خبرنامه الکترونیکی ۴۸

مرکز تخصصی آپا دانشگاه سمنان

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

در این شماره می‌خوانید:

علائم آلودگی به باج‌افزار و اقدامات پس از آن

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

حفاظت از آینده
با تأمین امنیت امروز...

مرکز آپا دانشگاه سمنان

فهرست

خبر

مشاهده بدافزار جدید مخفی Nerbian RAT در حملات مداوم ۵

بدافزاری که داده‌های مرورگر و کیف پول‌های ارزهای دیجیتال را سرقت می‌کند ۷

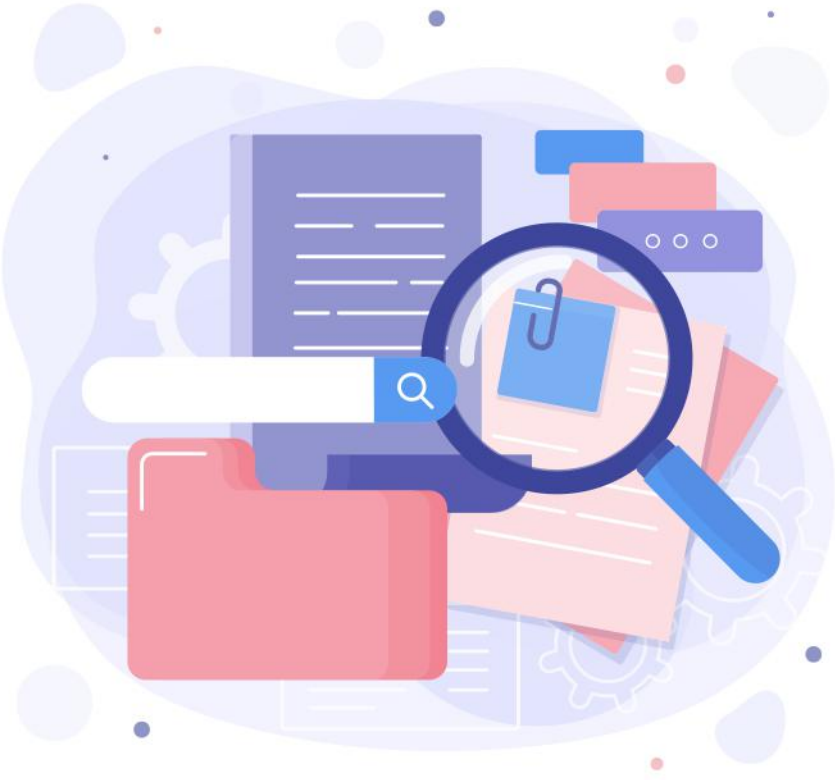
مایکروسافت: بدافزار جدید از باگ ویندوز سوء استفاده می‌کند ۱۰

آموزش

علائم آلودگی به باج‌افزار و اقدامات پس از آن ۱۳

خبرکوتاه

بدافزارهایی که وعده افزایش قابلیت اینستاگرام را می‌دهند! ۱۸



مرکز آپا دانشگاه سمنان

خبر

مشاهده بدافزار جدید مخفی Nerbian RAT در حملات مداوم

یک تروجان دسترسی از راه دور جدید به نام Nerbian RAT کشف شده است که شامل مجموعه‌ای غنی از ویژگی‌ها، از جمله توانایی فرار از شناسایی و تجزیه و تحلیل توسط محققان است.

نوع جدید بدافزار در Go نوشته شده است و آن را به یک تهدید ٦٤ بیتی بین پلتفرمی تبدیل می‌کند و در حال حاضر از طریق یک کمپین توزیع ایمیل در مقیاس کوچک که از پیوست‌های سند با ماکروها استفاده می‌کند، توزیع می‌شود.

این کمپین‌های ایمیل توسط محققان Proofpoint کشف شد.

جعل هویت سازمان جهانی بهداشت

کمپین بدافزار توزیع کننده Nerbian RAT، هویت سازمان بهداشت جهانی[1] را جعل می‌کند و ظاهراً اطلاعات COVID-19 را به اهداف ارسال می‌کند.

پیوست‌های RAR حاوی اسناد Word هستند که با کد ماکرو مخرب آغشته شده‌اند، بنابراین اگر در مایکروسافت آفیس با محتوای «فعال» باز شود، یک فایل bat یک مرحله اجرای PowerShell را برای دانلود یک بدافزار ٦٤ بیتی انجام می‌دهد.

بدافزار با نام "UpdateUAV.exe" نیز به زبان Golang نوشته شده است و در UPX بسته بندی شده است تا اندازه را قابل کنترل نگه دارد.

UpdateUAV از کدهای پروژه های مختلف GitHub استفاده مجدد می‌کند تا مجموعه ای غنی از مکانیسم های ضد تجزیه و تحلیل و تشخیص فرار را قبل از استقرار Nerbian RAT ترکیب کند.

جدای از آن، بدافزار همچنین با ایجاد یک کار برنامه ریزی شده که هر ساعت آن RAT را راه اندازی می کند، پایداری را ایجاد می‌کند.

1-WHO

Proofpoint فهرست ابزارهای ضد تحلیل را به شرح زیر خلاصه می‌کند:

- بررسی وجود برنامه‌های مهندسی معکوس یا اشکال زدایی در لیست فرآیندها
- بررسی آدرس‌های مک مشکوک
- بررسی رشته‌های WMI تا ببینید آیا نام دیسک‌ها مشروع هستند یا خیر
- بررسی اینکه آیا اندازه هارد دیسک زیر ۱۰۰ گیگابایت است یا خیر، زیرا اندازه زیر ۱۰۰ گیگابایت برای ماشین‌های مجازی معمول است
- بررسی اینکه آیا برنامه‌های تجزیه و تحلیل حافظه یا تشخیص دستکاری در لیست فرآیندها وجود دارد یا خیر
- بررسی مدت زمان سپری شده از زمان اجرا و مقایسه آن با یک آستانه تعیین شده
- استفاده از IsDebuggerPresent API برای تعیین اینکه آیا فایل اجرایی در حال اشکال زدایی است یا خیر

همه این بررسی‌ها عملاً اجرای RAT را در یک محیط sandbox شده مجازی غیرممکن می‌کند و از مخفی بودن طولانی‌مدت برای اپراتورهای بدافزار اطمینان می‌دهد.

ویژگی های Nerbian RAT

تروجان به عنوان "MoUsoCore.exe" دانلود می‌شود و در "C:\ProgramData\USOShared\" ذخیره می‌شود. چندین عملکرد را پشتیبانی می‌کند، در حالی که اپراتورهای آن این امکان را دارند که آن را با برخی از آنها پیکربندی کنند.

دو مورد از عملکردهای قابل توجه آن عبارتند از یک keylogger که ضربه‌های کلید را به صورت رمزگذاری شده ذخیره می‌کند و یک ابزار تصویربرداری از صفحه که روی همه پلتفرم‌های سیستم عامل کار می‌کند.

ارتباطات با سرور C۲ از طریق SSL (لایه سوکت‌های امن) انجام می‌شود، بنابراین همه تبادل داده‌ها رمزگذاری شده و از بازرسی حین انتقال از ابزارهای اسکن شبکه محافظت می‌شوند.

مواظب بودن

بدون شک، Proofpoint بدافزار جدید و جالب و پیچیده‌ای را شناسایی کرده است که از طریق بررسی‌های متعدد، ارتباطات رمزگذاری شده و مبهم سازی کد بر مخفی بودن تمرکز می‌کند.

با این حال، در حال حاضر، Nerbian RAT از طریق کمپین‌های ایمیل با حجم کم توزیع می‌شود، بنابراین هنوز یک تهدید بزرگ نیست، اما اگر نویسندگان آن تصمیم بگیرند تجارت خود را به روی جامعه جرایم سایبری گسترده تر باز کنند، ممکن است شرایط تغییر کند.

۶ مشاهده بدافزار جدید مخفی Nerbian RAT در حملات مداوم

بدافزاری که داده‌های مرورگر و کیف پول‌های ارزهای دیجیتال را سرقت می‌کند

ویندوز ۱۱ جعلی بدافزار است.

هکرها با ارتقا جعلی ویندوز ۱۱ که همراه با بدافزاری است که داده‌های مرورگر و کیف پول‌های ارزهای دیجیتال را سرقت می‌کند، کاربران ناآگاه را جذب می‌کنند.

این کمپین در حال حاضر فعال است و با تکیه بر مسموم کردن نتایج جست‌وجو، وب سایتی را push می‌کند که از صفحه تبلیغاتی مایکروسافت برای ویندوز ۱۱ تقلید می‌کند تا بدافزار سارق اطلاعات را توزیع کند.

مایکروسافت یک ابزار ارتقا به کاربران ارائه می‌دهد تا بررسی کند که آیا دستگاه آن‌ها از آخرین سیستم عامل این شرکت پشتیبانی می‌کند یا خیر. یکی از الزامات پشتیبانی از ماژول پلتفرم مورد اعتماد[1]، نسخه ۲٫۰ است که در ماشین‌هایی که بیش از چهار سال سن ندارند وجود دارد.

هکرها کاربرانی را طعمه قرار می‌دهند که بدون صرف وقت برای یادگیری اینکه سیستم عامل باید مشخصات خاصی را برآورده کند، به نصب ویندوز ۱۱ می پردازند.

وب سایت مخربی که ویندوز ۱۱ جعلی را ارائه می دهد هنوز فعال است. این سایت لوگو رسمی مایکروسافت، favicons و دکمه دعوت‌کننده «اکنون دانلود کنید» را دارد.

اگر بازدیدکننده وب‌سایت مخرب را از طریق اتصال مستقیم بارگیری کند (دانلود از طریق TOR یا VPN در دسترس نیست)، یک فایل ISO دریافت خواهد کرد که فایل اجرایی بدافزار سرقت اطلاعات جدید را در خود مخفی کرده است.

1-TPM

فرآیند آلودگی

به گفته CloudSEK، عوامل تهدید در پشت این کمپین از بدافزار جدیدی استفاده می‌کنند که محققان به دلیل استفاده از نصب کننده Inno Setup Windows آن را «Inno Stealer» نامیدند.

محققان می‌گویند که Inno Stealer هیچ شباهت کدی با سایر دزدهای اطلاعاتی که در حال حاضر در گردش هستند ندارد و شواهدی مبنی بر آپلود بدافزار در پلتفرم اسکن ویروس توتال پیدا نکرده‌اند.

فایل لودر (مبتنی بر دلفی) فایل اجرایی «setup ۱۱ Windows» موجود در ISO است، که پس از راه‌اندازی، یک فایل موقت به نام tmp.is-PN۱۳۱ می‌سازد و فایل TMP دیگری ایجاد می‌کند که لودر در آن ۳۰۷۸ کیلوبایت داده می‌نویسد.

CloudSEK توضیح می‌دهد که لودر فرآیند جدیدی را با استفاده از CreateProcess Windows API ایجاد می‌کند و به ایجاد فرآیندهای جدید، ایجاد ماندگاری و نصب چهار فایل کمک می‌کند.

ماندگاری با افزودن یک فایل .LNK[1] در دایرکتوری Startup و استفاده از icacls.exe برای تنظیم مجوزهای دسترسی آن برای مخفی کاری به دست می آید.

دو فایل از چهار فایل ایجاد شده عبارتند از اسکریپت فرمان ویندوز برای غیرفعال کردن امنیت رجیستری، اضافه کردن استثناهای Defender، حذف نصب محصولات امنیتی و حذف حجم سایه[2].

به گفته محققان، این بدافزار راه‌حل‌های امنیتی Emsisoft و ESET را نیز حذف می‌کند، احتمالاً به این دلیل که این محصولات آن را مخرب تشخیص می‌دهند.

فایل سوم یک ابزار اجرای دستور است که با بالاترین امتیازات سیستم اجرا می شود. و چهارمین فایل، یک اسکریپت VBA است که برای اجرای dfl.cmd مورد نیاز است.

درمرحله‌دوم‌آلودگی،فایلی‌باپسوند.SCRدردایرکتوری\\:C:\Users\AppData\Roaming\Windows۱۱InstallationAssistant سیستم در معرض خطر قرار می گیرد.

این فایل محموله دزد اطلاعات را باز می‌کند و با ایجاد یک فرآیند جدید به نام «Windows۱۱InstallationAssistant.scr»، آن را اجرا می کند.

قابلیت های Inno Stealer

قابلیت‌های Inno Stealer برای این نوع بدافزارها معمول است، از جمله جمع‌آوری کوکی‌های مرورگر وب و اطلاعات کاربری ذخیره شده، داده‌ها در کیف پول‌های ارزهای دیجیتال و داده‌های سیستم فایل.

مجموعه مرورگرهای مورد هدف و کیف پول های رمزنگاری گسترده است، از جمله Opera، Brave، Edge، Chrome، 360 Browser، Vivaldi و Comodo.

سارق همچنین می تواند محموله های اضافی را دریافت کند، عملی که فقط در شب انجام می شود، احتمالاً برای استفاده از دوره ای که قربانی پای رایانه نیست.

قابلیت‌های این محموله های اضافی شامل سرقت اطلاعات کلیپ‌بورد و استخراج داده‌های شمارش دایرکتوری است.

نکات امنیتی

کل وضعیت ارتقاء ویندوز ۱۱ زمینه مناسبی را برای گسترش این کمپین ها ایجاد کرده است و این اولین بار نیست که چنین چیزی گزارش می شود.

توصیه می‌شود از دانلود فایل‌های ISO از منابع مبهم خودداری کنید و فقط ارتقاهای اصلی سیستم‌عامل را از داخل کنترل پنل ویندوز ۱۰ خود انجام دهید یا فایل‌های نصب را مستقیماً از منبع دریافت کنید.

اگر ارتقاء به ویندوز ۱۱ در دسترس شما نیست، تلاش برای دور زدن محدودیت ها به صورت دستی فایده ای ندارد، زیرا این کار با مجموعه ای از جنبه های منفی و خطرات امنیتی شدید همراه خواهد بود.

۱-میانبر

2-shadow volume

مجرم سایبری

گرگ در لباس گوسفند

بدترین اقدامات،

هوشمندانه انجام می‌شوند.

مرکز آپا دانشگاه سمنان

مایکروسافت:
بدافزار جدید از باگ ویندوز
سوء استفاده می‌کند!

مایکروسافت بدافزار جدیدی را کشف کرده است که توسط گروه هک هافنیوم مورد حمایت چین برای حفظ ماندگاری بر روی سیستم‌های ویندوز در معرض خطر با ایجاد و پنهان کردن وظایف برنامه‌ریزی شده استفاده می‌شود.

این گروه پیش از این شرکت‌های دفاعی آمریکا، اتاق‌های فکر و محققان حملات سایبری را هدف قرار داده است.

این گروه همچنین یکی از گروه‌های حمایت شده دولتی است که به گفته مایکروسافت با بهره‌برداری مقیاس جهانی سال گذشته از ProxyLogon مرتبط بوده است. ProxyLogon نقص روز صفری بود که بر تمام نسخه‌های Microsoft Exchange پشتیبانی شده تأثیر می‌گذاشت.

ماندگاری از طریق حذف مقدار رجیستری ویندوز

تیم تشخیص و پاسخ مایکروسافت[1] گفت: «در حالی که مایکروسافت به دنبال کردن عامل تهدید HAFNIUM با اولویت بالا ادامه می‌دهد، فعالیت‌های جدیدی کشف شده است که از آسیب‌پذیری‌های روز صفر وصله نشده به عنوان بردارهای اولیه استفاده می‌کند.»

«بررسی بیشتر مصنوعات سرنخ‌های فارنزیک، استفاده از ابزار Impacket برای حرکت در عرض و اجرا و یک بدافزار گریز از دفاع به نام Tarrask را نشان می‌دهد که وظایف برنامه‌ریزی شده «پنهان» ایجاد می‌کند و اقداماتی را برای حذف ویژگی‌های وظیفه برای پنهان کردن وظایف برنامه‌ریزی شده از روش‌های سنتی شناسایی انجام می‌دهد.»

این ابزار هک که Tarrask نام دارد از یک باگ ناشناخته ویندوز استفاده می‌کند تا با حذف مقدار رجیستری مربوط به Security Descriptor آن‌ها را از «schtasks /query» و Task Scheduler پنهان کند.

گروه تهدید از این وظایف برنامه‌ریزی شده «پنهان» برای حفظ دسترسی به دستگاه‌های هک شده حتی پس از راه‌اندازی مجدد با برقراری مجدد اتصالات قطع شده به زیرساخت‌های فرمان و کنترل (C۲) استفاده کرده است.

در حالی که اپراتورهای Hafnium می‌توانستند تمام آثار به جا مانده بر روی دیسک، از جمله تمام کلیدهای رجیستری و فایل XML اضافه شده به پوشه سیستم را حذف کنند تا تمام آثار فعالیت‌های مخرب خود را پاک کنند، این کار باعث از بین رفتن ماندگاری در راه‌اندازی مجدد می‌شد.

1-DART

نحوه دفاع در برابر حملات Tarrask

وظایف «پنهان» را فقط می‌توان با بازرسی دستی دقیق‌تر رجیستری ویندوز پیدا کرد. به این منظور، باید به دنبال وظایف برنامه‌ریزی شده بدون مقدار SD[1] در task key بگردید.

مدیران سیستم همچنین می‌توانند لاگ‌های Security.evtx و Microsoft-Windows-TaskScheduler/Operational.evtx را برای بررسی رویدادهای کلیدی مرتبط با وظایف «پنهان» با بدافزار Tarrask فعال کنند.

مایکروسافت همچنین توصیه می‌کند ثبت لاگ را برای ‹TaskOperational› در Microsoft-Windows-TaskScheduler/Operational Task Scheduler log فعال کنید و بر روی اتصالات خارجی از دارایی‌های مهم طبقه صفر و طبقه یک نظارت داشته باشید.

DART افزود: «عاملان تهدید در این کمپین از وظایف برنامه‌ریزی شده پنهان برای حفظ دسترسی به دارایی‌های حیاتی در معرض اینترنت با برقراری مجدد ارتباطات خروجی با زیرساخت‌های C&C استفاده کردند.»

«ما می‌دانیم که وظایف برنامه‌ریزی شده ابزاری مؤثر برای دشمنان است تا وظایف خاصی را در حین دست‌یابی به پایداری خودکار انجام دهند، که باعث می‌شود ما آگاهی را در مورد این تکنیکی که اغلب نادیده گرفته شده است افزایش دهیم.»

۱-مشخص‌کننده امنیتی

مرکز آپا دانشگاه سمنان

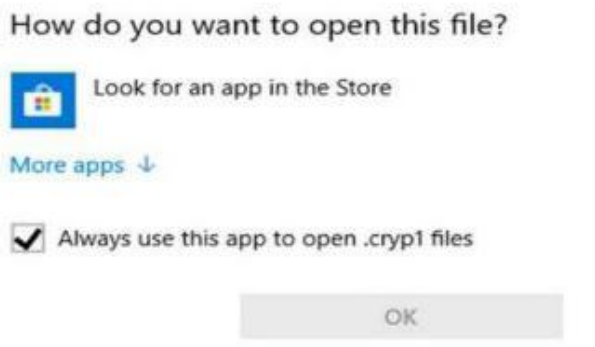
آموزش

علائم آلودگی به باج افزار و اقدامات پس از آن

علائم وقوع آلودگی به باج‌افزار

در خصوص حملات باج‌افزاری یک جمله معروف وجود دارد که می گوید «باج افزارها پر سر و صداتر از آن هستند که صدای آنها را نشنوید!» به عبارت دیگر باج‌افزارها در مرحله نفوذ و رمزنگاری فایل‌ها ممکن است مخفی بمانند ولی پس از آن تمام سعی خود را می‌کنند تا شما را از آلودگی مطلع سازند. در واقع ساز و کار و هدف باج‌افزارها این است که پس از آلوده شدن دستگاه، قربانی متوجه آن شده و نسبت به پرداخت باج اقدام نماید. لیکن در صورتی که علائم مشکوک زیر را در دستگاه خود مشاهده کردید ممکن است در مراحل اولیه آلودگی باج‌افزاری باشید:

۱. پردازش CPU بیش از حد طبیعی درگیر شده است.
۲. فن دستگاه با سرعت زیاد و غیر طبیعی کار می‌کند.
۳. میزان درگیر بودن هارد دستگاه به صورت غیرطبیعی افزایش یافته است.
٤. برخی از فایل‌ها از دسترس خارج شده‌اند و اجرا نمی‌شوند.
۵. نام یا پسوند برخی از فایل‌ها تغییر یافته است و در هنگام اجرا پیغام ناشناس بودن نوع فایل داده می‌شود.



٦. تصویر پس‌زمینه به صورت ناخواسته تغییر کرده است.
۷. پیغامی مبنی بر قفل شدن دستگاه و یا فایل‌ها دریافت کنید.

روش‌های تخصصی شناسایی باج‌افزارها

عموما پس از اینکه سیستم به باج‌افزار آلوده شود پس از گذشت مدتی، خود را اظهار کرده و تقاضای باج می‌کند. لیکن به صورت کلی ۳ روش تخصصی در این حوزه وجود دارد که معمولا سازندگان آنتی ویروس‌ها از آن استفاده کرده و با کمک آن می‌توانند پیش از آنکه باج‌افزار خودش اعلام و اظهار وجود کند، آلوده شدن دستگاه به آن را تشخیص دهند.

- روش مبتنی بر امضاء: این روش بدین صورت است که پس از کشف هر باج‌افزار، یک امضاء دیجیتال منحصر به فرد برای آن در نظر می‌گیرند و آن را به دیکشنری باج‌افزارها اضافه می‌کنند. سپس اگر برنامه‌ای قصد ورود به سیستم را داشته باشد و یا بر روی سیستم نصب باشد و قصد اجرا شدن داشته باشد، با این امضاءها مقایسه می‌شود و در صورت تطابق، به عنوان باج افزار شناسایی می‌شود.
- روش تحلیل داینامیک: در این روش بر خالف روش مبتنی بر امضاء، هدف شناسایی باج‌افزارهایی که قبلا شناخته شده‌اند نیست و به جای آن رفتار همه برنامه‌ها را نظر گرفته می‌شود و در صورتی که هرکدام از آنها رفتار مخرب و مشکوکی مشابه باج‌افزارها داشته باشند فورا شناسایی شده و از ادامه فعالیت آن جلوگیری می‌شود.
- روش ترکیبی: همانطورکه مشخص است، روش مبتنی بر امضاء، از دستگاه شما در برابر باج‌افزارهای شناخته شده محافظت می‌کند و روش تحلیل داینامیک نیز در سعی در کشف باج افزارهای جدید و ناشناخته دارد. به همین دلیل اکثر آنتیویروس‌های استاندارد از هر دو روش برای حفظ و برقراری امنیت دستگاه استفاده می‌کنند و یکی از دلایل کاهش سرعت سیستم پس از نصب آنتیویروس، همین موضوع است.

اقدامات ضرروی در صورت آلوده شدن به بدافزار

۱. **خاموش کردن رایانه مشکوک**: در صورتی که سیستمی که از آن استفاده می‌کنید علائمی مانند کند شدن، استفاده غیر معمول از اینترنت، قفل شدن یک فایل و... را از خود بروز دهد می‌بایست بلافاصله آن را خاموش کرده و از اینترنت جدا کنید.

۲. **جدا کردن سیستم آلوده از شبکه:** پس از خاموش کردن کامپیوتر مشکوک، اقدام بعدی که باید انجام شود این است که آن دستگاه را از سایر رایانه‌ها و دستگاه‌های ذخیره‌سازی موجود در شبکه محلی خود جدا نمایید. توجه داشته باشید که ممکن است بیش از یک سیستم آلوده وجود داشته باشد، به این معنی که باج افزار ممکن است از طریق چند رایانه وارد سازمان یا خانه شما شده باشد و هنوز در بعضی از سیستم‌ها خود را نشان ندهد. به همین دلیل ممکن است تمامی سیستم‌های متصل به شبکه آلوده شده باشند. اقدامات لازم را برای اطمینان از آلوده نشدن همه سیستم‌ها انجام دهید.

۳. شناسایی باج افزار: وب‌سایت‌های بی‌شماری وجود دارند که به شما در شناسایی باج‌افزار کمک می‌کنند. شناسایی نوع بدافزار به شما کمک می کند بفهمید با چه نوع باج‌افزاری روبرو هستید، چگونه انتشار می‌یابد، چه پرونده‌هایی را رمزگذاری می‌کند و گزینه‌های پیش روی شما برای مقابله با آن چیست.

٤. **کمک گرفتن از متخصصین:** بهتر است قبل از هر اقدامی به پیغام باج‌افزار دقت بیشتری کنید و از متخصصین امنیت و IT استفاده کنید. در برخی موارد، ابزارهای جانبی توسط شرکت‌های امنیتی معرفی می‌شوند که می‌توانند فایل‌های رمزگذار ی شده توسط برخی باج افزارهای خاص را رمزگشایی کنند.

۵. **بررسی شبکه:** می‌بایست تمام دستگاه‌های متصل به شبکه، توسط افراد متخصص برای یافتن تاثیر بدافزار در سایر نقاط شبکه مورد بررسی قرار گیرند.

٦. **تشخیص راه آلودگی:** به منظور جلوگیری از حملات مشابه می‌بایست راه آلودگی سیستم مشخص شده و برای آن چاره اندیشی گردد.

۷. **تعیین کردن گزینه‌های پیش روی برای مقابله با باج‌افزار:** گزینه‌های شما هنگام آلوده شدن به باج‌افزار عبارتند از: پرداخت هزینه درخواستی، حذف باج افزار و یا پاک کردن کل سیستم و نصب مجدد ویندوز. به طور کلی پرداخت پول درخواستی ایده خوبی تلقی نمی‌شود. این امر بیشتر باج‌افزار را به گرفتن باج بیشتر ترغیب می‌کند و در بسیاری از موارد نمی‌توانید قفل پرونده‌های رمزگذاری شده را باز کنید. ممکن است بتوانید با رمزگشاهای رایگان بخشی از فایل‌های رمزگذاری شده باج‌افزار را بازیابی کنید. پس از حمله باج‌افزار، بازیابی اطلاعات باج‌افزار کار دشواری خواهد بود خصوصاً اگر به باج‌افزار Encryption آلوده شده باشد. چون در بسیاری موارد باج‌افزار از الگوریتم‌های پیشرفته و پیچیده استفاده

می‌کنـد ممکـن اسـت هنـوز رمزگشـاهای آن هـا ارایـه نشـده باشـد. حتـی اگـر رمزگشـایی وجـود داشـته باشـد مشـخص نیسـت کـه نسـخه مناسـبی بـا بدافـزار را پوشـش دهـد. از طرفـی حتـی اگـر تصمیـم بـه پرداخـت هزینـه بگیریـد، ممکـن اسـت نتوانیـد داده‌هـای خـود را پـس بگیریـد.

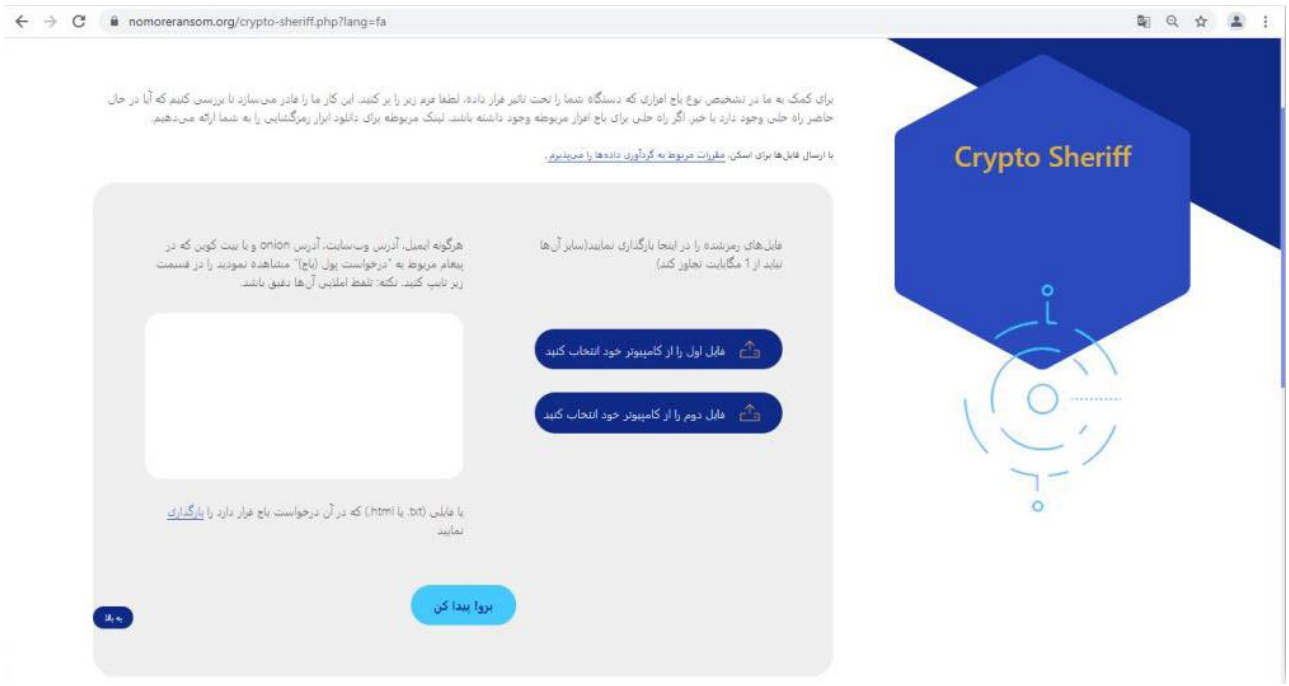
۸. **حفاظـت از فایل‌هـای رمـز شـده:** فایل‌هایـی کـه رمزنـگاری شـده‌اند و موفـق بـه بازگردانـدن آنهـا نشـده‌اید را در جـای امنـی نگـه‌داری کنیـد چراکـه معمـولا پـس از گذشـت چنـد مـاه از انتشـار بدافـزار، شـرکت‌های امنیتـی موفـق بـه ارائـه کلیـد آن خواهنـد شـد و در ایـن صـورت امـکان دسترسـی مجـدد بـه فایل‌هـای قفـل شـده وجـود دارد.

نحوه شناسایی نوع باج‌افزار

همانطـور کـه در علـم پزشـکی بـرای مقابلـه بـا یـک بیمـاری، تشـخیص نـوع آن بسـیار حائـز اهمیـت اسـت، در علـم کامپیوتـر نیـز تشـخیص نـوع حملـه و نـوع ویـروس یـا باج‌افـزاری کـه سیسـتم را آلـوده کـرده اسـت، یـک اصـل اساسـی می‌باشـد. لـذا مـا نیـاز بـه راهـکاری داریـم کـه بـا دنبـال کـردن آن بتوانیـم در صـورت وقـوع حملـه باج‌افـزاری، نـوع آن را تشـخیص دهیـم. خوشـبختانه چنـد ابـزار کارآمـد در ایـن خصـوص سـاخته شـده اسـت کـه در ادامـه آنهـا را معرفـی می‌کنیـم.

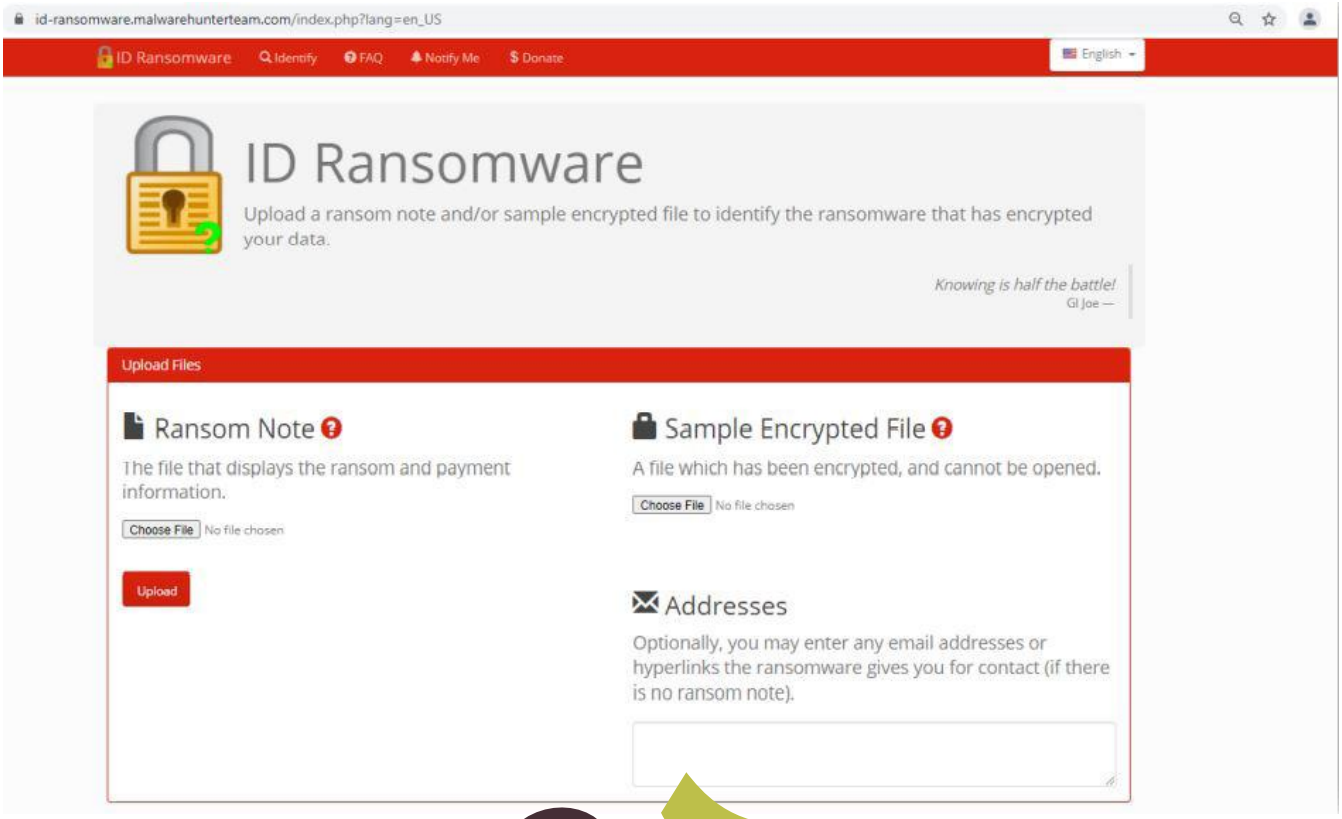
- ابزار Crypto Sheriff from No More Ransom

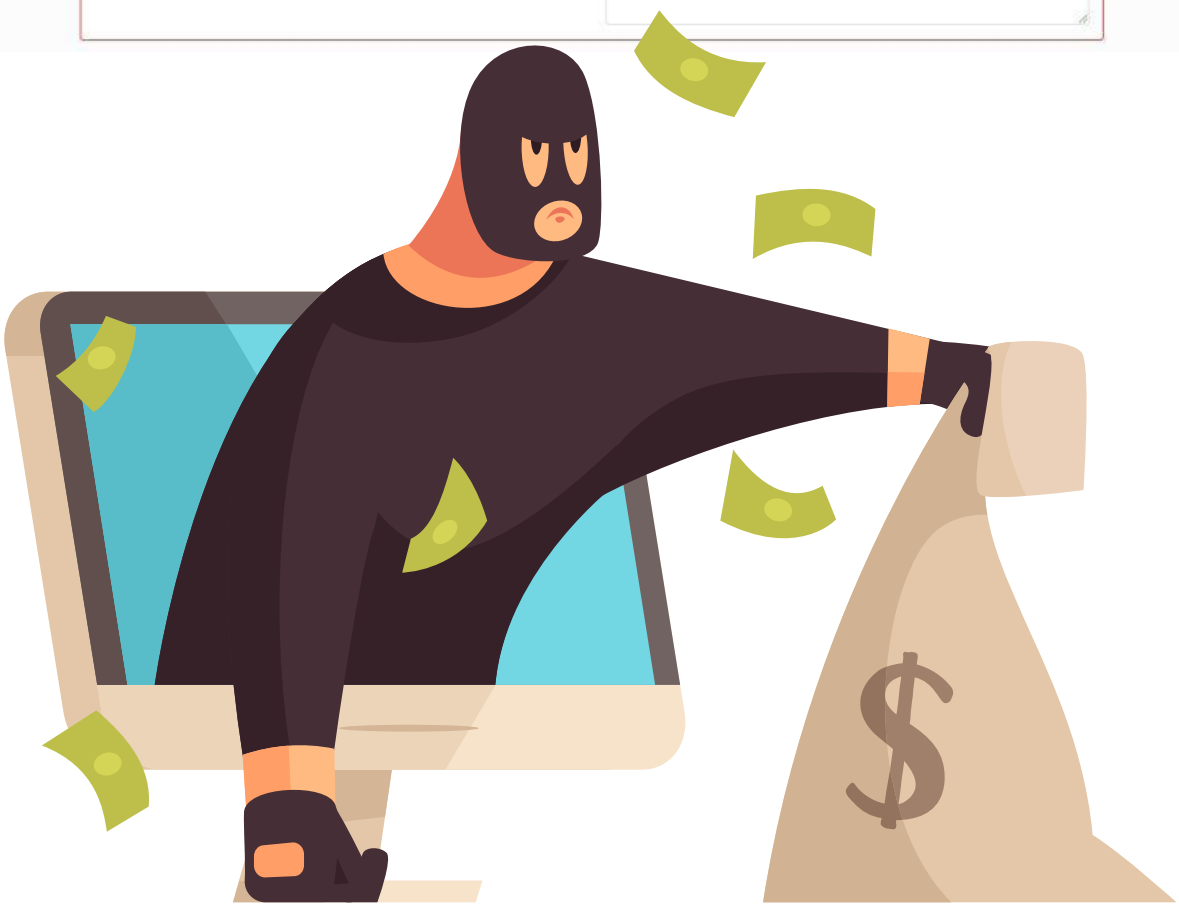
ابـزار Crypto Sheriff یکـی از کارآمدتریـن ابزارهـای موجـود در زمینـه تشـخیص نـوع باج‌افـزار می‌باشـد کـه از آدرس انترنتـی https://www.nomoreransom.org/crypto-sheriff.php قابـل دسترسـی اسـت. بـا ورود بـه ایـن سـایت همانطورکـه در قسـمت توضیحـات آن آمـده اسـت می‌بایسـت نمونـه فایل‌هـای رمزشـده را در آن آپلـود کـرد و یـا هرگونـه ایمیـل، آدرس وب‌سـایت، آدرس onion و یـا بیـت کویـن کـه در پیغـام مربـوط بـه «درخواسـت پـول (بـاج)» مشـاهده نمودیـد را وارد کنیـد و پـس از آن، ایـن ابـزار شـروع بـه بررسـی کـرده و عـلاوه بـر اینکـه نـوع باج‌افـزار را مشـخص می‌کنـد در صـورت امـکان راه‌حـل بـرای رمزگشـایی، آن را ارائـه می‌دهـد.



- ابزار ID Ransomware from MalwareHunter Team

این ابزار نیز برای تشخیص نوع باج‌افزاری که سیستم را آلوده کرده است بسیار کاربردی است. تنها کافی است به آدرس https://id-ransomware.malwarehunterteam.com مراجعه کرده و نمونه فایل رمز شده، یادداشت راهنمایی پرداخت باج که هکر برای شما گذاشته است و یا هر آدرس ایمیل، URL، آدرس کیف پول دیجیتال و... که از باج افزار دارید را در سایت آپلود کنید. سپس منتظر بمانید تا نوع باج‌افزار تشخیص داده شود.





مرکز آپا دانشگاه سمنان

خبر کوتاه

بدافزارهایی که وعده افزایش قابلیت اینستاگرام را می‌دهند!

semCERT
@semcert

⚠️بدافزارهایی که وعده افزایش قابلیت #اینستاگرام را می‌دهند

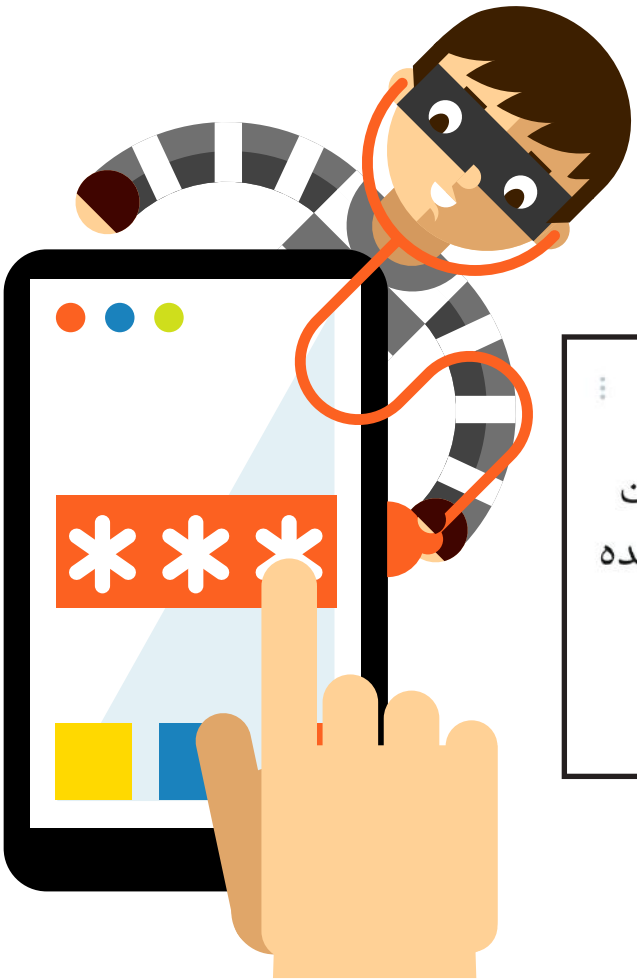
تیم تحقیقاتی موبایل #mcafee دو بدافزار جدید #اندروید را که کاربران اینستاگرامی را مورد هدف قرار می‌دهند کشف کردند. یکی کاربرانی که می‌خواهند تعداد لایک آخرین پستشان یا فالوئرهایشان را افزایش دهند و

semCERT
@semcert

دیگری کاربرانی است که از قابلیت‌های پیش‌فرض اینستاگرام راضی نیستند.

برنامه‌های مختلف تغییر اینستاگرام در حال حاضر برای کاربران در اینترنت وجود دارد.

بدافزار دوم وانمود می‌کند که یک برنامه MOD (برنامه‌ای که توسط سازنده اصلی یا برنامه ساخته نشده است-Modified (mobile App



semCERT
@semcert

محبوب است که از آپلود تصاویر با کیفیت بالا و دانلود عکس‌ها و فیلم‌های ارسال شده پشتیبانی می‌کند، اما در اصل اعتبارنامه اینستاگرام را می‌دزدد.

✅ منبع: mcafee

تلاش ما
حفظ امنیت
شماست...