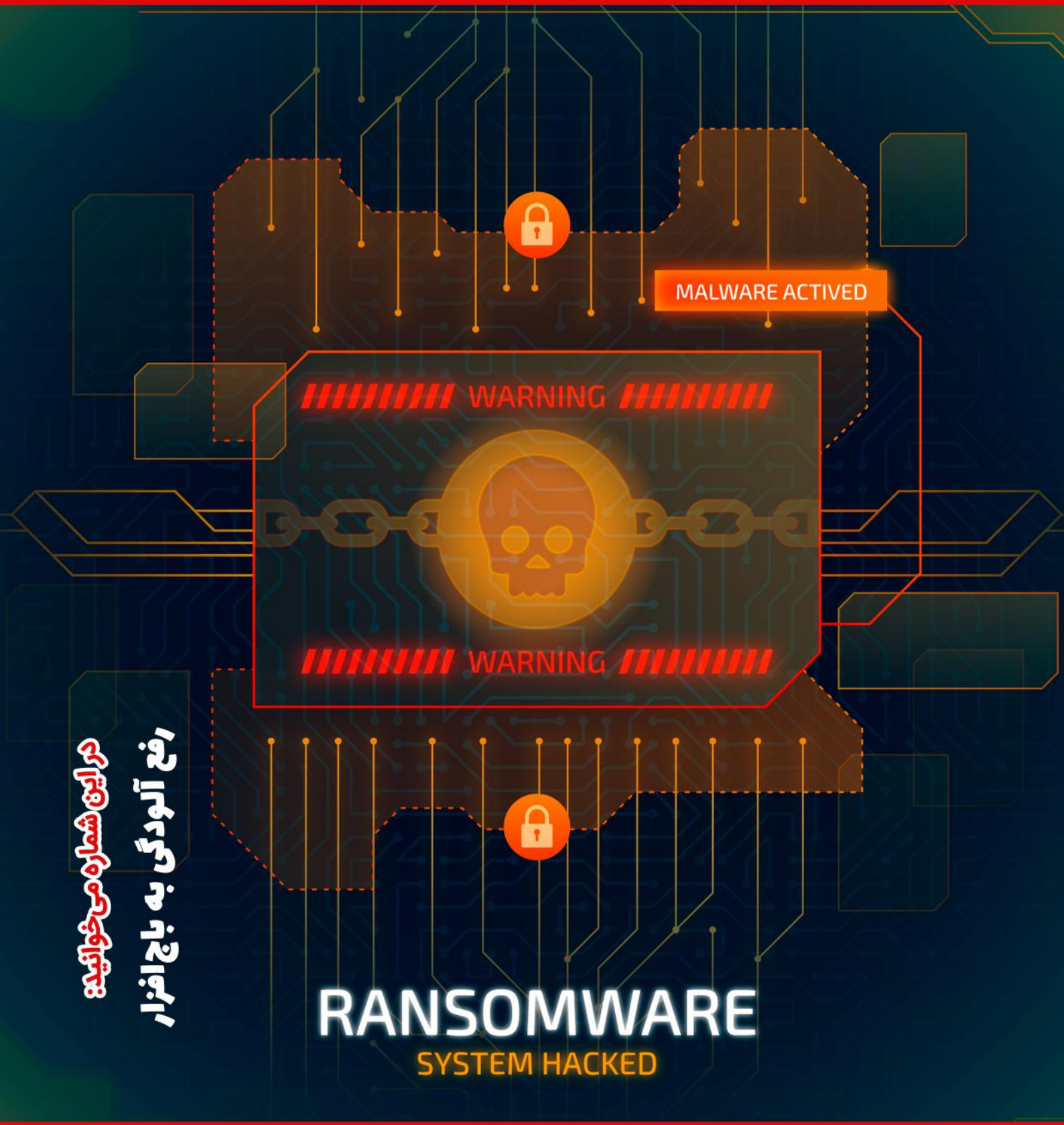
خبرنامه الکترونیکی ۴۹

مرکز تخصصی آپا دانشگاه سمنان

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



در این شماره می‌خوانید:
رفع آلودگی به باج‌افزار

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

سرمایه گذاری
روی دانش
بیشترین بهره را دارد.

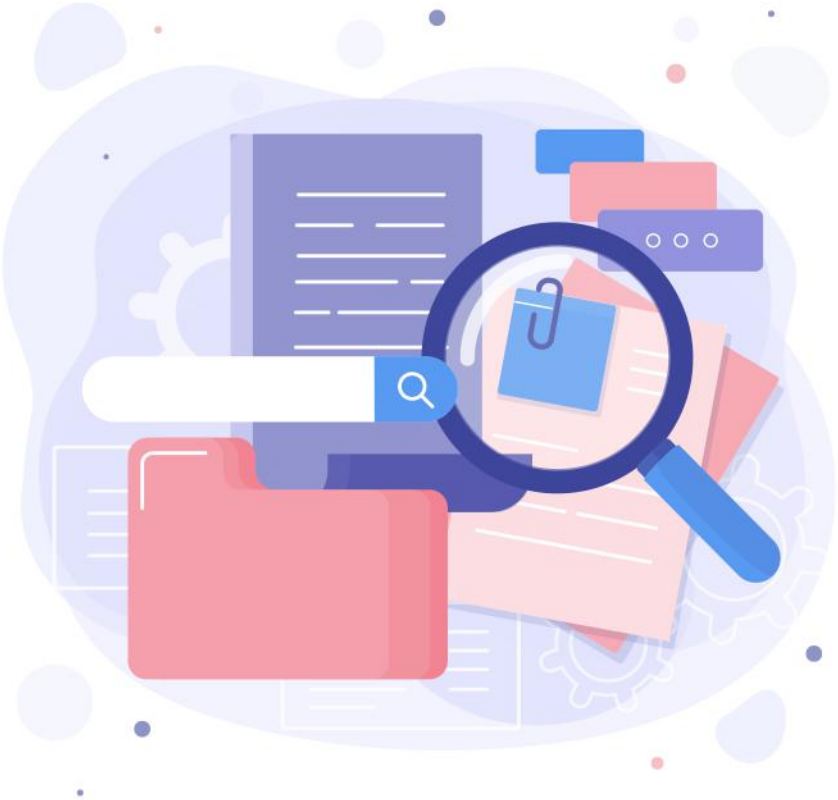
مرکز آپا دانشگاه سمنان

فهرست

خبر

آموزش

خبرکوتاه



مرکز آپا دانشگاه سمنان

خبر

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

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 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 اسکریپت های مخرب یا حذف کامل آن.

مهاجم می تواند یک subscriber (مشترک) یا مشتری ساده در وب‌سایت باشد تا از این آسیب پذیری سوء استفاده کند، بنابراین حمله پیش نیازهای محدود کننده ای ندارد.

کشف و رفع

طبق گفته Wordfence[1]، 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[2] به‌روزرسانی 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 نسخه 2.0.7. و قدیمی تر (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 نقص‌های اضافی، البته کمتر شدید، را کشف کرد که با به‌روزرسانی‌های امنیتی ذکر شده در ۱۰ می ۲۰۲۲ برطرف شد. این نقص‌ها عبارتند از:

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

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

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

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

این چهار آسیب‌پذیری اضافی برای بهره‌برداری نیاز به احراز هویت دارند و برای مشترکین و مشتریان سایت نیز قابل دسترسی هستند، اما عواقب آن‌ها چندان آسیب‌رسان نیست.

۱-تیم جهانی از تحلیلگران امنیت وردپرس
۲-توسعه‌دهنده افزونه

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

مایکروسافت اقداماتی برای کاهش یک نقص امنیتی به اشتراک گذاشته تا از حملاتی که از نقص جدید Office روز صفر سو استفاده می‌کنند، 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 آسیب‌پذیری اجرای کد از راه دور ابزار تشخیصی پشتیبانی ویندوز[1] توصیف شده و با نام CVE-2022-30190 ردیابی می‌شود، توسط crazyman از گروه Shadow Chaser گزارش شده است.

مایکروسافت می‌گوید این نقص بر تمامی نسخه‌های ویندوز که هنوز به‌روزرسانی‌های امنیتی را دریافت می‌کنند (ویندوز ۷+ و سرور ۲۰۰۸+) تأثیر می‌گذارد.

همانطور که محقق امنیتی nao_sec فهمید، این نقص توسط عاملان تهدید برای اجرای دستورات مخرب PowerShell از طریق MSDT استفاده می‌شود. مایکروسافت این حملات را به عنوان حملات خودسرانه اجرای کد[2] در هنگام باز کردن یا پیش نمایش اسناد Word توصیف می‌کند.

مایکروسافت توضیح می‌دهد: «مهاجمی که با موفقیت از این آسیب‌پذیری سوء استفاده می‌کند، می‌تواند کد دلخواه را با امتیازات برنامه فراخوان اجرا کند.»

«سپس مهاجم می‌تواند برنامه‌ها را نصب کند، داده‌ها را مشاهده، تغییر یا حذف کند، یا حساب‌های جدیدی را در زمینه‌ای که توسط حقوق کاربر مجاز است ایجاد کند.»

1-MSDT
2-ACE

راه حل موجود

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 پشتیبان گیری 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 آسیب پذیری احتمالی تحت امضاهای زیر ارائه می‌شود:

تروجان:Mesdetty.A/Win۳۲

تروجان:Mesdetty.B/Win۳۲

رفتار: MesdettyLaunch.A/Win۳۲

رفتار: MesdettyLaunch.B/Win۳۲

رفتار: MesdettyLaunch.C/Win۳۲

در حالی که مایکروسافت می‌گوید که protected view و Application Guard برنامه مایکروسافت آفیس حملات CVE-2022-30190 را مسدود می‌کند، ویل دورمان، تحلیلگر آسیب پذیری CERT/CC (و سایر محققان) فهمیدند که اگر هدف، اسناد مخرب را در Windows Explorer پیش نمایش کند، این ویژگی امنیتی تلاش های 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، بعدا 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.

مرکز آپا دانشگاه سمنان

آسیب‌پذیری در برابر مهندسی اجتماعی ضعف امنیتی که هیچ‌گاه بر طرف نمی‌شود!

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

Black Basta جدیدترین گروه باج‌افزاری است که از رمزگذاری ماشین‌های مجازی VMware ESXi که روی سرورهای لینوکس سازمانی اجرا می‌شوند، پشتیبانی می‌کند.

اکثر گروه‌های باج‌افزار در حال حاضر حملات خود را بر روی ماشین‌های مجازی ESXi متمرکز کرده‌اند، زیرا این تاکتیک با هدف‌گیری سازمانی آنها هماهنگ است. همچنین امکان سوء استفاده از رمزگذاری سریعتر چندین سرور با یک فرمان را فراهم می‌کند.

رمزگذاری ماشین‌های مجازی منطقی است زیرا بسیاری از شرکت‌ها اخیراً به ماشین‌های مجازی مهاجرت کرده‌اند، زیرا امکان مدیریت آسان‌تر دستگاه و استفاده کارآمدتر از منابع را فراهم می‌کنند.

باج افزار دیگری که سرورهای ESXi را هدف قرار می‌دهد!

در گزارشی جدید، تحلیلگران تهدید Uptycs فاش کردند که باینری‌های باج‌افزاری Black Basta جدید را شناسایی کرده‌اند که به‌طور خاص سرورهای VMWare ESXi را هدف قرار می‌دهند.

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

مانند سایر رمزگذارهای لینوکس، باج‌افزار Black Basta ، مسیر /vmfs/volumes / را روی سرور ESXi مورد حمله جستجو می‌کند. ماشین‌های مجازی، در این پوشه ذخیره می‌شوند (اگر چنین پوشه‌ای یافت نشد، باج‌افزار خارج می‌شود).

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 می‌کند. همچنین از مزایای پردازش چندنخی برای استفاده از چندین پردازنده و سرعت بخشیدن به فرآیند رمزگذاری استفاده می‌کند.

در حین رمزگذاری، باج‌افزار پسوند basta. را به نام فایل‌های رمزگذاری‌شده اضافه می‌کند و یادداشت‌هایی با نام readme.txt در هر پوشه ایجاد می‌کند.

این یادداشت ها 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 سیستم های 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 سیستم های 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 شرکت های سراسر جهان افزایش داد.

حتی اگر باج‌خواهی این گروه بین قربانیان متفاوت باشد، BleepingComputer حداقل یکی را می‌شناسد 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 RansomExx/Defray، Babuk، PureLocker، Snatch، GoGoogle، Mespinoza 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.»

مرکز آپا دانشگاه سمنان

آموزش

رفع آلودگی به باج افزار

رفع آلودگی

رفع آلودگی اولین کاریست که باید انجام شود چراکه در صورت باقی ماندن باج‌افزار در دستگاه، ممکن است تمام تلاش‌های بعدی برای بازیابی اطلاعات بی‌نتیجه باشد. به منظور رفع آلودگی راه‌های مختلفی وجود دارد که مهم‌ترین آنها به شرح زیر می‌باشند:

- 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 نکرده‌اید، می‌بایست از اتصال هرگونه تجهیزات جانبی ذخیره‌سازی به دستگاه آلوده خودداری نمایید. همچنین تا آن زمان سیستم مذکور می‌بایست در قرنطینه بوده و ارتباط شبکه‌ای با سایر دستگاه‌ها نداشته باشد.

مراحل حذف آلودگی باج افزار با کمک Restore Point

در صورتی که رایانه شما به باج‌افزار آلوده شده باشد و شما بخواهید این آلودگی را برطرف کنید می‌توانید 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 جهت‌دار گزینه mode safe را انتخاب کنید.
٤. با استفاده از نشانگر متنی که در صفحه ظاهر می‌شود، .exe rstrui را تایپ کنید.
٥. کلید Enter را فشار دهید.
٦. 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 نرم‌افزار معتبری دانلود کنید که توانایی غیرفعال کردن و حذف باج‌افزار از رایانه شما را داشته باشد.
۸. فایل نصبی نرم افزار را کپی کرده و در دستگاه آلوده به باج‌افزار نصب کنید.
۹. سیستم را به طور کامل اسکن کنید.
۱۰. تمام آلودگی‌های ایجاد شده توسط باج‌افزار را انتخاب کرده و آنها را از رایانه‌تان 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 پیچ یده باشد، رمزگشایی آنها بدون دسترسی به کلید ی که مهاجم در اختیار دارد، تقریبا غیرممکن است.

حذف آلودگی باج افزار با کمک Backup

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 کافیست آن را بازگردانید و به اکثر فایل‌ها خود دسترسی امن پیدا کنید. همانطور که می‌دانید تهیه نسخه پشتیبان نیز به روش‌های مختلف انجام می شود 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 زمان بیشتری می‌برد. برخی از بهترین ابزارهای تهیه نسخه پشتیبان در ادامه معرفی خواهند شد.

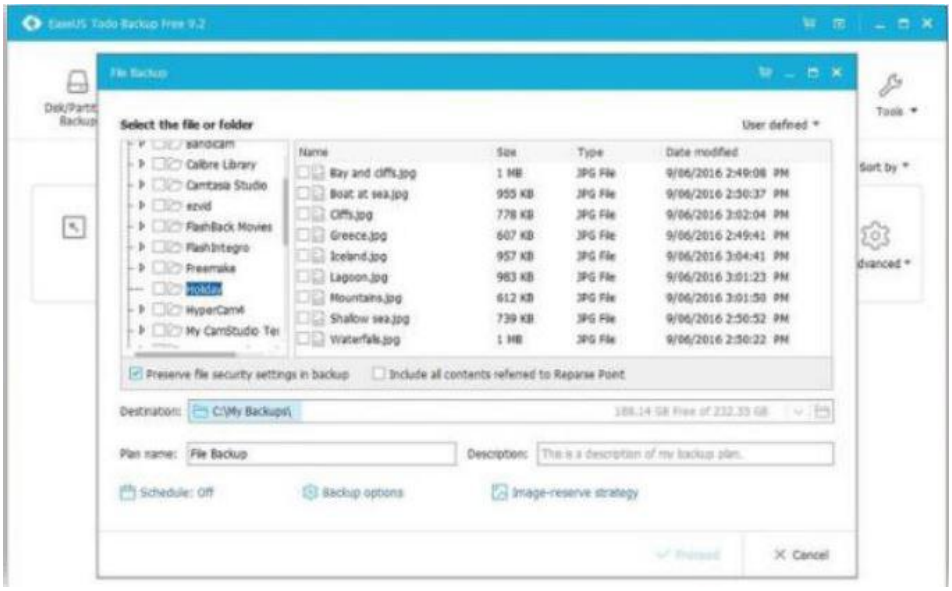
ابزار EaseUS Todo Backup Free

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

تکی و فولدرها، تمامی درایوها یا پارتیشن ها 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 معمولا بیشتر با آنها سر و کار دارید پشتیبان‌گیری می‌شوند و می توانید 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 تقریبا تمامی ویژگی‌های کارآمد را ارائه می‌دهد.مهمترین ویژگی‌های این برنامه را می‌توان به صورت زیر برشمرد:

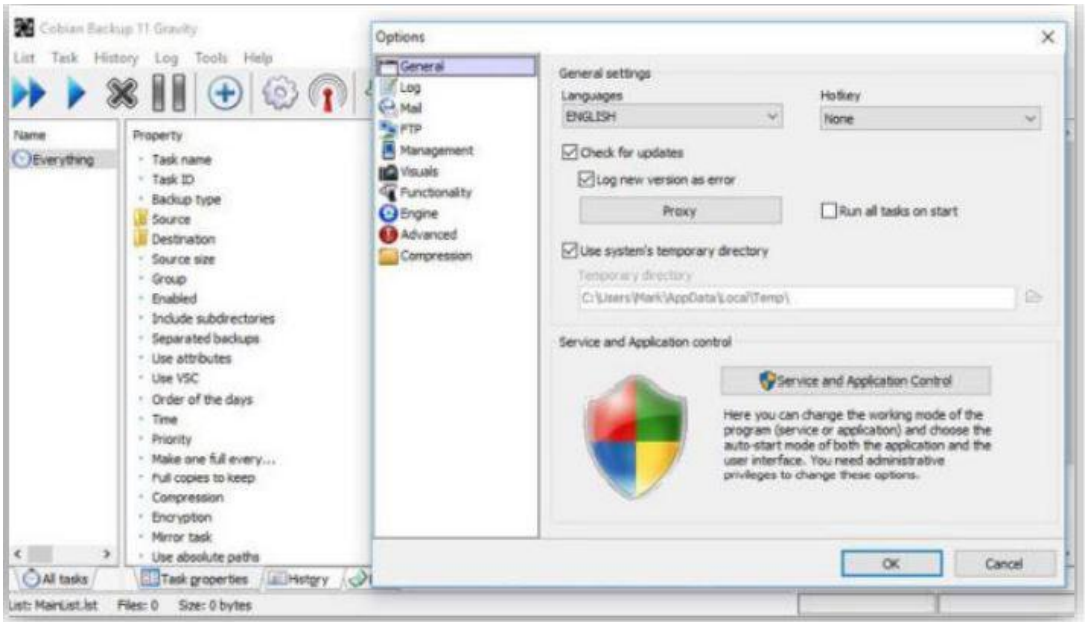
- پشتیبانی از انواع مدل‌های پشتیبان‌گیری
- برنامه‌دهی ساده
- پشتیبان‌گیری هوشمند و خودکار



ابزار Cobian Backup

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 مجازی 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 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 بکاپ گیری 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



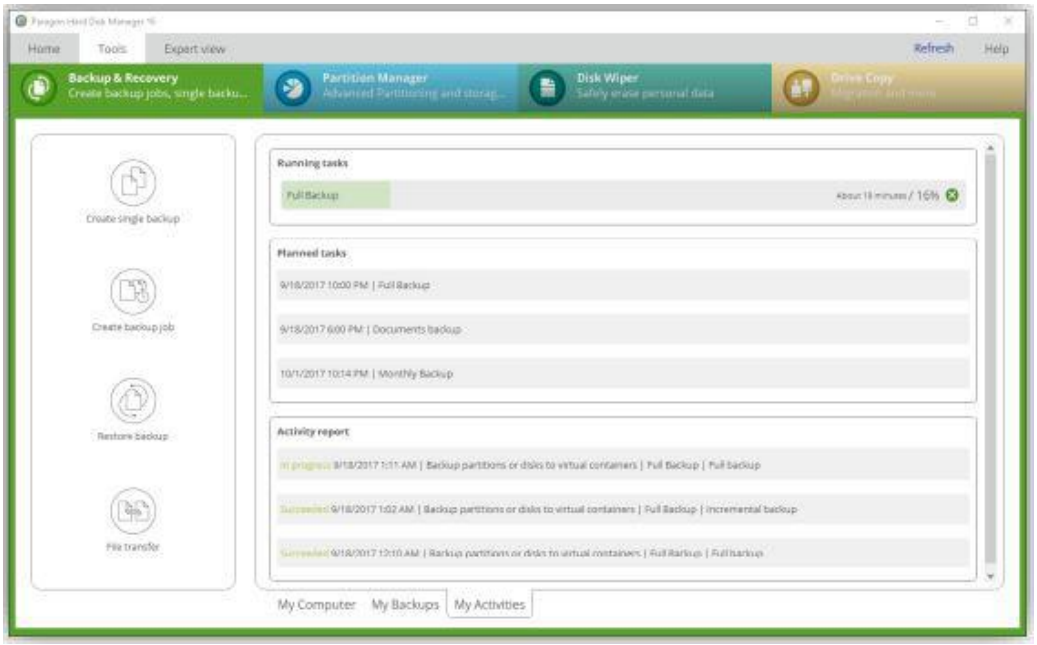
ابزار Paragon Backup & Recovery

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.

امکانات Paragon Backup & Recovery به اینجا ختم نمی‌شود و همانطور که از نام برنامه مشخص است، ابزار بازیابی 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 شخصی‌سازی زیاد
- مجهز به ریکاوری یا بازیابی پیشرفته

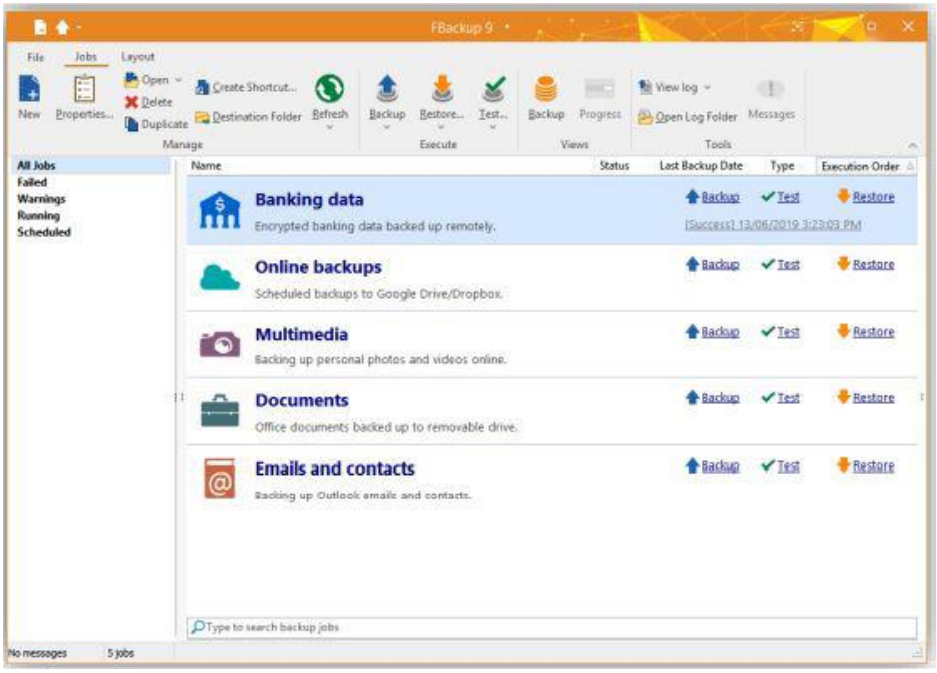


ابزار FBackup

ابـزار FBackup رابـط کاربـری مشـابه نرم‌افزارهـای آفیـس دارد کـه ممکـن اسـت چنـدان خوشـایند همـه نباشـد؛ امـا ایـن برنامـه صـرف نظـر از ظاهـر نـه چنـدان دلچسـب آن، ابـزاری توانمنـد در زمینـه‌ی پشـتیبان‌گیری بـه شـمار مـی‌رود؛ هرچنـد کـه از لحـاظ قابلیـت بـا نرم‌افزارهایـی ماننـد Par-agon Backup & Recovery در یـک رده قـرار نمـی گیـرد. امکاناتـی کـه FBackup در اختیـار می‌گـذارد، تنظیمـات مبتنـی بـر ویـزارد و حالت‌هـای پیشـرفته اسـت. هـر کـدام را کـه انتخـاب کنیـد، انجـام مراحـل پشـتیبان‌گیری سـاده خواهـد بـود. فایـل بـکاپ می‌توانـد در داخـل سیسـتم، درایوهـای شـبکه، دیسـک و حافظـه‌ی جانبـی یـا گـوگل درایـو ذخیـره شـود. بـه کمـک امـکان برنامه‌ریـزی انجـام بـکاپ، می‌توانیـد نسـخه‌ی پشـتیبان خـود را بـه‌روز نگـه داریـد.

مهمتریـن ویژگی‌هـای ایـن ابـزار عبارتنـد از:

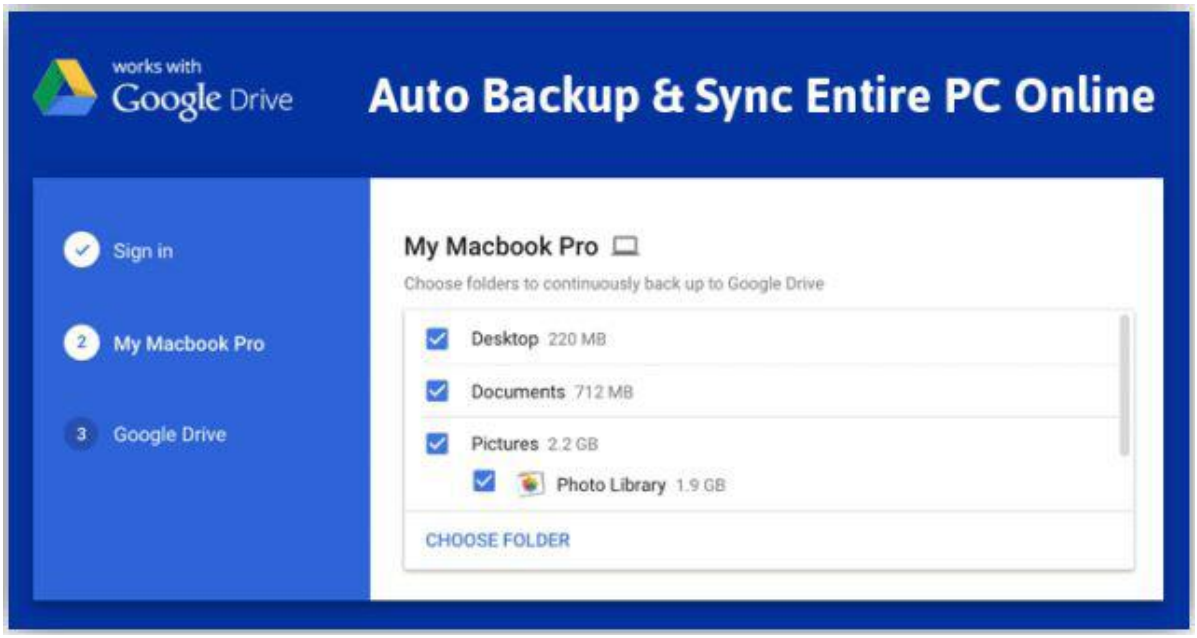
- برنامه‌ریزی خودکار
- تنظیمات مبتنی بر ویزارد
- فاقد رمزنگاری
- عدم پشتیبانی از بکاپ آخرین تغییرات



ابزار Google Backup and Sync

گـوگل بـکاپ ابـزاری مـدرن و مبتنـی بـر فضـای ابـری اسـت؛ یعنـی هرچقـدر در گـوگل درایـو فضـای بیشـتری در اختیار داشـته باشـید، فایـل بـکاپ شـما می‌توانـد پرحجم‌تـر باشـد. در ابتـدای اسـتفاده از ایـن ابـزار مقـدار فضـای رایـگان محـدودی در اختیـار شـما قـرار می‌گیـرد کـه راه‌هـای زیـادی بـرای افزایـش ایـن مقـدار بـدون هزینـه کـردن وجـود دارد. در مجمـوع بایـد گفـت نرم‌افـزار Google Backup and Sync بـرای پشـتیبان‌گیری از فایل‌هـای شـخصی مناسـب اسـت و بـه منظـور بـکاپ گرفتـن از کل سیسـتم کارآمـد نیسـت. بـرای بـکاپ گرفتـن از فایـل و فولدرهـای شـخصی بـا اسـتفاده از Google Backup and Sync کافـی اسـت هـر تعـداد فایـل و فولـدر را کـه مـد نظـر داریـد بـه برنامـه بدهیـد تـا برنامـه آنهـا را زیـر نظـر بگیـرد. در صـورت ایجـاد هـر گونـه تغییـر، حـذف و اضافـه در فایل‌هـا و فولدرهـای مذکـور، برنامـه بـه سـرعت همگام‌سـازی را انجـام خواهـد داد. همانطـور کـه از نـام نـرم افـزار بـر می‌آیـد، ایـن ابـزار می‌توانـد جهـت همگام‌سـازی فایل‌هـا بیـن رایانه‌هـای مختلـف مـورد اسـتفاده قـرار گیـرد. در ایـن صـورت، فایل‌هـای مـورد بحـث از طریـق اپلیکیشـن مبتنـی بـر وب گـوگل درایـو بـرای دسـتگاه‌های مختلـف در دسـترس خواهنـد بـود. Google Backup and Sync را فـارغ از محدودیـت حجمـی آن می‌تـوان ابـزاری عالـی بـرای پشـتیبان‌گیری بـه شـمار آورد. مهم‌تریـن ویژگی‌هـای ایـن ابـزار عبارتنـد از:

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



مرکز آپا دانشگاه سمنان

خبر کوتاه

آسیب‌پذیری روز صفر جدید آفیس در حملات استفاده می‌شود!

semCERT
@semcert

⚠️#آسیب‌پذیری روزصفر جدید آفیس درحملات استفاده می‌شود
محققان امنیتی یک آسیب‌پذیری جدید مایکروسافت آفیس راکه #Follina نامیده می‌شود،کشف کرده‌اند که درحملات برای اجرای دستورات مخرب PowerShell ازطریق Microsoft Diagnostic Tool (MSDT) به سادگی با بازکردن یک فایل Word 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

این آسیب‌پذیری، در را به روی یک بردار حمله حیاتی جدید باز می‌کند که از برنامه های #مایکروسافت #آفیس استفاده می کند؛ بدون امتیازات سطح بالا کار می کند، تشخیص Windows Defender را دور می زند و برای فعال کردن باینری ها یا اسکریپت ها نیازی به کد ماکرو ندارد.

semCERT
@semcert

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

✅ منبع: Bleeping_computer

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

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

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

semCERT
@semcert

پس از آن اگر ماکروها فعال باشند، از طریق فایل RTF، Snake Keylogger، 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...