

خبرنامه الکترونیکی ۴۹



مرکز آپا دانشگاه سمنان

مرکز تخصصی آپا دانشگاه سمنان

شماره چهل و نهم، سال پنجم، خرداد ۱۴۰۱ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان



MALWARE ACTIVATED

WARNING



WARNING



RANSOMWARE
SYSTEM HACKED

رفع آلودگی به باج افزار
در این شماره می خوانید:



خبر

۵

نقص‌های حیاتی پلاگین وردپرس Jupiter به هکرها اجازه کنترل سایت‌ها را می‌دهد

۷

نقص روز صفر Office که در حملات مورد سو استفاده قرار می‌گیرد

۱۰

نسخه لینوکس باج افزار Black Basta سرورهای VMware ESXi را هدف قرار می‌دهد

آموزش

۱۳

رفع آلودگی به باج‌افزار

خبر کوتاه

۱۹

آسیب‌پذیری روز صفر جدید آفیس در حملات استفاده می‌شود!

۲۰

قاچاق کردن PDF از سند Microsoft Word برای حذف بدافزار Snake Keylogger





مرکز آپا دانشگاه تهران

خبر

نقص‌های حیاتی پلاگین وردپرس Jupiter به هکرها اجازه کنترل سایت‌ها را می‌دهد

افزونه‌های آسیب‌پذیر استفاده می‌کند، اجازه می‌دهد تا امتیازات مدیریتی را به دست آورد. پس از سوء استفاده از آسیب‌پذیری، مهاجمان ممکن است اقدامات نامحدودی را در سایت انجام دهند، از جمله تغییر محتوای آن، تزریق اسکریپت‌های مخرب یا حذف کامل آن. مهاجم می‌تواند یک subscriber (مشترک) یا مشتری ساده در وبسایت باشد تا از این آسیب‌پذیری سوء استفاده کند، بنابراین حمله پیش نیازهای محدود کننده ای ندارد.

تحلیلگران امنیت وردپرس مجموعه‌ای از آسیب‌پذیری‌ها را کشف کرده‌اند که بر پلاگین Jupiter Theme و JupiterX Core در وردپرس تأثیر می‌گذارند، که یکی از آنها یک نقص حیاتی افزایش امتیاز است. Jupiter یک تم ساز قدرتمند با کیفیت بالا برای سایت‌های وردپرسی است که توسط بیش از ۹۰۰۰۰ وبلاگ محبوب، مجلات آنلاین و پلتفرم‌هایی که از ترافیک کاربران زیادی برخوردار هستند، استفاده می‌شود. این آسیب‌پذیری که به‌عنوان CVE-2022-1654 ردیابی می‌شود و به آن امتیاز CVSS 9.9 (بحرانی) داده شده است، به هر کاربر احراز هویت شده در یک سایت که از



کشف و رفع

طبق گفته Wordfence^۱، که این نقص را کشف کرده است، مشکل در تابعی به نام «uninstallTemplate» است که پس از حذف یک تم، سایت را بازنشانی می‌کند.

این تابع امتیازات کاربر را به ادمین ارتقا می‌دهد، بنابراین اگر یک کاربر وارد شده درخواست AJAX را با پارامتر عمل برای فراخوانی این تابع ارسال کند، بدون انجام هیچ کاری یا بررسی دیگری، امتیازات خود را افزایش می‌دهد.

تیم هوش تهدید Wordfence این مشکل را در ۵ آوریل ۲۰۲۲ کشف کرد و توسعه دهنده افزونه را با جزئیات فنی کامل مطلع کرد.

در ۲۸ آوریل ۲۰۲۲، طراح وردپرس اصلاحی جزئی برای پلاگین های آسیب دیده منتشر کرد. سپس، در ۱۰ مه ۲۰۲۲، Artbees^۲ به روزرسانی امنیتی دیگری را منتشر کرد که به طور کامل به این مشکلات پرداخت.

نسخه‌های تحت تأثیر CVE-2022-1654 عبارتند از Jupiter Theme نسخه 6.10.1 و قدیمی‌تر (رفع شده در 6.10.2)، JupiterX Theme نسخه 2.0.6 و قدیمی‌تر (رفع شده در 2.0.7)، و JupiterX Core Plugin (رفع شده در 2.0.7 و قدیمی‌تر (در 2.0.8 رفع شده است).

تنها راه حل مشکلات امنیتی این است که در اسرع وقت به آخرین نسخه های موجود به روز رسانی کنید یا افزونه را غیرفعال کنید و تم سایت خود را جایگزین کنید. در طی این بررسی امنیتی، Wordfence نقص های اضافی، البته کمتر شدید، را کشف کرد که با به روز رسانی های امنیتی ذکر شده در ۱۰ می ۲۰۲۲ برطرف شد. این نقص ها عبارتند از:

CVE-2022-1656: غیرفعال کردن دلخواه پلاگین و اصلاح تنظیمات با شدت متوسط (امتیاز 6.5 CVSS).

CVE-2022-1657: پیمایش مسیر با شدت بالا (امتیاز 8.1 CVSS) و گنجاندن فایل محلی.

CVE-2022-1658: حذف دلخواه پلاگین با شدت متوسط (امتیاز 6.5 CVSS).

CVE-2022-1659: با شدت متوسط (امتیاز 6.3 CVSS) افشای اطلاعات، اصلاح، و منع خدمت.

این چهار آسیب پذیری اضافی برای بهره برداری نیاز به احراز هویت دارند و برای مشترکین و مشتریان سایت نیز قابل دسترسی هستند، اما عواقب آنها چندان آسیب رسان نیست.

۱-تیم جهانی از تحلیلگران امنیت وردپرس
۲-توسعه دهنده افزونه



WORDPRESS



نقص روز صفر Office که در حملات مورد سوء استفاده قرار می گیرد

همانطور که محقق امنیتی nao_sec فهمید، این نقص توسط عاملان تهدید برای اجرای دستورات مخرب PowerShell از طریق MSDT استفاده می شود. مایکروسافت این حملات را به عنوان حملات خودسرانه اجرای کد^۱ در هنگام باز کردن یا پیش نمایش اسناد Word توصیف می کند.

مایکروسافت توضیح می دهد: «مهاجمی که با موفقیت از این آسیب پذیری سوء استفاده می کند، می تواند کد دلخواه را با امتیازات برنامه فراخوان اجرا کند.»
«سپس مهاجم می تواند برنامه ها را نصب کند، داده ها را مشاهده، تغییر یا حذف کند، یا حساب های جدیدی را در زمینه ای که توسط حقوق کاربر مجاز است ایجاد کند.»

مایکروسافت اقداماتی برای کاهش یک نقص امنیتی به اشتراک گذاشته تا از حملاتی که از نقص جدید Office روز صفر سوء استفاده می کنند، جلوگیری کند. این نقص توسط هکرها برای اجرای کدهای مخرب از راه دور مورد سوء استفاده قرار گرفته است.

این اشکال که توسط مایکروسافت به عنوان آسیب پذیری اجرای کد از راه دور ابزار تشخیصی پشتیبانی ویندوز^۲ توصیف شده و با نام CVE-2022-30190 ردیابی می شود، توسط crazyman از گروه Shadow Chaser گزارش شده است.

مایکروسافت می گوید این نقص بر تمامی نسخه های ویندوز که هنوز به روزرسانی های امنیتی را دریافت می کنند (ویندوز ۷+ و سرور ۲۰۰۸+) تأثیر می گذارد.

1-MSDT
2-ACE

راه حل موجود

تروجان: Mesdetty.A/Win۳۲
تروجان: Mesdetty.B/Win۳۲
رفتار: MesdettyLaunch.A/Win۳۲
رفتار: MesdettyLaunch.B/Win۳۲
رفتار: MesdettyLaunch.C/Win۳۲

طبق گفته مایکروسافت، مدیران و کاربران می‌توانند با غیرفعال کردن پروتکل URL MSDT، که عوامل مخرب از آن برای راه‌اندازی عیب‌یاب‌ها و اجرای کد روی سیستم‌های آسیب‌پذیر استفاده می‌کنند، حملاتی را که از CVE-2022-30190 سوء استفاده می‌کنند، مسدود کنند.

برای غیرفعال کردن پروتکل URL MSDT در یک دستگاه ویندوز، باید مراحل زیر را طی کنید:

۱- Command Prompt را به عنوان Administrator اجرا کنید.

۲- برای پشتیبان‌گیری از کلید رجیستری، دستور «reg export HKEY_CLASSES_ROOT\ms-msdt ms-msdt.reg» را اجرا کنید.

۳- دستور «reg delete HKEY_CLASSES_ROOT\ms-msdt /f» را اجرا کنید.

پس از اینکه مایکروسافت یک وصله CVE-2022-30190 را منتشر کرد، می‌توانید با راه‌اندازی یک command prompt با دسترسی سطح بالا و اجرای دستور reg import ms-msdt.reg راه‌حل را لغو کنید (نام فایل، نام پشتیبان رجیستری است که هنگام غیرفعال کردن پروتکل ایجاد می‌شود).

آنتی ویروس Microsoft defender نسخه 1.367.719.0 یا جدیدتر اکنون با شناسایی‌هایی برای سوء استفاده از آسیب‌پذیری احتمالی تحت امضاهای زیر ارائه می‌شود:

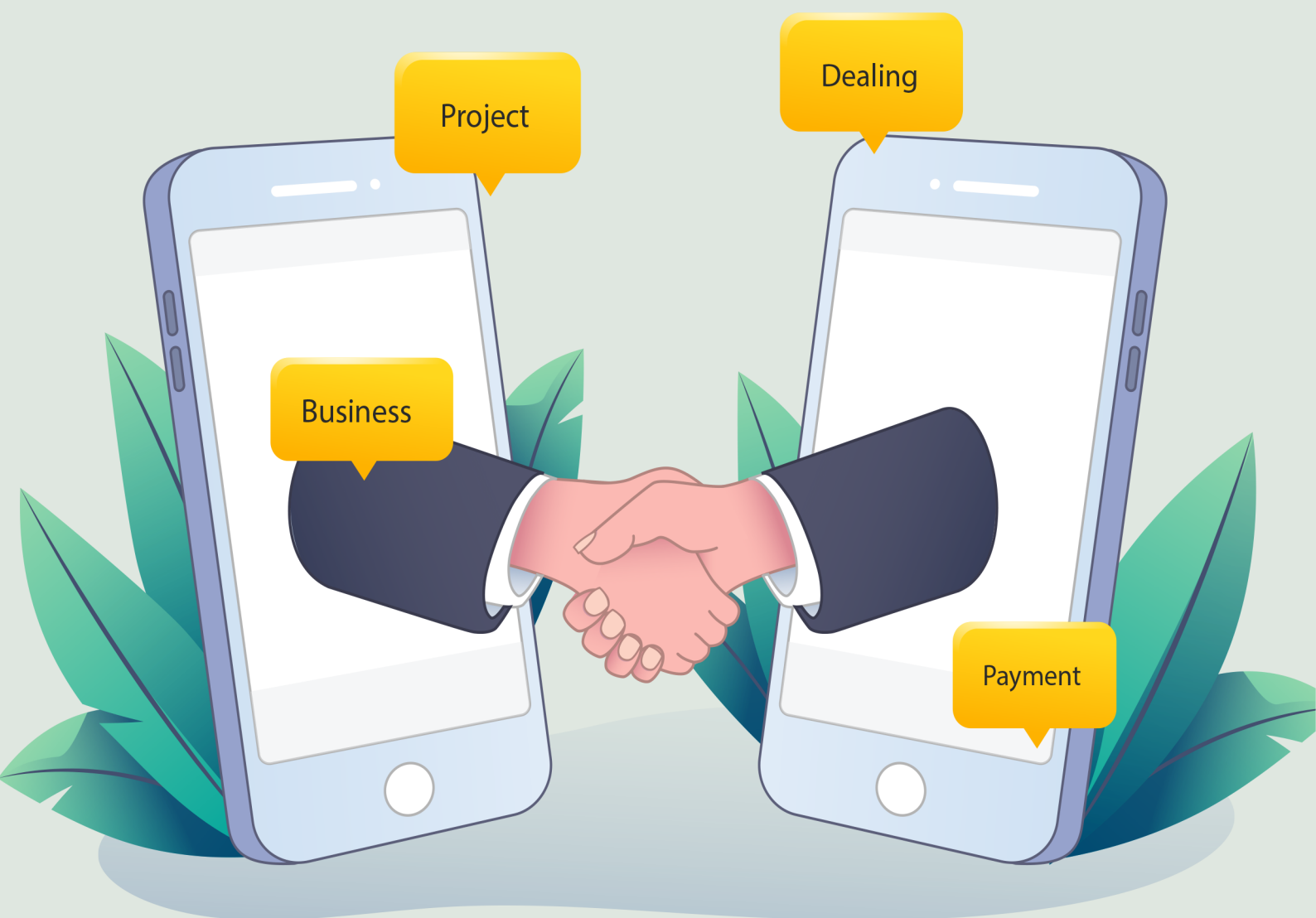
در حالی که مایکروسافت می‌گوید که protected view در حالی که Application Guard برنامه مایکروسافت آفیس حملات CVE-2022-30190 را مسدود می‌کند، ویل دورمان، تحلیلگر آسیب‌پذیری CERT/CC (و سایر محققان) فهمیدند که اگر هدف، اسناد مخرب را در Windows Explorer پیش‌نمایش کند، این ویژگی امنیتی تلاش‌های سوء استفاده را مسدود نخواهد کرد. بنابراین، همچنین توصیه می‌شود برای حذف این بردار حمله، پنل Preview را در Windows Explorer غیرفعال کنید.

به گفته crazyman از گروه Shadow Chaser (محققانی که برای اولین بار روز صفر را در آوریل شناسایی و گزارش کردند) مایکروسافت ابتدا این نقص را به عنوان «مسئله ای نامرتبط با امنیت» برچسب گذاری کرد. با این حال، بعداً گزارش ارسال آسیب‌پذیری را با تأثیر اجرای کد از راه دور مسدود کرد.

اولین حملات با بهره‌برداری از این باگ روز صفر بیش از یک ماه پیش با استفاده از دعوت‌نامه‌ها به مصاحبه‌های رادیویی اسپوتنیک و تهدیدهای اخاذی به عنوان فریب آغاز شد.



آسیب پذیری در برابر مهندسی اجتماعی ضعف امنیتی که هیچ گاه بر طرف نمی شود!





نسخه لینوکس باج افزار Black Basta

سرورهای VMware ESXi

را هدف قرار می دهد

Black Basta جدیدترین گروه باج افزاری است که از رمزگذاری ماشین های مجازی VMware ESXi که روی سرورهای لینوکس سازمانی اجرا می شوند، پشتیبانی می کند.

اکثر گروه های باج افزار در حال حاضر حملات خود را بر روی ماشین های مجازی ESXi متمرکز کرده اند، زیرا این تاکتیک با هدف گیری سازمانی آنها هماهنگ است. همچنین امکان سوء استفاده از رمزگذاری سریعتر چندین سرور با یک فرمان را فراهم می کند.

رمزگذاری ماشین های مجازی منطقی است زیرا بسیاری از شرکت ها اخیراً به ماشین های مجازی مهاجرت کرده اند، زیرا امکان مدیریت آسان تر دستگاه و استفاده کارآمدتر از منابع را فراهم می کنند.

باج افزار دیگری که سرورهای ESXi را هدف قرار می دهد!

در گزارشی جدید، تحلیلگران تهدید Uptycs فاش کردند که باینری های باج افزاری Black Basta جدید را شناسایی کرده اند که به طور خاص سرورهای VMware ESXi را هدف قرار می دهند.

رمزگذارهای باج افزار لینوکس چیز جدیدی نیستند و BleepingComputer از رمزگذارهای مشابه منتشر شده توسط چندین باند دیگر از جمله LockBit، HelloKitty، REvil، AvosLocker، RansomEXX و Hive گزارش داده است.

مانند سایر رمزگذارهای لینوکس، باج افزار Black Basta، مسیر / vmfs/volumes/ را روی سرور ESXi مورد حمله جستجو می کند. ماشین های مجازی، در این پوشه ذخیره می شوند (اگر چنین پوشه ای یافت نشد، باج افزار خارج می شود).

BleepingComputer نتوانست آرگومان های خط فرمان را برای هدف قرار دادن مسیرهای دیگر برای رمزگذاری پیدا کند، که نشان می دهد این رمزگذار به طور خاص برای هدف قرار دادن سرورهای ESXi طراحی شده است.

این باج افزار از الگوریتم ChaCha20 برای رمزگذاری فایل ها استفاده می کند. همچنین از مزایای پردازش چندنخی برای استفاده از چندین پردازنده و سرعت بخشیدن به فرآیند رمزگذاری استفاده می کند.

در حین رمزگذاری، باج افزار پسوند basta. را به نام فایل های رمزگذاری شده اضافه می کند و یادداشت هایی با نام readme.txt در هر پوشه ایجاد می کند.



که بیش از ۲ میلیون دلار باج بابت رمزگشایی و خودداری از افشای اطلاعات آنلاین دریافت کرده است. در حالی که اطلاعات زیادی در مورد باج افزار جدید در دست نیست، این احتمالاً یک عملیات جدید نیست، بلکه تغییر نام تجاری به دلیل توانایی اثبات شده آنها در نفوذ سریع به قربانیان جدید و سبک مذاکره (احتمالاً نام تجاری مجدد عملیات باج افزار Conti) است. Fabian Wosar مدیر ارشد فناوری Emsisoft قبلاً به BleepingComputer گفته است که گروه‌های باج‌افزار دیگر (علاوه بر باج‌افزارهایی که در مورد آنها گزارش کرده‌ایم)، از جمله Babuk، RansomExx/Defray، Mespinoza، GoGoogle، Snatch، PureLocker و DarkSide نیز رمزگذارهای لینوکس خود را توسعه داده‌اند و از آنها استفاده کرده‌اند. Wosar توضیح داد: «دلیل اینکه اکثر گروه‌های باج‌افزار نسخه مبتنی بر لینوکس از باج‌افزار خود را پیاده‌سازی می‌کنند، هدف قرار دادن خاص ESXi است.»

این یادداشت‌ها شامل یک پیوند به پنل پشتیبانی چت و یک شناسه منحصر به فرد است که قربانیان می‌توانند از آن برای برقراری ارتباط با مهاجمان استفاده کنند.

Siddharth Sharma و Nischay Hegde از Uptcys گفتند: «Black Basta برای اولین بار امسال در ماه آوریل مشاهده شد، که انواع سیستم‌های ویندوز را هدف قرار دادند.»

بر اساس پیوند پشتیبانی چت و پسوند فایل رمزگذاری شده، ما معتقدیم که عوامل پشت این کمپین همان کسانی هستند که سیستم‌های ویندوز را قبلاً با باج افزار Black Basta هدف قرار دادند.

از آوریل فعال است

باج افزار Black Basta برای اولین بار در هفته دوم آوریل مشاهده شد و این عملیات به سرعت حملات خود را علیه شرکت‌های سراسر جهان افزایش داد. حتی اگر باج‌خواهی این گروه بین قربانیان متفاوت باشد، BleepingComputer حداقل یکی را می‌شناسد



مرکز آپا دانشگاه گیلان

آموزش

رفع آلودگی به باج افزار

رفع آلودگی

رفع آلودگی اولین کاریست که باید انجام شود چراکه در صورت باقی ماندن باج افزار در دستگاه، ممکن است تمام تلاش های بعدی برای بازیابی اطلاعات بی نتیجه باشد. به منظور رفع آلودگی راه های مختلفی وجود دارد که مهم ترین آنها به شرح زیر می باشند:

- استفاده از آنتی ویروس آپدیت
- حذف باج افزار به صورت دستی
- استفاده از Point Restore
- بازگرداندن نسخه پشتیبان
- نصب مجدد ویندوز
- و...

نکته مهمی که وجود دارد این است که تا زمانی که از رفع کامل آلودگی اطمینان حاصل نکرده اید، می بایست از اتصال هرگونه تجهیزات جانبی ذخیره سازی به دستگاه آلوده خودداری نمایید. همچنین تا آن زمان سیستم مذکور می بایست در قرنطینه بوده و ارتباط شبکه ای با سایر دستگاه ها نداشته باشد.

مراحل حذف آلودگی باج افزار با کمک Restore Point

در صورتی که رایانه شما به باج افزار آلوده شده باشد و شما بخواهید این آلودگی را برطرف کنید می توانید از روش زیر استفاده کنید. البته این روش زمانی به درستی عمل خواهد کرد که شما در تاریخی قبل از آلوده شدن دستگاه اقدام به تهیه Restore Point کرده باشید.

۱. سیستم خود را ری استارت کنید.
۲. هم زمان با بالا آمدن سیستم کلید F۸ را فشار دهید.

۳. با استفاده از کلیدهای جهت دار گزینه mode safe را انتخاب کنید.
۴. با استفاده از نشانگر متنی که در صفحه ظاهر می شود، exe. rstrui را تایپ کنید.
۵. کلید Enter را فشار دهید.
۶. در صفحه Restore System Windows، تاریخ بازیابی قبل از آلوده شدن را انتخاب کنید و رایانه خود را به این مرحله بازگردانید.
۷. با استفاده از یک دستگاه دیگر نرم افزار معتبری دانلود کنید که توانایی غیرفعال کردن و حذف باج افزار از رایانه شما را داشته باشد.
۸. فایل نصبی نرم افزار را کپی کرده و در دستگاه آلوده به باج افزار نصب کنید.
۹. سیستم را به طور کامل اسکن کنید.
۱۰. تمام آلودگی های ایجاد شده توسط باج افزار را انتخاب کرده و آنها را از رایانه تان پاک کنید.

نکته مهم: فراموش نکنید که با این روش گرچه می توانید بدافزار را از رایانه تان حذف کرده و مجدداً کنترل سیستم خود را در دست بگیرید. اما، رمزگشایی پرونده های شما ممکن نخواهد بود و اگر بدافزار بسیار پیچیده باشد، رمزگشایی آنها بدون دسترسی به کلید ی که مهاجم در اختیار دارد، تقریباً غیرممکن است.



حذف آلودگی باج افزار با کمک Backup

زمان بیشتری می‌برد. برخی از بهترین ابزارهای تهیه نسخه پشتیبان در ادامه معرفی خواهند شد.

ابزار EaseUS Todo Backup Free

نرم افزار EaseUS درواقع ابزاری برای محافظت از فایل‌ها به صورت دستی و خودکار است که کارایی نسبتاً مناسبی دارد. این برنامه بسیاری از قابلیت‌های اساسی ابزار بکاپ‌گیری را پوشش می‌دهد. قابلیت‌هایی مانند پشتیبان‌گیری از فایل‌های

تکی و فولدرها، تمامی درایوها یا پارتیشن‌ها یا امکان تهیه‌ی پشتیبان از کل سیستم در این نرم‌افزار گنجانده شده است. همچنین گزینه‌ای تحت عنوان smart نیز در نظر گرفته شده است که در صورت استفاده از آن فایل‌های مسیرهایی از سیستم که معمولاً بیشتر با آنها سر و کار دارید پشتیبان‌گیری می‌شوند و می‌توانید این بکاپ‌ها را در فضای ذخیره سازی ابری نیز بارگذاری کنید. با استفاده از Todo EaseUS از انواع بکاپ‌های برنامه‌ریزی شده، بکاپ از آخرین تغییرات یا اینکرمنتال و بکاپ از تغییرات نسبت به نسخه‌ی اولیه یا دیفرنشال بهره‌مند شوید. خوشبختانه نسخه‌ی رایگان این برنامه تقریباً تمامی ویژگی‌های کارآمد را ارائه می‌دهد. مهمترین ویژگی‌های این برنامه را می‌توان به صورت زیر برشمرد:

- پشتیبانی از انواع مدل‌های پشتیبان‌گیری
- برنامه‌دهی ساده
- پشتیبان‌گیری هوشمند و خودکار

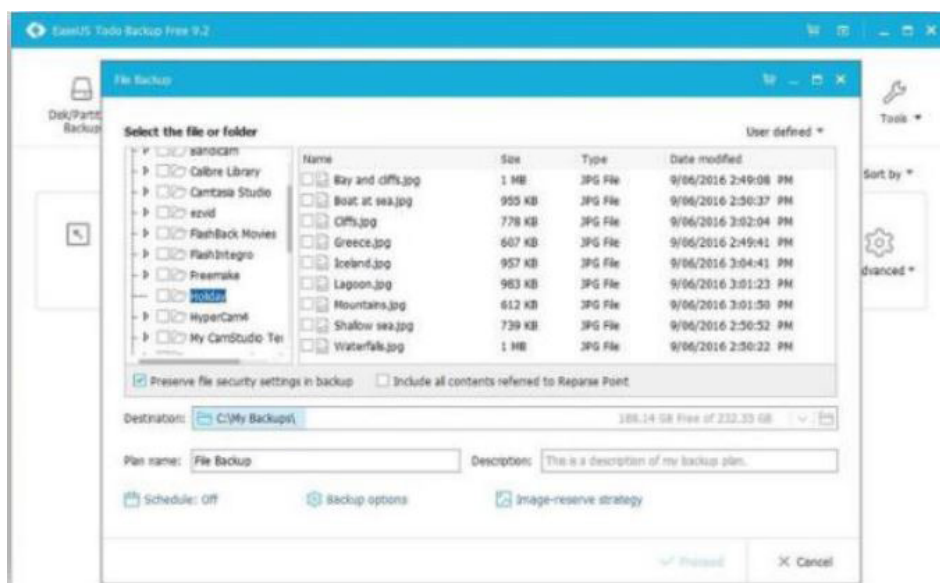
در صورتی که برنامه منظمی جهت تهیه نسخه پشتیبان داشته باشید از حملات باج‌افزاری کمترین آسیب را خواهید دید. چراکه این روش بهترین راهکار خلاص شدن از شر باج‌افزار و آثار مخرب آن است و در بدترین حالت تنها برخی از فایل‌های ایجاد شده پس از آخرین بکاپ‌گیری را از دست خواهید داد. لذا اگر قبل از قفل شدن رایانه خود، نسخه پشتیبان تهیه کرده‌اید تنها کافیه آن را بازگردانید و به اکثر فایل‌ها خود دسترسی امن پیدا کنید. همانطور که می‌دانید تهیه نسخه پشتیبان نیز به روش‌های مختلف انجام می‌شود که عبارتند از:

بکاپ کامل یا فول بکاپ: این بکاپ یک کپی از داده‌های منتخب شما است.

دیفرنشال بکاپ: این بکاپ یک کپی از داده‌هایی است که بعد از گرفتن آخرین بکاپ کامل اضافه شده یا تغییر پیدا کرده‌اند.

اینکرمنتال بکاپ: این بکاپ یک کپی از داده‌هایی است که در مقایسه با آخرین بکاپ گرفته شده (از هر نوع که باشد) دست خوش تغییر شده‌اند.

هر بکاپ دیفرنشال نسبت به بکاپ دیفرنشال قبلی حجیم‌تر است؛ اما شما برای بازگردانی سیستم خود تنها به بکاپ کامل و آخرین بکاپ دیفرنشال نیاز خواهید داشت. بکاپ‌های اینکرمنتال حجم کمتری نسبت به دیفرنشال‌ها دارند؛ اما در صورتی که بخواهید از اینکرمنتال‌ها استفاده کنید، به فایل بکاپ کامل و تمام بکاپ‌های اینکرمنتال بعد از آن نیاز خواهید داشت که

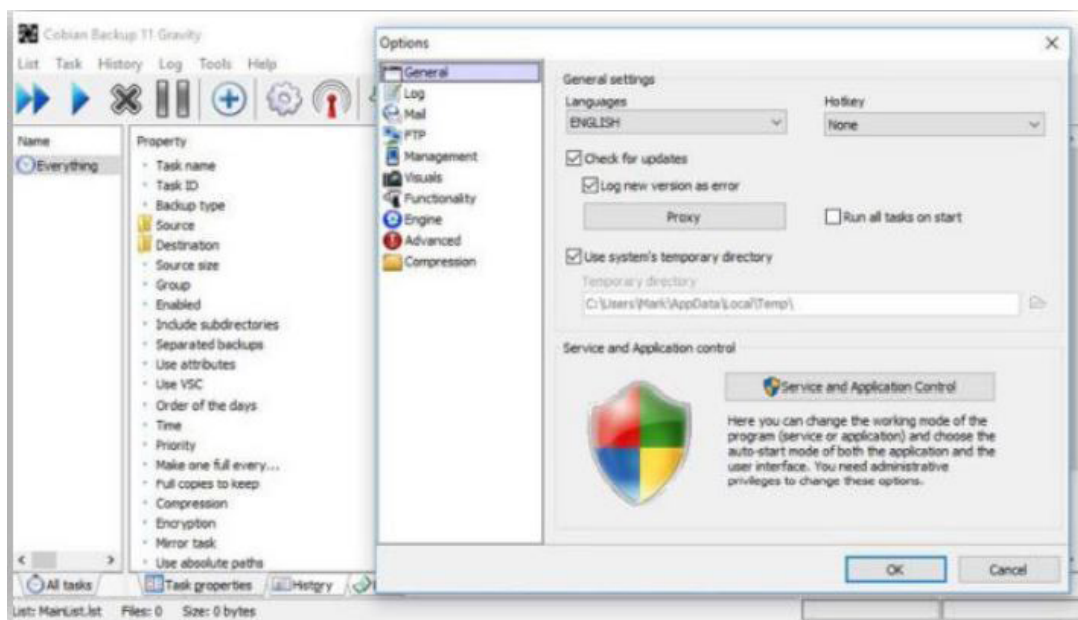


ابزار Cobian Backup

کوبیان بکاپ می‌توانید فایل‌های بکاپ را فشرده‌سازی کنید تا فضای کمتری اشغال کنند. گزینه‌ی دلخواهی نیز جهت رمزنگاری داده‌ها در نظر گرفته شده است. بنابراین کوبیان بکاپ را می‌توان یکی از قدرتمندترین ابزارهای رایگان موجود جهت بکاپ‌گیری از داده‌های ارزشمند شما لقب داد. مهمترین ویژگی‌های این ابزار به شرح زیر است:

- قابلیت‌های شخصی سازی زیاد
- رمزنگاری اختیاری
- فاقد راهنما برای کاربران مبتدی

نرم افزار Backup Cobian را شاید بتوان پیشرفته‌ترین ابزار پشتیبان‌گیری رایگان موجود دانست؛ از این جهت شاید باب میل تمام کاربران نباشد؛ اما اگر بدانید چه‌طور آن را تنظیم کنید، می‌توانید کارایی مطلوب را از آن انتظار داشته باشید. کوبیان بکاپ می‌تواند برای ساخت و برنامه‌ریزی بکاپ‌های مختلف مورد استفاده قرار گیرد. فایل‌های تهیه‌شده توسط این برنامه می‌توانند در درایو مجزایی در سیستم یا شبکه یا در صورت دسترسی در FTP آرشیو شوند. کوبیان بکاپ می‌تواند بکاپ را به صورت همزمان در محل‌های مختلف ذخیره کند؛ بنابراین، امکان پشتیبان‌گیری چند کاناله و همزمان نیز وجود دارد. با



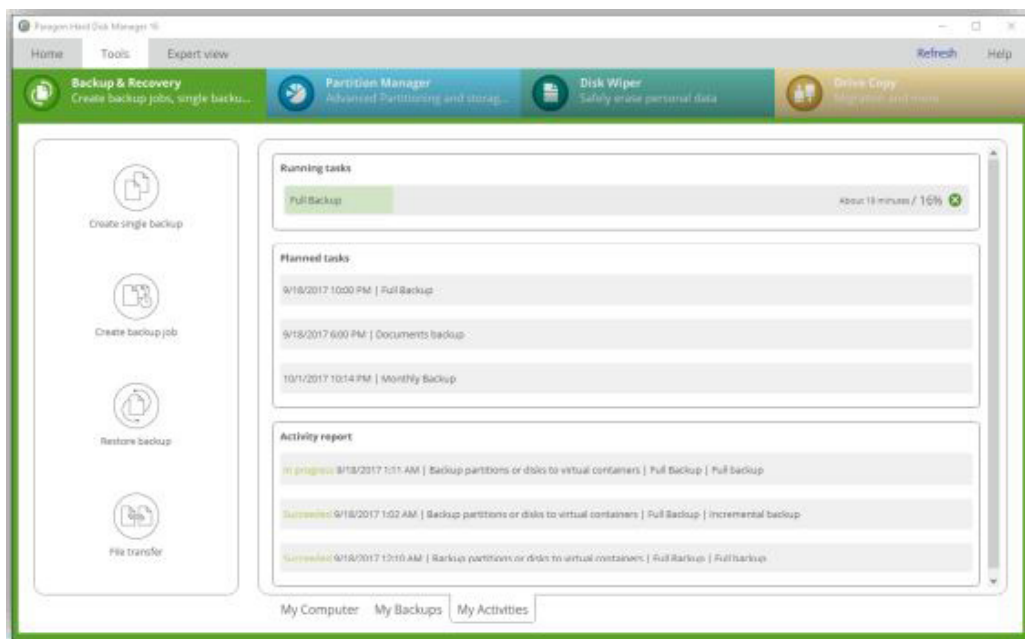
ابزار Paragon Backup & Recovery

امکانات Paragon Backup & Recovery به اینجا ختم نمی‌شود و همان‌طور که از نام برنامه مشخص است، ابزار بازبازی اطلاعات نیز در این برنامه گنجانده شده است؛ به این معنی که، می‌توانید از آن برای ریکاوری نیز استفاده کنید. رایگان بودن این ابزار نیز استفاده از آن را بسیار جذاب کرده است.

مهم‌ترین ویژگی‌های این ابزار عبارتند از:

- تنظیم به کمک ویزارد
- قابلیت‌های شخصی سازی زیاد
- مجهز به ریکاوری یا بازبازی پیشرفته

ابزار بکاپ و ریکاوری Paragon، فرآیند پشتیبان‌گیری را بسیار ساده می‌کند. رابط کاربری مبتنی بر ویزارد این برنامه شما را در استفاده از آن یاری خواهد کرد. می‌توانید تعیین کنید که برنامه از تمام حافظه‌ی رایانه، پارتیشن‌های مشخص یا فایل‌ها و فولدرهای انتخابی شما بکاپ بگیرد. امکان بکاپ‌گیری از فایل‌هایی با فرمت خاص نیز وجود دارد. پس از انجام تنظیمات فوق، کافی است برنامه‌ریزی برای زمان انجام پشتیبان‌گیری و نوع بکاپ را مشخص کنید و با خیال آسوده برنامه را ترک کنید. پاراگون به صورت خودکار و طبق برنامه امور را مدیریت خواهد کرد.

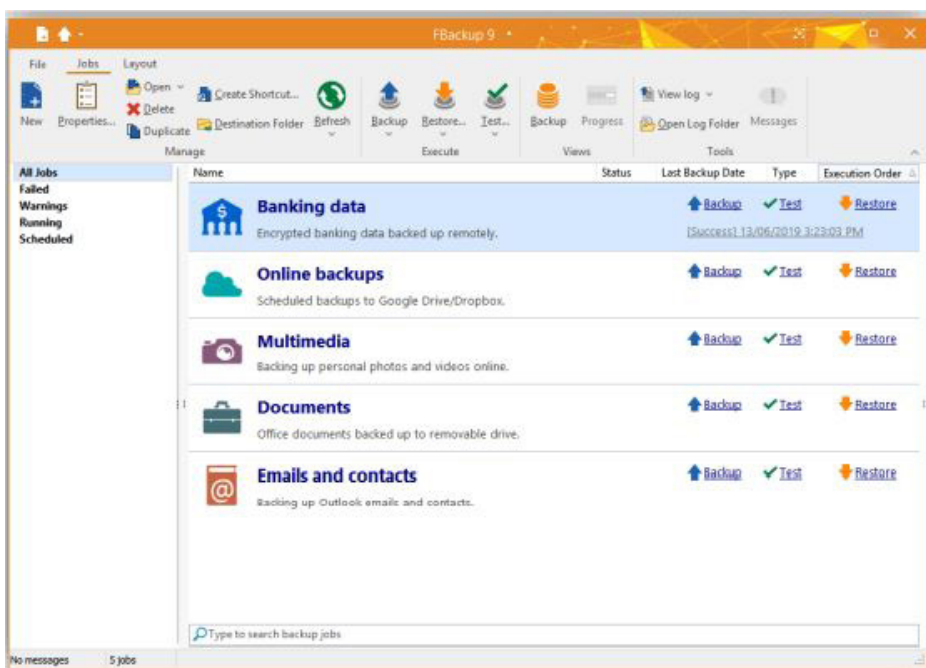


ابزار FBackup

خواهد بود. فایل بکاپ می‌تواند در داخل سیستم، درایوهای شبکه، دیسک و حافظه‌ی جانبی یا گوگل درایو ذخیره شود. به کمک امکان برنامه‌ریزی انجام بکاپ، می‌توانید نسخه‌ی پشتیبان خود را به‌روز نگه دارید. مهمترین ویژگی‌های این ابزار عبارتند از:

- برنامه‌ریزی خودکار
- تنظیمات مبتنی بر ویزارد
- فاقد رمزنگاری
- عدم پشتیبانی از بکاپ آخرین تغییرات

ابزار FBackup رابط کاربری مشابه نرم‌افزارهای آفیس دارد که ممکن است چندان خوشایند همه نباشد؛ اما این برنامه صرف نظر از ظاهر نه چندان دلچسب آن، ابزاری توانمند در زمینه‌ی پشتیبان‌گیری به شمار می‌رود؛ هرچند که از لحاظ قابلیت با نرم‌افزارهایی مانند Paragon Backup & Recovery در یک رده قرار نمی‌گیرد. امکاناتی که FBackup در اختیار می‌گذارد، تنظیمات مبتنی بر ویزارد و حالت‌های پیشرفته است. هر کدام را که انتخاب کنید، انجام مراحل پشتیبان‌گیری ساده

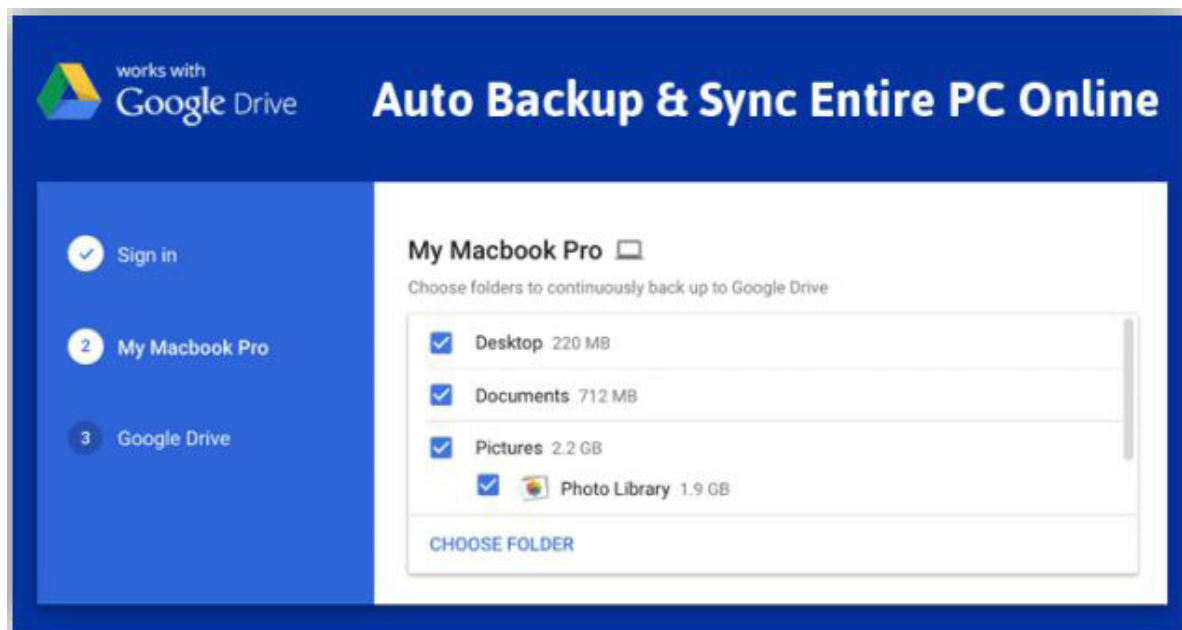


ابزار Google Backup and Sync

مذکور، برنامه به سرعت همگام‌سازی را انجام خواهد داد. همانطور که از نام نرم افزار بر می‌آید، این ابزار می‌تواند جهت همگام‌سازی فایل‌ها بین رایانه‌های مختلف مورد استفاده قرار گیرد. در این صورت، فایل‌های مورد بحث از طریق اپلیکیشن مبتنی بر وب گوگل درایو برای دستگاه‌های مختلف در دسترس خواهند بود. Google Backup and Sync را فارغ از محدودیت حجمی آن می‌توان ابزاری عالی برای پشتیبان‌گیری به شمار آورد. مهم‌ترین ویژگی‌های این ابزار عبارتند از:

- تنظیمات واضح و ساده
- نامناسب برای پشتیبان‌گیری کامل از سیستم
- گزینه های شخصی سازی محدود

گوگل بکاپ ابزاری مدرن و مبتنی بر فضای ابری است؛ یعنی هرچه قدر در گوگل درایو فضای بیشتری در اختیار داشته باشید، فایل بکاپ شما می‌تواند پر حجم‌تر باشد. در ابتدای استفاده از این ابزار مقدار فضای رایگان محدودی در اختیار شما قرار می‌گیرد که راه‌های زیادی برای افزایش این مقدار بدون هزینه کردن وجود دارد. در مجموع باید گفت نرم‌افزار Google Backup and Sync برای پشتیبان‌گیری از فایل‌های شخصی مناسب است و به منظور بکاپ گرفتن از کل سیستم کارآمد نیست. برای بکاپ گرفتن از فایل و فولدرهای شخصی با استفاده از Google Backup and Sync کافی است هر تعداد فایل و فولدر را که مد نظر دارید به برنامه بدهید تا برنامه آنها را زیر نظر بگیرد. در صورت ایجاد هر گونه تغییر، حذف و اضافه در فایل‌ها و فولدرهای





مرکز آپا دانشگاه سمنان

خبر کوتاه

آسیب‌پذیری روز صفر جدید آفیس

در حملات استفاده می‌شود!



semCERT

@semcert



این آسیب‌پذیری در آفیس 2013، 2016، آفیس پرو پلاس از آوریل (در ویندوز 11 با به‌روزرسانی‌های ماه می) و نسخه اصلاح‌شده آفیس 2021 وجود دارد.

semCERT

@semcert



مهاجم می‌تواند از این آسیب‌پذیری برای دسترسی به مکان‌های دور در شبکه قربانی استفاده کند و به او اجازه می‌دهد تا هش رمزهای عبور ماشین قربانی ویندوز را جمع‌آوری کند.

منبع: Bleeping_computer ✓

semCERT

@semcert



⚠️ #آسیب‌پذیری روز صفر جدید آفیس در حملات استفاده می‌شود
محققان امنیتی یک آسیب‌پذیری جدید مایکروسافت آفیس را که #Follina نامیده می‌شود، کشف کرده‌اند که در حملات برای اجرای دستورات مخرب PowerShell از طریق Microsoft Diagnostic Tool (MSDT) به سادگی با بازکردن یک فایل Word استفاده می‌شود



semCERT

@semcert



این آسیب‌پذیری، در را به روی یک بردار حمله حیاتی جدید باز می‌کند که از برنامه‌های #مایکروسافت #آفیس استفاده می‌کند؛ بدون امتیازات سطح بالا کار می‌کند، تشخیص Windows Defender را دور می‌زند و برای فعال کردن بایرنی‌ها یا اسکریپت‌ها نیازی به کد ماکرو ندارد.

قاچاق کردن PDF از سند Microsoft Word

برای حذف بدافزار Snake Keylogger

semCERT

@semcert



از آنجایی که نام سند "تأیید شده است" می‌باشد، ممکن است گیرندگان باور کنند که فایل #adobe را قانونی تأیید کرده است و باز کردن فایل امن است.

semCERT

@semcert



⚠ قاچاق کردن PDF از سند Microsoft Word برای حذف بدافزار Snake Keylogger

تحلیلگران تهدید، یک کمپین توزیع #بدافزار جدید را که از پیوست‌های PDF برای قاچاق اسناد بدافزار Word استفاده کرده و کاربران را با بدافزار آلوده می‌کند، کشف کرده‌اند.



semCERT

@semcert



پس از آن اگر ماکروها فعال باشند، از طریق فایل Snake Keylogger، RTF، یک دزد اطلاعات ماژولار را دانلود و اجرا می‌کند. این دزد اطلاعات دارای قابلیت‌های مانایی، بالا، فرار از دفاع، دسترسی به اعتبارنامه‌ها، جمع‌آوری و خارج کردن اطلاعات است.

منبع: bleeping_computer ✓



semCERT

@semcert



امروزه اکثر ایمیل‌های مخرب با پیوست‌های DOCX یا XLS همراه با کدهای ماکرو بارگیری بدافزار ارسال می‌شوند. هنگامی که PDF دریافتی باز می‌شود، Adobe Reader از کاربر می‌خواهد که یک فایل DOCX موجود در داخل PDF را باز کند،



تلاش ما حفظ امنیت شماست...

