# خبرنامه الکترونیکی ۵۱

## مرکز تخصصی آپا دانشگاه سمنان

شماره پنجاه و یکم، سال پنجم، مرداد ۱۴۰۱ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

**بازگرداندن فایل‌های آلوده شده به باج‌افزار به کمک ابزارهای رمزگشا**

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

# از "نه" گفتن نترسید...

## اطلاعات شخصی خود را با افراد غریبه به اشتراک نگذارید.

# فهرست

## خبر

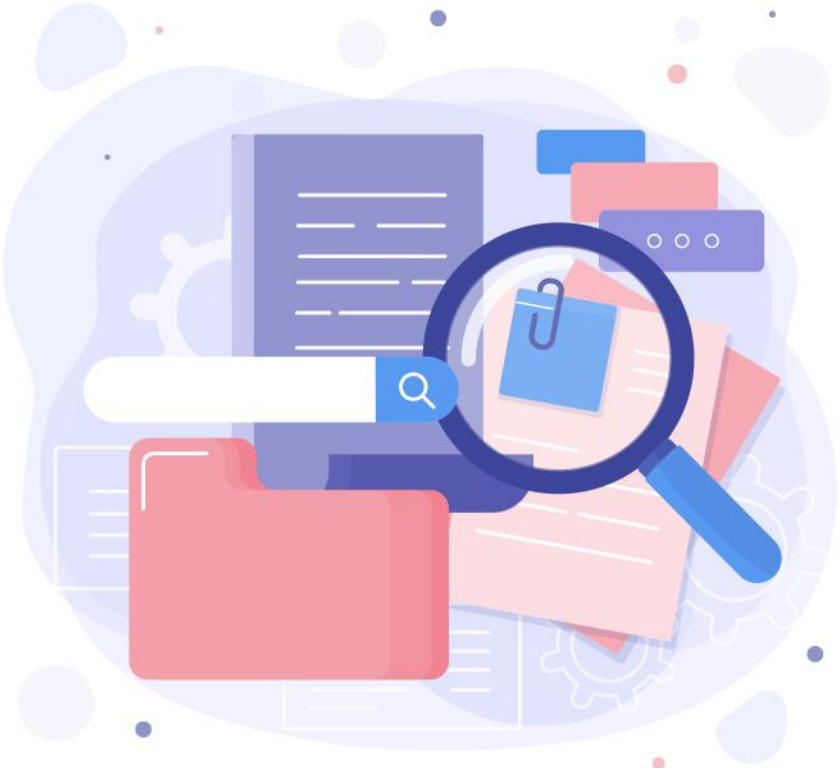


## آموزش



## خبرکوتاه





مرکز آپا دانشگاه سمنان

# خبر

# ورود باج افزار HavanaCrypt به بازار به عنوان یک به روز رسانی جعلی گوگل

## مشکل در شناسایی، پنهان کردن پنجره آن با استفاده از تابع ShowWindow در ویندوز

یک خانواده باج‌افزار جدید در قالب به‌روزرسانی جعلی نرم‌افزار Google ظهور کرده است. این باج افزار در بخشی از حمله خود از قابلیت‌های مایکروسافت استفاده می‌کند.

محققان Trend Micro می‌گویند که آخرین تهدیدی را که کشف کرده‌اند «HavanaCrypt» نام دارد و یک بسته باج‌افزاری است که خود را به‌عنوان یک به‌روزرسانی نرم‌افزار Google معرفی می‌کند، اگرچه یک برنامه کامپایل‌شده توسط .NET است.

چندین ویژگی تشخیص آن را دشوار می‌کند. این بدافزار از Obfuscar استفاده می کند، یک مبهم کننده open-source در .NET. که برای ایمن سازی کدها در مجموعه .NET. طراحی شده است.

پس از اولین اجرا، باج‌افزار پنجره خود را با استفاده از تابع ShowWindow در سیستم پنهان می‌کند و به آن پارامتر ۰ می‌دهد.

محققان نوشتند: «این بدافزار همچنین دارای چندین تکنیک ضد مجازی‌سازی است که به آن کمک می‌کند هنگام اجرا در یک ماشین مجازی از تجزیه و تحلیل پویا جلوگیری کند.» همچنین اضافه کردند که اگر این بدافزار بفهمد که سیستم در محیط VM در حال اجرا است، خودش را نابود می‌کند.

این بررسی VM را در چهار مرحله اجرا می‌کند: بررسی سرویس‌های موجود در ماشین‌های مجازی مانند VMware Tools و vmmouse، جستجوی فایل‌هایی که معمولاً مربوط به برنامه‌های VM هستند و جستجوی نام فایل‌هایی که ماشین‌های مجازی برای فایل‌های اجرایی خود استفاده می‌کنند. در نهایت، بدافزار به آدرس MAC سیستم نگاه می‌کند و آن را با پیشوندهای شناسایی منحصربه‌فرد سازمانی[1] که معمولاً توسط ماشین‌های مجازی استفاده می‌شود، مقایسه می‌کند.

هنگامی که HavanaCrypt تشخیص داد که سیستم قربانی در VM اجرا نمی‌شود، یک فایل را از آدرس IP سرویس میزبانی وب مایکروسافت دانلود می‌کند، آن را به عنوان یک فایل batch ذخیره می‌کند و سپس اجرا می‌کند.

1-OUI

این بدافزار بیش از ۸۰ فرآیند را خاتمه می‌دهد، از جمله آنهایی که بخشی از برنامه‌های مرتبط با پایگاه داده مانند Microsoft SQL Server و MySQL و همچنین نرم افزارهای دسکتاپ مانند Office و Steam هستند. سپس کپی‌های سایه‌ای[1] از فایل‌ها را حذف می‌کند.

HavanaCrypt متعاقباً نسخه‌های اجرایی خود را در پوشه‌های «ProgramData» و «StartUp» قرار می‌دهد، آنها را فایل‌های سیستمی مخفی می‌کند و Task Manager را غیرفعال می‌کند.

این باج‌افزار اطلاعات مربوط به سیستم - شناسه منحصر به فرد[2] - را از تعداد هسته های پردازنده، شناسه و نام تراشه، سازنده و نام مادربرد، شماره محصول و نسخه BIOS جمع‌آوری می‌کند. همه اینها به سرور کنترل و فرمان[3] بدافزار، که آدرس IP سرویس میزبانی وب مایکروسافت است، ارسال می‌شود. محققان Trend Micro نوشتند که استفاده از سرور C2 که بخشی از خدمات میزبانی وب مایکروسافت است غیرعادی است.

در طول رمزگذاری، HavanaCrypt از تابع CryptoRandom در KeePass Password Safe - یک ابزار مدیریت رمز عبور متن‌باز که بیشتر برای ویندوز استفاده می‌شود - برای تولید کلیدهای تصادفی استفاده می‌کند و پسوند «Havana.» را به فایل های رمزگذاری شده اضافه می‌کند.

محققان نوشتند: «احتمال زیادی وجود دارد که نویسنده باج‌افزار قصد داشته باشد از طریق مرورگر Tor ارتباط برقرار کند، زیرا دایرکتوری Tor از جمله دایرکتوری‌هایی است که از رمزگذاری فایل‌ها در آن اجتناب می‌کند. لازم به ذکر است که HavanaCrypt همچنین فایل متنی


foo.txt را رمزگذاری می کند و یادداشت باج‌خواهی نمی دهد. این ممکن است نشان دهنده این باشد که HavanaCrypt هنوز در مرحله توسعه خود است.»

HavanaCrypt بخشی از هجوم رو به رشد خانواده‌های باج‌افزار و حملات است. Trend Micro در سه ماهه اول بیش از ٤/٤ میلیون تهدید باج‌افزاری را که از طریق ایمیل، آدرس‌های اینترنتی و لایه‌های فایل ارسال می‌شد، شناسایی و مسدود کرده است.

این شامل یک به‌روزرسانی جعلی ویندوز است که باج‌افزار Magniber را توزیع می‌کند - تهدیدی که حداقل از سال ۲۰۱۷ وجود داشته است - و حملاتی که از به‌روزرسانی‌های جعلی مایکروسافت اج و مرورگر Google برای تحت فشار قرار دادن آسیب‌پذیری Magnitude استفاده می‌کنند.

1-shadow copy
2-UID
3-C2

# حمله Roaming Mantis به کاربران اندروید و iOS

پس از حمله به آلمان، تایوان، کره جنوبی، ژاپن، ایالات متحده و بریتانیا، هدف بعدی عملیات Roaming Mantis، کاربران اندروید و iOS در فرانسه بود و احتمالاً ده‌ها هزار دستگاه را به خطر انداخت.

اعتقاد بر این است که Roaming Mantis یک عامل تهدید با انگیزه مالی است که در فوریه شروع به هدف قرار دادن کاربران اروپایی کرد.

در کمپینی که اخیراً مشاهده شده است، عامل تهدید از ارتباطات SMS به منظور فریب دادن کاربران برای دانلود بدافزار در دستگاه‌های اندرویدی خود استفاده می‌کند. اگر قربانی احتمالی از iOS استفاده کند، برای اطلاعات اعتبارنامه اپل به صفحه فیشینگ هدایت می‌شود.

## رها کردن XLoader

در گزارشی که امروز منتشر شد، محققان شرکت امنیت سایبری SEKOIA می گویند که گروه Roaming Mantis اکنون کد XLoader[1] را بر روی دستگاه های اندرویدی رها می‌کند، یک بدافزار قدرتمند که ویژگی‌هایی مانند دسترسی از راه دور، سرقت اطلاعات و ارسال هرزنامه پیامک را محاسبه می‌کند.

کمپین در حال پیشرفت Roaming Mantis کاربران فرانسوی را هدف قرار می‌دهد و با یک پیامک که برای قربانیان جدید ارسال می‌شود شروع شده و از آنها می‌خواهد که یک URL را دنبال کنند.

پیامک از بسته ای خبر می‌دهد که برایشان ارسال شده و باید آن را بررسی و تحویل آن را هماهنگ کنند.

اگر کاربر در فرانسه واقع شده باشد و از یک دستگاه iOS استفاده کند، به صفحه فیشینگ هدایت می‌شود که اعتبارنامه اپل را می‌دزدد. کاربران اندروید به سایتی هدایت می‌شوند که فایل نصبی را برای یک برنامه تلفن همراه ارائه می‌دهد (یک کیت بسته Android - APK ).

برای کاربران خارج از فرانسه سرورهای Roaming Mantis خطای ۴۰۴ را نشان می‌دهند و حمله متوقف می‌شود.

APK نصب Chrome را اجرا و تقلید می‌کند و مجوزهای خطرناکی مانند رهگیری پیامک، برقراری تماس تلفنی، خواندن و

1-MoqHao

نوشتن فضای ذخیره‌سازی، مدیریت هشدارهای سیستم، دریافت فهرست حساب‌ها و موارد دیگر را درخواست می‌کند.

پیکربندی سرور کنترل و فرمان از یک صفحه در وب‌سایت imgur خوانده می‌شود که آدرس آن به طور ثابت در کد بدافزار قرار گرفته است. البته برای فرار از تشخیص، آدرس سرور به شکل base۶۴ کدگذاری شده است.

SEKOIA تایید کرد که تا کنون بیش از ۹۰۰۰۰ آدرس IP منحصر به فرد، XLoader را از سرور اصلی C2 درخواست کرده‌اند، بنابراین تعداد قربانیان ممکن است قابل توجه باشد.

تعداد کاربران iOS که اعتبارنامه Apple iCloud خود را در صفحه فیشینگ Roaming Mantis تحویل داده‌اند ناشناخته است و می‌تواند یکسان یا حتی بیشتر باشد.

## جزئیات زیرساخت

تحلیلگران SEKOIA گزارش می‌دهند که زیرساخت Roaming Mantis از آخرین تجزیه و تحلیل آن از تیم Cymru در آوریل گذشته تغییر چندانی نکرده است.

سرورها همچنان دارای پورت‌های باز در TCP/5985، TCP/443 TCP/10081 و TCP/47001 هستند، در حالی که همان گواهینامه‌هایی که در ماه آوریل مشاهده شد هنوز در حال استفاده هستند.

SEKOIA در این گزارش توضیح می‌دهد: «دامنه‌های مورد استفاده در پیام‌های SMS یا با Godaddy ثبت شده‌اند یا از سرویس‌های DNS پویا مانند duckdns.org استفاده می‌کنند. » جالب اینجاست که عملیات smishing متکی به سرورهای C2 مجزا از سرورهای مورد استفاده XLoader است و تحلیلگران می‌توانند ۹ مورد از آن‌هایی را که در EHOSTIDC و VELIANET Autonomous Systems میزبانی شده‌اند شناسایی کنند.

۱- فیشینگ پیامکی

# پیدا شدن بدافزار CosmicStrand UEFI در مادربردهای گیگابایت و ایسوس

هکرهای چینی زبان حداقل از سال ۲۰۱۶ از بدافزاری استفاده می‌کنند که در تصاویر سیستم‌عامل برخی از مادربردها وجود دارد و تقریبا مخفی مانده بود، یکی از دائمی‌ترین تهدیدات که معمولاً به عنوان روت کیت UEFI شناخته می‌شود.

محققان شرکت امنیت سایبری Kaspersky آن را CosmicStrand نامیدند، اما نوع قبلی این تهدید توسط تحلیلگران بدافزار در Qihoo360 کشف شد که آن را Spy Shadow Trojan نامیدند.

مشخص نیست که عامل تهدید چگونه توانسته است روت کیت را به تصاویر سیستم عامل ماشین‌های مورد نظر تزریق کند، اما محققان این بدافزار را در دستگاه‌هایی با مادربردهای ASUS و Gigabyte پیدا کردند.

## روت کیت Mystery UEFI

نرم افزار Unified Extensible Firmware Interface[1] چیزی است که سیستم عامل کامپیوتر را با ثابت‌افزار سخت افزار زیرین متصل می‌کند.

کد UEFI اولین کدی است که در طول توالی بوت شدن کامپیوتر، پیش از سیستم عامل و راه حل‌های امنیتی موجود اجرا می‌شود.

نه تنها شناسایی بدافزار کاشته شده در تصویر سیستم‌عامل UEFI آن دشوار است، بلکه بسیار پایدار است زیرا با نصب مجدد سیستم عامل یا با جایگزینی درایو ذخیره‌سازی قابل حذف نیست.

گزارش از Kaspersky جزئیات فنی درباره CosmicStrand از مؤلفه UEFI آلوده تا استقرار یک ایمپلنت در سطح هسته در سیستم ویندوز در هر بار بوت ارائه می‌دهد.

کل فرآیند شامل راه اندازی قلاب‌هایی[2] برای تغییردادن بارگزارکننده سیستم عامل و به دست گرفتن کنترل کل جریان اجرا است تا کد پوسته‌ای را راه اندازی کند که پیلودش را از سرور فرمان و کنترل دریافت می‌کند.

Mark Lechtik، مهندس معکوس سابق Kaspersky، اکنون در Mandiant که در این تحقیق شرکت داشت، توضیح می‌دهد که تصاویر سیستم‌عامل آسیب‌دیده با یک درایور CSMCORE DXE تغییر داده شده ارائه شده‌اند که فرآیند بوت قدیمی را امکان‌پذیر می‌کند.

1-UEFI
2-hooks

Lechtik در توییتی در روز دوشنبه گفته است: « این درایور به گونه ای تغییر یافت که توالی بوت را رهگیری کند و منطق مخرب را به آن اضافه کند.»

در حالی که نوع CosmicStrand کشف شده توسط Kaspersky جدیدتر است، محققان Qihoo360 در سال ۲۰۱۷ اولین جزئیات مربوط به نسخه اولیه این بدافزار را فاش کردند.

محققان چینی پس از آنکه یک قربانی گزارش داد که کامپیوترش ناگهان یک حساب کاربری جدید ساخته است و نرم افزار آنتی ویروس مدام در مورد نفوذ بدافزار هشدار می‌دهد، شروع به تجزیه و تحلیل ایمپلنت کردند.

بر اساس گزارش آنها، سیستم در معرض خطر روی یک مادربرد دست دوم ایسوس که مالک آن از یک فروشگاه آنلاین خریداری کرده بود، کار می‌کرد.

Kaspersky توانست تشخیص دهد که روت کیت CosmicStrand UEFI در تصاویر سیستم‌عامل مادربردهای گیگابایت یا ایسوس که طراحی‌های مشترکی با استفاده از چیپست H81 دارند، قرار دارد.

این به سخت افزار قدیمی بین سال‌های ۲۰۱۳ تا ۲۰۱۵ اشاره دارد که امروزه اکثرا تولیدشان متوقف شده است.

مشخص نیست که چگونه ایمپلنت روی رایانه‌های آلوده قرار داده شده است زیرا این فرآیند شامل دسترسی فیزیکی به دستگاه یا از طریق یک بدافزار پیش‌ساز است که قادر به وصله خودکار تصویر سیستم‌عامل است.

قربانیان شناسایی شده توسط Kaspersky همچنین سرنخ‌های کمی در مورد عامل تهدید و هدف آنها ارائه می دهند زیرا سیستم های آلوده شناسایی شده متعلق به افراد خصوصی در چین، ایران، ویتنام و روسیه است که نمی توانند به یک سازمان یا صنعت مرتبط شوند.

با این حال، محققان CosmicStrand را به یک عامل چینی زبان بر اساس الگوهای کدی که در بات نت رمزنگاری MyKings نیز دیده می‌شد، مرتبط کردند، جایی که تحلیلگران بدافزار در Sophos اثرات زبان چینی را یافتند.

Kaspersky می‌گوید که روت‌کیت سیستم‌عامل CosmicStrand UEFI می‌تواند برای تمام عمر رایانه روی سیستم باقی بماند و از پایان سال ۲۰۱۶ سال‌ها در عملیات‌ها استفاده شده است.

## بدافزار UEFI رایج تر می‌شود

اولین گزارش گسترده در مورد روت کیت UEFI یافت شده ، LoJax، در سال ۲۰۱۸ از ESET ارائه شد و در حملات هکرهای روسی در گروه APT28[1] از آن استفاده شد.

تا الان تعداد حملات بدافزار UEFI بیشتر شده است و فقط هکرهای پیشرفته نبودند که این گزینه را بررسی کردند:

ما در مورد MosaicRegressor در سال ۲۰۲۰ از Kaspersky یاد گرفتیم، اگرچه در حملات سال ۲۰۱۹ علیه سازمان‌های غیر دولتی از آن استفاده شد.

در پایان سال ۲۰۲۰ این خبر منتشر شد مبنی بر اینکه توسعه دهندگان TrickBoot ، TrickBot را ایجاد کرده‌اند، ماژول جدیدی که ماشین‌های در معرض خطر را از نظر آسیب‌پذیری‌های UEFI بررسی می‌کند.

یکی دیگر از روت کیت های UEFI در اواخر سال ۲۰۲۱ معرفی شد که توسط گروه Gamma به عنوان بخشی از راه حل نظارتی FinFisher آنها توسعه داده شد.

در همان سال، جزئیاتی از ESET در مورد یک بوت کیت دیگر به نام ESPecter منتشر شد که گمان می‌رود عمدتاً برای جاسوسی استفاده می‌شود و منشا آن به سال ۲۰۱۲ باز می‌گردد.

MoonBounce، که یکی از پیچیده‌ترین ایمپلنت‌های سیستم‌عامل UEFI محسوب می‌شود، در ژانویه امسال همانطور که توسط Winnti، یک گروه هکر چینی زبان[2] استفاده می‌شد، فاش شد.

1- با نام مستعار Sofacy، Fancy Bear، Sednit

2- همچنین به عنوان APT41 شناخته می‌شود

# دوره آموزشی مجازی
# Security+

مدت دوره: ۳۰ ساعت
شروع دوره: چهارشنبه ۲ شهریور ۱۴۰۱
پایان دوره: شنبه ۱۹ شهریور ۱۴۰۱
زمان برگزاری:
روزهای زوج ساعت ۱۴ الی ۱۸
پیش‌نیاز: Network+، آشنایی کافی با مباحث شبکه
آزمون: پنج‌شنبه ۲۴ شهریور ۱۴۰۱
هزینه دوره: ~~۹۸۰۰۰۰~~ ۸۵۰۰۰۰ 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.

# کارگاه
# امنیت
# کاربری

مدت دوره: ۲ ساعت
روزهای برگزاری:
(این کارگاه ۴ بار برگزار می‌شود.)

- ۱۰ مرداد ساعت ۲۰-۱۸
- ۱۴ شهریور ساعت ۲۰-۱۸
- ۲۶ مرداد ساعت ۲۰-۱۸
- ۱۷ شهریور ساعت ۱۱-۹

تمام افرادی که از اینترنت، تلفن هوشمند، تبلت، لپ تاپ و... استفاده می‌کنند.
پیش‌نیاز: ندارد
هزینه دوره: ۵۰۰۰۰ 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.

مرکز آپا دانشگاه سمنان

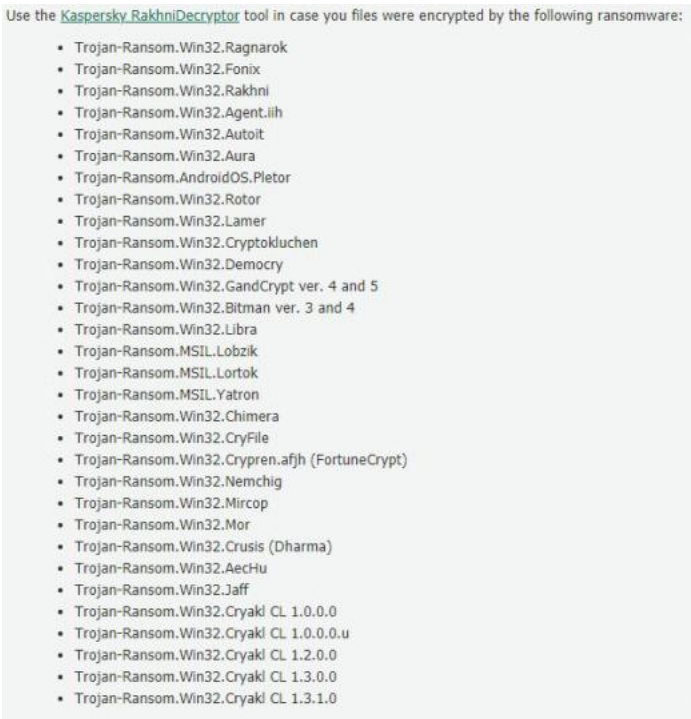
# آموزش

# بازگرداندن فایل‌های آلوده شده به باج‌افزار به کمک ابزارهای رمزگشا

خبر خوب این است که بسیاری از باج‌افزارها توسط متخصصان امنیتی و شرکت‌های بزرگ تولید کننده آنتی ویروس، رمزگشایی شده‌اند و کلید آن در دسترس می‌باشد. همچنین اگر دستگاه شما مورد حمله باج‌افزاری قرار گرفت که در حال حاضر کلید رمزگشایی آن در دسترسی نباشد، کماکان این شانس وجود دارد که در آینده نزدیک کلید آن کشف و منتشر شود. بنابراین توصیه می‌شود فایل‌های رمز شده خود را در جای امنی نگهداری کنید تا زمانی که موفق به یافتن کلید رمزگشایی آن شوید. در ادامه برخی از مهم‌ترین ابزارهایی که ممکن است در این زمینه کمک کننده باشند معرفی خواهند شد.

## ابزار Kaspersky RakhniDecryptor

Kaspersky RakhniDecryptor نام نرم‌افزاری کوچک و کم حجم، به منظور نابودسازی نوع خاصی از باج‌گیرها در دنیای دیجیتال است. در حال حاضر آخرین نسخه آن ۱۲۱/۱۵/۵ می‌باشد که توسط کمپانی کسپراسکای[1] توسعه یافته است. این شرکت با سال‌ها فعالیت در زمینه امنیت و تجربه در زمینه تولید نرم‌افزارهای امنیتی، ضد ویروس‌ها، در سال‌های اخیر تمرکز ویژه‌ای بر حملات باج‌افزاری داشته است. مطابق توضیحات سایت رسمی کسپراسکای، از این ابزار برای رمزگشایی موارد روبه‌رو می‌توان استفاده کرد.

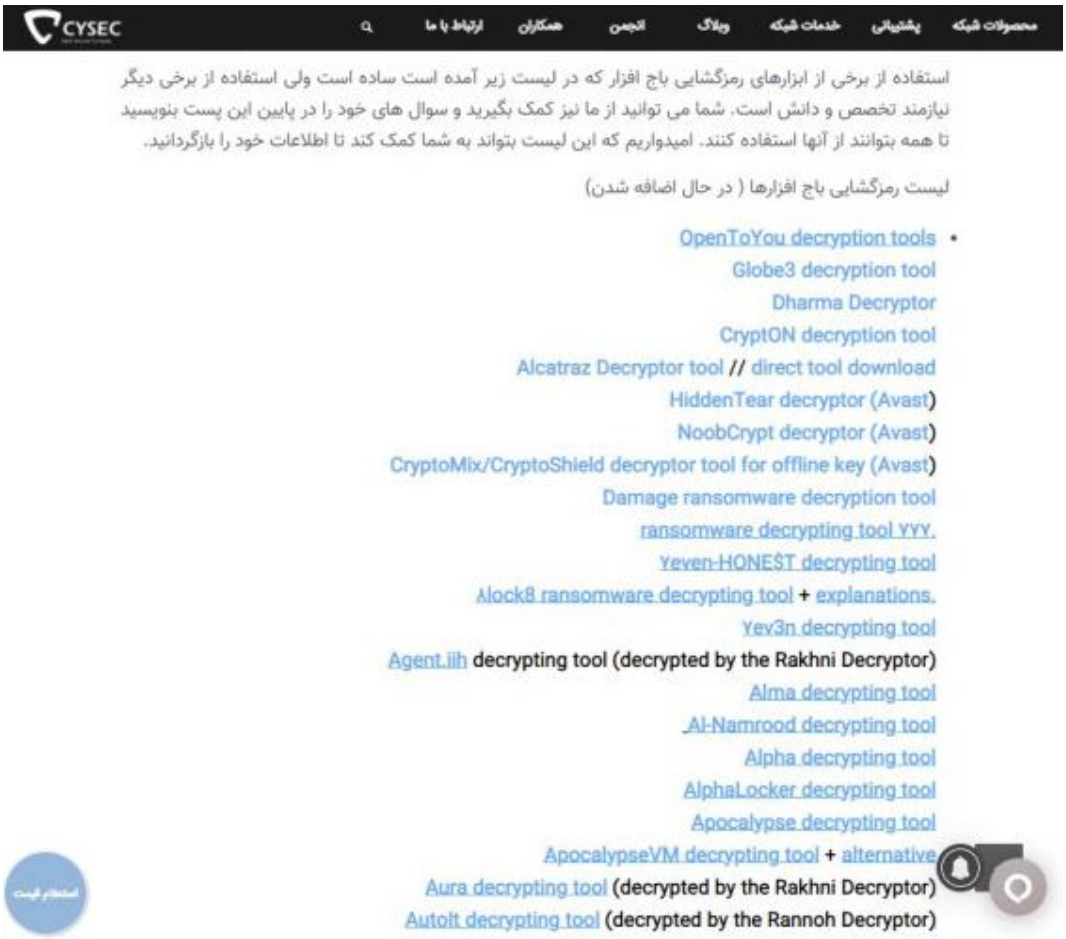


Use the Kaspersky RakhniDecryptor tool in case you files were encrypted by the following ransomware:

- Trojan-Ransom.Win32.Ragnarok
- Trojan-Ransom.Win32.Fonix
- Trojan-Ransom.Win32.Rakhni
- Trojan-Ransom.Win32.Agent.iih
- Trojan-Ransom.Win32.Autoit
- Trojan-Ransom.Win32.Aura
- Trojan-Ransom.AndroidOS.Pletor
- Trojan-Ransom.Win32.Rotor
- Trojan-Ransom.Win32.Lamer
- Trojan-Ransom.Win32.Cryptokluchen
- Trojan-Ransom.Win32.Democry
- Trojan-Ransom.Win32.GandCrypt ver. 4 and 5
- Trojan-Ransom.Win32.Bitman ver. 3 and 4
- Trojan-Ransom.Win32.Libra
- Trojan-Ransom.MSIL.Lobzik
- Trojan-Ransom.MSIL.Lortok
- Trojan-Ransom.MSIL.Yatron
- Trojan-Ransom.Win32.Chimera
- Trojan-Ransom.Win32.CryFile
- Trojan-Ransom.Win32.Crypren.afjh (FortuneCrypt)
- Trojan-Ransom.Win32.Nemchig
- Trojan-Ransom.Win32.Mircop
- Trojan-Ransom.Win32.Mor
- Trojan-Ransom.Win32.Crusis (Dharma)
- Trojan-Ransom.Win32.AecHu
- Trojan-Ransom.Win32.Jaff
- Trojan-Ransom.Win32.Cryakl CL 1.0.0.0
- Trojan-Ransom.Win32.Cryakl CL 1.0.0.0.u
- Trojan-Ransom.Win32.Cryakl CL 1.2.0.0
- Trojan-Ransom.Win32.Cryakl CL 1.3.0.0
- Trojan-Ransom.Win32.Cryakl CL 1.3.1.0

## رمزگشاهای موجود در وب‌سایت cysec-co.com

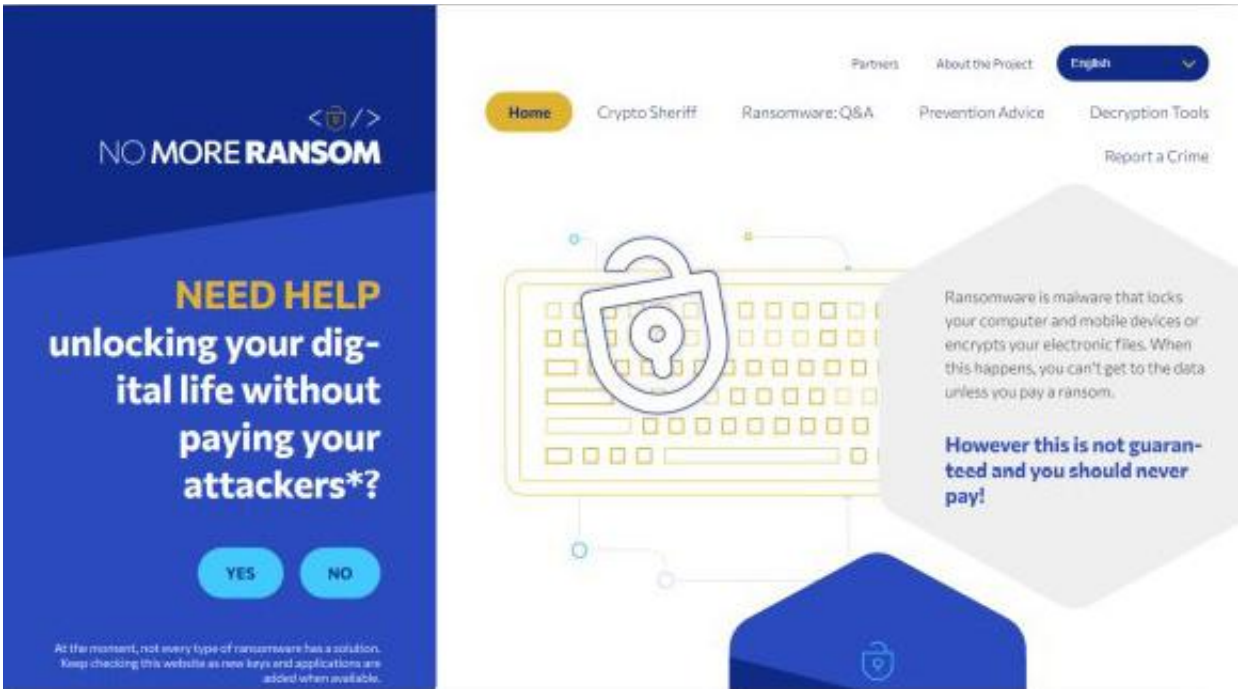
وب‌سایت ایرانی سایسک[2] نیز یکی از بهترین کلکسیون‌های ابزارهای رمزگشایی باج‌افزارهای مختلف (بالغ بر ۱۲۶ ابزار مختلف) را در اختیار شما خواهد گذاشت. این وب‌سایت که اطلاعات و ابزارهای آن همواره در حال توسعه و بروزرسانی می‌باشد لیست جامعی از کلیدهای رمزگشایی باج‌افزارهای مختلف را گردآوری کرده است. در تصویر صفحه بعد برخی از این ابزارها را مشاهده می‌کنید.


1-Kaspersky
2-Cysec




## رمزگشاهای موجود در وب‌سایت nomoreransom.org

وب‌سایت مذکور یکی از معتبرترین و به‌روزترین مراجع مقابله با باج‌افزارها می‌باشد و یکی از ویژگی‌های بارز آن، پشتیبانی کامل از زبان فارسی است. در این وب‌سایت جدیدترین اطلاعات در خصوص باج‌افزارها به همراه ابزارهای متنوع رمزگشایی ارائه شده است.



## ابزار Trend Micro Lock Screen Ransomware Tool

ابـزار Unlocker Screen Ransomware Screen Lock Micro Trend بـا وجـود اینکـه نـام بلنـد و عجیـب و غریبـی دارد امـا می‌توانـد در شـرایطی کـه سیسـتم‌تان بـه باج‌افـزار آلـوده شـده بـه شـدت مفیـد واقـع شـود. در واقـع اگـر باج‌افـزاری دسترسـی بـه کامپیوترتـان را غیـر ممکـن کـرده باشـد، می‌توانیـد بـه واسـطه ایـن برنامـه و از طریـق Mode Safe بـه اطلاعـات خـود دسـت پیـدا کنیـد و دوبـاره کنتـرل سیسـتم را بـه دسـت بگیریـد.


## ابزار Avast anti-ransomware tools

Avast Ransomware Decryption Tools نرم افزار بسـیار کاربـردی جهـت رمزگشـایی فایل‌هایـی کـه توسـط باج‌گیرهـا قفـل شـده انـد می‌باشـد. برنامـه Avast Ransomware Decryption شـامل ابـزار رمزگشـایی ۲۰ نـوع از باج‌افزارهـای مطـرح موجـود در لیسـت شـرکت Avast می‌باشـد.

### لیست برخی باج افزارهای قابل بازگشایی

| | | | |
|---|---|---|---|
| AES_NI - | BTCWare - | FindZip - | SZFLocker - |
| Alcatraz Locker - | Crypt888 - | Globe HiddenTear - | TeslaCrypt - |
| Apocalypse - | CryptoMix (Offline) - | Jigsaw - | XData - |
| BadBlock - | CrySiS - | Legion NoobCrypt - | |
| Bart - | EncrypTile - | Stampado - | |

## ابزار Emsisoft Ransomware Decryption Tools

ایـن یکـی از بهتریـن نرم‌افزارهـای رمزگشـایی ransomware بـا بالاتریـن امتیـاز اسـت کـه می‌توانیـد در ویـنـدوز کامپیوتـر داشته باشید. این ابزار بسیار قدرتمند است و قادر به رمزگشایی پرونده‌های رمزگذاری شده توسط Ransomware می‌باشد.

بـه راحتـی می‌توانیـد پرونده‌هـای رمزگـذاری شـده توسـط Stampado، Xorist و BadBlock Ransomware را رمزگشـایی کنید .

### ابزار AVG Free Ransomware Decryption

این ابزار نیز که محصول شرکت امنیتی AVG می‌باشد، برای بازیابی فایل‌های قفل شده توسط باج‌افزار می‌تواند مورد استفاده قرار گیرد. نرم افزار امنیتی AVG رمزگشایی باج‌افزارهای زیر را به خوبی انجام می‌دهد:

- Apocalypse
- BadBlock
- Bart
- Crypt888
- Legion
- SZFLocker
- TeslaCrypt

### ابزار BitDefender Anti-ransomware

Bitdefender Anti Ransomware نام یکی از نرم‌افزارهای رایگان و قدرتمند از سوی کمپانی Bitdefender است.

این کمپانی سازنده نرم‌افزارهای ضدویروس قدرتمند، اکنون با ابزاری برای مبارزه با نسل آینده ویروس‌ها پا به دنیای آنتی‌ویروس‌ها و ضد بد افزارها می‌گذارد. با استفاده از Bitdefender Anti Ransomware می‌توانید جلوی باج‌افزارهای Locky، Petya، CTB Locker و TeslaCrypt را رمزگشایی کنید. ویژگی‌های نرم‌افزار Bitdefender Anti Ransomware به شرح زیر می‌باشد:

- امکان اسکن سیستم‌های کامپیوتری برای فعالیت‌های باج‌افزارها و خنثی‌سازی آنان
- قابلیت جلوگیری از عملکردهای باج‌افزارهای Locky، CTB Locker و TeslaCrypt
- دارا بودن حجم کم و سبک برای کارکرد مناسب و عدم تداخل با فعالیت آنتی‌ویروس
- به‌روز رسانی رایگان از سرورهای قدرتمند بیت دفندر

### ابزار McAfee Ransomware Recover

برای رفع مشکل باج‌افزار می‌توانید از ابزارهای McAfee Ransomware Recover استفاده کنید. ابزارهای McAfee به‌روز هستند و برای باج‌افزارهایی که به صورت مداوم آپدیت می‌شوند، مناسب هستند. با این ابزارها می‌توانید نرم‌افزارها، فایل‌ها، دیتابیس و تمامی فایل‌های رمزگذاری شده را باز کنید. این ابزارها شامل موارد زیر می شوند:

- Tesladecrypt
- Ransomware Interceptor
- Shade Ransomware Decryption Tool
- WildFire Ransomware Decryption Tool

مرکز آپا دانشگاه سمنان

# خبر کوتاه

# آسیب‌پذیری در عملکرد احراز هویت خارجی Cisco Secure Email و Web Manager

semCERT
@semcert

#آسیب_پذیری جدید #Cisco

یک آسیب‌پذیری در عملکرد احراز هویت خارجی Cisco Secure Email و Web Manager، که قبلاً با نام Cisco Security Management Appliance (SMA) و Cisco Email Security Appliance (ESA) شناخته می‌شد، می‌تواند به مهاجم احراز هویت نشده و از راه دور اجازه دهد


semCERT
@semcert

تا احراز هویت را دور بزند و به رابط مدیریت وب دستگاه آسیب دیده واردشود.
این آسیب‌پذیری به دلیل بررسی‌های احراز هویت نامناسب در زمانی است که دستگاه از پروتکل LDAP برای احراز هویت خارجی استفاده می‌کند. یک مهاجم می‌تواند با وارد کردن یک ورودی خاص در صفحه ورود دستگاه آسیب‌پذیر

semCERT
@semcert

از این باگ سوء استفاده کند. اکسپلویت موفق می‌تواند به مهاجم اجازه دسترسی غیرمجاز به رابط مدیریت مبتنی بر وب دستگاه را بدهد.
سیسکو به روز رسانی‌های نرم افزاری را منتشر کرده است که این آسیب پذیری را برطرف می‌کند.

✅ منبع: tools.cisco.com

# سرقت اطلاعات ۵,۴ میلیون کاربر توییتر

semCERT
@semcert

⚠️#سرقت اطلاعات 5.4 میلیون کاربر #توییتر

کاربر با شناسه "devil" در فروم هکری Breached Forums، اطلاعاتی را برای فروش بارگذاری کرده است که ادعا میکند مربوط به 5.4 میلیون کاربر توییتر است.
در ماه ژانویه، یک آسیب پذیری روی توییتر گزارش شد که بعدا توییتر آن را وصله کرد.

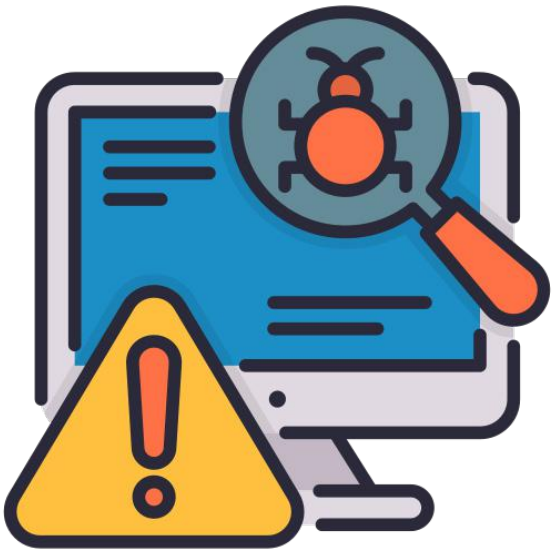
semCERT
@semcert

اما قبل از وصله، هکرها موفق شدند با استفاده از این باگ اطلاعات برخی از کاربران شامل شماره تلفن و آدرس #ایمیل آنها را سرقت کنند. مدیر وبسایت Breached Forums درستی اطلاعات پست شده را تایید کرده است.
سخنگوی #توییتر در ایمیلی به The Register نوشت:

semCERT
@semcert

«ما در حال بررسی آخرین داده‌ها برای تأیید صحت ادعاها و اطمینان از امنیت حساب‌های مورد نظر هستیم. ما گزارشی از این حادثه را چند ماه پیش از طریق برنامه پاداش باگ (bug bounty) دریافت کردیم، بلافاصله به طور کامل بررسی شد و آسیب‌پذیری برطرف گردید.»
منبع : theregister.com

# نصب درب پشتی توسط بدافزار CloudMensis



**semCERT**
@semcert

نصب در پشتی توسط #بدافزار
#CloudMensis

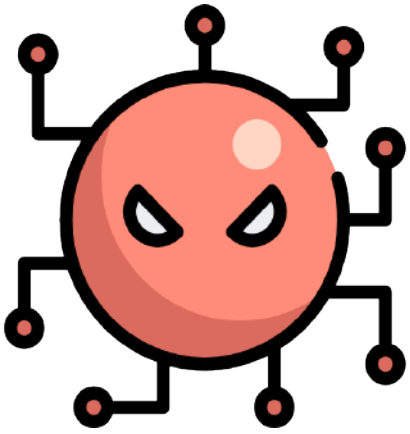
مهاجمین ناشناخته از بدافزارهایی که قبلاً شناسایی نشده بودند برای قرار دادن درپشتی در دستگاه‌های macOS و استخراج اطلاعات در مجموعه ای از حملات بسیار هدفمند استفاده می‌کنند.

**semCERT**
@semcert

ابتدا محققان ESET بدافزار جدید را در آوریل 2022 شناسایی کردند و نام آن را CloudMensis گذاشتند زیرا آن از خدمات ذخیره سازی ابری عمومی pCloud، Yandex Disk و Dropbox برای ارتباطات فرمان و کنترل (C2) استفاده می‌کند.

**semCERT**
@semcert

هدف اصلی اپراتورهای آن جمع‌آوری اطلاعات حساس از مک‌های آلوده از طریق روش هایی مثل اسکرین شات‌ها، حذف اسناد و ضربه‌های کلید، و همچنین فهرست کردن پیام‌های ایمیل، پیوست‌ها و فایل‌های ذخیره شده از حافظه قابل جابجایی است. این بدافزار از ده‌ها دستور پشتیبانی می‌کند



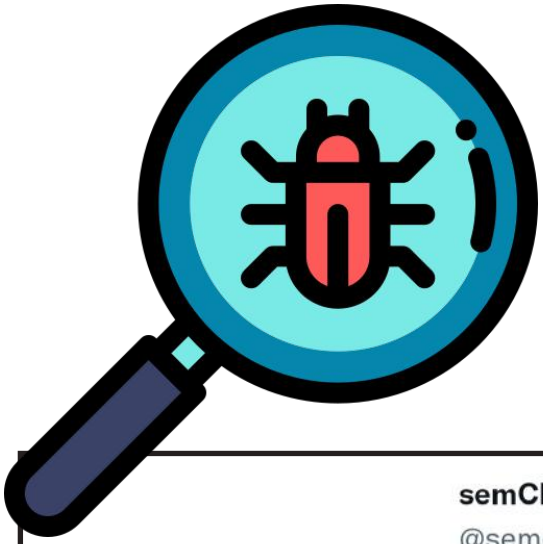
**semCERT**
@semcert

و به اپراتورهای خود اجازه می‌دهد تا لیست طولانی از اقدامات را روی مک‌های آلوده انجام دهند، از جمله:

📌تغییر مقادیر در پیکربندی CloudMensis: ارائه دهندگان فضای ذخیره سازی ابری و توکن‌های احراز هویت، پسوند فایل‌هایی که جالب به نظر می‌رسند، نرخ بررسی ذخیره سازی ابری و غیره.

**semCERT**
@semcert

📌فهرست کردن فرآیندهای در حال اجرا
📌شروع تصویربرداری از صفحه نمایش
📌فهرست کردن پیام‌های ایمیل و پیوست‌ها
📌فهرست کردن فایل‌های ذخیره سازی قابل جابجایی
📌اجرا کردن دستورات پوسته و آپلود خروجی در فضای ذخیره سازی ابری



**semCERT**
@semcert

📌دانلود و اجرای فایل های دلخواه

بر اساس تجزیه و تحلیل ESET، مهاجمان اولین مک را در 4 فوریه 2022 به CloudMensis آلوده کردند. ازآن زمان، آنها فقط به صورت پراکنده از درپشتی برای هدف قرار دادن وبه خطر انداختن دیگر مک‌ها استفاده کرده‌اند که به ماهیت بسیارهدفمند کمپین اشاره می‌کند.

**semCERT**
@semcert

ناقل آلودگی نیز ناشناخته است و توانایی های کدنویسی Objective-C مهاجمان نیز نشان می‌دهد که با پلتفرم macOS آشنا نیستند.

✅منبع: Bleeping_Computer

# تلاش ما
# حفظ امنیت
# شماست...