل در قابلیت جدید "privacy protection" معرفی شده توسط اپل در نسخه "macOS Mojave 10.14" وجود دارد، آن دسته از کاربران اپل که از سیستم‌عامل با نسخه‌های قدیمی‌تر مانند "High Sierra" در رایانه‌های مک خود استفاده می‌کنند، تحت تأثیر این آسیب‌پذیری قرار نمی‌گیرند.

Scan Link

منبع خبر :

https://thehackernews.com/2019/02/macos-mojave-privacy-hack.html?m=1

اخبار کوتاه

فریب پیامک جعلی

"سهام عدالت به همراه 500 هزار تومان عیدی " را نخورید

گروه ناجا- معاون اجتماعی پلیس فتا ناجا از شهروندان خواست فریب پیامک جعلی " ثبت اطلاعات کارتی خود در سامانه سهام عدالت به همراه 500 هزار تومان عیدی سال نو" را نخورند.

سرهنگ "رامین پاشایی" در گفت و گو با خبرنگار پایگاه اطلاع‌رسانی پلیس فتا با اعلام این خبر، اظهارداشت: بسیاری از هموطنان گرامی در روزهای گذشته پیامکی دریافت کرده‌اند مبنی بر اینکه " فقط تا پایان اسفند ماه فرصت باقیست جهت ثبت اطلاعات کارتی خود در سامانه سهام عدالت به همراه 500 هزار تومان عیدی سال نو" اقدام کنند.

این مقام انتظامی گفت: پیامک مذکورهیچ‌گونه ارتباطی با سامانه رسمی سهام عدالت ندارد و اطلاعات شخصی و بانکی افراد مانند رمز دوم، شماره حساب، cvv2 و ... با این ترفند توسط مجرمان سایبری جهت کلاهبرداری‌های اینترنتی به سرقت برده می‌شود.

معاون اجتماعی پلیس فتا ناجا بیان کرد: شهروندان می‌توانند در صورت مواجهه با موارد مشکوک و غیرقانونی در فضای مجازی آن‌راازطریق‌سایت‌پلیس‌فتا(www.cyberpolice.ir)به‌این‌پلیس‌اعلام‌کنند.

پلیس فتا هشدار داد

کپی شدن اطلاعات کارت بانکی با ترفند اسکیمر

خطر در کمین شما!

مواظب کارت‌های بانکی خود باشید.

اسکیمرها یا دستگاه‌های کپی کارت بانکی بسیار فراوان شده‌اند. به راحتی از روی کارت شما یک المثنی ساخته و رمز هم که خودتان در اختیارشان قرار می‌دهید.

چه کار کنیم که در دام این نوع سوء استفاده‌ها نیفتیم؟

- حتماً چند کارت بانکی داشته باشید و از کارتی برای خریدهای روزانه خود استفاده کنید که مبلغ زیادی داخل آن نباشد که اگر در معرض کلاهبرداری قرار گرفتید زندگی شما با مخاطره روبرو نشود.
- حتماً رمز را خودتان وارد کنید. همان‌طور که از نامش پیداست اسمش رمز است و باید فقط در اختیار خودتان باشد.
- وقتی از مشاغلی که سیار هستند خرید می‌کنید احتیاط بیشتری داشته باشید گرچه حتی گزارش داشتیم طرف مغازه ثابت اجاره کرده برای کلاهبرداری با دستگاه اسکیمر، کارت‌های بانکی مشتری‌هایش را کپی کند.

در دنیای الکترونیک جدید مواظب خودمان باشیم.

آسیب پذیری

کشف آسیب‌پذیری حیاتی در سوئیچ‌های Small Business سیسکو

گردآورنده: سیده مرضیه حسینی

شدت آسیب‌پذیری

شدت این آسیب‌پذیری **Critical** می‌باشد.

خلاصه آسیب‌پذیری

این آسیب‌پذیری با شناسه CVE-2018-15439، در واقع یک آسیب‌پذیری حیاتی در سوئیچ‌هایSmall Business سیسکو است که به مهاجم از راه دور اجازه می‌دهد مکانیزم تأیید هویت کاربر را در یک دستگاه آسیب‌دیده دور بزند.

در این آسیب‌پذیری، یک حساب کاربری منحصر به فرد بدون اطلاع مدیران سیستم، فعال می‌شود. مهاجم می‌تواند با استفاده از این حساب کاربری برای ورود به یک دستگاه آسیب‌دیده و اجرای دستورات با حقوق و امتیازات کامل مدیر، استفاده نماید.

محصولات زیر، تحت تأثیر این آسیب‌پذیری قرار دارند:

- Cisco Small Business 200 Series Smart Switches
- Cisco Small Business 300 Series Managed Switches
- Cisco Small Business 500 Series Stackable Managed Switches
- Cisco 250 Series Smart Switches
- Cisco 350 Series Managed Switches
- Cisco 350X Series Stackable Managed Switches
- Cisco 550X Series Stackable Managed Switches

شرکت سیسکو تاکنون بروزرسانی‌های نرم‌افزاری برای رفع این آسیب‌پذیری، منتشر نکرده است.

راهکارهای ارائه شده

سیسکو به مدیران توصیه می‌کند که حداقل یک حساب کاربری با حق دسترسی سطح 15در پیکربندی دستگاه اضافه نمایند، به طوری که حساب کاربری پیش‌فرض غیرفعال شود. جهت دریافت اطلاعات بیشتر می‌توانید به لینک زیر مراجعه نمایید:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181107-sbsw-privacc

Scan Link

منبع خبر :

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181107-sbsw-privacc

انتشار phpMyAdmin نسخه 4.8.5 و رفع آسیب‌پذیری‌های SQL injection و Arbitrary File Read

گردآورنده: سیده مرضیه حسینی

نسخه 4.8.5 از نرم‌افزارphpMyAdmin برای رفع چندین آسیب‌پذیری بحرانی و حفره‌های امنیتی، منتشر شد. phpMyAdmin نرم‌افزاری رایگان برای مدیریت پایگاه‌داده MySQL است.

اصلاحات امنیتی phpMyAdmin 4.8.5

- **Arbitrary File Read (آسیب‌پذیری خواندن فایل دلخواه)**

اگر گزینه AllowArbitraryServer بر روی True تنظیم شده باشد،

یک مهاجم با فریب دادن سرور MySQL می‌تواند فایل‌هایی را که کاربران وب سرور به آن‌ها دسترسی دارند بخواند.

این آسیب‌پذیری از جمله آسیب‌پذیری‌های حیاتی محسوب می‌شود و می‌توان با تنظیم AllowArbitraryServer به صورت false از آن پیشگیری نمود.

از نسخه 4.0 تا نسخه 4.8.4 نرم‌افزار phpMyAdmin تحت تأثیر این آسیب‌پذیری قرار دارند و از نسخه 4.8.5 به بعد این آسیب‌پذیری رفع گردیده است.

- **SQL injection (آسیب‌پذیری تزریق SQL)**

مهاجم می‌تواند این آسیب‌پذیری را با یک نام کاربری خاص که می‌تواند برای حمله تزریق SQL مورد استفاده قرار گیرد، اکسپلویت نماید.

این یک آسیب‌پذیری مهم و خطرناک است و نسخه‌های 4.5.0 تا 4.8.4 نرم‌افزار phpMyAdmin را تحت تأثیر قرار می‌دهد و از نسخه 4.8.5 به بعد رفع گریده است.

- **دیگر حفره‌های امنیتی اصلاح شده**

* در دسترس نبودن Export در قالب SQL
* عدم نمایش کد QR هنگام اضافه کردن احراز هویت دو مرحله‌ای به یک حساب کاربری
* مشکل اضافه کردن یک کاربر جدید در نسخه MySQL 8.0.11 و نسخه‌های جدیدتر
* مسدود شدن رابط مربوط به پلاگین Text_Plain_Sql
* حذف tab مربوط به Table level Operations

Scan Link

منبع خبر :

https://gbhackers.com/phpmyadmin-4-8-5-released

آسیب‌پذیری اجرای کد از راه دور در کتابخانه Apache Struts Commons FileUpload محصولات سیسکو

گردآورنده: آتوسا خدامرادی

شدت آسیب‌پذیری

با توجه به گزارشات منتشر شده، شدت این آسیب‌پذیری **Critical** (حیاتی) می‌باشد.

خلاصه آسیب‌پذیری

در تاریخ 5 نوامبر 2018 تیم Apache Struts یک آگهی امنیتی مبنی بر ارتقاء کتابخانه Commons FileUpload به نسخه 1.3.3، منتشر نمود. این کتابخانه در سیستم‌هایی که از Struts نسخه 2.3.36 یا قبل‌تر از آن استفاده می‌نمایند به کار رفته است. سیستم‌هایی که از نسخه‌های قبلی این کتابخانه استفاده می‌نمایند در معرض حملاتی قرار دارند که می‌توانند کدهای دلخواهی را اجرا نموده و یا فایل‌ها را در سیستم تغییر دهد. این مسئله ناشی از آسیب‌پذیری کتابخانه Apache Commons FileUpload است که پیش از این گزارش شده و شناسه CVE-2016-1000031 به آن اختصاص یافته است.

این آسیب‌پذیری ناشی از اعتبارسنجی نامناسب اطلاعات ورودی کاربر در برنامه آسیب‌پذیر می‌باشد. هکر می‌تواند این آسیب‌پذیری را توسط ارسال داده ساختگی به سیستم آسیب‌پذیر، اکسپلویت نماید. اکسپلویت موفق این آسیب‌پذیری به هکر اجازه می‌دهد که کدهای دلخواه خود یا فایل‌های تغییر داده شده را در سیستم هدف اجرا نماید.

تیم Response Team Incident Security سیسکو ادعا می‌کند که تاکنون گزارشی از سوءاستفاده از آسیب‌پذیری مذکور دریافت ننموده است.

راهکارهای امنیتی ارائه شده تا کنون

تیم Apache Struts توصیه می‌کند که کاربران هر چه سریعتر Struts نسخه 2.3.36 یا قبل‌تر از آن را به منظور استفاده از آخرین نسخه‌کتابخانهCommonsFileUpload(که‌درحال‌حاضرنسخه1.3.3است) ارتقاء دهند. جهت کسب اطلاعات بیشتر می‌توانید به لینک زیر مراجعه نمایید:

https://www.mail-archive.com/announce-ments@struts.apache.org/msg00093.html

Scan Link

منبع خبر :

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181107-struts-commons-fileupload

آسیب‌پذیری جدید ارتقاء سطح دسترسی systemd و تأثیر آن بر اغلب توزیع‌های لینوکس

گردآورنده: آتوسا خدامرادی

محققان امنیتی سه آسیب‌پذیری جدید در Systemd کشف نموده‌اند. Systemd یک [4] init محبوب و مدیر سرویس برای اغلب سیستم‌عامل‌های مبتنی بر لینوکس است. این آسیب‌پذیری‌ها به مهاجمان محلی با سطح دسترسی پایین یا برنامه‌های مخرب اجازه می‌دهند که به سطح دسترسی root در سیستم‌های هدف دست یابند.

این آسیب‌پذیری‌ها که به شناسه‌های CVE-2018-16865،CVE-2018-16864 و CVE-2018-16866 مشخص شده‌اند، در واقع باگ مربوط به سرویس "systemd-journald" است که اطلاعات را از منابع مختلف جمع‌آوری نموده و توسط اطلاعات ورود کاربر در journal، لاگ‌های رویداد را ایجاد می‌کند.

این آسیب‌پذیری‌ها که توسط محققان امنیتی Qualys کشف شده‌اند، تمام توزیع‌های لینوکس مبتنی بر systemd، مانند Redhat و Debian را تحت تأثیر قرار می‌دهند.

برخی دیگر از توزیع‌های لینوکس مانند SUSE Linux Enterprise 15 , openSUSE Leap 15.0 و Fedora (28 و 29) تحت تأثیر این آسیب‌پذیری‌ها قرار نمی‌گیرند.

دو آسیب‌پذیری اول باگ‌های مربوط به خرابی حافظه و آسیب‌پذیری سوم باگ خارج از محدوده خواندن، در systemd-journald می‌باشد که می‌تواند داده‌های حساس حافظه پردازنده را از بین ببرد.

محققان موفق به ایجاد اکسپلویت اثبات مفهومی (proof-of-concept) برای این آسیب‌پذیری شده و به زودی آن را منتشر خواهند نمود.

محققان در گزارش منتشر شده روز چهارشنبه نوشتند که: "ما یک اکسپلویت برای CVE-2018-16865 و CVE-2018-16866 توسعه داده‌ایم که به طور متوسط ظرف مدت 10 دقیقه در معماری i386 و 70 دقیقه در معماری amd64، دسترسی root در shell را به‌دست می‌آورد."

CVE-2018-16864 شباهت بسیاری به آسیب‌پذیری Stack Clash دارد که محققان Qualys آن را در سال 2017 کشف نمودند. این آسیب‌پذیری توسط بدافزار یا کاربران با سطح دسترسی پایین، اکسپلویت شده و به موجب آن سطح دسترسی به root

[4] init کوتاه شده Initialization، نام برنامه یا پروسه‌ای در سیستم عامل‌های کامپیوتری مبتنی بر یونیکس است که تمام پروسه‌های دیگر را ایجاد می‌نماید و بالا می‌آورد. این برنامه به صورت یک دمون و معمولاً با PID 1 اجرا می‌شود. بارگذار بوت، هسته را شروع می‌نماید و هسته init را شروع می‌نماید.

ارتقاء داده می‌شد.

راه‌حل ارائه شده

چنان‌چه از توزیع‌های آسیب‌پذیر لینوکس استفاده می‌کنید، آخرین به‌روزرسانی مربوطه را دریافت نموده و وصله‌های امنیتی که به زودی ارائه می‌شوند را نصب نمایید.

Scan Link

منبع خبر :

https://thehackernews.com/2019/01/linux-systemd-exploit.html

آسیب‌پذیری سرریز بافر در SD-WAN Solution سیسکو

گردآورنده: آتوسا خدامرادی

شدت آسیب‌پذیری

با توجه به گزارشات منتشر شده، شدت این آسیب‌پذیری **Critical** (حیاتی) می‌باشد.

خلاصه آسیب‌پذیری

این آسیب‌پذیری با شناسه CVE-2019-1651، در vContainer از SD-WAN Solution سیسکو یافت شده است که به هکر احراز هویت شده اجازه می دهد از راه دور موجب حمله منع سرویس (DoS) شده و کد دلخواه خود را به عنوان کاربر root اجرا نماید.

این آسیب‌پذیری ناشی از بررسی نادرست محدوده‌ها توسط vContainer می‌باشد. هکر می‌تواند با ارسال یک فایل مخرب به vContainer آسیب‌پذیر، این آسیب‌پذیری را اکسپلویت نماید. اکسپلویت موفق این آسیب‌پذیری به هکر اجازه می‌دهد که موجب سرریز بافر در vContainer آسیب‌پذیر شده و در نتیجه حمله منع سرویس (DoS) صورت گیرد که موجب اجرای کد دلخواه به عنوان کاربر root می‌شود.

راهکارهای امنیتی ارائه شده تا کنون

تا کنون راهکار امنیتی برای این آسیب‌پذیری ارائه نشده است. اما در بروزرسانی رایگانی که سیسکو ارائه نموده است این آسیب‌پذیری نیز مورد پوشش قرار داده شده است. لذا توصیه می‌شود که مدیران در اسرع وقت بروزرسانی مورد نظر را اعمال نمایند.

Scan Link

منبع خبر :

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-bo

تهدید روترهای RV320 / RV325 سیسکو توسط اکسپلویت‌های جدید

گردآورنده: پویان مسعودی نیا

شدت آسیب‌پذیری

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

خلاصه آسیب‌پذیری

اگر از روترهای RV325 یا RV320 Dual Gigabit WAN VPN سیسکو در سازمان خود استفاده می‌کنید، توصیه می‌شود هر چه سریع‌تر به‌روزرسانی‌های منتشر شده توسط شرکت سیسکو را اعمال نمایید.

مهاجمان سایبری پس از انتشار کد اثبات مفهومی این اکسپلویت توسط یک محقق امنیتی در اینترنت، اقدام به اکسپلویت حدود 9000 روتر مدل RV320/RV325 سیسکو نمودند.

آسیب‌پذیرهای ذکر شده موجب بروز مشکلاتی چون نقص تزریق فرمان (کنترل سیستم) با شناسه "CVE-2019-1652" و نقص افشای اطلاعات با شناسه "CVE-2019-1653" می‌شوند.

لازم به ذکر است که ترکیب این دو آسیب‌پذیری، برای یک مهاجم از راه دور امکان کنترل کامل روتر سیسکو را فراهم می‌آورد.

اولین مشکل در روترهای مدل RV320 و RV325 Dual Gigabit WAN VPN سیسکو، که دارای سیستم‌عامل‌های نسخه 1.4.2.15 و 1.4.2.19 می‌باشند به وجود آمده است.

هر دو آسیب‌پذیری توسط متخصصان تست نفوذ یک شرکت آلمانی با نام RedTeam کشف و گزارش شده است. در واقع این آسیب‌پذیری‌ها سبب دسترسی از راه دور مهاجمان به روتر می‌شوند که امکان دسترسی کامل به روتر را برای مهاجمان فراهم می‌آورد، جزئیات این آسیب‌پذیری‌ها به شرح ذیل می‌باشند:

- **شناسه CVE-2019-1652**: این نقص اجازه خواهد داد تا یک مهاجم احراز هویت نشده با دسترسی از راه دور بتواند با امتیاز مدیر به روتر آسیب‌پذیر دسترسی داشته باشد، و هر دستور مخرب و دلخواهی را بر روی آن اجرا نماید.
- **شناسه CVE-2019-1653**: این نقص نیز نیازی به احرازهویت برای دسترسی به پورتال مدیریت روتر، مبتنی بر وب ندارد. به طوری که مهاجمان را قادر به بازیابی اطلاعات محرمانه‌ای می‌کند که در نهایت، افشاء اطلاعات سیستم را درپی خواهد داشت.

مهاجمان با استفاده از این کد اثبات مفهومی روترهای RV320/RV325 سیسکو را هدف قرار دادند. اولین اکسپلویت با شناسه CVE-2019-1653، به منظور دریافت فایل پیکربندی روتر منتشر گردید. سپس آسیب‌پذیری دوم با شناسه CVE-2019-1652، موجب اجرای کدهای مخرب دلخواه شده و به دست آوردن دسترسی کامل به روتر آسیب‌پذیر را سبب می‌گردد. محققان شرکت Bad Packets اذعان داشتند که حداقل 9000 روتر RV320 و RV325 Dual Gigabit WAN VPN سیسکو در سرتاسر جهان مخصوصاً در ایالات متحده توسط این دو آسیب‌پذیری تهدید می‌شوند.

به گفته این شرکت، هکرها با سوءاستفاده از این آسیب‌پذیری‌ها تلاش می‌نمایند به روترها نفوذ کرده و مدیریت سیستم را به صورت کامل به دست بگیرند، و همچنین اطلاعات حیاتی را نیز به دست آورند.

راهکارهای امنیتی ارائه شده تا کنون

بهترین راه به منظور جلوگیری از خسارات جبران‌ناپذیر این آسیب‌پذیری‌ها، نصب سیستم‌عامل نسخه 1.4.2.20 در روترهای RV320 و RV325 می‌باشد. اکیداً توصیه می‌گردد افرادی که این نسخه از سیستم‌عامل را نصب ننموده‌اند هر چه سریع‌تر رمزعبور admin روتر و وای‌فای خود را تغییر دهند تا از نفوذ مهاجمان جلوگیری نمایند.

Scan Link

منبع خبر :

https://thehackernews.com/2019/01/hacking-cisco-routers.html

مقالات آموزشی

آموزش بازیابی رمز عبور در روترها

گردآورنده: سیده آرزو حسنی

Password Recovery (بازیابی و یا تغییر رمز عبور)

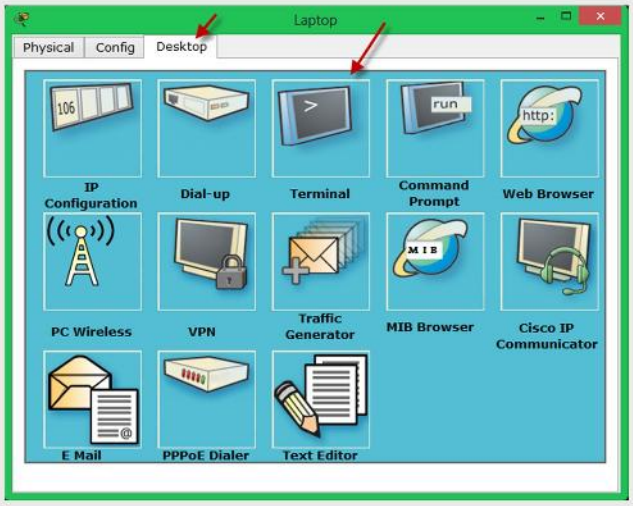
چنان چه مدیر یک شبکه هستید و روی روتر خود، رمز عبور قرار می‌دهید تا کسی بدون اجازه وارد روتر نشود، باید بدانید ممکن است زمانی شما این رمزعبور را فراموش کنید و آن زمان است که درگیر این رمز می‌شوید تا رمز موردنظر روتر را به یاد آورید. برای رفع این مشکل، باید تغییراتی را درون تنظیمات روتر انجام دهیم که بتوانیم رمز دیگری را جایگزین رمز قبلی کنیم.

وقتی روتر را روشن می‌کنیم به مرحله‌ی Post رفته و سخت‌افزارهای آن چک می‌شوند. در صورت سالم بودن آن‌ها به مرحله‌ی BootStarp رفته و محل ios را پیدا و اجرا می‌کند که این کار توسط مقادیر Register انجام می‌شود. اگر مقدار رجیستر برابر 0x2102 باشد، اطلاعات ذخیره شده روی Nvram را به Ram انتقال می‌دهد و وارد CLI می‌شود، یعنی وقتی شما رمز عبور برای روتر خود قرار می‌دهید، این اطلاعات بر روی nvram ذخیره می‌شود و در زمان اجرای مجدد روتر از nvram خوانده می‌شود، اما اگر مقدار رجیستر به 0x2142 تغییر کند، دیگر روتر به حافظه‌ی nvram توجه نمی‌کند و مستقیم وارد Setup Mode می‌شود، پس باید روشی را به کار ببریم تا روتر موقع اجرا شدن، شماره‌ی رجیستر 0x2142 را اجرا کند، یعنی باید روتر را گمراه کنیم.

با یک مثال این موضوع را تشریح می‌نماییم:

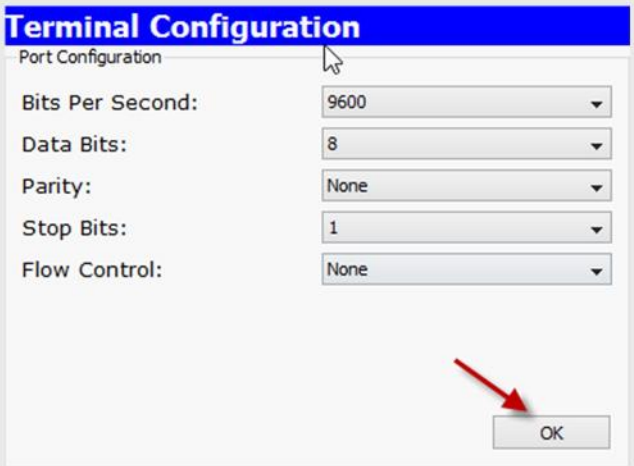
یک روتر 2811 به همراه یک لپ تاپ به صفحه اضافه کنید و از طریق کابلConsol ، این دو را به هم متصل کنید.

بعد از اتصال این دو به هم، وارد Laptop شده و از تب Desktop ، گزینه‌ی Terminal را انتخاب کنید.

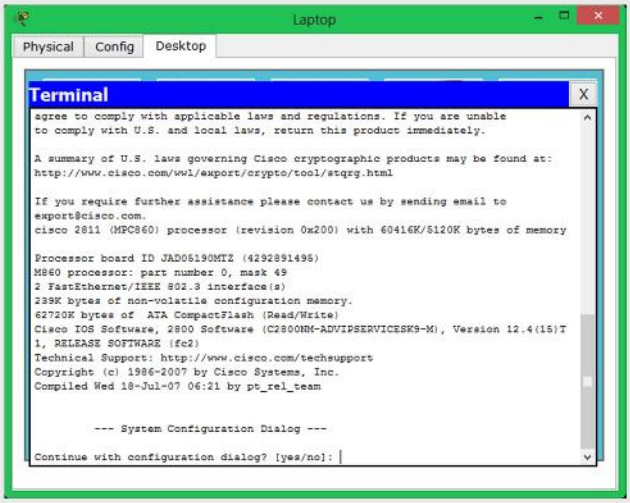


در این قسمت، باید سرعت انتقال اطلاعات که Bits per Second است را مشخص کنید. بدون تغییر تنظیمات پیش‌فرض، روی ok کلیک کنید.

علاوه بر مورد ذکر شده می‌توان از طریق نرم‌افزارهایی، مانند hyper Terminal و از طریق کابل console به روتر متصل شد.



همانطور که مشاهده می‌کنید، وارد مد CLI روتر شدیم.



برای انجام Password Recovery ، بر روی روتر یک رمز عبور قرار می‌دهیم و تنظیمات را ذخیره می‌کنیم، سپس آن را ریکاوری می‌کنیم:

Router(config-line)#**line console 0**

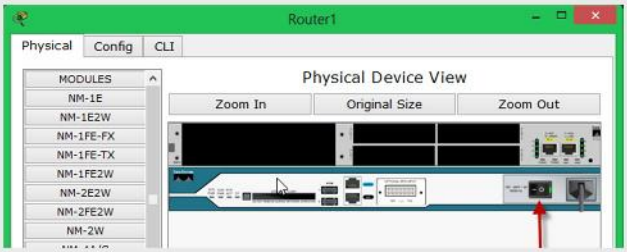
Router(config-line)#**password 123**

Router(config-line)#**login**

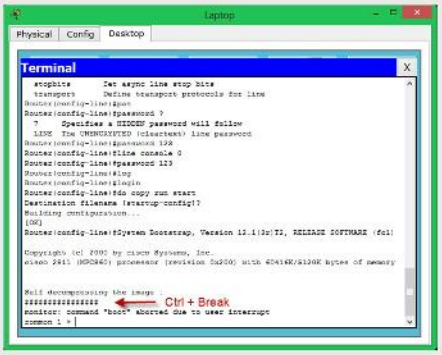
Router(config-line)#**do copy run start**

همانطور که مشاهده می‌کنید، رمز عبور 123 را تعریف و بعد از آن اطلاعات را از Ram به Nvram انتقال خواهیم داد.

در این لحظه باید روتر را خاموش و دوباره روشن کنید و در زمان بالا آمدن روتر باید درlaptop ، کلید ترکیبی Ctrl + Break را فشار دهید تا بتوانید وارد مد مانیتورینگ شوید.



در شکل بالا، کلید Power روتر 2811 را مشاهده می‌کنید که در واقعیت هم به همین صورت است. این کلید را بر روی off قرار دهید و دوباره روشن کنید. در زمان روشن شدن، وارد laptop شوید و کلید ترکیبی Ctrl+Break را فشار دهید، مانند شکل زیر:



با فشار دادن همزمان کلید ترکیبی Ctrl + Break ، وارد مد Rommon 1> خواهیم شد. سپس در این قسمت از دستورات زیر استفاده می‌کنیم:

rommon 1 > **confreg 0x2142**

rommon 3 > **reset**

در دستور اول، شماره‌ی رجیستر که 0x2102 می‌باشد را به شماره 0x2142 تغییر داده و پس از آن روتر را Reset کرده تا مجدد اجرا شود.

بعد از اینکه روتر راه‌اندازی شد وارد Setup mode می‌شود، و بایستی کارهای زیر را برای تغییر رمز انجام داد:

Router#copy startup-config running-config

Router#conf t

Router(config)#enable secret 1234

Router(config)#config-register 0x2102

Router(config)#exit

Router#copy run start

در مرحله‌ی اول با دستور **copy startup-config running-config** اطلاعات موجود را بر روی Nvram کپی می‌کنیم .پس از آن، وارد مد Global شده و رمز جدید را جایگزین رمز قبلی می‌کنیم. پس از آن، شماره‌ی رجیستری را که قبلاً تغییر داده بودیم با دستور **config-register 0x2102** به حالت اول برمی‌گردانیم و در نهایت اطلاعات را دوباره در Nvram کپی می‌کنیم. اکنون می توان با رمز جدید وارد روتر شد.

Scan Link

منبع خبر :

http://www.3isco.ir/

امنیت کاربر رایانه

محافظت از اطلاعات شخصی از مهم‌ترین مواردی هست که همیشه در دنیای فناوری مورد توجه کاربران بوده است. به همین منظور کاربران نیز همیشه در جستجوی بهترین نرم‌افزارها جهت حفاظت از سیستم خود هستند. بهترین دفاع در برابر تهدیدات اینترنتی یک آنتی‌ویروس خوب است. نرم‌افزار آنتی‌ویروس می‌تواند شما را از فایل‌های آلوده پیوست شده به ایمیل‌ها، وب‌سایت‌های ویروسی، کرم‌های اینترنتی، نرم‌افزارهای جاسوسی و غیره محافظت نماید.

در این شماره از بولتن خبری قصد داریم در فصل "حفاظت از سیستم‌ها با استفاده از آنتی‌ویروس"، مطالبی را در راستای شناسایی تهدیدات، و راهنمایی استفاده از آنتی‌ویروس‌های مناسب آموزش دهیم.

با ما همراه باشید...

خطرناک ترین ویروس های کامپیوتری

- در سال های اخیر کامپیوترهای زیادی توسط ویروس ها آلوده شده اند، و ویروس های کامپیوتری نیز بوده اند که به شدت بر روی رشد اقتصاد جهانی تأثیر گذاشته اند
- ده مورد از مخرب ترین ویروس های کامپیوتری در زیر آورده شده است:

- CIH (1998)
- Melissa (1999)
- ILOVEYOU (2000)
- Code Red (2001)
- SQL Slammer (2003)

- Blaster (2003)
- Sobig.F (2003)
- Bagle (2004)
- MyDoom (2004)
- Sasser (2004)

معرفی آنتی ویروس

- کامپیوتری که به اینترنت متصل است همیشه در معرض خطر قرار دارد، و بنابراین توصیه می گردد همیشه بر روی سیستم خود آنتی ویروس داشته باشید
- یک ویروس کامپیوتری می تواند سرعت عملکرد سیستم را کاهش داده و داده های ذخیره شده بر روی آن را حذف نماید
- آنتی ویروس، کامپیوتر را در مقابل ویروس ها، کرم ها، تروجان ها، جاسوس افزارها و غیره محافظت می نماید




لزوم وجود آنتی ویروس بر روی سیستم

در دنیای دیجیتال امروز، داده ها بر روی کامپیوتر ذخیره می گردند و حفاظت از این داده ها بسیار حائز اهمیت است

زمانی که یک کامپیوتر به اینترنت متصل است، باید با برنامه های مخرب مختلفی مانند ویروس ها، کرم ها، تروجان ها، جاسوس افزارها، ابزارهای تبلیغاتی مزاحم و غیره دست و پنجه نرم کند

مجرمان سایبری مانند مهاجمان و هکرها از برنامه های مخرب به عنوان ابزار استفاده نموده و اطلاعات مهمی مانند داده های شخصی ذخیره شده بر روی کامپیوتر افراد را سرقت می کنند

چنین برنامه هایی یک تهدید جدی برای کامپیوتر محسوب می شوند و ممکن است به شیوه های مختلف عملکرد سیستم را مختل نمایند

برنامه های مخرب از طرق مختلف، مانند پیوست های ایمیل، ایمیل اسپم، درایوهای USB و بازدید از وب سایت های جعلی و غیره به کامپیوتر راه می یابند

با توجه به هجوم برنامه های مخرب در فضای سایبری، وجود آنتی ویروس بر روی کامپیوترها ضروری است

اگر یک آنتی ویروس خوب بر روی کامپیوتر شما نصب شده باشد، از انواع برنامه های مخرب در امان خواهد ماند

آنتی ویروس چگونه کار می کند؟

اکثر آنتی ویروس های تجاری از دو تکنیک استفاده می کنند:

- استفاده از دیکشنری ویروس هنگام بررسی فایل ها، برای جستجوی ویروس های شناخته شده
- تشخیص رفتار مشکوک هر یک از برنامه ها

شیوه های دیگر برای تشخیص ویروس ها

- یکی دیگر از روش های تشخیص ویروس این است که آنتی ویروس قبل از اینکه کنترل را به برنامه قابل اجرا بدهد ابتدا رفتار آن را شبیه سازی کند تا متوجه شود برنامه چه کاری می خواهد انجام دهد
- اگر به نظر برسد برنامه یک ویروس است یا از کد Self-modifing استفاده میکند آنتی ویروس باید سریعاً قسمت ها ی دیگر برنامه بررسی کند

تکنیک رفتار مشکوک

- در این تکنیک، آنتی ویروس به جای جستجوی ویروس های شناخته شده، رفتار تک تک برنامه ها را تحت نظر می گیرد
- زمانی که برنامه ای با رفتار مشکوک یافت شود، به کاربر هشدار داده و از وی می پرسد چه کاری باید انجام دهد

تکنیک دیکشنری ویروس

- در این تکنیک، هنگام اسکن فایل ها آنتی ویروس به دیکشنری ویروس های شناخته شده، که توسط طراح آنتی ویروس مشخص شده اند مراجعه می کند
- اگر یک بیت از کد داخل فایل با یکی از ویروس های دیکشنری مطابقت داشته باشد، آنگاه آنتی ویروس می تواند فایل را حذف کند، با حذف ویروس فایل را ترمیم نماید و یا آن را قرنطینه کند

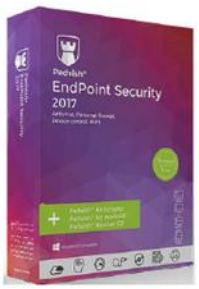
معرفی چند آنتی ویروس رایج

http://www.mcafee.com

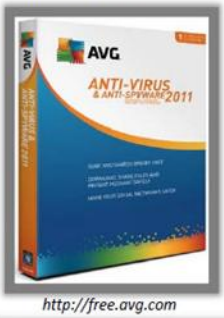
http://www.symantec.com

http://www.avast.com

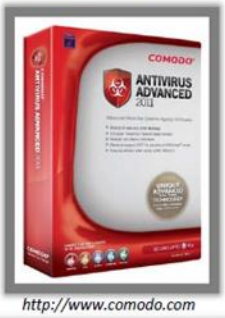
http://www.kaspersky.com



https://padvish.com/fa-ir/main

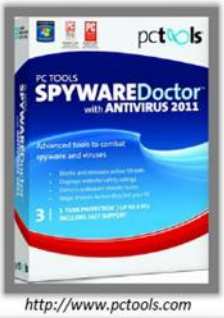


http://free.avg.com



http://www.comodo.com

http://www.bitdefender.com



http://www.pctools.com

http://www.eccouncil.org

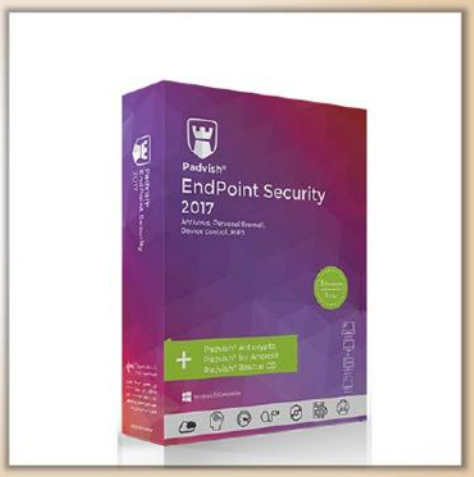
انتخاب بهترین آنتی ویروس

هنگام خرید آنتی ویروس به دنبال قابلیت های مختلف باشید ببینید آن ها چگونه می توانند به نحو احسن نیازهای شما را مرتفع نمایند

یکی از مهم ترین مواردی که باید مدنظر قرار دهید:

اسکن آنتی ویروس است

- **دقت تشخیص آنتی ویروس**
  بررسی نمایید که آنتی ویروس کار اسکن، و تشخیص ویروس ها را به دقت انجام داده و بتواند اکثر تهدیدات را شناسایی کند
- **سرعت اسکن**
  بررسی نمایید که آیا آنتی ویروس می تواند با سرعت و به صورت کارآمد کار اسکن را انجام دهد
- **بهره وری از منابع**
  اطمینان حاصل کنید که آنتی ویروس از حداقل منابع سیستم استفاده کند و هنگام انجام اسکن عملکرد سیستم را تحت تأثیر قرار ندهد



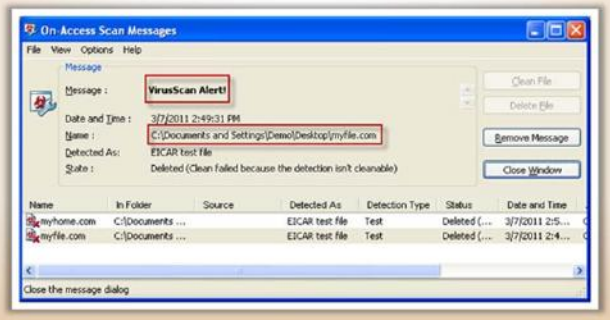

انتخاب بهترین آنتی ویروس
مسدود کردن هکر
این قابلیت از دسترسی غیرمجاز کاربران به سیستم، و سرقت داده های مهم توسط آن ها مانند پسوردها و سایر اطلاعات محرمانه جلوگیری می کند
فایروال دو طرفه
بررسی نمایید که آیا آنتی ویروس برای اسکن ترافیک های ورودی و خروجی به فایروال مجهز شده است یا خیر؟
پشتیبانی فنی
آنتی ویروس باید دارای پشتیبانی فنی خوب باشد تا در مواقع لزوم مشکلات به راحتی برطرف گردند
کنترل والدین
قابلیت کنترل والدین را در آنتی ویروس بررسی نمایید تا کودک شما بتواند با خیال آسوده از اینترنت استفاده نماید
نصب آسان و استفاده آسان
آنتی ویروس باید کاربرپسند بوده و استفاده از آن آسان باشد
اسکن مبتنی برتقاضا و زمانبندی شده
این گزینه امکان اسکن بر اساس زمانبندی مدنظر کاربر را فراهم می نماید. کاربر باید بتواند اسکن را به صورت روزانه، هفتگی و ماهیانه زمانبندی کند
آپدیت خودکار
این ویژگی کاربر را از تهدیدات آنلاین دور نگه می دارد، چرا که بدون نیاز به مراجعه ی کاربر به سایت عرضه کننده، آنتی ویروس وی همیشه آپدیت است
تشخیص جاسوس افزارها و جلوگیری از ورود آن ها
به منظور مقابله با جاسوس افزارها، آنتی ویروس را از لحاظ داشتن ضدجاسوس افزار بررسی نمایید
اسکن ایمیل
مکانیزم حفاظت از ایمیل می تواند پورت های POP و SMTP را بررسی نموده و اطمینان دهد که خطری کامپیوتر شما را تهدید نمی کند


مراحل نصب آنتی ویروس بر روی کامپیوتر
1
اکثر آنتی ویروس ها با استفاده از ویزارد نصب می شوند، و اجزای مورد نیاز به صورت پیش فرض بر روی سیستم نصب می گردد
2
آنتی ویروس را دانلود نموده و با دابل کلیک بر روی فایل نصبی آن، ویزارد را اجرا نمایید
3
در صفحه توافقنامه حقوقی، گزینه "I agree" را انتخاب نموده و برای ادامه بر روی Next کلیک نمایید
4
یک بار دیگر تنظیمات را مرور نموده و سپس بر روی Next کلیک نمایید تا نصب به اتمام برسد
5
پس از اتمام نصب، کامپیوتر خود را ریستارت نمایید

چگونه آنتی ویروس خود را تست کنیم؟

جهت تست کارکرد آنتی ویروس خود مراحل زیر را دنبال کنید:

1. **notepad** را باز نموده، کد زیر را در آن کپی نمایید و فایل را ذخیره کنید:
X5OIP%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
2. نام فایل را از **New Text Document.TXT** به **myfile.com** تغییر دهید
3. فایل **myfile.com** را با آنتی ویروس خود اسکن نمایید
4. اگر آنتی ویروس درست کار کند، باید یک پیغام هشدار تولید نموده و فایل را حذف نماید



توجه: اکثر آنتی ویروس ها در مرحله اول یک پیغام هشدار نمایش می دهند

ادامه مبحث " حفاظت از سیستم‌ها با استفاده از آنتی‌ویروس" را در شماره‌های بعدی ما دنبال کنید...

اخبار داخلی

برگزاری کارگاه آموزشی "امنیت فضای مجازی" در نمایشگاه دستاوردهای چهل ساله انقلاب اسلامی ایران

در تاریخ ۱۶ بهمن ۱۳۹۷، کارگاهی با موضوع "امنیت فضای مجازی" در محل دائمی نمایشگاه‌های بین‌المللی کرمانشاه توسط مرکز تخصصی آپا دانشگاه با همکاری اداره کل ارتباطات و فناوری اطلاعات استان، و به مناسبت چهلمین سالگرد پیروزی شکوهمند انقلاب اسلامی برگزار گردید.

در این کارگاه، پس از معرفی اجمالی مرکز آپا، ابتدا لزوم امنیت در فضای مجازی تشریح شده و سپس به بررسی چالش‌های موجود در این فضا پرداخته شد.

در ادامه، راه‌های مقابله با چالش‌ها و تهدیدات موجود، معرفی شده و توصیه‌های امنیتی لازم بیان گردید.

سرفصل‌های مطرح شده در این کارگاه آموزشی به شرح ذیل می‌باشند:

- لزوم امنیت در فضای مجازی
- تهدیدات فضای مجازی
  - آشنایی با حملات فیشیگ و راه‌های مقابله با آن
  - انواع روش‌های فیشینگ
  - آشنایی با مهندسی اجتماعی
- توصیه‌های امنیتی

شـــهروندان مراقب ســـایت جعلـــی با موضوع ثبت‌نـــــام یارانه‌ها باشند!

رییـــس پلیس فتا خوزســـتان گفـــت: در چند روز اخیـــر کلاهبرداران ســـایبری باز هـــم با سوءاســـتفاده از موضـــوع یارانه‌هـــا اقدام به ســـاخت ســـایت جعلـــی بـــا نـــام www.yaranehe.com کـــرده و بـــا عنوان ثبت‌نـــام یارانـــه و اعتـــراض به قطـــع یارانه، اطلاعات حساب بانکی افراد را به سرقت می‌برند.

ســـرهنگ شـــاهین حسنوند رییس پلیس فتـــا خوزستان در گفت و گـــو با خبرنـــگار پایـــگاه اطلاع‌رســـانی پلیس فتـــا اظهار داشـــت: کلاهبرداران در ابتدا ســـایتی مشابه ســـایت اصلی طراحی کـــرده و در مرحله بعد با تبلیغـــات فراوان در شـــبکه‌های اجتماعی و یا با ارســـال پیام‌هایـــی به تلفن همراه شـــهروندان مبنـــی بر قطع یارانـــه، به آنها هشـــدار می‌دهند کـــه جهت جلوگیـــری از قطع دائم و اتصـــال مجـــدد یارانه، بـــه آدرس ســـایت مذکور مراجعـــه کنند. شـــهروندان نیز پس از مراجعه به ســـایت نامبرده، اطلاعات حســـاب بانکی خـــود را وارد کـــرده که در پـــی آن، اطلاعات آنها به دســـت کلاهبرداران می‌رسد.

این مقام انتظامی افزود: شـــهروندان هیچ‌گاه به تبلیغات در شـــبکه‌های اجتماعـــی و یا پیامک‌هـــای ناشـــناس مبنی بر ثبت‌نـــام یارانه، ســـهام عدالت و ســـبد حمایتی کالا توجه نکرده و اطلاعـــات و اخبار مورد نیـــاز خود را فقط از منابع معتبر کســـب کننـــد، همچنین بـــا توجه بـــه جعلی بـــودن این ســـایت، در صورتی کـــه به صفحه مراجعـــه و اطلاعـــات کارت بانکـــی خـــود را وارد کرده‌انـــد، هر چه سریعتر نسبت به تغییر رمز دوم خود اقدام کنند.

سرهنگ حســـنوند بیان کرد: متأســـفانه برخی شـــهروندان در هنگام ثبت‌نـــام به آدرس ســـایت دقت کافـــی نمی‌کنند و با جســـتجو در اینترنت و یـــا رفتن به لینک‌هایـــی که در ســـایت‌های مختلف ارائه شـــده در دام کلاهبرداران ســـایبری می‌افتند که پیامـــد این بی‌دقتی منجر به سرقت اطلاعات بانکی آنها می‌شود.

وی افزود: بـــرای ثبت‌نام فقط ســـایتwww.yaraneh10.ir از طرف مراجع رســـمی کشـــور اعلام شـــده و لازم اســـت در هنگام ثبت‌نام، آدرس ســـایت را به دقت بررســـی کرده و سپس اطلاعـــات خود را وارد کنند.

رییـــس پلیس فتا خوزســـتان در پایان گفت: بـــرای دریافت اطلاعات، هشـــدارها و توصیه‌هـــای پلیس فتـــا هموطنان عزیـــز می‌توانند به ســـایت پلیـــس فتـــا بـــه آدرس www.cyberpolice.ir مراجعه کـــرده و در صورت مشـــاهده موارد مشـــکوک نیز گـــزارش خود را در بخش ثبت گزارش مردمی به ما اطلاع دهند.

منبع خبر : پایگاه اطلاع‌رسانی پلیس فتا

دومین دوره مسابقات

فتح پرچم

غرب کشور

دانشگاه رازی کرمانشاه

2nd Razi University CTF Contest

کارگاه‌های آموزشی : ۲ تا ۵ اردیبهشت ماه ۱۳۹۸

مسابقه فتح پرچم : ۱۱ و ۱۲ اردیبهشت ماه ۱۳۹۸

اختتامیه و اعلام نتایج : ۱۳ اردیبهشت ماه ۱۳۹۸

شروع ثبت نام رایگان از ۱ اسفند ماه ۱۳۹۷ در:

ctf.razi.ac.ir

مکان برگزاری: دانشگاه رازی، دانشکده برق و کامپیوتر

سرفصل های اصلی مسابقه

Web Security Network Security Reverse Engineering

Cryptography Digital Forensics Industrial Electronic Systems Security

۰۸۳-۳۴۲۷۳۳۹۰ cert.razi.ac.ir @raziCTF2

جهت **کسب اطلاعات بیشتر** به **وب سایت** ما مراجعه نمایید

مرکز تخصصی آپا دانشگاه رازی