



مرکز آپ دانشگاه سمنان

خبرنامه الکترونیکی

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 می خوانید:

علام آسودگی به باج افزار
و اقدامات پس از آن



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

حافظت از آینده

با تأمین امنیت امروز...



مرکز آمادگی و امنیت
دانشگاه همدان

فهرست

خبر

۵

مشاهده بدافزار جدید مخفی Nerbian RAT در حملات مداوم

۷

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

۱۰

مايكروسافت: بدافزار جدید از باگ ويندوز سوء استفاده می‌کند

آموزش

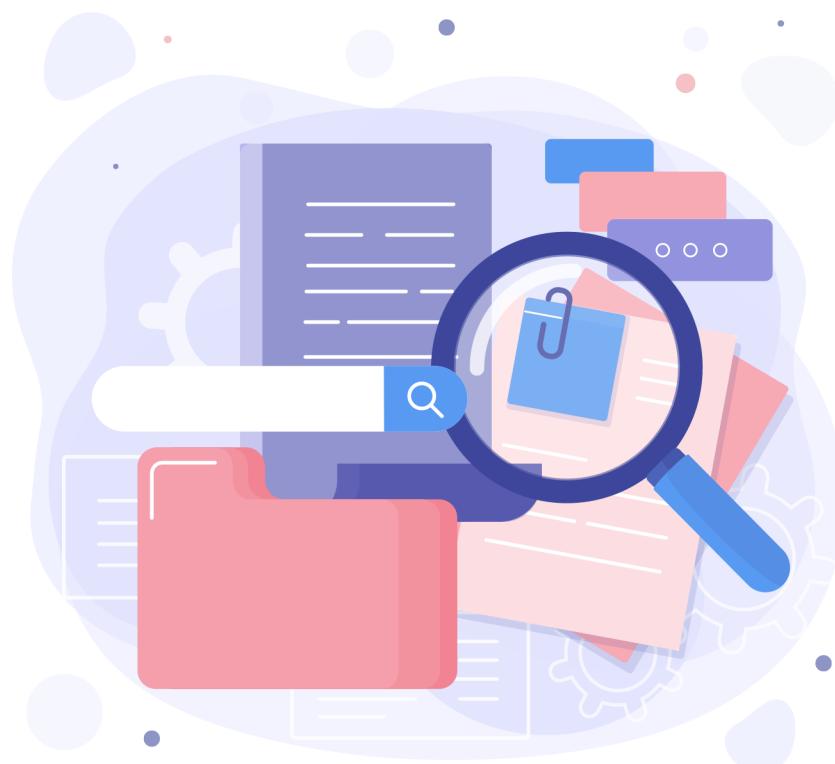
۱۳

علائم آلودگی به باج‌افزار و اقدامات پس از آن

خبرکوتاه

۱۸

بدافزارهایی که وعده افزایش قابلیت اينستاگرام را می‌دهند!





مرکز آپادانشگاه سمنان

خبر

Nerbian RAT مشاهده بدافزار جدید مخفی

در حملات مداوم

بیوستهای 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 ۶۴ 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.

GitHub از کدهای پروژه‌های مختلف UpdateUAV استفاده مجدد می‌کند تا مجموعه‌ای غنی از مکانیسم‌های ضد تجزیه و تحلیل و تشخیص فرار را قبل از استقرار Nerbian RAT ترکیب کند.

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

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 G0 نوشته شده است و آن را به یک تهدید ۶۴ بیتی بین پلتفرمی تبدیل می‌کند و در حال حاضر از طریق یک کمپین توزیع ایمیل در مقیاس کوچک که از بیوستهای 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 بهداشت جهانی^۱ را جعل می‌کند و ظاهراً اطلاعات COVID-19 را به اهداف ارسال می‌کند.



1-WHO



Nerbian RAT ویژگی های

تروعان به عنوان "MoUsCore.exe" دانلود می شود و در "C:\ProgramData\USOShared\" ذخیره می شود. چندین عملکرد را پشتیبانی می کند، 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 ضربه های کلید را به صورت رمزگذاری شده ذخیره می کند و یک ابزار تصویربرداری از صفحه که روی همه پلتفرم های سیستم عامل کار می کند. ارتباطات با سرور C2 از طریق SSL (لایه سوکت های امن) انجام می شود، بنابراین همه تبادل داده ها رمزگذاری شده و از بازرسی حین انتقال از ابزارهای اسکن شبکه محافظت می شوند.

مواظب بودن

بدون شک، Proofpoint بدافزار جدید و جالب و پیچیده ای را شناسایی کرده است که از طریق بررسی های متعدد، ارتباطات رمزگذاری شده و مبهم سازی کد بر مخفی بودن تمرکز می کند.

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

فهرست ابزارهای ضد تحلیل را به شرح زیر خلاصه می کند:

- بررسی وجود برنامه های مهندسی معکوس یا اشکال زدایی در لیست فرآیندها
 - بررسی آدرس های مک مشکوک
 - بررسی رشته های WMI تا بینید آیا نام دیسک ها مشروع هستند یا خیر
 - بررسی اینکه آیا اندازه هارد دیسک زیر ۱۰۰ گیگابایت است یا خیر، زیرا اندازه زیر ۱۰۰ گیگابایت برای ماشین های مجازی معمول است
 - بررسی اینکه آیا برنامه های 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 بررسی ها عملأً اجرای RAT را در یک محیط sandbox شده مجازی غیرممکن می کند و از مخفی بودن طولانی مدت برای اپراتورهای بدافزار اطمینان می دهد.





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

ویندوز ۱۱ جعلی بدافزار است.

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 می‌پردازند.

وب سایت مخربی که ویندوز ۱۱ جعلی را ارائه می‌دهد 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.

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 جستجو، 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، نسخه ۲۰ است که در ماشین‌هایی که بیش از چهار سال سن ندارند وجود دارد.



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 Chrome، Edge، Brave، Opera، از جمله گسترده است، از جمله Comodo و Vivaldi، 360 Browser

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 را بانده نمی ستد.

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

نکات امنیتی

کل وضعیت ارتقاء ویندوز ۱۱ زمینه مناسبی را برای گسترش این کمپیون‌ها ایجاد کرده است و این اولین بار نیست که چنین حیزی گزارش می‌شود.

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 محدودیت‌ها به صورت دستی فایده‌ای ندارد، زیرا این کار با مجموعه‌ای از جنبه‌های منفی و خطرات امنیتی شدید همراه خواهد بود.



فرآیند آلودگی

به گفته CloudSEK، عوامل تهدید در پشت این کمپیون از بدافزار جدیدی استفاده می‌کنند که محققان به دلیل استفاده از نصب کننده Inno Stealer آن را «نامیدند. محققان می‌گویند که Inno Stealer هیچ شbahت کدی با سایر زدهای اطلاعاتی که در حال حاضر در گردش هستند ندارد و شواهدی مبنی بر آپلود بدافزار در پلتفرم اسکن ویروس توتال بیدا نکرده‌اند.

فایل لودر (مبتنی بر دلفی) فایل اجرایی «Windows Setup» موجود در ISO است، که پس از راهاندازی، یک فایل موقت به نام tmp.IS-PN1۳۱۳۱۷۸۳۰ که لودر در آن کیلمایات داده می‌نماید.

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 LNK¹ در دایرکتوری Startup و استفاده از cacls.exe برای تنظیم مجوزهای دسترسی آن برای مخفف، کام، به دست م. 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.^۲ به گفته محققان، این بدافزار را حل‌های 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 VBA سیستم اجرا می شود. و چهارمین فایل، یک اسکریپت است که برای اجرای dfl.cmd مورد نیاز است.

در مرحله دوم آلودگی، فایلی با پسوند SCR در دایرکتوری C:\Users\{{User}}\AppData\Roaming\Windows\InstallationAssistant سیستم در معرض خطر قرار می‌گیرد.

این فایل محموله دزد اطلاعات را باز می‌کند و با ایجاد یک فرآیند جدید به نام «Windows\InstallationAssistant.scr»، آن را احرا می‌کند.

صفات

2-shadow volume

بدافزار، که داده‌های صورگ و کیف بیان‌های اینها، دیجیتاً، با سقت می‌کند



مجرم سایبری

گرگ در لباس گوسفند



بدترین اقدامات،
هوشمندانه انجام می‌شوند.



مرکز آمادگی کاه همان

مايكروسافت:

بدافزار جدید از باگ ويندوز سوء استفاده می کند!

مايكروسافت بدافزار جدیدی را کشف کرده است که توسط گروه هک هافنیوم مورد حمایت چین برای حفظ ماندگاری بر روی سистемهای 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 مايكروسافت 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 جیستری ویندوز

تیم تشخیص و پاسخ مايكروسافت گفت: «در حالی که مايكروسافت 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 سرخهای فارنزیک، استفاده از 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 جیستری مربوط به Security Descriptor آن‌ها را از «scrtasks /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 (C2) 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.



نحوه دفع در برابر حملات Tarrask

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

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

مايكروسافت همچنین توصیه می‌کند ثبت لاغ را برای TaskOperational در Microsoft-Windows- TaskScheduler/Operational Task Scheduler log فعال کنید و بر روی اتصالات خارجی از دارایی‌های مهم طبقه

۱-مشخص کننده امنیتی



مرکز آماده دانشگاه سمنان

آموزش

علائم آلودگی به باج افزار

و اقدامات پس از آن

علام وقوع آلودگی به باج افزار

- ۶. تصویر پس زمینه به صورت ناخواسته تغییر کرده است.
- ۷. پیغامی مبنی بر قفل شدن دستگاه و یا فایل‌ها دریافت کنید.

روش‌های تخصصی شناسایی باج افزارها

عموماً پس از اینکه سیستم به باج افزار 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 عموماً سازندگان آنتی ویروس‌ها از آن استفاده کرده و با کمک آن می‌توانند پیش از آنکه باج افزار 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 باج افزار، یک امضاء دیجیتال منحصر به فرد برای آن در نظر می‌گیرند و آن را به دیکشنری باج افزارها 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.

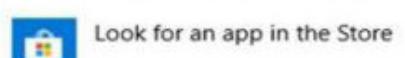
- **روش تحلیل داینامیک:** در این روش برخلاف روش مبتنی بر امضاء، هدف شناسایی باج افزارهایی که قبل از شناخته شده‌اند نیست و به جای آن رفتار همه برنامه‌ها را نظر گرفته می‌شود و در صورتی که هر کدام از آنها رفتار مخرب و مشکوکی مشابه باج افزارها داشته باشد فوراً شناسایی شده و از ادامه فعالیت آن جلوگیری می‌شود.

- **روش ترکیبی:** همانطورکه مشخص است، روش مبتنی بر امضاء، از دستگاه شما در برابر باج افزارهای 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.

در خصوص حملات باج افزاری یک جمله معروف وجود دارد که می‌گوید «باج افزارها پرس و صدای از آن هستند که صدای آنها را نشنوید!» به عبارت دیگر باج افزارها در مرحله نفوذ و رمزگاری 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 باج افزارها 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 باج افزاری باشید:

۱. پردازش CPU بیش از حد طبیعی درگیر شده است.
۲. فن دستگاه با سرعت زیاد و غیرطبیعی کار می‌کند.
۳. میزان درگیر بودن هارد دستگاه به صورت غیرطبیعی افزایش یافته است.
۴. 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.

How do you want to open this file?



Look for an app in the Store

[More apps](#)

Always use this app to open .cryp1 files

OK



اقدامات ضرروی در صورت آلوده شدن به بدافزار

- به شبکه آلوده شده باشند. اقدامات لازم را برای اطمینان از آلوده نشدن همه سیستم‌های انجام دهید.
- ۳. شناسایی باج افزار:** وبسایت‌های بی‌شماری وجود دارند که به شما در شناسایی باج افزار کمک می‌کنند. شناسایی نوع بدافزار به شما کمک می‌کند به فهمید با چه نوع باج افزاری روبرو هستید، چگونه انتشار می‌یابد، چه پروندهایی را رمزگذاری می‌کند و گزینه‌های پیش روی شما برای مقابله با آن چیست.
 - ۴. کمک گرفتن از متخصصین:** بهتر است قبل از هر اقدامی به پیغام باج افزار دقت بیشتری کنید و از متخصصین امنیت و IT استفاده کنید. در برخی موارد، ابزارهای جانبی توسط شرکت‌های امنیتی معرفی می‌شوند که می‌توانند فایل‌های رمزگذاری 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.
 - ۶. تشخیص راه آلودگی:** به منظور جلوگیری از حملات مشابه می‌بایست راه آلودگی سیستم مشخص شده و برای آن چاره‌اندیشی گردد.
 - ۷. تعیین کردن گزینه‌های پیش روی برای مقابله با باج افزار:** گزینه‌های شما هنگام آلوده شدن به باج افزار 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 باج افزار را به گرفتن باج بیشتر ترغیب می‌کند و در بسیاری از موارد نمی‌توانید قفل پروندهای رمزگذاری شده را باز کنید. ممکن است بتوانید با رمزگشایی رایگان بخشی از فایل‌های رمزگذاری شده باج افزار را بازیابی کنید. پس از حمله باج افزار، بازیابی اطلاعات باج افزار کار دشواری خواهد بود خصوصاً اگر به باج افزار Encryption آلوده شده باشد. چون در بسیاری موارد باج افزار از الگوریتم‌های پیشرفته و پیچیده استفاده

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 بلاfaciale 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



اساسی می‌باشد. لذا ما نیاز به راهکاری داریم که با دنبال کردن آن بتوانیم در صورت وقوع حمله باج‌افزاری، نوع آن را تشخیص دهیم. خوشبختانه چند ابزار کارآمد در این خصوص ساخته شده است که در ادامه آنها را معرفی می‌کنیم.

• ابزار Crypto Sheriff from No More Ransom

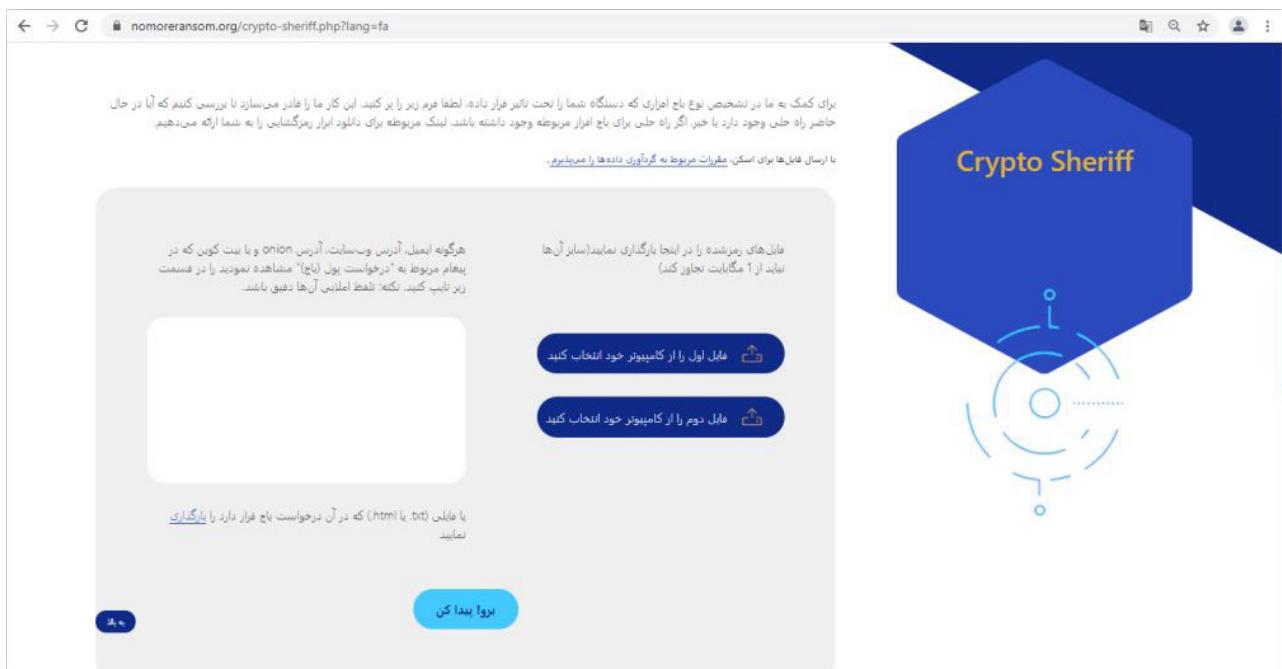
ابزار **Crypto Sheriff** یکی از کارآمدترین ابزارهای موجود در زمینه تشخیص نوع باج‌افزار می‌باشد که از آدرس اینترنتی <https://www.nomoreransom.org/crypto-sheriff.php> قابل دسترسی است. با ورود به این سایت همانطورکه در قسمت توضیحات آن آمده است می‌بایست نمونه فایل‌های رمزشده را در آن آپلود کرد و یا هرگونه ایمیل، آدرس وبسایت، آدرس onion و یا بیت کوین که در پیغام مربوط به «درخواست پول (باچ)» مشاهده نمودید را وارد کنید و پس از آن، این ابزار شروع به بررسی کرده و علاوه بر اینکه نوع باج‌افزار را مشخص می‌کند در صورت امکان راه حل برای رمزگشایی، آن را ارائه می‌دهد.

می‌کند ممکن است هنوز رمزگشاهی آن‌ها ارایه نشده باشد. حتی اگر رمزگشایی وجود داشته باشد مشخص نیست که نسخه مناسبی با بدافزار را پوشش دهد. از طرفی حتی اگر تصمیم به پرداخت هزینه بگیرید، ممکن است نتوانید داده‌های خود را پس بگیرید.

۸. حفاظت از فایل‌های رمزشده: فایل‌هایی که رمزگاری شده‌اند و موفق به بازگرداندن آنها نشده‌اید را در جای امنی نگه‌داری کنید چراکه معمولاً پس از گذشت چند ماه از انتشار بدافزار، شرکت‌های امنیتی موفق به ارائه کلید آن خواهند شد و در این صورت امکان دسترسی مجدد به فایل‌های قفل شده وجود دارد.

نحوه شناسایی نوع باج‌افزار

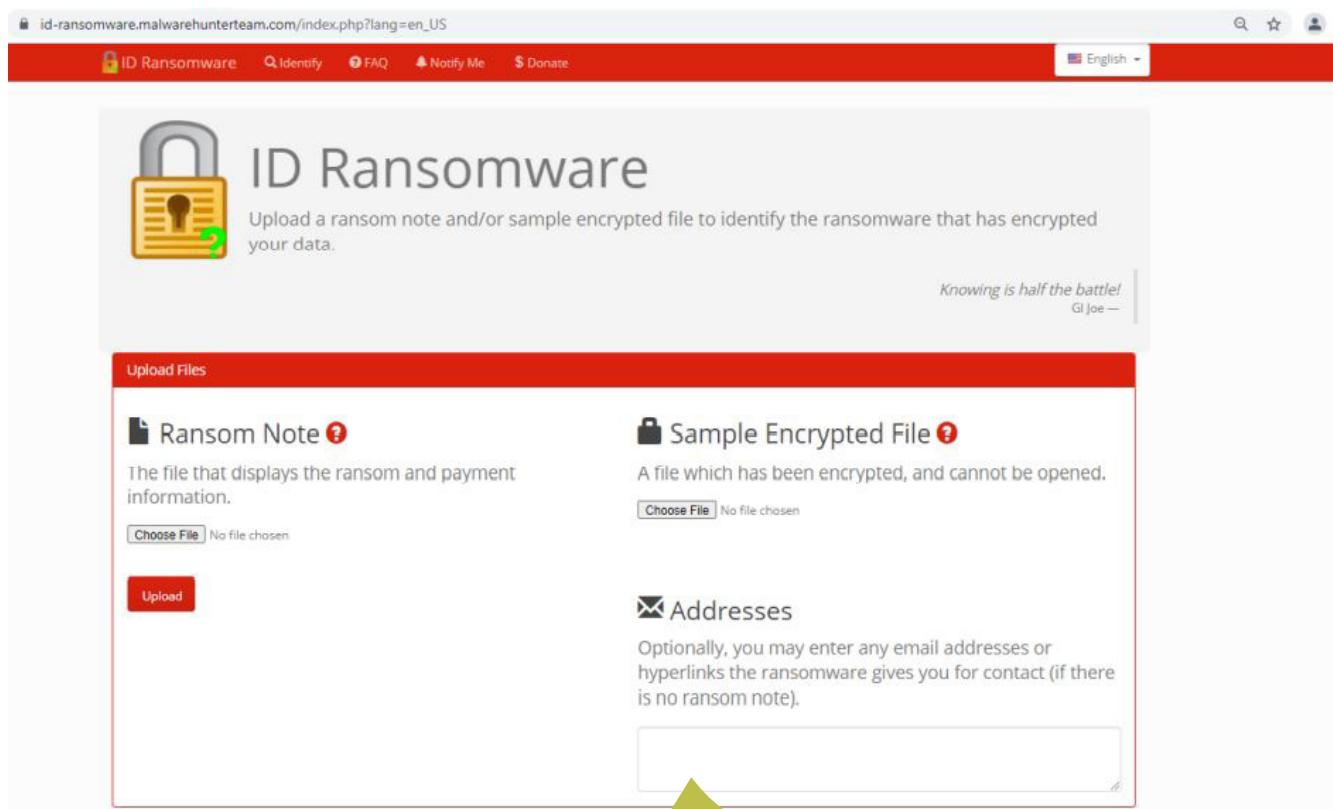
همانطور که در علم پزشکی برای مقابله با یک بیماری، تشخیص نوع آن بسیار حائز اهمیت است، در علم کامپیوتر نیز تشخیص نوع حمله و نوع ویروس یا باج‌افزاری که سیستم را آلوده کرده است، یک اصل



• ابزار ID Ransomware from MalwareHunter Team

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 باج افزار تشخیص داده شود.

این ابزار نیز برای تشخیص نوع باج افزاری 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



The screenshot shows the homepage of ID Ransomware. At the top, there's a navigation bar with links for 'ID Ransomware', 'Identify', 'FAQ', 'Notify Me', and '\$ Donate'. The main title 'ID Ransomware' is displayed next to a padlock icon with a question mark. Below the title, a sub-instruction says 'Upload a ransom note and/or sample encrypted file to identify the ransomware that has encrypted your data.' A quote 'Knowing is half the battle!' by Gi Joe is visible on the right. The central part of the page has two main sections: 'Upload Files' and 'Sample Encrypted File'. The 'Upload Files' section contains fields for 'Ransom Note' (with a note about displaying ransom and payment info) and 'Sample Encrypted File' (with a note about being encrypted and unopenable). Both sections include 'Choose File' buttons and 'Upload' buttons. The 'Sample Encrypted File' section also includes a text input field for 'Addresses' with a note about entering email addresses or hyperlinks provided by the ransomware.





مرکز آمادگی دانشگاه سمنان

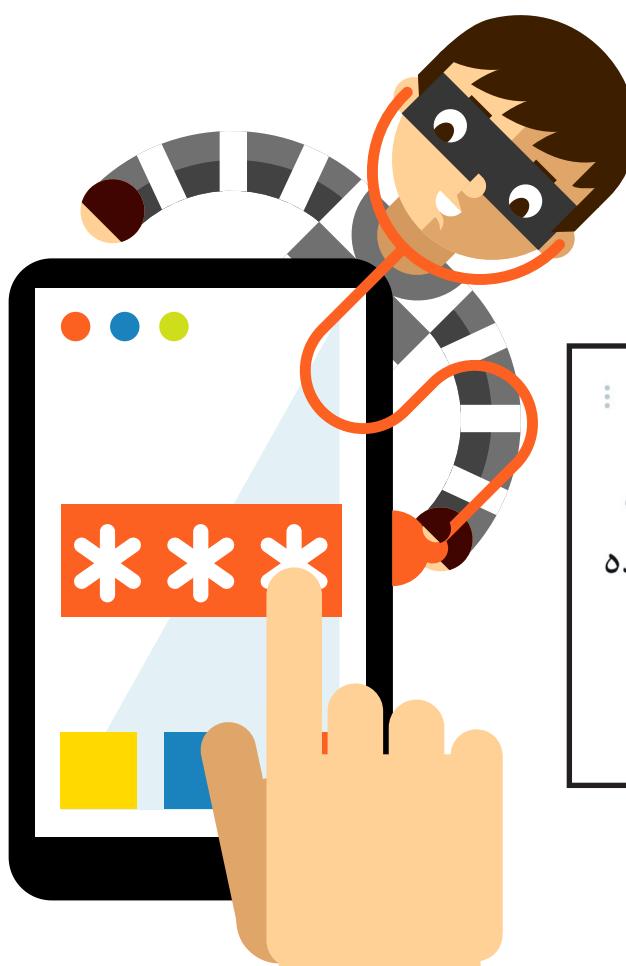
خبر
کوتاه

بدافزارهایی که وعده افزایش قابلیت اینستاگرام را می‌دهند!

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 برنامه ساخته نشده است- MOD (mobile App) Modified.



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 فالوئرهاشان را افزایش دهند و



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 می‌دزد.

mcafee منبع: 

تلash ما

حفظ امنیت

شماست...

