خبرنامه الکترونیکی ۵۰

مرکز تخصصی آپا دانشگاه سمنان

شماره پنجاهم، سال پنجم، تیر ۱۴۰۱ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

بازگرداندن فایل‌های آلوده شده به باج‌افزار

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

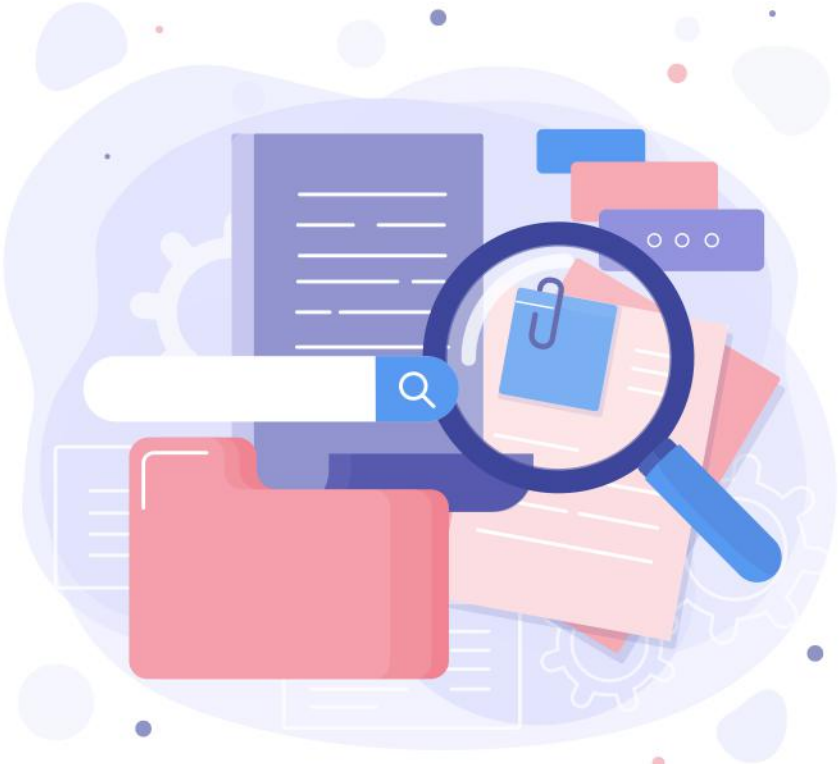
sec_rity بدون u کامل نیست.

فهرست

خبر

آموزش

خبرکوتاه



مرکز آپا دانشگاه سمنان

خبر

در پشتی در سرورهای exchange

مهاجمان از یک بدافزار تازه کشف شده برای در پشتی قرار دادن در سرورهای Microsoft Exchange متعلق به سازمان‌های دولتی و نظامی از اروپا، خاورمیانه، آسیا و آفریقا استفاده کردند.

این بدافزار که اولین بار در اوایل سال ۲۰۲۲ توسط محققان امنیتی کسپرسکی مشاهده شد و SessionManager نام گرفت، یک ماژول کد بومی مخرب برای نرم‌افزار وب‌سرور Microsoft's Internet Information Services[1] است.

این بدافزار حداقل از مارس ۲۰۲۱، درست پس از شروع موج عظیم حملات ProxyLogon در سال گذشته، بدون شناسایی مورد استفاده قرار گرفته است.

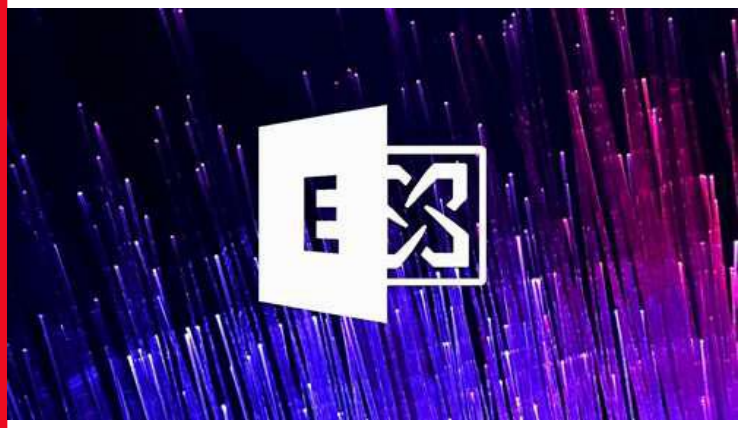
کسپرسکی روز پنجشنبه فاش کرد: «درپشتی SessionManager به عوامل تهدید امکان می‌دهد تا دسترسی مداوم، مقاوم در برابر به‌روزرسانی و نسبتاً پنهانی به زیرساخت فناوری اطلاعات یک سازمان هدف را حفظ کنند.

مجرمان سایبری پس از ورود به سیستم قربانی، می‌توانند به ایمیل‌های شرکت دسترسی پیدا کنند، دسترسی‌های مخرب بیشتری را با نصب انواع دیگر بدافزارها به‌روزرسانی کنند یا به‌طور مخفیانه سرورهای آسیب‌دیده را مدیریت کنند، که می‌تواند به عنوان زیرساخت مخرب مورد استفاده قرار گیرد.»

برخی از قابلیت‌های SessionManager عبارتند از:

- حذف و مدیریت فایل‌های دلخواه در سرورهای در معرض خطر
- اجرای فرمان از راه دور در دستگاه‌هایی که در پشتی دارند
- اتصال به نقاط پایانی در شبکه محلی قربانی و دستکاری ترافیک شبکه

در اواخر آوریل ۲۰۲۲، کسپرسکی در حالی که هنوز حملات را بررسی می‌کرد، فهمید که بیشتر نمونه‌های بدافزاری که قبلا شناسایی شدند هنوز در ۳۴ سرور ۲۴ سازمان مستقر هستند (هنوز تا ژوئن ۲۰۲۲ اجرا می‌شدند).



علاوه بر این، ماه‌ها پس از کشف اولیه، آنها هنوز توسط «یک سرویس اسکن فایل آنلاین محبوب[2]» به عنوان مخرب علامت‌گذاری نشده بودند.

پس از استقرار، ماژول مخرب IIS به اپراتورهای خود اجازه می‌دهد تا اعتبارنامه‌ها را از حافظه سیستم جمع کرده، اطلاعات را از شبکه قربانیان و دستگاه‌های آلوده جمع‌آوری کنند و پیلودهای اضافی را تحویل دهند (مانند بارگذار بازتابی Mimikatz مبتنی بر PowerSploit، Mimikatz SSP، ProcDump و ابزار قانونی تخلیه حافظه Avast).

پیر دلچر، محقق ارشد امنیتی، اضافه کرد: «سو استفاده از آسیب‌پذیری‌های سرور exchange از سه ماهه اول ۲۰۲۱ مورد علاقه مجرمان سایبری بوده است که به دنبال ورود به زیرساخت‌های مورد هدف هستند. SessionManager که اخیراً کشف شده به مدت یک سال به خوبی تشخیص داده نشده و هنوز مستقر است».

در مورد سرورهای Exchange، ما نمی‌توانیم به اندازه کافی بر آن تاکید کنیم: آسیب‌پذیری‌های سال گذشته آنها را به اهدافی عالی تبدیل کرده است، صرف نظر از اینکه نیت بدخواهانه چه باشد. بنابراین، این سرورها حتی اگر قبلاً مورد بازرسی و نظارت قرار نگرفته‌اند، از این به بعد باید به دقت مورد بازرسی و نظارت قرار گیرند.

1-IIS
2-virusTotal

کسپرسکی بدافزار SessionManager را کشف کرد در حالی که به جستجوی درهای پشتی IIS مشابه Owowa، یک ماژول مخرب IIS دیگر که توسط مهاجمان بر روی سرورهای Microsoft Exchange Outlook Web Access از اواخر سال ۲۰۲۰ برای سرقت اطلاعات کاربری Exchange مستقر شده بود، ادامه می‌داد.

پیوندهای گروه Gelsemium APT

بر اساس قربانی شناسی مشابه و استفاده از یک نوع سرور درپشتی HTTP به نام OwlProxy، کارشناسان امنیتی کسپرسکی معتقدند که درب پشتی SessionManager IIS در این حملات توسط عامل تهدید Gelsemium به عنوان بخشی از یک عملیات جاسوسی در سراسر جهان مورد استفاده قرار گرفته است.

این گروه هکر حداقل از سال ۲۰۱۴ فعال بوده است، زمانی که برخی از ابزارهای مخرب آن توسط آزمایشگاه امنیتی G DATA در حین بررسی کمپین جاسوسی سایبری «عملیات TooHash» مشاهده شد. در سال ۲۰۱۶، IoC[1] جدید Gelsemium در ارائه سیستم‌های Verint در طول کنفرانس HITCON ظاهر شد.

دو سال بعد، در سال ۲۰۱۸، VenusTech نمونه‌های بدافزار مرتبط با Operation TooHash و یک گروه APT ناشناخته را معرفی کرد که بعداً توسط شرکت امنیت اینترنتی اسلواکی ESET به‌عنوان نسخه‌های اولیه بدافزار Gelsemium برچسب‌گذاری شد.

ESET همچنین سال گذشته فاش کرد که محققان آن Gelsemium را به Operation NightScout، یک حمله زنجیره تامین که سیستم به‌روزرسانی شبیه‌ساز اندروید NoxPlayer برای ویندوز و macOS (با بیش از ۱۵۰ میلیون کاربر) را هدف قرار می‌دهد، پیوند داده‌اند تا بین سپتامبر ۲۰۲۰ تا ژانویه ۲۰۲۱ سیستم‌های گیمرها را آلوده کند.

به غیر از آن، گروه Gelsemium APT عمدتاً برای هدف قرار دادن دولت‌ها، تولیدکنندگان لوازم الکترونیکی و دانشگاه‌ها از شرق آسیا و خاورمیانه شناخته شده است و عمدتاً زیر رادار پرواز می‌کند.

۱-نشانگر نفوذ

صدها وب‌سایت و برنامه تحت تأثیر حمله روی NPM

یک حمله زنجیره تأمین NPM که مربوط به دسامبر ۲۰۲۱ است، از ده‌ها ماژول NPM مخرب حاوی کد جاوا اسکریپت مبهم‌سازی شده برای به خطر انداختن صدها برنامه و وب‌سایت دسکتاپ استفاده کرد.

همانطور که محققان در شرکت امنیتی زنجیره تأمین ReversingLabs کشف کردند، عوامل تهدید در پشت این کمپین[1] از typosquatting[2] برای آلوده کردن توسعه‌دهندگانی استفاده کردند که به دنبال بسته‌های بسیار محبوب مانند umbrellajs و ماژول‌های ionic.io NPM هستند.

اگر این توسعه‌دهندگان با نام‌گذاری ماژول که بسیار مشابه اصلی است فریب بخورند، عوامل تهدید بسته‌های مخربی را که برای سرقت داده‌ها از فرم‌های تعبیه‌شده (از جمله آن‌هایی که برای ورود به سیستم استفاده می‌شوند) طراحی شده‌اند، به برنامه‌ها یا وب‌سایت‌های آنها اضافه می‌کنند.

به عنوان مثال، یکی از بسته‌های مخرب NPM مورد استفاده در این کمپین (بسته آیکون) بیش از ۱۷۰۰۰ بار دانلود دارد و به گونه‌ای طراحی شده است که داده‌های فرم را به چندین دامنه تحت کنترل مهاجم منتقل کند.

کارلو زانکی، مهندس معکوس در ReversingLabs، می‌گوید «IconBurst متکی بر typo-squatting است، تکنیکی که در آن مهاجمان بسته‌هایی را از طریق مخزن‌هایی[3] با نام‌هایی که شبیه بسته‌های قانونی یا دارای غلط املایی رایج هستند، ارائه می‌دهند.»

علاوه بر این، شباهت‌های بین دامنه‌های مورد استفاده برای استخراج داده‌ها نشان می‌دهد که ماژول‌های مختلف در این کمپین تحت کنترل یک عامل واحد هستند.

برخی از ماژول‌های مخرب هنوز برای دانلود در دسترس هستند.

اگرچه که تیم ReversingLabs در ۱ ژوئیه ۲۰۲۲ با تیم امنیتی NPM تماس گرفت تا یافته‌های خود را گزارش کند، برخی از بسته‌های مخرب IconBurst هنوز در رجیستری NPM در دسترس هستند.

زانکی افزود: «در حالی که تعدادی از بسته‌های نام‌برده از NPM حذف شده‌اند، اکثر آنها هنوز در زمان انتشار این گزارش برای دانلود در دسترس هستند.»

از آنجایی که تعداد بسیار کمی از سازمان‌های توسعه‌دهنده توانایی شناسایی کدهای مخرب در کتابخانه‌ها و ماژول‌های open source را دارند، این حملات ماه‌ها قبل از اینکه مورد توجه ما قرار بگیرند ادامه یافت.»

اگرچه محققان می‌توانند فهرستی از بسته‌های مخرب مورد استفاده در حمله زنجیره تأمین IconBurst تهیه کنند، اما تأثیر آن هنوز مشخص نشده است، زیرا هیچ راهی برای دانستن اینکه چه مقدار داده و اعتبارنامه از طریق برنامه‌ها و صفحات وب آلوده از دسامبر ۲۰۲۱ به سرقت رفته است وجود ندارد.

تنها معیارهای موجود در آن زمان تعداد دفعاتی است که هر ماژول NPM مخرب نصب شده است و آمار ReversingLabs کاملاً شگفت‌آور است.

زانکی گفت: در حالی که گستره کامل این حمله هنوز مشخص نیست، بسته‌های مخربی که ما کشف کردیم احتمالاً توسط صدها، یا حتی هزاران اپلیکیشن موبایل و دسکتاپ و همچنین وب‌سایت‌ها استفاده می‌شود.

«کدهای مخرب همراه با ماژول‌های NPM در تعداد ناشناخته‌ای از برنامه‌های کاربردی موبایل و دسکتاپ و صفحات وب اجرا می‌شوند و مقادیر بی‌شماری از داده‌های کاربر را جمع‌آوری می‌کنند.»

«ماژول‌های NPM که تیم ما شناسایی کرده است، مجموعاً بیش از ۲۷۰۰۰ بار دانلود شده‌اند.»

۱-معروف به IconBurst

۲-حمله مبتنی بر شباهت املایی

3-repositories

نگذارید دیگران زباله ها؟
شما را بازیافت و
به طلا (اطلاعات)
تبدیل کنند.

مرکز آپا دانشگاه سمنان

آموزش

بازگرداندن فایل‌های آلوده شده به باج‌افزار

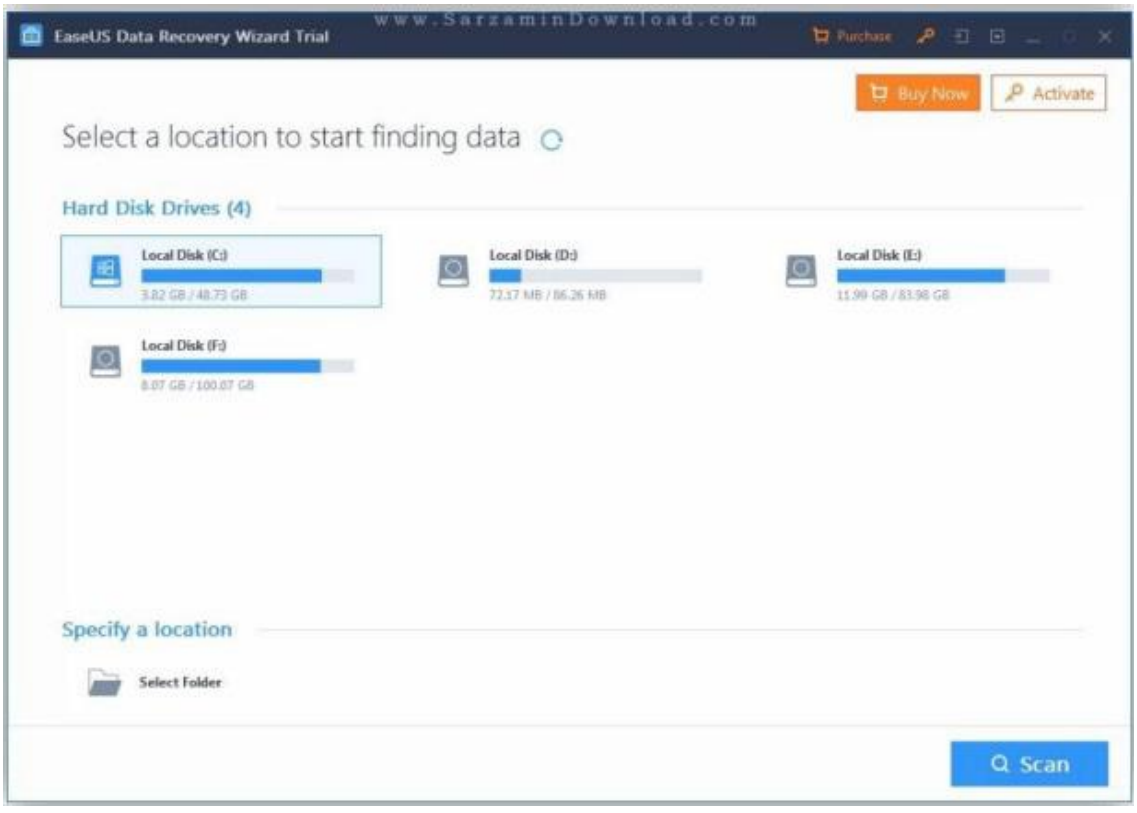
شاید این سوال مطرح شود که ریکاوری کردن هارد دیسک، دستگاهی که مورد حمله باج‌افزاری قرار گرفته است چه کارایی ممکن است داشته باشد؟ در پاسخ باید گفت خوشبختانه تعداد زیادی از باج‌افزارها بدین صورت عمل می‌کنند که هریک از فایل‌های شما را رمزنگاری کرده و سپس فایل اصلی را حذف می‌کنند. بنابراین اگر ظرفیت دیسک شما به حدی باشد که اطلاعات حذف شده رونویسی نشده باشند به راحتی می‌توان با ریکاوری هارد دیسک بخشی از اطلاعات را بازگرداند.

در ادامه برخی از بهترین ابزارهای ریکاوری معرفی خواهند شد.

ابزار EaseUS Data Recovery Wizard

این برنامه از رابط کاربری خلاقانه و ساده‌ای بهره می‌برد. در صفحه اصلی هرآنچه برای بازیابی اطلاعات هارد و کارت حافظه نیاز داشته باشید، در اختیارتان قرار می‌گیرد. نرم افزار Wizard Recovery Data EaseUS کار خود را در سه مرحله اسکن، پیش نمایش و ریکاوری انجام می‌دهد. این نرم افزار اطلاعات را در مسیرها و انواع مختلف بخش‌بندی می‌کند و به همین دلیل می‌توانید به راحتی موقعیت فایل را متوجه شده و آن را از مسیر اصلی یا نوع آن مانند فایل صوتی، تصویری، ایمیل یا اسناد بازیابی کنید. برای این کار شاید نیازی به اسکن صدها یا هزاران سند نداشته باشید چرا که امکان جستجو در این نرم‌افزار وجود دارد و همچنین درون آن فیلترهایی مانند حجم فایل و همچنین تاریخ ایجاد آن نیز به چشم می‌خورد.

اگر نتوانستید یک فایل حذف شده را پیدا کنید، درون فولدرهایی با عنوان «RAW Files» یا «Label RAW Files» را جستجو کنید. در این فولدرها فایل‌هایی که نام یا مسیر اصلی خود را گم کرده‌اند، ذخیره می‌شوند. از این برنامه علاوه بر کامپیوتر و کارت حافظه، می‌توانید برای ریکاوری اطلاعات از دستگاه‌های صوتی مانند آیپاد نیز استفاده کنید. در نسخه پولی به تمام قابلیت‌های آن دست پیدا می‌کنید و امکان نسخه کامل نرم‌افزار EaseUS Data Recovery Wizard در سایت‌های داخلی وجود دارد.



ابزار Stellar Data Recovery

یکی دیگر از بهترین و قوی‌ترین نرم‌افزارهای بازیابی اطلاعات هارد و کارت حافظه، Stellar Data Recovery نام دارد که درون آن شخصی‌سازی اسکن نوع اطلاعات برای شما ممکن است. برای مثال اگر به دنبال یک فایل ویدیویی باشید، می‌توانید تنها گزینه ویدیوها را فعال کرده و سایر گزینه‌ها را غیرفعال کنید تا سریع‌تر به فایل موردنظر خود دسترسی پیدا کنید.

اگر تنها انتخاب فایل‌های ویدیویی برای شما مناسب نیست و به دنبال جستجوی بهتر و دقیق‌تری هستید، می‌تواند فرمت دقیق فایل موردنظرتان را نیز انتخاب کنید. برای مثال می‌توانید به نرم افزار Stellar Data Recovery دستور دهید که تنها به دنبال فایل‌های ویدیویی با فرمت MP4 باشد یا اینکه تنها تصاویر با فرمت PNG را جستجو کند. چنین کاری ساده است، هرچند باید در منوی تنظیمات آن را شخصی‌سازی کنید. این ابزار برای سیستم عامل ویندوز و مک او اس موجود است و همانطور که می‌توان انتظار داشت، بهترین ویژگی‌های آن در نسخه پولی به چشم می‌خورد که هزینه‌ای برابر ۷۹ دلار در هر سال از کاربران درخواست می‌کند. در نسخه رایگان می‌توانید تا ۱ گیگابایت اطلاعات را بازیابی کنید که برای فایل‌های سبک مانند اسناد مناسب است. لازم به ذکر است که امکان دانلود کرک نرم‌افزار Stellar Data Recovery در سایت‌های داخلی وجود دارد.

ابزار Disk Drill

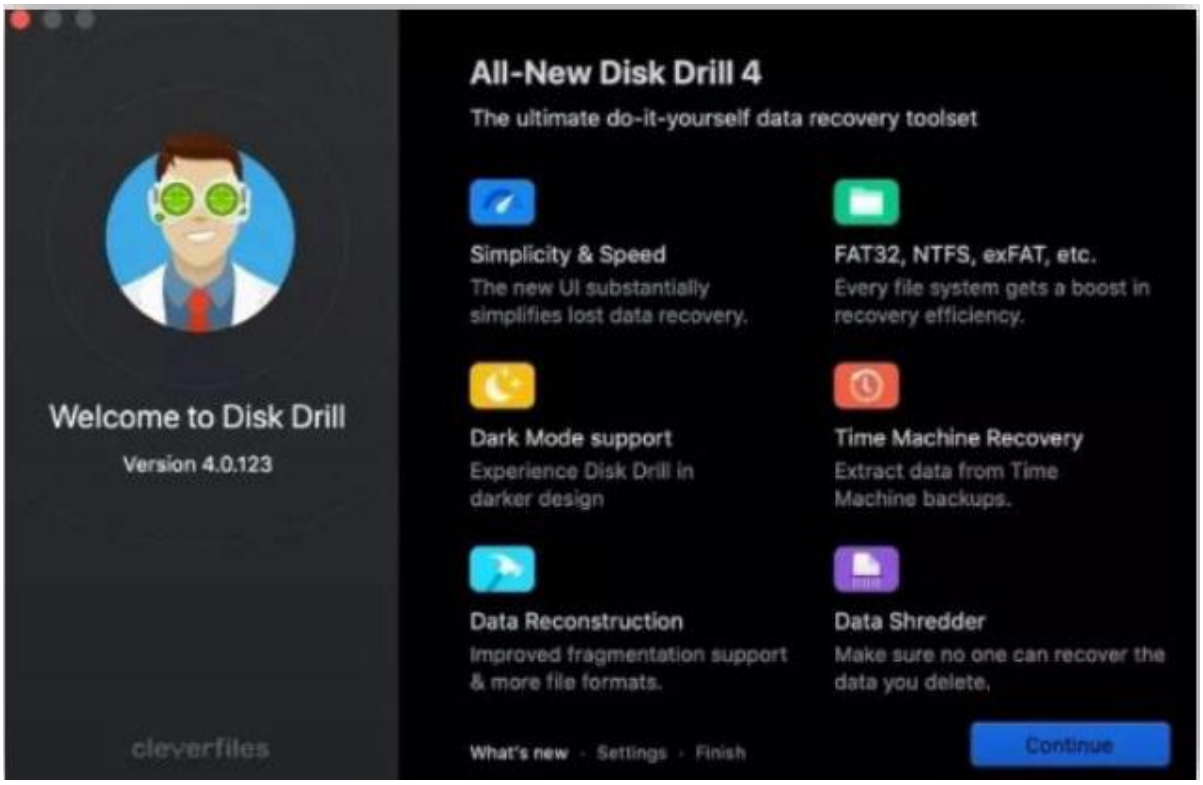
نرم‌افزار Disk Drill یک ابزار فوق‌العاده برای بازیابی اطلاعات محسوب می‌شود که کارایی بیش از بازیابی اطلاعات هارد و کارت حافظه دارد. این ابزار دارای بخش‌هایی برای ریکاوری فایل‌های حذف شده در سیستم عامل iOS و اندروید است. این نرم‌افزار از چندین روش بازیابی برای ریکاوری اطلاعات حذف شده استفاده می‌کند که در ادامه نگاه دقیق‌تری به آنها خواهیم داشت. درون نرم‌افزار Disk Drill با سه روش برای بازیابی اطلاعات روبه رو هستیم:

اسکن سریع: این روش سریع و مناسب اطلاعاتی است که اخیرا حذف شده‌اند و بیشتر برای فایل‌هایی که به تازگی از سطل زباله حذف کرده‌اید، مناسب است. کارایی این روش بستگی به مدت زمان حذف فایل‌ها دارد، برای مثال اگر به دنبال ریکاوری یک فایل دو ساعت پس از حذف باشید، شانس این کار بسیار بالاتر از فایلی است که ۴۸ ساعت از حذف آن می‌گذرد.

تخصیص اطلاعات موجود: در صورتی که نمی‌توانید یک فایل را درون اکسپلورر کامپیوتر ویندوزی خود یا فایندر مک او اس پیدا کنید، به سراغ این روش بازیابی بروید.

تمام روش‌های ریکاوری: در این روش شاهد استفاده از ترکیبی از دو شیوه بالا هستیم تا موقعیت فایل‌های حذف شده را پیدا کرده و آنها را بازیابی کند.

اسکن دیسک شما با توجه به اطلاعات موجود در آن، چندین دقیقه طول می‌کشد، اما پیش از اتمام اسکن نرم افزار Disk Drill امکان بررسی موارد پیدا شده را برای شما فراهم می‌کند.



برای جلوگیری از انتشار ویروس
به سیستم خود، از دانلود فایل‌های
ناشناس بپرهیزید.

مرکز آپا دانشگاه سمنان

خبر کوتاه

AstraLocker 2.0 کاربران را مستقیماً از پیوست‌های Word آلوده می‌کند!

semCERT
@semcert

🔴 AstraLocker 2.0 کاربران را مستقیماً از پیوست‌های #Word آلوده می‌کند!

نوع #باج‌افزار کمتر شناخته شده به نام #AstraLocker اخیراً دومین نسخه اصلی خود را منتشر کرده است و به گفته تحلیلگران تهدید،

semCERT
@semcert

اپراتورهای آن درگیر حملات سریعی هستند که کد خود را مستقیماً از طریق پیوست‌های ایمیل انتقال می‌دهند.
این رویکرد کاملاً غیرمعمول است زیرا در حملات ایمیلی معمولاً مراحل میانی وجود دارند که به گریز از روش‌های امنیتی کمک می‌کنند، اما در این مورد، این مراحل حذف شده‌اند.

semCERT
@semcert

فریب استفاده شده توسط اپراتورهای AstraLocker 2.0 یک سند #مایکروسافت ورد است که یک شیء OLE دارای باج‌افزار را پنهان می‌کند.
برای اجرای #بدافزار، کاربر باید روی «اجرا» در هشداری که پس از باز کردن سند ظاهر می‌شود، کلیک کند و این امر نیز شانس موفقیت عامل‌های تهدید را کاهش می‌دهد.

semCERT
@semcert

به نظر نمی‌رسد این تهدید، کار یک عامل حرفه‌ای باشد، بلکه بیشتر مصمم است تا حد امکان حملات مخرب را انجام دهد.

✅ منبع : Bleeping_Computer

باگ روز صفر فایروال Sophos

semCERT
@semcert

⚠️باگ روز صفر #فایروال Sophos# چند هفته قبل از رفع مشکل مورد سوء استفاده قرار گرفت!

هکرهای چینی (گروه DriftingCloud) از یک آسیب‌پذیری روز صفر با شدت بحرانی در فایروال Sophos برای به خطر انداختن یک شرکت و نفوذ به وب‌سرورهای میزبانی شده توسط قربانی استفاده کردند.

semCERT
@semcert

از این #آسیب‌پذیری برای دور زدن احراز هویت که بر پورتال کاربر و وب‌ادمین فایروال Sophos تأثیر می‌گذارد و برای اجرای کد دلخواه از راه دور می‌توان سوء استفاده کرد.
محققان می‌گویند که دسترسی به فایروال Sophos اولین گام حمله بود

semCERT
@semcert

و به دشمن اجازه داد تا حمله مرد میانی (MitM) را از طریق دستکاری پاسخ‌های DNS برای وب‌سایت‌های خاص تحت مدیریت شرکت قربانی انجام دهد.

semCERT
@semcert

مهاجم در این تلاش موفق بوده است زیرا با استفاده از کوکی‌های جلسه به سرقت رفته به صفحات مدیریت CMS دسترسی پیدا کرده و افزونه File Manager را برای مدیریت (آپلود، دانلود، حذف و ویرایش) فایل‌ها در وب‌سایت نصب کرده است.

✅ منبع : Bleeping_computer

Skimmer کارت اعتباری WooCommerce از ربات تلگرام برای استخراج اطلاعات سرقت شده استفاده می‌کند

semCERT
@semcert

⚠ Skimmer کارت اعتباری WooCommerce از ربات تلگرام برای استخراج اطلاعات سرقت شده استفاده می‌کند

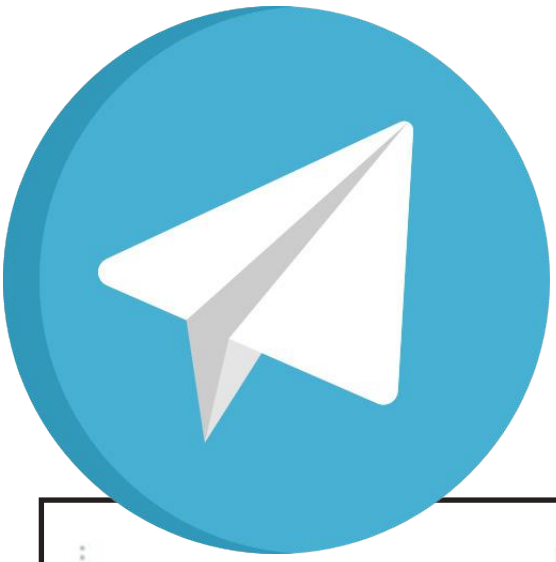
WordPress/WooCommerce به سرعت تبدیل به برترین پلتفرم CMS برای بدافزارهای اسکیمینگ کارت اعتباری شده است و درطول سال گذشته از Magento ودیگر پلتفرم‌های تجارت الکترونیک پیشی گرفته است.

semCERT
@semcert

به تازگی #اسکیمر جدیدی کشف شده است که از #woocommerce استفاده میکند.
اولین بخش این اسکیمر، در فایلی به نام script.js قرار دارد، یک فایل سفارشی که به تِم محبوب فروشگاه Storefront WooCommerceاضافه شده و در صفحه پرداخت موجود است.

semCERT
@semcert

اسکریپت مخرب از btoa تابع جاوا اسکریپت برای سریال سازی و سپس کدگذاری base64 محتوا استفاده می کند.
سپس آن را به همراه فایل feed-rss-comments.php واقع در پوشه فایل‌های اصلی wp-includes ارسال می‌کند.
در اینجا feed-rss-comments.php به هیچ وجه یک فایل اصلی #وردپرس نیست.



semCERT
@semcert

بعد از گرفتن اطلاعات ارسال شده از script.js ،اقدامات زیر را انجام می دهد:

- ورودی ارائه شده به آن، اطلاعات کاربر و IP را دریافت می‌کند
- محتوای کدگذاری شده base64 را رمزگشایی می‌کند
- از API تلگرام برای ارسال آن محتوا به یک ربات چت تعیین شده از طریق CURL استفاده می‌کند

semCERT
@semcert

بنابراین، هر بار که سفارشی در وب‌سایت آلوده ثبت شود، جزئیات کارت اعتباری به اتاق چت تلگرام منتقل شده (جایی که به سرعت در بازار سیاه فروخته می‌شود) و منجر به تراکنش‌های جعلی روی کارت‌های اعتباری قربانی می‌شود.

semCERT
@semcert

با توجه به ماهیت رمزگذاری شده سرویس ارتباطی، #تلگرام به عنوان یک سرویس مفید برای مهاجمان دیده می شود. این به مهاجمان اجازه می دهد تا داده ها را به سرقت ببرند در حالی که می توانند در پشت پوشش ناشناس پنهان شوند.

✅ منبع :

blog.sucuri.net
Website Security News | Sucuri Blog

دوره آموزشی مجازی
Network+
بارویکرد امنیتی

مدت دوره: ۳۰ ساعت
شروع دوره: یکشنبه ۹ مرداد ۱۴۰۱
پایان دوره: پنج‌شنبه ۲۷ مرداد ۱۴۰۱
زمان برگزاری:
یکشنبه‌ها و سه شنبه‌ها ساعت ۱۵ الی ۱۹
و پنج‌شنبه‌ها ساعت ۹ الی ۱۳
پیش‌نیاز: علاقه‌مندی به شبکه و امنیت
آزمون: پنج‌شنبه ۳ شهریور
هزینه دوره: ~~۷۸۰۰۰۰ تومان~~ ۶۵۰۰۰۰ تومان

مدرس:
مهندس غزاله مصطفایی علائی
کارشناس ارشد مهندسی کامپیوتر،
فعال حوزه امنیت فناوری اطلاعات

اعطای گواهی معتبر از
مرکز آپا دانشگاه سمنان
دارای مجوز رسمی از سازمان
فناوری اطلاعات ایران

@semcert
@semcert_admin
023-31535021
info.cert@semnan.ac.ir

جهت ثبت نام به وب‌سایت https://cert.semnan.ac.ir مراجعه کنید.

دوره آموزشی مجازی
طراحی امن وب‌سایت و فروشگاه اینترنتی با وردپرس

مدت دوره: ۳۰ ساعت
شروع دوره: جمعه ۱۴ مرداد ۱۴۰۱
پایان دوره: پنج‌شنبه ۳۱ شهریور ۱۴۰۱
زمان برگزاری:
جمعه‌ها ساعت ۹ الی ۱۳
پیش‌نیاز: آشنایی با کامپیوتر
آزمون: جمعه ۱ مهر ۱۴۰۱
هزینه دوره: ~~۶۵۰۰۰۰ تومان~~ ۵۸۰۰۰۰ تومان

مدرس:
مهندس محمدرضا عرب عامری
دانشجو کارشناسی ارشد مهندسی کامپیوتر،
۶ سال سابقه طراحی وب‌سایت با وردپرس

پروژه نهایی این دوره، ساخت وب‌سایت شخصی شماست.

اعطای گواهی معتبر از
مرکز آپا دانشگاه سمنان
دارای مجوز رسمی از سازمان
فناوری اطلاعات ایران

@semcert
@semcert_admin
023-31535021
info.cert@semnan.ac.ir

جهت ثبت نام به وب‌سایت https://cert.semnan.ac.ir مراجعه کنید.

تلاش ما
حفظ امنیت
شماست...