بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره نهم اسفند ماه ۱۳۹۷

سیستم های مدیریت محتوا در معرض حمله هکرها!

در این شماره می‌خوانید :

فهرست

مرکز تخصصی آپا دانشگاه رازی

پیشرو در ارائه خدمات امنیت فناوری و اطلاعات

صاحب امتیاز :
مرکز تخصصی آپا دانشگاه رازی

سردبیر :
سهیلا مرادی

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

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

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

۰۸۳۳۴۲۷۳۳۹۰

cert.razi.ac.ir

apa@razi.ac.ir

اخبار امنیتی

سرقت ۶ ترابایت اطلاعات حساس، از کمپانی معروف Citrix، توسط هکرهای ایرانی!

گردآورنده: سهیلا مرادی

طبق اخبار منتشر شده، هفته گذشته اطلاعات گسترده‌ای از شبکه داخلی شرکت نرم‌افزاری معروف Citrix، که به سازمان‌های حساسی مانند ارتش ایالات متحده آمریکا، FBI و بسیاری از شرکت‌ها و سازمان‌های دولتی ایالات متحده خدمات ارائه می‌نماید توسط مجرمان سایبری بین‌المللی افشاء شده است.

شرکت Citrix اظهار داشت که: "روز چهارشنبه،FBI در رابطه با تسخیر سیستم‌های IT توسط هکرهای خارجی و ربوده شدن اسناد شرکتی و تجاری هشدار داد، و افزود که این شرکت دقیقاً نمی‌داند که چه مدارکی از شرکت توسط هکرها سرقت شده و آن‌ها چگونه به این اطلاعات دست یافته‌اند!"

FBI معتقد است که احتمالاً مهاجمان از حمله "password spraying" استفاده کرده‌اند، در این حمله مهاجمان توانسته‌اند پسوردهای ضعیف را حدس بزنند و از این طریق در شبکه مستقر شوند، سپس حملات گسترده‌تری را پیاده نمایند.

همانطور که در این پست وبلاگ آمده است، به گفته شرکت Citrix : "با اینکه این احتمال هنوز قطعی نشده، اما FBI از اینکه احتمالاً هکرها از تاکتیک شناخته شده‌ی password spraying استفاده کرده‌اند خبر داده است. این تاکتیک شیوه‌ای است که پسوردهای ضعیف را اکسپلویت می‌نماید، زمانی که راه نفوذی با سطح دسترسی محدود یافت شد، تلاش می‌کند تا سایر لایه‌های امنیتی را از بین ببرد."

اگرچه Citrix اطلاعات زیادی در رابطه با این افشای اطلاعات منتشر ننموده است، اما محققان شرکت infosec firm Resecurity این رویداد را به روشنی به تصویر کشیده و ادعا نموده‌اند که قبلاً به Citrix در رابطه با این حمله _targeted attack and data breach_ هشدار داده شده است!

Resecurity اعلام نمود که یک گروه هکر ایرانی با نام IRIDIUM، در دسامبر سال گذشته و مجدداً در روز دوشنبه، 4 مارس سال جاری، شرکت Citrix را در معرض حمله قرار داده و حداقل 6 ترابایت از اطلاعات حساس آن شامل ایمیل‌ها، طرح‌ها و سایر اسناد را به سرقت برده است.

IRIDIUM، یک گروه هکر ایرانی است که در حملات سایبری اخیر، بیش از 200 سازمان دولتی، مانند شرکت‌های نفت و گاز، شرکت‌های فناوری و سایر سازمان‌ها را در سراسر جهان مورد حمله قرار داده است.

گروه IRIDIUM از تکنیک‌های انحصاری مانند دور زدن احراز هویت چند عامله برای سرویس‌ها و برنامه‌های کاربردی حساس به منظور دسترسی غیرمجاز به کانال‌های VPN و SSO (Single Sign-On) استفاده می‌کند.

محققان شرکت Resecurity در یک پست وبلاگ نوشتند: "این افشای گسترده اطلاعات در Citrix به عنوان بخشی از یک حرکت جاسوسی سایبری پیشرفته به منظور هدف قرار دادن دولت، صنایع نظامی و صنعتی، سازمان‌های انرژی، مؤسسات مالی و شرکت‌های بزرگ شناخته شده است."

رئیس تیم امنیتیResecurity ، چارلز یوو، به خبرگزاری NBC اعلام داشت که این تیم هکر (IRIDIUM) حدود ده سال پیش به شبکه داخلی Citrix راه پیدا کرده و تا به امروز هم از سیستم‌های این شرکت خارج نشده است.

شرکت مستقر در فلوریدا خاطرنشان کرد که نشانه‌ای از به خطر افتادن سرویس‌ها یا محصولات Citrix توسط هکرها وجود ندارد، و گویا

شـــرکت Citrix یک تحقیقات جرم‌شناســـی را آغاز نموده اســـت و در این راســـتا از یک شـــرکت برتـــر در زمینه امنیت ســـایبری به منظور انجـــام اقدامات لازم جهت ایمن‌ســـازی شـــبکه داخلـــی خود کمک گرفته است.

Scan Link

منبع خبر :

https://thehackernews.com/2019/03/citrix-data-breach.html

امکان اجرای حمله DoS در ویندوز ســـرورهای دارای وب‌سرور IIS، از طریق درخواست‌های مخرب HTTP/2

گردآورنده: سهیلا مرادی

مشـــاور امنیتی مایکروسافت نقص امنیتی جدیدی را در سرور IIS منتشر نموده اســـت، که به موجـــب آن زمانی که درخواســـت‌های HTTP/2 مخرب به ویندوز ســـرور ارسال می‌شـــوند، میزان اســـتفاده از CPU بـــه 100% افزایـــش می‌یابـــد. این فرآینـــد مخرب، تـــا زمانی که توسط سرور IIS خاتمه داده نشـــود، به طور مستمر CPU را درگیر نموده و به طور موقت میزان استفاده از آن را به 100% می‌رساند.

مهاجمان می‌توانند با ارســـال درخواست‌های HTTP/2 ساختگی موجب حمله DoS شده و میزان استفاده از CPU را تا 100% افزایش دهند که در این شرایط IIS به اجبار اتصالات مخرب را قطع می‌کند.

IIS یک وب‌ســـرور تولید شـــده توســـط مایکروسافت است کـــه پروتکل‌های SMTP، FTPS، FTP، HTTPS، HTTP/2، HTTP، و NNTP را پشتیبانی می‌کند.

این آسیب‌پذیـــری بالقوه، نسخه‌های نرم‌افزاری IIS را در ویندوز 10، ویندوز سرور و ویندوز سرور 2016 تحت تأثیر قرار می‌دهد.

HTTP/2 یک نســـخه اصلاح شده از پروتکل شـــبکه HTTP است که توســـط شـــبکه جهانی وب مـــورد اســـتفاده قـــرار می‌گیـــرد، و HTTP/2 اولین نسخه جدید پس از HTTP1.1 می‌باشد.

مایکروســـافت در تشـــریح نقص یاد شـــده، اذعان داشـــت: "قابلیت‌های HTTP/2 به کلاینت‌ها اجـــازه می‌دهد که هر تعداد فریم SETTINGS را با هر تعداد دلخواه پارامتر SETTINGS تنظیم نمایند. در برخی از مـــوارد، ایـــن تنظیمات می‌توانـــد موجب ناپایـــداری ســـرویس‌ها شـــده و میـــزان اســـتفاده از CPU را تـــا زمـــان قطع ارتباط افزایش دهد."

مایکروســـافت بـــرای رفع باگ مورد نظـــر، یک به‌روزرســـانی امنیتی تحت عنوان "Defense in Depth" منتشر نموده است.

مایکروســـافت برای نقص مذکور هیچ اطلاعات فنی منتشـــر ننموده، اما یک مقدار آســـتانه برای تعداد SETTINGSهای HTTP/2 موجود در یک درخواســـت مشـــخص نموده اســـت که می‌توانـــد در کاهش میزان خطر کمک‌کننده باشد.

پس از اعمال به‌روزرســـانی، مدیران IIS قـــادر خواهند بود که تنظیمات HTTP/2 را بـــه منظور جلوگیری از درخواســـت‌های مخرب، و افزایش میزان استفاده از CPU تغییر دهند.

*لـــذا توصیـــه می‌گـــردد، مدیـــران هر چه ســـریعتر نســـبت به بروزرسانی و اعمال وصله مورد نظر اقدام نمایند.

Scan Link

منبع خبر :

https://gbhackers.com/malicious-http-2-requests-on-iis-server-cause-the-system-cpu-usage-to-spike-to-100/

حمله Skimming علیه دستگاه‌های خودپرداز

سرقت رمز کارت کاربران از طریق دوربین‌های کار گذاشته شده در دستگاه‌های خودپرداز

گردآورنده: سهیلا مرادی

اخیراً یک حمله اسکیمینگ جدید علیه دستگاه‌های ATM پیاده‌سازی شده است که از دوربین امنیتی درون‌ساخت دستگاه برای سرقت رمز کارت کاربران استفاده می‌کند.

نحوه عملکرد این حمله بدین صورت است که یک اسکیمر شامل دوربین (علاوه بر دوربین امنیتی خود دستگاه)، داخل دستگاه خودپرداز قرار داده می‌شود و زاویه آن به شکلی تنظیم می‌گردد که به سمت پنل اعداد دستگاه باشد و بتواند از طریق آن رمز کارت کاربران را ضبط نماید.

بر اساس گزارش امنیتی Kerbs، دوربین به کار برده شده برای ثبت رمز کارت کاربران، یک دوربین بسیار باریک است که با باطری کار می‌کند و در دهانه محل دریافت کارت قرار داده می‌شود، به گونه‌ای که اسکیمرِ کارت خارج از دستگاه خودپرداز قابل مشاهده نباشد.

اسکیمرهایی که در این‌گونه حملات مورد استفاده قرار می‌گیرند بسیار ظریف بوده و برای قرار گرفتن در قسمت بالایی محل دریافت کارت طراحی شده‌اند.

اسکیمرها در واقع کارت‌خوان‌های مخربی هستند که اطلاعات نوار مغناطیسی کارت را به پایانه‌های پرداخت متصل می‌کنند.

یافتن اسکیمر وصل شده به دستگاه خودپرداز کار دشواری است، محققان دانشگاه فلوریدا یک Skim Reaper را توسعه داده‌اند که مشخصات فیزیکی را برای طیف وسیعی از اسکیمرها که اطلاعات کارت را سرقت می‌نمایند مشخص می‌کند.

دولت ایالات متحده در رابطه با این شیوه جدید حمله علیه دستگاه‌های خودپرداز تحت عنوان " Wiretapping"، که مؤسسات مالی را هدف قرار می‌دهند، هشدار داد.

مجرمان، این حمله را با ایجاد یک سوراخ کوچک در دستگاه ATM و سرقت اطلاعات مشتری به صورت مستقیم از خواننده کارت داخل دستگاه انجام می‌دهند.

و در نهایت، ساده‌ترین راه برای مقابله با این‌گونه حملات پوشاندن پنل دستگاه خودپرداز با کیف پول یا دست است که در صورت قرار گرفتن دوربین‌های اسکیمر در دستگاه خودپرداز، اجازه نمی‌دهد هنگام وارد نمودن رمز عبور، رمز کاربر ثبت گردد.

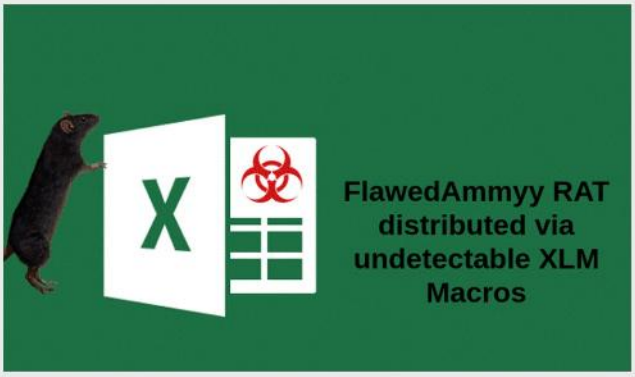
Scan Link

منبع خبر :

https://gbhackers.com/atm-skimming-attack-scammers-hijack/

انتشار بدافزار FlawedAmmyy از طریق MS Excel Macros

گردآورنده: سیده مرضیه حسینی



گروه TA505، اخیراً در حال انتشار بدافزار قدرتمند FlawedAmmyy RAT از طریق اسناد MS Excel با استفاده از Excel 4.0 macro مخرب هستند که توسط کنترل‌های امنیتی استاندارد، به سختی

قابل شناسایی است.

نمونه FlawedAmmyy RAT دیده شده بسیار پیچیده است و می‌تواند قربانیان آلوده شده را از راه دور کنترل نموده و نرم‌افزار امنیتی را دور بزند.

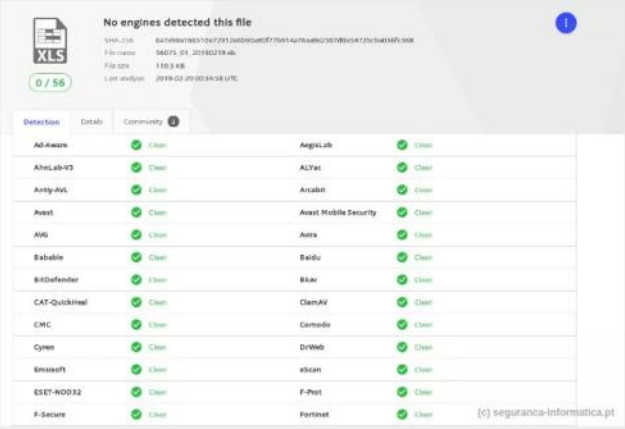
TA505 یک گروه شناخته شده در جرایم سایبری است که تاکنون میلیون‌ها قربانی را با بدافزارهای خطرناکی همچون Locky، Dridex و GlobeImposter آلوده نموده است.

این بدافزار دارای قابلیت‌هایی است که موجب می‌گردد تنها زمانی که برای اولین بار توسط فایل MSI (نصب کننده ویندوز) اجرا گردد، شناسایی شود.

محققان با بررسی دقیق منبع افشا شده، گزارش داده‌اند که FlawedAmmyy RAT می‌تواند عملیات مختلفی از جمله کنترل از راه دور دسکتاپ، مدیریت سیستم‌فایل، پشتیبانی پراکسی و چت صوتی را انجام دهد.

علاوه بر عملیات مخرب ذکر شده، این بدافزار همچنین می‌تواند دسترسی کامل به دستگاه قربانی را نیز برای مهاجمان فراهم نموده و سرقت فایل‌ها، اعتبارنامه‌ها، جمع‌آوری کردن عکس‌ها و دسترسی به دوربین و میکروفن را امکان‌پذیر نماید.

به گفته‌ی یک محقق امنیتی به نام Pedro Tavares از seguranca-informatica، در تحقیقات صورت گرفته، اخیراً موج جدیدی از انتشار بدافزار FlawedAmmyy RAT از طریق ماکروهای XML شناسایی شده است که به سختی توسط ابزارهای امنیتی مانند آنتی‌ویروس‌ها تشخیص داده می‌شود. این محقق به منظور بررسی دقیق‌تر موضوع نمونه‌ای از این بدافزار را در سایت VirusTotal ارسال نموده و همانطور که در تصویر زیر مشاهده می‌شود هیچ فعالیت مشکوکی شناسایی نشده است.

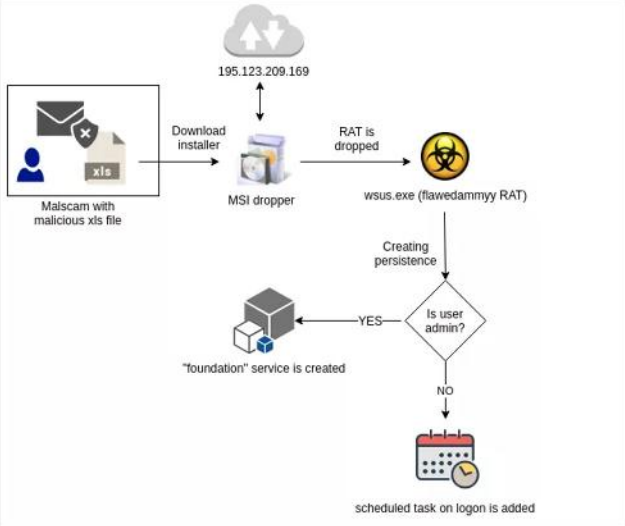


فرایند انتشار FlawedAmmyy

گروه TA505، در ابتدا از ایمیل‌های malspam و تاکتیک‌های قدیمی برای گسترش FlawedAmmyy RAT، به منظور هدف قرار دادن قربانیان استفاده می‌نمود.

این ایمیل حاوی اسناد اکسل و محتویاتی برای فریب کاربران جهت باز کردن فایل‌هایی است که کد مخرب Excel 4.0 macro را حمل و اجرا می‌کنند.

کد مخرب XLM macro در یک فرم مخفی قرار می‌گیرد تا از دید قربانیان دور بماند. نام مخفی این بدافزار در زبان روسی به صورت "Макрос1" و در زبان انگلیسی "Macro 1" می‌باشد.



پس از اجـــرای موفقیت آمیز ماکـــرو، MSI dropper آماده مرحله اول فراینـــد msiexec.exe بدافـــزار آماده خواهد بود، کـــه یکی دیگر از دریافت‌کننده‌هـای اصلـــی FlawedAmmyy RAT (wsus.exe) می‌باشد.

ســـپس ارتباط با ســـرور C2 برقرار می‌شـــود که در آنجا دستورات از مهاجم دریافـــت می‌گردد. بر اســـاس اظهارات محققان، ســـرور C2 استفاده شده توسط مهاجم در حال حاضر آفلاین می‌باشد.

محققان توصیـــه می‌کننـــد: " کاربرانی که ایمیل‌هایـــی با فایل‌های پیوست xls دریافت می‌کنند، باید آگاه باشند که این فایل‌هـــا می‌توانند حامـــل فایلی جهت انتشـــار هـــر نوع نرم‌افـــزار مخرب ناشـــناخته باشـــند. کاربـــران بایـــد اطمینـــان حاصـــل کننـــد که macrosهای برنامه‌های Microsoft Office آنها غیرفعال شده باشد."

Scan Link

منبع خبر :

https://gbhackers.com/flawedammyy-malware-via-excel

انتشار به‌روزرسانـــــی امنیتی سیسکو و رفـــع 35 آسیب‌پذیری در محصولات این شرکت

گردآورنده: آتوسا خدامرادی

شـــرکت سیســـکو به منظـــور حفاظت از مشـــتریان خـــود در برابر هکرهای مخـــرب، به‌روزرســـانی امنیتی جدیدی را منتشـــر نموده که در آن 35 آســـیب‌پذیری کـــه محصـــولات مختلـــف این شـــرکت را تحت تأثیر قرار می‌دهد وصله نموده است.

در میـــان این 35 آسیب‌پذیری، سیسکـــو یکی را به عنـــوان آســـیب‌پذیری حیاتی یا Critical، 27آســـیب‌پذیری را بـــا درجه اهمیت High ، 6آسیب‌پذیری را با درجه اهمیـــت Medium و یـــک آسیب‌پذیری را با درجه اهمیت Informational مشخص نموده است.

آسیـــب‌پـذیـــری Critical آن Remote Command Execution Vulnerability CVE-2019-1663 می‌باشد که روترهای RV110W، RV130W و RV215W و نیـــز Wireless-N VPN و رابـــط مدیریت Firewall را تحت تـــأثیر قـــرار می‌دهد و اجـــازه می‌دهد که یـــک هکـــر از راه دور کد دلخواه خود را در دستگاه آسیب‌پذیر اجرا نماید.

آســـیب‌پذیری Critical، تمام نســـخه‌های قبل از موارد ذکر شـــده در زیر را تحت تأثیر قرار داده می‌دهد:

- RV110W Wireless-N VPN Firewall
- RV130W Wireless-N Multifunction VPN Router
- RV215W Wireless-N VPN Router

هکرها از راه دور با ارسال درخواســـت HTTP مخرب به دستگاه هدف، این آســـیب‌پذیری را اکســـپلویت نموده و با ســـطح دسترســـی بالا کنترل کامل دستگاه تحت تأثیر را به دست می‌گیرند.

در این به‌روزرســـانی امنیتی، 27 آســـیب‌پذیری با درجه اهمیـــت High وجـــود دارد که باعث برخـــی حملات خطرنـــاک مانند اجرای کد دلخواه، ارتقاء ســـطح دسترســـی، دسترســـی غیرمجاز به سیستم فایـــل، حمـــلات منـــع ســـرویس بـــه LAN و وب ســـرویس، تزریق دستور و غیره می‌شود.

آســـیب‌پذیری‌های Medium، برخی از محصولات تجاری سیسکو مانند Cisco Nexus 5600و ســـوییچ‌هـــای ســـری 6000، Cisco Enterprise Chat and Email و Cisco Nexus 9000 Series Fabric Switches را تحت تأثیر قرار می‌دهند.

نرم‌افـــزار Cisco NX-OS تحت تأثیر چندین آســـیب‌پذیری قرار دارد و بعضی از این آســـیب‌پذیری‌ها بـــه هکر احراز هویت شـــده (هکر داخلی) اجازه می‌دهد که به دسترســـی بالا در دســـتگاه آســـیب‌پذیر دست یابد.

جزئیـــات این به‌روزرســـانی در لینک خبر و ســـایت سیســـکو موجود می‌باشد:

Scan Link

منبع خبر :

https://gbhackers.com/cisco-security-updates/

آسیب پذیری

کشف آسیب‌پذیری حیاتی از نوع RCE در سامانه مدیریت محتوای دروپال!

گردآورنده: پویان مسعودی نیا

توسعه‌دهندگان سیستم مدیریت محتوای دروپال _یک سیستم مدیریت محتوای محبوب متن‌باز که میلیون‌ها وب سایت از آن استفاده می‌کنند_ آخرین نسخه نرم‌افزار خود را به منظور وصله نمودن یک آسیب‌پذیری حیاتی منتشر نمودند. این آسیب‌پذیری امکان هک از راه دور سایت را برای مهاجمان فراهم می‌نماید.

این به‌روزرسانی دو روز پس از هشدار تیم امنیتی دروپال به مدیران سایت‌های دروپالی، مبنی بر اعمال وصله‌ها و به‌روزرسانی نرم‌افزار، به منظور جلوگیری از سوءاستفاده هکرها از حفره‌های امنیتی منتشر گردید.

با توجه به اظهارات تیم امنیتی دروپال، آسیب‌پذیری مورد نظر یک نقص مهم در هسته دروپال است که اجرای کد از راه‌دور (RCE) را موجب شده و در برخی موارد می‌تواند منجر به اجرای کد دلخواه PHP شود.

با اینکه که تیم امنیتی دروپال هیچ جزئیات فنی از این آسیب‌پذیری (باشناسه CVE-2019-6340) منتشر ننموده است، اما لازم به ذکر است که این نقص در واقع به دلیل عملکرد نامناسب داده برای نوع داده‌ی فیلدها از منابع غیررسمی می‌باشد، که هسته‌های دروپال 7 و 8 را تحت تأثیر قرار داده است.

البته لازم به ذکر است که سایت دروپالی شما تنها در صورتی در معرض خطر این آسیب‌پذیری قرار می‌گیرد که ماژول RESTful Web Services فعال باشد، و اجازه درخواست POST یا PATCH را داشته باشد، و یا اینکه ماژول وب‌سرویس دیگری بر روی آن فعال شده باشد.

اگر شما در حال حاضر قادر به نصب آخرین به‌روزرسانی نیستید، می‌توانید موقتاً اثرات این آسیب‌پذیری را به‌راحتی با غیرفعال کردن تمام ماژول‌های سرویس‌های وب، و یا پیکربندی وب سرور خود به منظور عدم پذیرش درخواست‌های PUT / PATCH / POST به منابع سرویس‌های وب، کاهش دهید.

دروپال در گزارش امنیتی خود که روز چهارشنبه منتشر شد، هشدار داد که "باید توجه داشته باشید که منابع سرویس‌های وب، بسته به پیکربندی سرور شما ممکن است در مسیرهای مختلف در دسترس باشند، حتماً زمان انجام اقدامات امنیتی جهت مصون ماندن از خطرات آسیب‌پذیری مذکور، این نکته را مد نظر داشته باشید."

به عنوان مثال، برای دروپال 7 معمولاً منابع از طریق مسیرهای "clean URLs" و از طریق آرگومان پرس و جوی "q" در دسترس هستند، و برای دروپال 8، ممکن است مسیرها هنوز با index.php کار کنند.

با این حال، با توجه به محبوبیت دروپال در میان هکرها و علاقه به سوءاستفاده از آسیب‌پذیری‌های آن، اکیداً توصیه می‌گردد که آخرین نسخه به‌روزرسانی را نصب نمایید:

- اگر از نسخه 8.6.x دروپال استفاده می‌کنید، وب‌سایت خود را به دروپال نسخه 8.6.10 ارتقاء دهید.
- اگر از نسخه 8.5.x دروپال یا نسخه‌های قبل از آن استفاده می‌کنید، وب‌سایت خود را به دروپال نسخه 8.5.11 ارتقاء دهید.

دروپال همچنین اذعان داشته که ماژول سرویس‌های دروپال نسخه 7 به خودیِ خود در این لحظه نیاز به به‌روزرسانی ندارند، اما کاربران باید در نظر داشته باشند که در صورت استفاده ازسرویس‌ها باید به‌روزرسانی‌های مربوطه را اعمال نمایند.

منبع خبر :

https://thehackernews.com/2019/02/hacking-drupal-vulnerability.html

وصله آسیب‌پذیری روز صفرم در مرورگر محبوب Google Chrome

گردآورنده: آتوسا خدامرادی

هر چه سریعتر Google Chrome خود را به روز نمایید...

یک محقق امنیتی به نام Clement Lecigne از Threat Analysis Group (گروه تحلیل تهدید)، ماه گذشته یک آسیب‌پذیری با درجه اهمیت High در مرورگر محبوب Chrome کشف نموده و گزارش کرده است که این آسیب‌پذیری می‌تواند به هکر راه دور اجازه دهد که کد دلخواه خود را در کامپیوترهای هدف اجرا نموده و کنترل کامل آن‌ها را به دست گیرد.

این آسیب‌پذیری که با شناسه CVE-2019-5786 شناخته می‌شود، برنامه مرورگر وب را در تمامی سیستم‌عامل‌ها، شامل مایکروسافت ویندوز، Apple macOS و لینوکس تحت تأثیر قرار می‌دهد.

تیم امنیتی Chrome، بدون انتشار جزئیات این آسیب‌پذیری، عنوان نمود که مشکل در واقع یک آسیب‌پذیری در مؤلفه FileReader مربوط به مرورگر Chrome است که موجب حمله اجرای کد از راه دور (RCE) خواهد شد.

گوگل هشدار داده است که این آسیب‌پذیری RCE به صورت فعالانه‌ای توسط هکرها مورد استفاده قرار می‌گیرد.

تیم امنیتی گوگل اشاره کرد که: "دسترسی به جزئیات این حفره امنیتی و پیوندهای آن تا زمانی‌که اکثریت کاربران به‌روزرسانی را انجام نداده باشند، محدود خواهد بود. هم‌چنین اگر آسیب‌پذیری در کتابخانه ثالثی که پروژه‌های دیگر به آن وابسته‌اند و هنوز مشکل آن رفع نشده است وجود داشته باشد، ما محدودیت‌ها را حفظ خواهیم کرد."

FileReader یک API استاندارد بوده، و هدف از طراحی آن فراهم نمودن امکان خواندن ناهمگام محتوای فایل‌ها یا بافرهای داده‌های خام ذخیره شده در سیستم کاربر، برای برنامه‌های تحت وب می‌باشد، این کار با استفاده از اشیاء File یا Blob جهت مشخص نمودن فایل یا خواندن داده استفاده می‌شود.

آسیب‌پذیری use-after-free یکی از حفره‌های امنیتی حافظه می‌باشد که اجازه تخریب یا تغییر داده‌ها در حافظه را می‌دهد و کاربر غیر مجاز قادر خواهد بود سطح دسترسی خود را در سیستم یا نرم‌افزار آلوده ارتقاء دهد.

آسیب‌پذیری use-after-free در مؤلفه FileReader می‌تواند هکرها را قادر سازد که به مرورگر وب دسترسی پیدا نموده، و بتوانند محیط محافظت شده sandbox را دور زده و کد دلخواه خود را در سیستم هدف اجرا نمایند.

به نظر می‌رسد برای اکسپلویت این آسیب‌پذیری، تمام کاری که یک هکر باید انجام دهد این است که قربانیان خود را تا باز کردن صفحه وب دلخواه خود دنبال و هدایت نماید، بدون این‌که به تعامل بیشتری نیاز داشته باشد.

وصله این آسیب‌پذیری امنیتی در قالب به‌روزرسانی مرورگر chrome به نسخه 72.0.3626.121 برای سیستم‌عامل‌های ویندوز، Mac و لینوکس ارائه شده است.

در نهایت مطمئن شوید که آخرین نسخه مرورگر chrome روی سیستم شما در حال اجرا است.

منبع خبر :

https://thehackernews.com/2019/03/update-google-chrome-hack.html?m=1

امکان هک سایت‌های وردپرسی توسط آسیب‌پذیری CSRF در وردپرس

گردآورنده: سهیلا مرادی

اگر سایت وردپرسی شما به هر دلیلی هنوز به آخرین نسخه ارتقاء داده نشده است، اکیداً توصیه می‌گردد پیش از آنکه هکرها بتوانند از آسیب‌پذیری جدید کشف شده در این سیستم استفاده کرده و سایت شما را هک نمایند، هرچه سریعتر آن را به روزرسانی نمایید!

سیمون اسکنل، محقق شرکت RIPS Technologies GmbH، که قبلاً هم چندین آسیب‌پذیری را در وردپرس گزارش نموده بود، بار دیگر آسیب‌پذیری جدیدی را در این سیستم مدیریت محتوای محبوب کشف نمود که می‌تواند منجر به حملات اجرای کد از راه دور گردد.

این آسیب‌پذیری ناشی از یک باگ CSRF در بخش نظرات (بخش دیدگاه کاربران) وردپرس است. این قسمت یکی از اجزای اصلی وردپرس است که به صورت پیش‌فرض فعال شده و تمامی نسخه‌های قبل از 5.1.1 را تحت تأثیر قرار می‌دهد.

برخلاف حملات قبلی ثبت شده علیه وردپرس، آسیب‌پذیری جدید حتی به یک مهاجم احراز هویت نشده از راه دور اجازه می‌دهد که سایت وردپرسی را تسخیر نموده و بتواند کد دلخواه خود را در سایت آسیب‌پذیر اجرا نماید.

آسیب‌پذیری منتشر شده توسط اسکنل شامل موارد زیر است:

- زمانی که یک کاربر نظر جدیدی را ارسال می‌کند، وردپرس از اعتبارسنجی CSRF استفاده نمی‌کند و این امر اجازه می‌دهد مهاجم نظرات خود را از طرف مدیر ارسال نماید.
- نظرات ارسال شده توسط حساب کاربری ادمین sanitize نمی‌شود و می‌تواند حاوی تگ‌های HTML و حتی تگ‌های SCRIPT باشد.
- frontend وردپرس توسط هدر X-Frame-Options محافظت نشده، و به مهاجمان اجازه می‌دهد سایت وردپرسی مورد هدف را در یک iFrame مخفی از یک وب‌سایت تحت کنترل مهاجم باز کنند.

با در نظرگرفتن مسائل مطرح شده‌ی فوق، مهاجم می‌تواند به صورت مخفیانه یک پی‌لود XSS ذخیره شده را تنها با فریب مدیر لاگین شده برای بازدید از یک وب‌سایت مخرب که حاوی کد اکسپلویت است، در سایت وردپرسی مورد هدف تزریق نماید.

به گفته این محقق، مهاجم حتی می‌تواند با تزریق یک پی‌لود XSS که با گنجاندن یک PHP backdoor مخرب می‌تواند مستقیماً قالب وردپرسی را تغییر دهد، بدون اینکه مدیر سایت متوجه شود، کنترل کامل سایت وردپرسی را از راه دور به دست گیرد.

پس ازآنکه اسکنل این آسیب‌پذیری را در اکتبر سال گذشته گزارش نمود، تیم وردپرس عوض فعال نمودن امکان محافظتCSRF، با در نظر گرفتن یک nonce اضافی برای مدیران در فرم نظرات کاربران سعی نمود خطرات ناشی از این باگ را کاهش دهد.

با وجود انجام این اقدام ازسوی تیم وردپرس،

اسکنل توانست این شیوه را دور بزند، و پس از این جریان بالاخره تیم وردپرس نسخه 5.1.1 را با یک وصله پایدار در روز چهارشنبه منتشر نمود.

از آنجا که وردپرس به صورت خودکار وصله‌های امنیتی را نصب می‌کند، تنها کاری که مدیران وب‌سایت‌های وردپرسی باید انجام دهند این است که سایت خود را به آخرین نسخه ارتقاء دهند.

اگر قابلیت آپدیت خودکار برای سایت وردپرسی شما غیرفعال شده است، توصیه می‌گردد تا زمان نصب وصله امنیتی، به طور موقت بخش نظرات کاربران را در سایت خود غیرفعال نموده و از حساب کاربری خود (حساب کاربری ادمین) log out نمایید.

Scan Link

منبع خبر :

https://thehackernews.com/2019/03/hack-wordpress-websites.html

بهره‌برداری از نقص نرم‌افزار WinRAR برای هک کامپیوترهای ویندوزی!

گردآورنده: سیده مرضیه حسینی

محققان اخیراً آسیب‌پذیری حیاتی جدیدی در نرم‌افزار محبوب WinRAR کشف نموده‌اند که در دیگری را برای هک کامپیوترها به روی مهاجمان گشوده است.

سایت The Hacker News چند روز پیش در مورد یک آسیب‌پذیری اجرای کد از راه دور 19 ساله که توسط Check Point در کتابخانه UNACEV2.dll از WinRAR کشف شده بود را گزارش نمود. این آسیب‌پذیری می‌تواند یک فایل آرشیو ACE مخرب را برای اجرای کد دلخواه در سیستم هدف بارگزاری نماید.

WinRAR نرم‌افزار محبوب فشرده‌سازی فایل در ویندوز، با 500 میلیون کاربر در سراسر جهان است، اما یک آسیب‌پذیری بحرانی به نام "Absolute Path Traversal" با شناسه (CVE-2018-20250) در کتابخانه UNACEV2.DLL آن وجود دارد که مهاجمان را قادر به استخراج یک فایل اجرایی فشرده از آرشیو ACE به یکی از فولدرهای Startup ویندوز می‌سازد.

جهت اکسپلویت موفقیت‌آمیز این آسیب‌پذیری و در دست گرفتن کنترل کامل کامپیوتر مورد هدف، مهاجم تنها باید کاربران را متقاعد نماید که یک فایل آرشیو فشرده شده مخرب را با نرم‌افزار WinRAR باز نمایند.

محققان امنیتی اخیراً با بررسی 360 مرکز اطلاعات جاسوسی (360TIC) دریافتند که یک گروه ایمیل malspam، از آخرین آسیب‌پذیری WinRAR برای نصب بدافزار در کامپیوترهایی که نسخه آسیب‌پذیر WinRAR بر روی آنها نصب شده است، برای گسترش یک فایل آرشیو RAR مخرب استفاده کرده‌اند.

هنگام اجرای نرم‌افزار WinRAR به عنوان administrator، و یا بر روی یک سیستم هدف با UAC (User Account Control) غیرفعال، این بدافزار برای آلوده کردن کامپیوتر هدف با یک درب پشتی، یک فایل exe مخرب (CMSTray.exe) را در پوشه Startup ویندوز قرار می‌دهد.

از آنجا کـــه UAC محدودیت‌هایی را بـــر روی مجوزها اعمال می‌کند، تلاش برای اســـتخراج فایل آرشـــیو بوسیله UAC فعال شده، جهت قرار دادن فایل exe مخرب در پوشه C:\ProgramData با شکست مواجه می‌شود.

بهترین راه پیشـــگیری از حملـــه این بدافزار، بروزرســـانی و نصب آخرین نســـخه نرم‌افزار WinRAR بر روی سیســـتم در اســـرع وقـــت، و همچنین اجتنـــاب از باز کـــردن فایل‌های دریافت شده از منابع ناشناس می‌باشد.

تیم توسعه WinRAR در ســـال 2005 به جای حل این مسئله، دسترسی به کد منبع کتابخانه آســـیب‌پذیر UNACEV2.DLL را حـــذف نمود، و در حال حاضر نســـخه 5.70 beta 1 نرم‌افزار WINRar را منتشر نموده اســـت که از فرمت‌های DLL و ACE پشـــتیبانی نمی‌کند. با توجه بـــه رفع این حفـــره امنیتی، در عین حـــال تمـــام پشـــتیبانی‌های ACE از WinRAR حذف شده است.

Scan Link

منبع خبر :

https://thehackernews.com/2019/02/winrar-hacking-exploit.html?m=1

محصولات سیســـکو، تحـــت تأثیرآســـیب‌پذیری ارتقاء سطح دسترسی در Container

گردآورنده: آتوسا خدامرادی

شدت آسیب‌پذیری

با توجـــه به گزارشات منتشر شده، شدت ایـــن آسیـــب‌پذیری **High** می‌باشد.

خلاصه آسیب‌پذیری

این آسیب‌پـــذیری با شناسه CVE-2019-5736، در واقـــع یـــک آســـیب‌پذیری درOpen Container Initiative، مربوط به ابزار مبتنی بر خط فرمان runc می‌باشد که توسط محصولات مختلفی مورد استفاده قـــرار می‌گیـــرد، و می‌تواند به هکر احـــراز هویت نشـــده اجازه دهد که از راه دور، سطح دسترسی را در سیستم هدف ارتقاء دهد.

این آسیب‌پذیـــری ناشی از [1] file descriptors نامناســـب در مسیر /proc/self/exe می‌باشـــد. هکـــر می‌تواند این آســـیب‌پذیری را به دو صـــورت اکســـپلویت نماید: هـــم می‌تواند با ترغیـــب کاربر یک container[2] جدیـــد را توســـط تصویـــر تحت کنتـــرل هکر ایجاد نماید، و هم از دستور docker exec برای دسترسی به container موجودی کـــه هکر از قبل به آن دسترســـی داشـــته اســـت، اســـتفاده نماید. اکســـپلویت موفق این آســـیب‌پذیری بـــه هکر اجـــازه می‌دهد که فایـــل باینـــری ابـــزار runc میزبـــان را توســـط یـــک فایـــل مخـــرب بازنویســـی نمایـــد، ســـپس از container خارج شـــده و دســـتورات دلخواه خود را با امتیاز کاربر root در سیســـتم میزبان اجرا می‌کند.

راهکارهای امنیتی ارائه شده تا کنون

هرگونه راه‌حلی برای محصولات یا سرویس‌های اختصاصی Cisco در بخش Vulnerable Products سیسکو مستند می‌شود.

Scan Link

منبع خبر :

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190215-runc

[1] file descriptors (FD) یـــا توصیفگـــر فایـــل در یونیکس و سیســـتم‌عامل‌های مربوطه، یک شـــاخص انتزاعی می‌باشـــد که به منظور دسترســـی بـــه یک فایل یا دیگر منابع ورودی/خروجی مانند pipe یا سوکت شبکه، مورد استفاده قرار می‌گیرد.

[2] زیرســـاختی اســـت که توســـعه دهندگان یا اســـتفاده از آن، ســـاده‌تر از ماشـــین مجازی می‌توانند نرم‌افزارهای خود را روی پلتفرم‌های مختلف دیپلـــوی نمایند. در واقـــع Container اطمینـــان می‌دهـــد کـــه نرم‌افزار فـــارغ از این‌کـــه روی چه پلتفرمی قـــرار دارد، به درســـتی اجـــرا گردد و روی همـــه آن‌ها عملکرد یکســـانی داشته باشد.

مقالات آموزشی

قابلیت‌های امنیتی IIS

بخش اول: Dynamic IP Restriction

مقدمه

ماژول Dynamic IP Restrictions (DIPR) در IIS 7.0 و بالاتر امکان محافظت در برابر حملات انکار سرویس (DDoS) و brute force بر روی وب سرورها و وب سایت‌ها را فراهم می‌آورد. به منظور ایجاد این حفاظت، ماژول نامبرده موقتاً آدرس‌های IP از کلاینت‌های HTTP را که منجر به ایجاد تعداد بسیار زیادی درخواستِ همزمان می‌گردند یا که تعداد زیادی درخواست را در مدت زمان کوتاهی ایجاد می‌کنند مسدود (block) می‌نماید.

ویژگی‌ها

• مسدود نمودن آدرس‌های IP بر اساس تعداد درخواست‌های همزمان_ اگر تعداد درخواست‌های همزمان یک کلاینتِ HTTP از حد مجاز بیشتر شود، آدرس IP آن کلاینت به طور موقت مسدود می‌گردد.

• مسدود نمودن آدرس‌های IP بر اساس تعداد درخواست‌ها در طول یک دوره‌ی زمانی_ اگر تعداد درخواست‌های یک کلاینتِ HTTP در یک بازه‌ی زمانیِ مشخص بیش از حد مجاز باشد، آدرس IP آن کلاینت به طور موقت مسدود می‌گردد.

• امکان لیست نمودن آدرس‌های IP که نمی‌خواهید مسدود شوند_ شما می‌توانید لیستی از آدرسIP کلاینت‌هایی که می‌خواهید از قاعده‌ی مسدود شدن توسط ماژول نامبرده (صرف‌نظر از پیکربندی‌های دیگر) مستثنی باشند ایجاد نمایید.

• اقدامات رد درخواست مختلف_ شما می‌توانید مشخص کنید که برای یک کلاینت HTTP که آدرس IPآن مسدود شده است چه پاسخی بازگردانده شود. ماژول می‌تواند کد وضعیت 403، 404 یا فقط خاتمه‌ی اتصال HTTP را بازگرداند یا اینکه هیچ پاسخی بازنگرداند.

• امکان پشتیبانی برای وب‌سرورها از پشت پراکسی_ اگر وب سرور شما پشت یک پراکسی باشد، شما می‌توانید ماژول را جهت استفاده از آدرس IP کلاینت از یک هدر X-Forwarded-For پیکربندی نمایید.

• _ این ماژول به طور کامل آدرس‌های IPV6 را پشتیبانی می‌کند.

نصب ماژول Dynamic IP Restrictions (DIPR)

شما می‌توانید این ماژول را از لینک زیر دانلود نمایید:

https://www.iis.net/downloads/microsoft/dynamic-ip-restrictions

پیش‌نیازها:

شما باید یکی از سیستم‌عامل های زیر را داشته باشید:

- Windows Server 2008
- Windows Vista SP1
- Windows Server 2008 R2
- Windows 7

نسخه‌ی Betaی ماژول DIPR را حذف نمایید

اگر شما از نسخه‌ی first Beta ماژول DIPR استفاده می‌کنید باید قبل از نصب نسخه‌ی جدید آن را حذف نمایید، در غیر این‌صورت نصب با خطا مواجه خواهد شد.

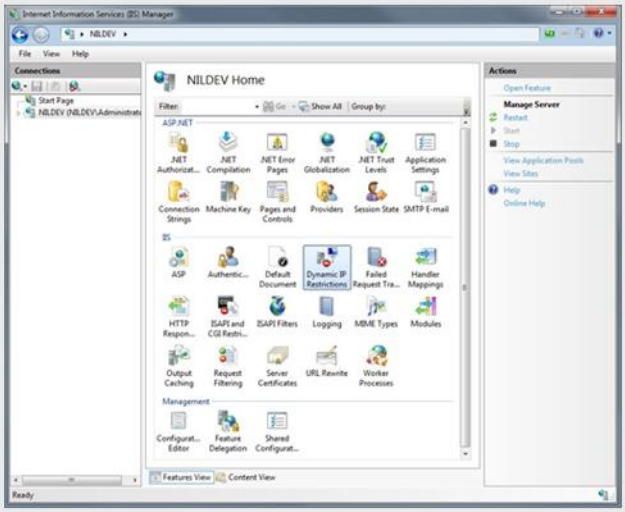
توجه: قبل از حذف نسخه‌ی Beta حتما از تنظیمات خود بک آپ تهیه نمایید.

در صورت استفاده از نسخه ی Beta2 ماژول DIPR، شما می‌توانید مستقیماً آن را به نسخه‌ی نهایی ارتقاء دهید. با این کار تنظیمات شما حفظ خواهد شد.

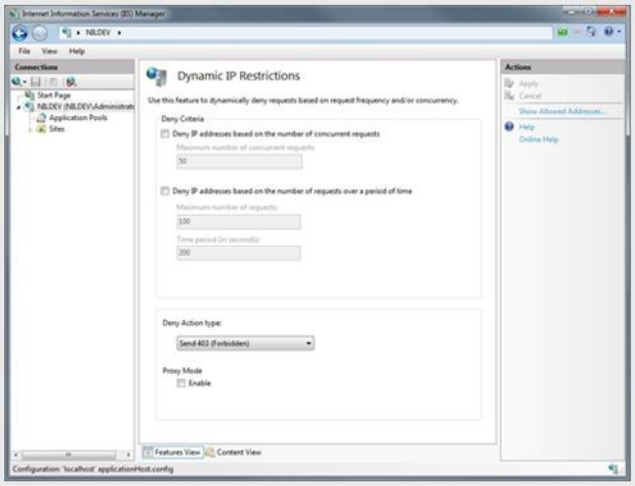
قابلیت Dynamic IP Restrictions را می‌توان با استفاده از **configuration API IIS ، Manager IIS** یا از طریق ابزار خط فرمان **appcmd** پیکربندی نمود.

جهت دسترسی به تنظیمات *Dynamic IP Restrictions* در *IIS Manager* به صورت زیر عمل نمایید:

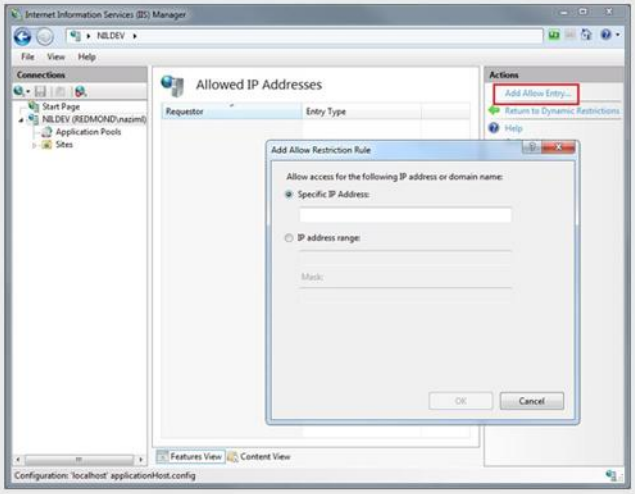
1. IIS Manager را باز کنید.
2. در نمای درختی سمت چپ:
   - اگر می‌خواهید تنظیمات سمت سرور را پیکربندی کنید قسمت Server را انتخاب نمایید.
   - اگر می‌خواهید تنظیمات سایت خاصی را پیکربندی کنید قسمت Site را انتخاب نمایید.
3. در پنجره‌ی باز شده پنجره‌ی(Features view) بر روی"Dynamic IP Restrictions" کلیک کنید.



4. در صفحه ی اصلیِ "Dynamic IP Restrictions" شما می‌توانید هر ویژگی دلخواه را فعال یا پیکربندی نمایید. جهت افزودن یک آدرس IP به لیست مجاز (Allow) می‌توانید بر روی لینک "Show Allowed Addresses" در سمت راست کلیک نمایید:



5. پس از انتخاب "Show Allowed Addresses" پنجره‌ای به شکل زیر نشان داده می‌شود که شما می‌توانید در آن لیست تمام آدرس‌های IPای که می‌توانند صحت اعتبار Dynamic IP Restriction را دور بزنند ببینید. شما می‌توانید با انتخاب "..Add Allow Entry" در قسمت بالای سمت راست آدرس‌های IP بیشتری به لیست اضافه نمایید.



مسدود کردن آدرس‌های IP بر اساس تعداد درخواست‌های همزمان

هنگام استفاده از این گزینه، سرور به هر آدرس IP کلاینت اجازه خواهد داد که تنها تعداد قابل تنظیمی درخواستِ همزمان ارسال نماید. هرگونه درخواستی که از این حد تعیین شده تجاوز نماید رد خواهد شد.

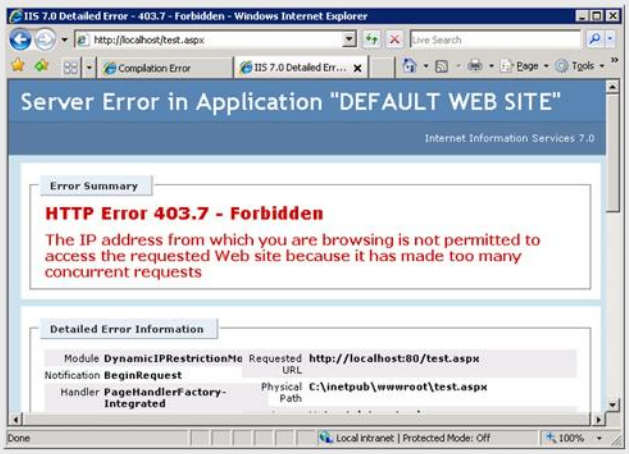
یک راه ساده جهت آزمودن این ویژگی این است که حداکثر تعداد درخواست‌های همزمان را مقدار2 تنظیم نمایید، این کار را می‌توانید با استفاده از UI یا اجرای خط فرمان appcmd انجام دهید.

```
%WINDIR%\system32\inetsrv\appcmd.exe set config -setion:system.web-
Server/security/dynamicIpSecurity

/denyByConcurrentRequests.enabled:"True"

/denyByConcurrentRequests.maxConcurrentRequests:"2"

/commit:apphost
```

در پوشه‌ی ریشه (Root) وب‌سایت یک فایل test.aspx ایجاد کنید و محتوای زیر را در آن کپی نمایید.

```
aspx
<%@ Page Language="C#" %>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org
<script runat="server">
protected void Page_Load(object sender, EventArgs e)
{
 System.Threading.Thread.Sleep(3000);
}
</script>
<html xmlns="http://www.w3.org/1999/xhtml">
 <head runat="server">
 <title>Dynamic IP Restrictions Test</title>
 </head>
 <body>
 <form id="form1" runat="server">
 <div>
 <h1>Hello World!</h1>
 </div>
 </form>
 </body>
</html>
```

این صفحه‌ی ASP.NET قبل از بازگرداندن هر گونه پاسخی به مدت 3 ثانیه نشان داده خواهد شد. این فایل را ذخیره نموده و سپس مرورگر خود را باز کنید، آدرس http://localhost/test.aspx را در آن وارد نمایید، در ادامه کلید F5 را جهت رفرش نمودن صفحه بفشارید. این در مرورگر منجر به ایجاد بیش از 2 درخواست همزمان خواهد شد و همان‌طور که می‌بینید خطای 403 مشاهده می‌شود_ خطای Forbidden از جانب سرور:



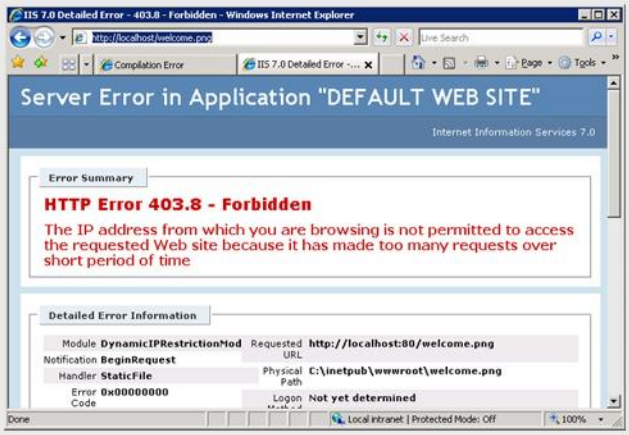
مسدود کردن آدرس‌های IP بر اساس تعداد درخواست‌ها در طول زمان

هنگام استفاده از این گزینه، سرور، درخواستِ هر آدرس IP کلاینتِ HTTP را که تعداد درخواست آن بیش از تعداد تنظیم شده در طول یک دوره‌ی زمانی باشد رد خواهد نمود. این آدرس IP در حالت مسدود باقی خواهد ماند تا زمانی که تعداد درخواست‌های آن در یک دوره ی زمانی کمتر از مقدار تنظیم شده باشد.

برای تست این ویژگی، با استفاده از IIS Manager و یا با اجرای خط فرمان appcmd، مقدار "Maximumnumber of requests" را 5 و "Time period" را 5000 تنظیم نمایید.

```
%WINDIR%\system32\inetsrv\appcmd.exe set config -section:system.web-
Server/security/dynamicIpSecurity

/denyByRequestRate.enabled:"True" /denyByRequestRate.maxRequests:"5"

/denyByRequestRate.requestIntervalInMilliseconds:"5000" /commit:apphost
```

مرورگر را باز کرده و آدرس http://localhost/welcome.png را وارد نمایید، سپس کلید F5 را به طور مداوم جهت رفرش نمودن صفحه بفشارید. این در واقع بیش از 5 بار درخواست در طول 5 ثانیه است و همان‌طور که در تصویر زیر می‌بینید سرور کد خطای 403 را بازمی‌گرداند_ کد وضعیتِ Forbidden



اگـــر شـــما 5 ثانیـــه دیگر صبـــر کنید که تمـــام درخواســـت‌های قبلی اجرا شـــــوند و سپـــــس درخواست ارسال نمایید، درخواست موفقیت‌آمیز خواهد بود.

اقدامات رد درخواست

این ماژول می‌تواند جهـــــــت انجام اقدامـــــــات زیر هنـــگام رد درخواستِ آدرس‌های IP پیکربندی گردد:

- ارسال پاسخ 403 برای کلاینت (Forbidden)
- ارسال پاسخ 404 برای کلاینت (File not found)
- نادیده گرفتن درخواست با قطع کردن اتصال HTTP، بدون ارسال هیچ گونه پاسخی برای کلاینت

Scan Link

منبع خبر :

https://docs.microsoft.com/en-us/iis/manage/configuring-security/using-dynamic-ip-restrictions

اخبار کوتاه

مایکروسافت از افزایـــش 250 درصدی فیشینـــــگ و کاهـش 34 درصدی حملات بدافزار در جهان خبر می‌دهد

طبـــق گزارش‌های رســـیده حملات فیشـــینگ در ماه‌هـــای ژانویه و دسامبر در ســـراسر جهان رشد بسیـــار بـــالا و چشمگیر 250 درصدی داشته است. در بســـیاری از این حملات از قبیل ارســـال ایمیل حاوی فایل‌های فشـــرده فیشـــینگ و باج‌افزار، تغییر آدرس‌هـــا ودامنه‌های نزدیـــک بـــه دامنه‌هـــای اصلـــی و ... مهاجمان طی یـــک حمله، همزمان اطلاعات چندین قربانی را در اختیار می‌گیرند.

سرویس جدید فایرفاکس، ارسال امن و سریع فایل

فایرفاکس ســـرویس جدیدی برای ارســـال امن فایل‌هـــا راه‌اندازی نموده اســـت. فایل‌ها به صـــورت end-to-end رمزگذاری شـــده و به شـــما این اطمینـــان را می‌دهد که فایـــل ارســـالی از امنیت بالایی برخوردار است.

فایل‌های تـــا 1 گیگابایت بدون نیاز به ثبت‌نام ارســـال می‌شـــوند و بیشـــترین حجمـــی که بـــا ثبت‌نـــام قابل ارســـال اســـت تا 2.5 گیگابایت می‌باشد.

ایـــن امـــکان نیز فراهم شـــده اســـت تـــا فایل‌ها در یـــک زمان مشخص و یا بعد از یک تعداد دانلود مشخص از بین بروند.

لینک این سرویس:

https://send.firefox.com

تا اطلاع ثانـــوی ، از بازکردن فایل‌هـــای PDF درون مرورگر کروم خودداری کنید!

به دلیل وجود آسیب‌پذیری zero-day، هکرها قادرند مستندات PDF آلوده را از طریـــق گـــوگل کروم به کاربـــران انتقـــال داده و اطلاعاتی از آنها جمع‌آوری نمایند.

* برای دیدن فایل های PDF از کروم استفاده نشود.

امنیت کاربر رایانه

حتی اگر شما کاربری حرفه‌ای باشید، باز هم نیاز به استفاده از یک برنامه آنتی ویروس دارید. علاوه بر ویروس‌های متداولی که به نیت‌های مختلف ساخته می‌شوند و روزانه با فلش‌ها و ایمیل‌ها جابه‌جا می‌شوند، بسیاری از اوقات شما در معرض آسیب‌پذیری‌های نرم‌افزاری نیز هستید. مثلاً آسیب‌پذیری‌هایی که هر از گاهی در افزونه فلش و یا مرورگرها کشف می‌شوند. حتی اگر شما به موقع نسبت به نصب جدیدترین نسخه برنامه مربوطه اقدام کنید، باز هم این احتمال وجود دارد که بوسیله یک آسیب‌پذیری جدید و یا کشف نشده و تنها با بازدید ازیک صفحه وب، آلوده شوید. هر چند شاید این‌گونه آلوده شدن خیلی هم متداول نباشد، ولی به هر حال وجود دارد. یک آنتی‌ویروس قدرتمند، لایه محافظتی مهمی است که حتی از آلوده شدن رایانه شما با چنین آسیب‌پذیری‌هایی جلوگیری می‌کند.

در این شماره از بولتن خبری قصد داریم در فصل "حفاظت از سیستم‌ها با استفاده از آنتی‌ویروس" ، نحوه پیکربندی و استفاده از آنتی‌ویروس معروف کسپرسکی را که در بسیاری از سازمان‌ها و ارگان‌های دولتی و نیز بر روی کامپیوترهای شخصی مورد استفاده قرار می‌گیرد معرفی نماییم.

با ما همراه باشید...

پیکربندی آنتی ویروس Kaspersky PURE

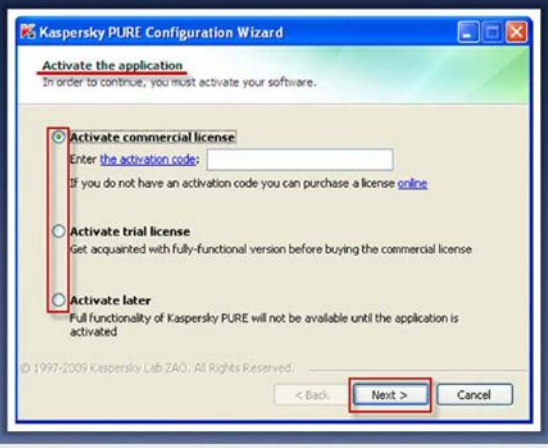
پس از نصب موفقیت آمیز Kaspersky PURE، مراحل زیر را برای پیکربندی آن دنبال کنید :

مرحله اول: برنامه را فعال کنید

- برای اینکه بتوانید از تمام قابلیت های برنامه استفاده کنید باید آن را فعال نمایید

شما می توانید یکی از گزینه های زیر را انتخاب کنید:

- فعالسازی لایسنس تجاری با خرید کد فعالسازی
- فعالسازی نسخه آزمایشی سی روزه و آشنایی با امکانات برنامه
- به تعویق انداختن فعالسازی، با انتخاب این گزینه مرحله فعالسازی Kaspersky PURE رد شده و برنامه بر روی سیستم شما نصب می گردد اما شما زمانی می توانید برنامه را آپدیت کنید که برنامه را فعال کرده باشید
- برای ادامه روند فعالسازی بر روی Next کلیک نمایید
- پس از فعالسازی لایسنس، برای بقیه تنظیمات بر روی Next کلیک کنید

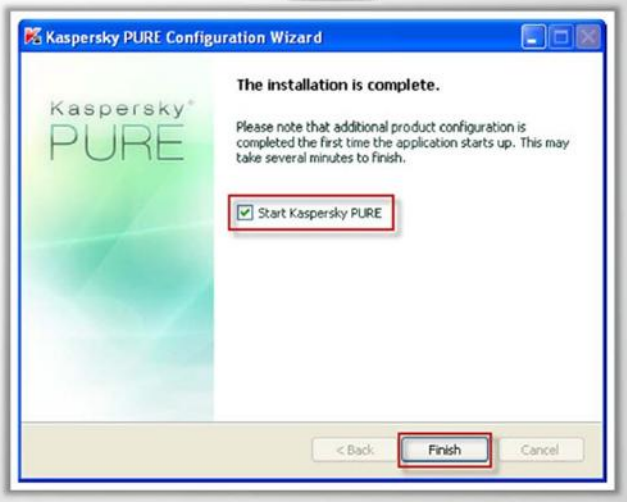


پیکربندی آنتی ویروس Kaspersky PURE

مرحله دوم: تجزیه و تحلیل سیستم

ویزارد نصب، اطلاعات سیستم را تجزیه و تحلیل نموده و قوانینی را برای برنامه های مورد اعتمادی که در سیستم عامل ویندوز موجود هستند ایجاد می کند، صبر کنید تا روند کامل شود

پیکربندی آنتی ویروس Kaspersky PURE



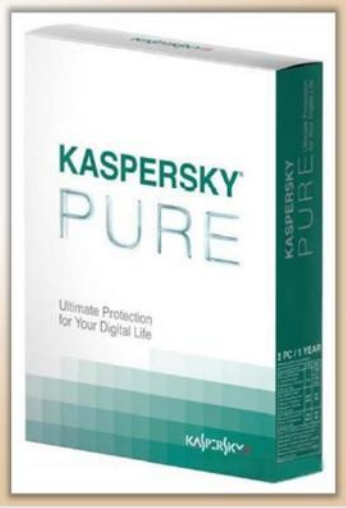
مرحله سوم: تکمیل فرآیند نصب

پس از اتمام فرآیند نصب، ویزارد پیکربندی Kaspersky PURE با پیغامی مشابه آنچه در تصویر آمده است (The installation is compelete) کاربر را از کامل شدن فرآیند نصب مطلع خواهد نمود

- اگر می خواهید برنامه بلافاصله پس ازبسته شدن ویزارد پیکربندی اجرا شود، از تیک دار بودن گزینه Start Kaspersky PURE اطمینان حاصل کنید
- اگر می خواهید برنامه بعداً اجرا شود تیک گزینه Start Kaspersky PURE را بردارید
- برای بسته شدن ویزارد پیکربندی بر روی دکمه Finish کلیک نمایید

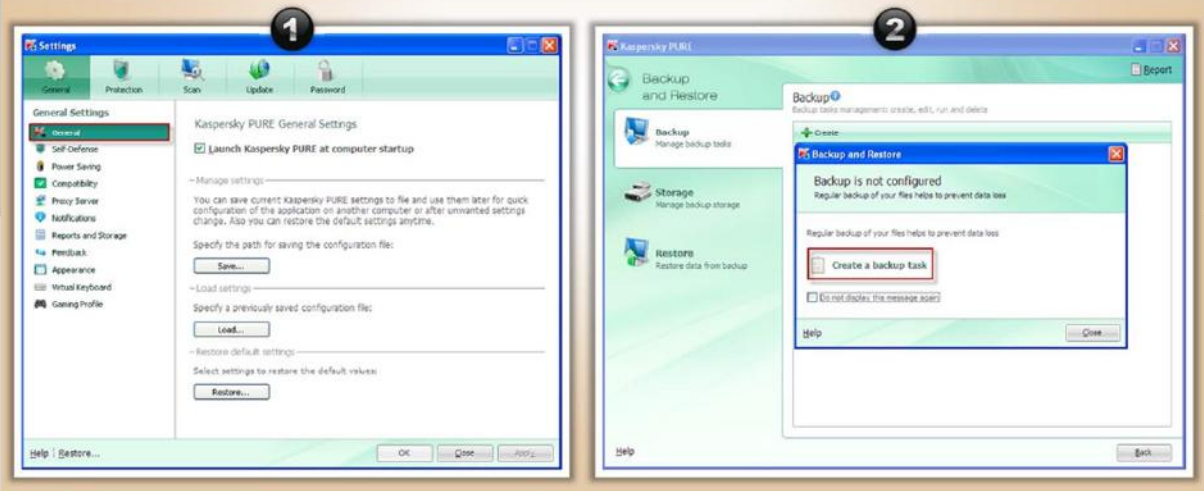
پیکربندی Kaspersky PURE: پشتیبان گیری و بازیابی

- پس از پیکربندی آنتی ویروس Kaspersky PURE، برنامه را راه اندازی نمایید.
  اکنون برنامه برای استفاده آماده است.



پیکربندی Kaspersky PURE: پشتیبان گیری و بازیابی

- برای پیکربندی پشتیبان گیری، بر روی Back up and Restore کلیک نمایید
- در پنجره Backup and Restore بر روی Create a backup task کلیک کنید

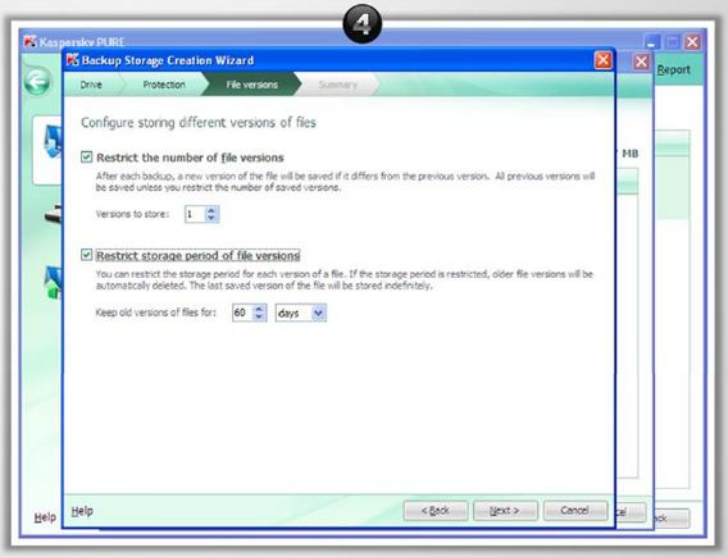


پیکربندی Kaspersky PURE: پشتیبان گیری و بازیابی

- محل فایل ها را انتخاب کرده و بر روی Next کلیک کنید -> درایو مدنظر خود را برای ذخیره فایل های پشتیبان انتخاب نموده و سپس مجدداً Next را بزنید
- به منظور محافظت داده ها از دسترسی های غیرمجاز، یک رمز عبور تعیین نموده و Next را بزنید

پیکربندی Kaspersky PURE: پشتیبان گیری و بازیابی

در پنجره Configure storing different تنظیمات لازم را اعمال versions of files نمایید-> بر روی Next کلیک کنید -> و در نهایت بر روی Finish کلیک کنید

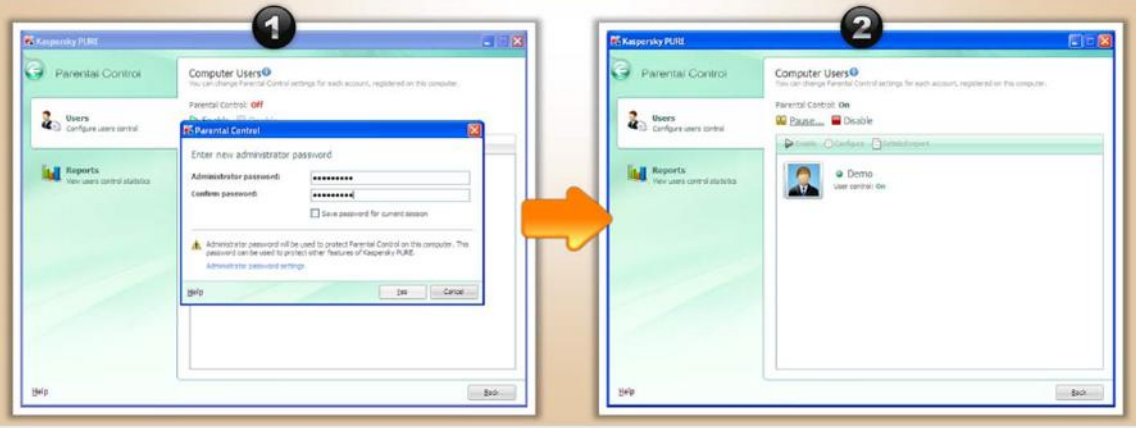


پیکربندی Kaspersky PURE: حفاظت از کامپیوتر

- مؤلفه های Computer Protection کامپیوتر شما را در مقابل تهدیدات مختلف محافظت نموده، تمام سیستم را به منظور تشخیص ویروس ها و آسیب پذیری ها اسکن می نمایند، و به طور منظم پایگاه داده آنتی ویروس و ماژول های برنامه را آپدیت می کنند

پیکربندی Kaspersky PURE: کنترل والدین

- به منظور محافظت کودکان و نوجوانان از تهدیدات مرتبط با استفاده از کامپیوتر و اینترنت، شما باید تنظیمات کنترل والدین را برای تمامی کاربران پیکربندی نمایید
- اگر شما برای اولین بار هنگام نصب برنامه پسورد را فعال نکرده اید، توصیه می شود که به منظور جلوگیری از دستکاری های غیرمجاز تنظیمات، یک رمز عبور تعیین کنید
- اکنون شما می توانید قابلیت کنترل والدین را فعال نموده و محدودیت های موردنظر را برای استفاده از کامپیوتر و اینترنت، و نیز برای پیام ها بر روی تمامی حساب های کاربری موجود در سیستم اعمال نمایید

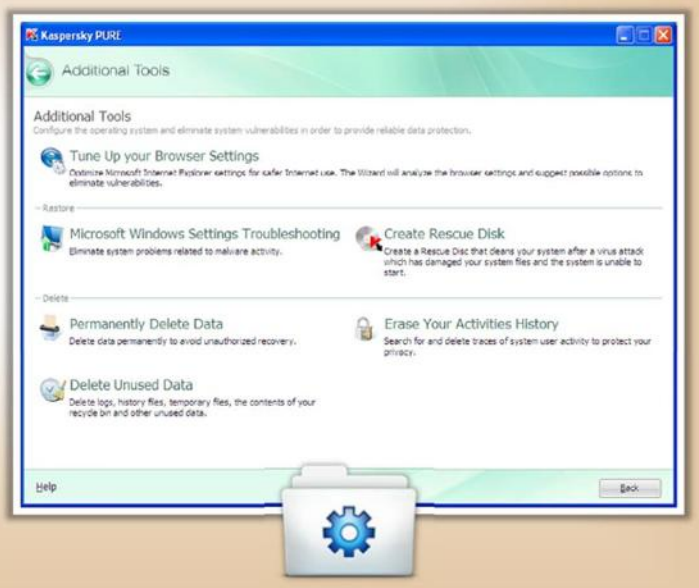


Kaspersky PURE: ابزارهای مدیریتی

با استفاده از ابزارهای مدیریتی، کاربر می تواند آسیب پذیری های سیستم را به منظور حفاظت از داده ها حذف نماید

کاربر می تواند:

1. مرورگرخود را تنظیم کند
2. با استفاده از گزینه **Microsoft Windows Settings Troubleshooting** مشکلات مربوط به فعالیت های مخرب را بیابد
3. داده ها را به صورت دائمی حذف کند
4. برخی از داده های بلااستفاده را حذف نماید
5. یک دیسک نجات ایجاد کند، تا در مواقع حمله ویروس ها از آن استفاده کند
6. فعالیت های کاربر را به منظور حفظ حریم شخصی حذف نماید



خلاصه فصل

- آنتی ویروس کامپیوتر را در مقابل ویروس ها، کرم ها، جاسوس افزارها و تروجان ها محافظت می کند
- کامپیوتری که به اینترنت متصل است همیشه در معرض خطر قرار دارد، بنابراین توصیه می گردد همیشه بر روی سیستم خود آنتی ویروس داشته باشید
- اکثر آنتی ویروس های تجاری از دو تکنیک استفاده می کنند:
  - استفاده از دیکشنری ویروس، برای جستجوی ویروس هاس شناخته شده، هنگام اسکن فایل ها
  - تشخیص رفتارهای مشکوک هر یک از برنامه ها
- در رویکرد دیکشنری ویروس، آنتی ویروس هنگام اسکن فایل ها به دیکشنری ویروس های شناخته شده ای که توسط طراح نرم افزار به آن معرفی شده است مراجعه می کند
- هرگاه برنامه ای با رفتار مشکوک یافت شود، آنتی ویروس به کاربر هشدار داده و از او می پرسد چه کاری باید انجام دهد

چک لیست امنیتی آنتی ویروس

- از چند برنامه آنتی و یروس به طور همزمان بر روی سیستم خود استفاده نکنید
- به منظور دست یافتن به حداکثر بهره وری، آنتی ویروس خود را آپدیت نمایید
- همیشه سایت عرضه کنندگان نرم افزار را به منظور دانلود آخرین وصله های امنیتی بررسی نمایید
- قابلیت اسکن لحظه ای را فعال نمایید
- همیشه لینک ها و ایمیل ها را اسکن کنید
- فایروال را فعال کنید
- آنتی ویروس را به گونه ای تنظیم کنید که اسکن را به صورت زمانبندی شده انجام دهد

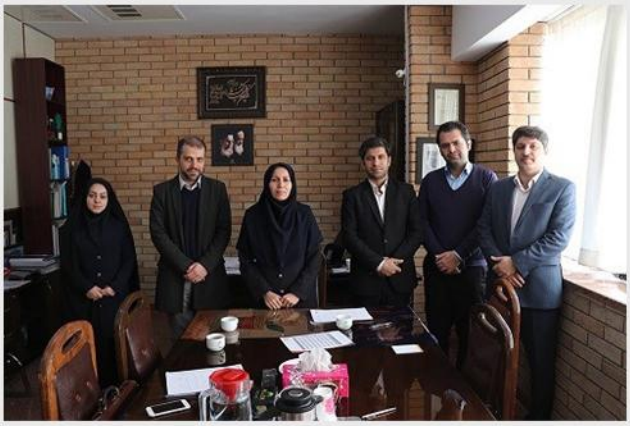
اخبار داخلی

امضای تفاهم‌نامه سه جانبه بین مرکز تخصصی آپا، پارک علم و فناوری کرمانشاه و سازمان نظام صنفی رایانه‌ای کرمانشاه

طی جلسه‌ای که مورخ ۱۳۹۷/۱۲/۰۵در دفتر سرکار خانم دکتر خان‌احمدی ریاست پارک علم و فناوری کرمانشاه برگزار گردید، تفاهم‌نامه همکاری مابین مرکز تخصصی آپا دانشگاه رازی، پارک علم و فناوری کرمانشاه و سازمان نظام صنفی رایانه‌ای کرمانشاه به امضا رسید.

طی این قرارداد طرفین متعهد گشتند که در ارائه خدمات مورد نیاز طرف مقابل نهایت تلاش خود را به کار گیرند. از جمله مواردی که در این جلسه به آن پرداخته شد دوره‌های آموزشی مرکز آپا می‌باشد که با توجه به نیاز حوزه فناوری اطلاعات به تربیت نیروی متخصص، در رابطه با برگزاری مستمر این دوره‌ها و حضور نیروها و شرکت‌های پارک علم و فناوری و نظام صنفی رایانه‌ای راهکارهای اجرایی ارائه شد.

در ادامه طرفین بر لزوم داشتن تأییدیه امنیتی افتا برای سامانه‌ها و نرم‌افزارهای شرکت‌های تحت حمایت پارک علم و فناوری و سازمان نظام صنفی رایانه‌ای تأکید کردند. مدیر مرکز تخصصی آپا نیز پیشنهاداتی را در خصوص نحوه اجرای فرایند ارزیابی محصولات ارائه نمود. مقرر شد با استناد به مفاد تفاهم نامه حاضر، و با همکاری طرفین تسهیلاتی در جهت ارزیابی امنیتی و دریافت تأییدیه امنیتی محصولات ارائه گردد.



علاوه بر این در رابطه با برگزاری دومین مسابقه فتح پرچم غرب کشور توسط مرکز آپا نیز مباحثی عنوان شد و طی مذاکرات انجام شده پارک علم و فناوری کرمانشاه و سازمان نظام صنفی رایانه‌ای حمایت مادی و معنوی خود را در جهت هر چه بهتر برگزار شدن این مسابقه اعلام نمودند، و نیز آمادگی خود را در جهت حمایت از نفرات برتر مسابقه اعلام نمودند.

کلاهبرداری میلیاردی با استفاده از دستگاه‌های اسکیمر در کرمانشاه!

باتوجه به اظهارات سرهنگ کریمی رئیس پلیس فتا استان کرمانشاه، در روز ۱۸ بهمن بیش از ۴۰ شهروند کرمانشاهی با این

ادعا کـــه مبالغی از حسابشـــان بدون اطلاع آنها برداشـــت شـــده است به پلیس فتا مراجعه نمودند.

با بررسی‌های صورت گرفته توسط کارشناسان پلیس فتا مشخص شد که تعدادی افراد سودجو با کپی کردن کارت‌های بانکی افراد و با استفاده از رمز کارت ارائه شده توسط صاحب کارت، اقدام به برداشت غیرمجاز از حساب افراد نموده‌اند، به گونه‌ای که از عصر پنجشنبه (۱۸ بهمن) حدود ساعت ۱۷ تا شنبه (۲۰ بهمن) بیش از ۱۰۰ میلیارد ریال از حساب مالباختگان برداشت شده است.

نکته جالب این اســـت که متهمـــان در بازجویی‌هـــای ابتدایی عنوان کردند که از حدود یک ســـال قبـــل اقدام به کپی کـــردن کارت بانکی شـــهروندان کرده و بـــا تصور تعطیل بـــودن ادارات و ســـازمان‌ها و همچنیـــن مراکز پلیـــس، نیت خـــود را در تعطیلات اخیـــر عملیاتی کردند، که خوشـــبختانه با هوشـــیاری پلیس فتا و اقـــدام به موقع، تمام حســـاب‌ها بلافاصله مســـدود و افراد ســـودجو که قصد خروج از کشور را داشتند دستگیر شدند.

اسکیمر چیســـت و چگونه موجب ســـرقت اطلاعات کارت‌های بانکی می‌شود؟

اسـکیمر را می‌تـوان یـک دسـتگاه کارت‌خـوان در نظر گرفت کـه اطلاعات کارت بانکـی افـراد را سـرقت می‌کند، بدیـن صورت که از نوار مغناطیسـی کارت‌هـای بانکـی یـک کپـی تهیـه می‌کند. فـرد سـارق که خود فروشـنده می‌باشـد، یـک دسـتگاه اسـکیمر را در کنـار دسـتگاه POS اصلـی قـرار داده و از مشـتری درخواسـت می‌کنـد تـا کارتش را برای تسـویه حسـاب در اختیـار وی قـرار دهـد. در این شـرایط اگر خریـدار به فروشـنده اعتماد کـرده و کارت را در اختیـار وی بگـذارد، در یـک لحظـه سـارق کارت را در دسـتگاه اسـکیمر کشیده و سـپس سـریعاً در دسـتگاه اصلی وارد می‌کند. بـه ایـن ترتیـب اطلاعات در دسـتگاه اسـکیمر ذخیره شـده و چـون رمز را نیـز کاربـر به فروشـنده اعـلام می‌کنـد، فروشـنده آن را به ذهن سـپرده و پـس از اتمـام خریـد، آن را در جایـی یادداشـت می‌کنـد و در نهایـت اطلاعـات کپـی شـده را در کارت‌هـای بانکـی خـام کپـی نمـوده و از ایـن طریق از حساب قربانی به صورت غیر مجاز، برداشت می‌کند.

* امـــا توصیه به شـــهروندان این اســـت کـــه در هنـــگام خرید از فروشـــگاه‌ها تحت هیچ شـــرایطی کارت و رمـــز کارت بانکی خود را در اختیار فروشـــنده قرار ندهند، رمـــز خود را به صـــورت دوره‌ای تغییر دهنـــد، و نیز برای خریدهـــای روزمره خود از کارت‌هـــای با موجودی کم اســـتفاده نمایند تا در صـــورت بروز چنین اتفاقاتـــی متحمل ضرر بالایی نگردند.

اخبار کوتاه

مشـــکل امنیتی، پســـورد میلیون‌هـــا کاربر اینســـتاگرام و فیسبوک را فاش کرد

ظاهراً فیســـبوک پســـورد صدها میلیون از کاربران خـــود را به صورت متن ساده ذخیره کرده است که بـــاعث شده عده زیـــادی بـــه آن‌ها دسترسی پیدا کنند.

بر اســـاس گزارشـــی که اخیراً منتشر شده، در گذشته پســـورد کاربران معمولاً رمزگذاری می‌شـــد اما یک مشـــکل در اپلیکیشـــن فیسبوک باعـــث شـــده تـــا 20 هـــزار نفـــر از کارمنـــدان ایـــن کمپانی به پســـوردهای کاربران دسترســـی پیداکنند. ظاهراً تحـــت تاثیر این اتفـــاق، بیـــن 200 الـــی 600 میلیون نفـــر از کاربران فیســـبوک از این قضیه آسیب دیده‌اند.

ویندوز دیفندر به سیستم‌عامل مک می‌آید

مایکروسافت هفته گذشته آنتـــی ویـــروس ویندوز دیفندر را بـــرای سیستم‌عامل مک منتشر نمود.

در نتیجه، اسم این آنتی‌ویروس از ویندوز دیفندر به مایکروسافت دیفندر تغییر پیدا کرده است. در واقع مایکروسافت آنتی‌ویروس ATP جداگانه‌ای را برای سیستم‌عامل مک توسعه داده که قادر به شناسایی ویروس‌ها و محافظت از سیستم‌عامل با اسکن کردن آن است. در واقع ATP مخفف تهدید پیشرفته مستمر (Advanced Presistent Threat) به روش‌های پیشرفته و مخفی برای به دست آوردن اطلاعات حساس امنیتـــی گفته می‌شود.

پست بانک ایران پس از تصویب اساسنامه توسط هیئت محترم وزیران از دی ماه سال ۱۳۷۵ فعالیت خود را به طور رسمی آغاز کرد، و در حال حاضر با دارا بودن ۱۴۵۰۰ شعبه، دفتر و مرکز در سراسر کشور انواع خدمات بانکی و مالی را به هموطنان عزیز ارائه می‌دهد.

بر اساس مصوبه مورخ ۱۳۹۵/۵/۶ مجلس شورای اسلامی و تایید شورای نگهبان، پست بانک ایران به عنوان بانک توسعه ای و تخصصی حوزه ICT کشور و همچنین بزرگترین خرده بانکدار حوزه روستایی تعیین شد.

- ☑ بانک توسعه ای و تخصصی حوزه ارتباطات و فناوری اطلاعات
- ☑ بانک عامل صندوق توسعه ملی در پرداخت تسهیلات اشتغال زائی
- ☑ کارگزار بانک مرکزی برای ارائه خدمات شعبه ای به حساب های دولتی

اپلیکیشن پست بانک ایران

- انتقال وجه
- حوالجات الکترونیکی بین بانکی پایا و ساتنا
- کارت به کارت شتابی
- پرداخت اقساط تسهیلات و قبوض
- خرید شارژ تلفن همراه
- دریافت شماره شبای حساب
- مانده حساب
- تراکنش های حساب
- مسدودی کارت

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 ۸ 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

پست بانک استان کرمانشاه

سازمان نظام صنفی رایانه‌ای استان کرمانشاه

جهاد دانشگاهی — یاری علم و فناوری کرمانشاه — Kermanshah Science & Technology Park

جمهوری اسلامی ایران — وزارت کشور — استانداری کرمانشاه

مرکز تخصصی آپا دانشگاه رازی

دانشگاه رازی — معاونت پژوهش و فناوری

اداره کل ارتباطات و فناوری اطلاعات استان کرمانشاه

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

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


مرکز تخصصی آپا دانشگاه رازی