شبکه گستر

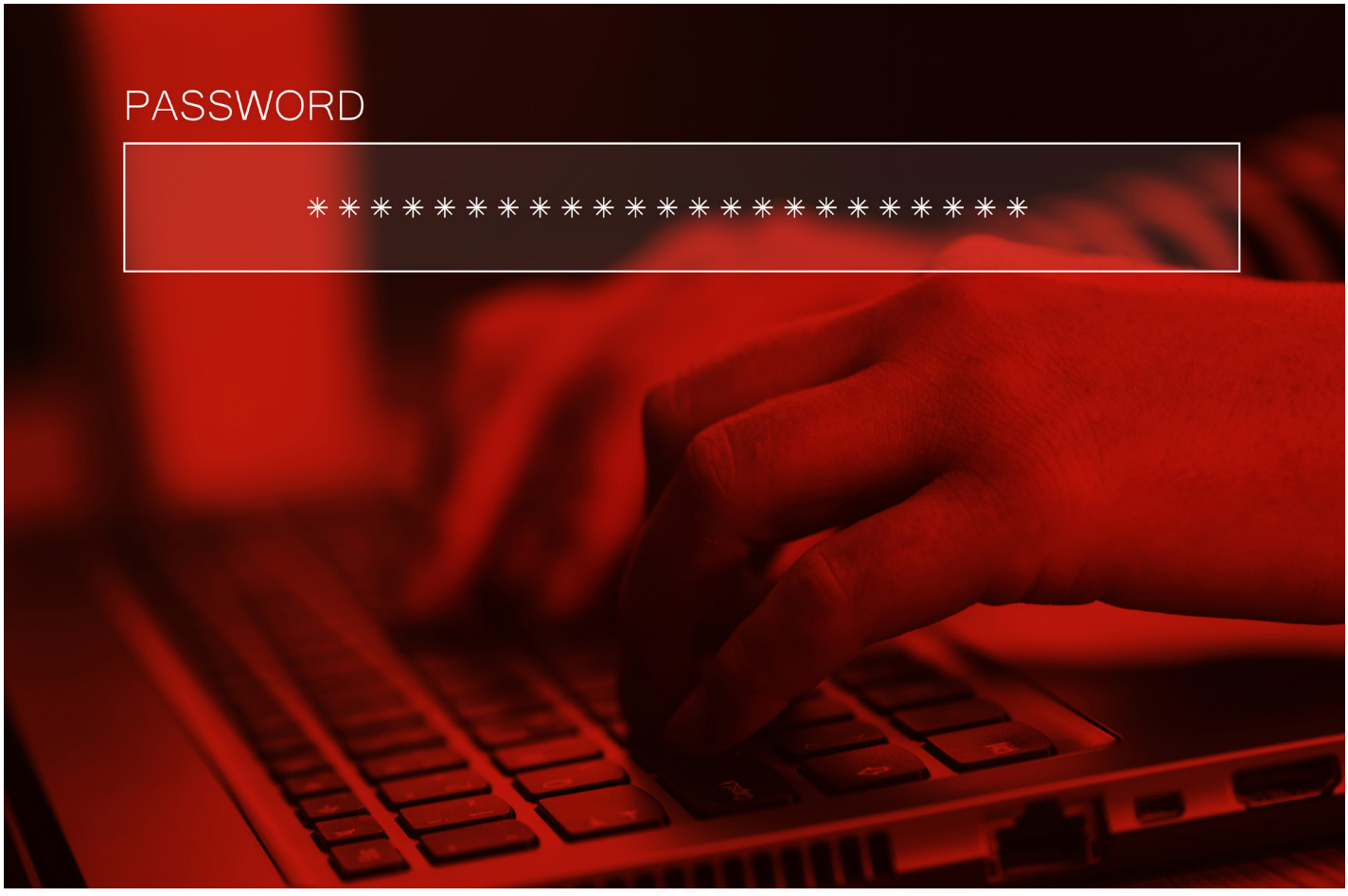
فصلنامه شرکت مهندسی شبکه گستر

# امنیت فناوری اطلاعات

سه ماهه چهارم سال ۱۳۹۵ / انتشار: اسفند ماه ۱۳۹۵

## در این شماره می خوانید





## شبکه گستر

در سومین 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 چهارم ۱۳۹۵ مورد بررسی قرار گرفته است. در این دوره نیز، بخش قابل توجهی از آلودگی‌های گزارش شده مربوط به باج‌افزارها بوده است. در سومین شماره از فصلنامه شرکت مهندسی شبکه گستر، چندین باج‌افزار از جمله باج‌افزارهای DynA-Crypt، Satan، CryptoMix و Spora که با عملکرد خاص خود کاربران را در فصل زمستان هدف قرار دادند مورد بررسی قرار گرفته است. گرچه نتایج یک تحقیق که مشروح آن را در این فصلنامه خواهید یافت نشان می‌دهد که برخی تبهکاران سایبری بدون نوشتن کدهای پیچیده و حرفه‌ای، تنها با ادعای رمزگذاری شدن اطلاعات دستگاه، موفق به اخاذی از بسیاری از سازمان‌های بزرگ می‌شوند.

همچنین در بهمن ماه محققان امنیتی از انتشار بدافزاری خبر دادند که هدف آن صنعت دفاعی آمریکا معرفی شده است. برخی از این افراد بدافزار مذکور را کار ایران دانسته‌اند که جزییات کامل آن را می‌توانید در این فصلنامه مطالعه کنید.

با پایان سال ۲۰۱۶، همانطور که در این شماره به آن پرداخته شده است سیستم عامل Google Android به‌عنوان آسیب‌پذیرترین نرم‌افزار و شرکت Oracle به‌عنوان تولیدکننده نرم‌افزار با بیشترین آسیب‌پذیری در این سال شناخته شدند. این رده‌بندی‌ها بر مبنای تعداد آسیب‌پذیری‌های گزارش شده توسط محققان در سال گذشته میلادی صورت گرفته است.

در زمستان امسال بیش از ۲۰ هکر و گروه نفوذگر اقدام به تغییر ظاهر سایت‌های مبتنی بر یکی از نسخه‌های آسیب‌پذیر سامانه مدیریت محتوای WordPress کردند که مطالعه مشروح آن در این فصلنامه به تمامی مدیران سایت توصیه می‌شود.

همچنین در آستانه فرا رسیدن سال نو بر آن شدیم تا بر اساس رویدادها و تجارب کسب شده در گذشته به بررسی و پیش‌بینی اتفاقات حوزه امنیت فناوری اطلاعات در سال ۹۶ بپردازیم. با این امید که همگی با آمادگی هر چه بیشتر سال جدید را آغاز کنیم.

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 بهعنوان 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

اخبار

# اخبار بد برای Yahoo، یکی پس از دیگری

به گزارش شرکت مهندسی شبکه گستر، ۲۷ بهمن ماه، شرکت Yahoo اقدام به ارسال ایمیل هشدار به آن دسته از کاربرانی کرد که احتمال می‌رود حساب کاربری آنها در جریان حملاتی در بین سال‌های ۲۰۱۵ و ۲۰۱۶ هک شده باشد.

در ایمیل، به کاربر اعلام می‌شود که ممکن است مهاجمان با جعل کوکی (Forged Cookie) به حساب کاربری او دست یافته باشند.

در آذر ماه نیز شرکت Yahoo اعلام کرد که در نفوذی که تاریخ آن به حدود سه سال پیش باز می‌گردد، اطلاعات حساب کاربری بیش از ۱ میلیارد کاربر این شرکت سرقت شده. کمتر از سه ماه قبل از آن نیز، Yahoo خبر داده بود که در اواخر سال ۲۰۱۴ در جریان یک نفوذ دولتی (State-Sponsored) جزییات حداقل ۵۰۰ میلیون حساب کاربری از شبکه این شرکت سرقت شده بودند.

در این حملات جعل کوکی، مهاجمان، سرویس‌دهنده را به‌نحوی فریب می‌دادند که بدون نیاز به استفاده از گذرواژه، به حساب کاربری قربانی دست پیدا کنند. در حقیقت مهاجمان بدون در اختیار داشتن گذرواژه، به‌عنوان کاربر اصالت‌سنجی شده به سرور متصل می‌شده‌اند.

در ایمیل ارسالی، بدون اشاره به نام کشوری، اجرای حمله دولتی اعلام شده است.

همچنین اعلام شده که آسیب‌پذیری به حمله جعل کوکی بر روی سرورهای این شرکت ترمیم شده است.

از کاربران خواسته شده تا با مراجعه به این لینک و مطالعه دستورالعمل آن، اقدامات احتیاطی را برای حفاظت از حساب کاربری خود در برابر حملات اجرا شده در نظر بگیرند.

در پی انتشار اخبار این هک‌ها، در ۳ اسفند ماه نیز اعلام شد که شرکت Verizon شرکت Yahoo را ۳۵۰ میلیون دلار کمتر از قیمت توافق شده اولیه خریداری خواهد کرد. در عین حال هر دو شرکت در رسیدگی و پرداخت جریمه‌ها و خسارات احتمالی به نهادهای قانونی و شاکیان ثالث، ناشی از این دو هک شریک خواهند بود. البته پرداخت خسارت احتمالی به سهامداران شاکی تنها توسط شرکت Yahoo انجام خواهد شد.

در اوایل مرداد امسال، شرکت Verizon بر سر خرید Yahoo با قیمت ۴٫۸۳ میلیارد دلار توافق کرد. هدف از این خرید ادغام دو شرکت Yahoo و AOL - که Verizon آن را در سال ۲۰۱۵ میلادی خرید - به‌منظور رقابت قدرتمندتر با غول‌های رسانه‌ای دیجیتال اعلام شده بود.

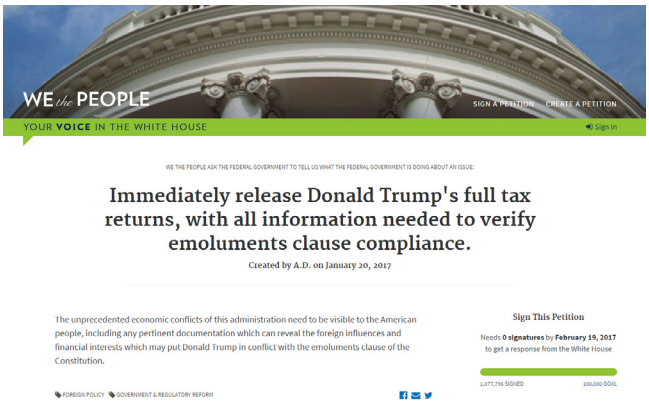
# درخواست WikiLeaks از هکرها برای انتشار اظهارنامه‌های مالیاتی ترامپ

به گزارش شرکت مهندسی شبکه گستر، WikiLeaks از مردم خواسته که با دست یافتن به اظهارنامه‌های مالیاتی دونالد ترامپ، رئیس جمهور جدید آمریکا آنها را به‌صورت ناشناس به این سازمان ارسال کنند تا از این طریق همگان از جزییات این اظهارنامه‌ها آگاه شوند.

این درخواست WikiLeaks پس از آن انجام شد که یکی از مشاوران ارشد ترامپ در گفتگو با شبکه ABC خبر داد که رئیس جمهور جدید قصد انتشار اظهارنامه‌های مالیاتی خود را ندارد.

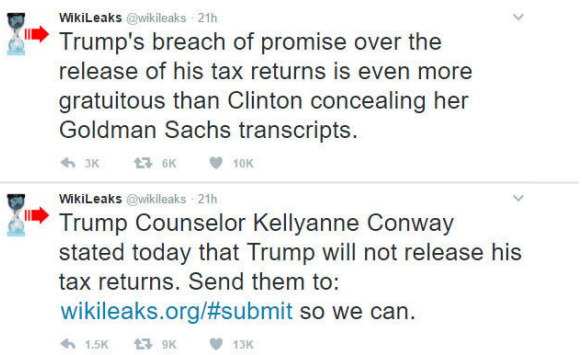
با وجود نظرسنجی انجام شده توسط ABC که نشان می‌دهد بسیاری از آمریکایی ها مایل به انتشار عمومی اظهارنامه مالیاتی ترامپ هستند این مشاور گفته: "مردم اهمیتی نمی‌دهند؛ آنها به او رأی دادند و اجازه بدهید که شفاف بگویم: بسیاری از آمریکایی‌ها در زمانی که ترامپ در دفتر ریاست جمهوری است بر روی اظهارنامه مالیاتی خودشان تمرکز دارند و نه اظهارنامه او."

این در حالی است که در روز تحلیف ترامپ بر روی سایت کاخ سفید دادخواستی اینترنتی تشکیل شد که در آن خواسته شده که جزییات کامل اظهارنامه‌های مالیاتی ترامپ اعلام شود. این دادخواست تا کنون توسط بیش از یک میلیون نفر امضاء شده است. بر طبق قوانین دادخواست‌های



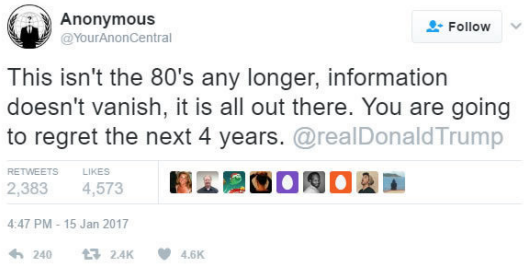

اینترنتی کاخ سفید در صورتی که تعداد امضاها تنها به ۱۰۰ هزار عدد برسد کاخ سفید ملزم به پاسخگویی می‌شود. گزارش شده که ترامپ در زمان انتخابات از انتشار اظهارنامه‌ها به بهانه تحت بررسی بودن آنها امتناع می‌کرده اما وعده داده بود که پس از پایان بررسی‌ها آنها را منتشر کند. اما در آن زمان هم برخی کارشناسان اعلام کردند که تحت بررسی بودن مغایرتی با انتشار عمومی اظهارنامه مالیاتی ندارد.

WikiLeaks هم که از امتناع ترامپ خشنود به نظر نمی‌رسد خلف وعده ترامپ در خصوص انتشار اظهارنامه‌های مالیاتی را از قضیه کمک‌های مالی



Goldman Sachs که خانم کلینتون آن را مخفی کرده بود بدتر دانسته و از کاربران خواسته که با دست یافتن به اطلاعات اظهارنامه و ارسال آنها به WikiLeaks این سازمان را قادر به انتشار آنها کنند.

WikiLeaks تنها سازمان و گروهی نیست که بدنبال انتشار برخط دادهای ترامپ است .گروه نفوذگران ناشناس (Anonymous) نیز پیش‌تر ادعا کرده بود که ترامپ ارتباطات مالی و شخصی با جنایتکاران، قاچاقچیان کودک و خلافکاران پول‌شوی روسی دارد. این گروه وعده داده که ترامپ در طی چهار سال آینده افسوس خواهد خورد.




بررسی و تحلیل حملات

**MAGIC HOUND**

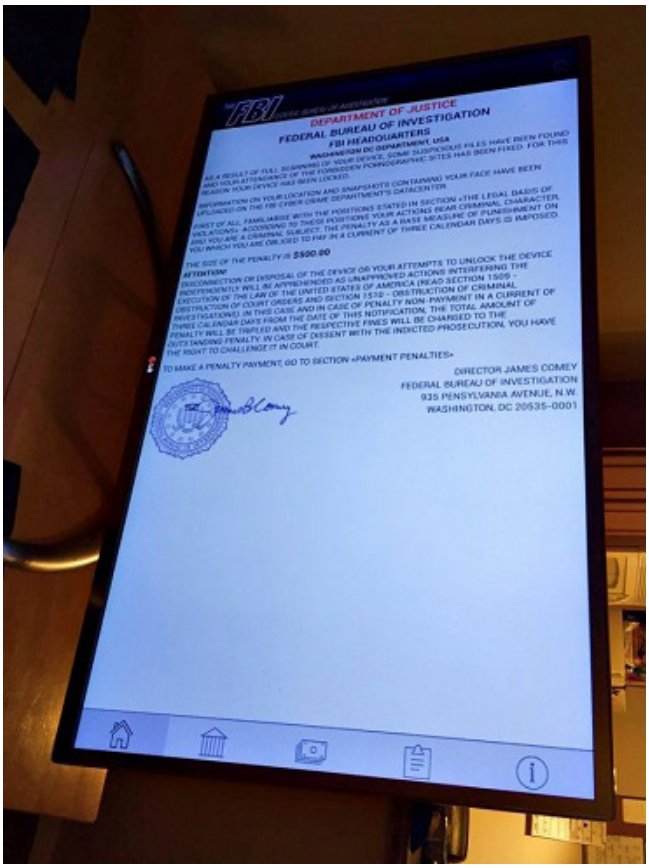
# آلودگی تلویزیون LG به باج‌افزار

به گزارش شرکت منهدسی شبکه گستر به نقل از سایت HackRead.com، کاربری در حساب Twitter خود مطلبی را به اشتراک گذاشته و در آن از آلوده شدن یک تلویزیون هوشمند LG با پلتفرم Google TV به باج‌افزار تحت سیستم عامل Android خبر داده است.


بر طبق توضیحات این کاربر با هر بار روشن شدن تلویزیون آلوده شده به این باج‌افزار، تصویری ثابت بر روی صفحه نمایش داده می‌شود. در این تصویر این طور وانمود می‌شود که دسترسی به دستگاه، توسط پلیس FBI محدود شده و ضمن منع کاربر به انجام هر گونه عملیات بازگشایی دسترسی به دستگاه، از او می‌خواهد تا مبلغ ۵۰۰ دلار را به عنوان غرامت - در حقیقت باج - پرداخت کند.

بر خلاف باج‌افزارهای رمزگذار، خلاص شدن از شر باج‌افزارهای قفل‌کننده تصویر کار چندان دشواری نیست.

این کاربر نیز پس تماس با شرکت LG Electronics و دریافت دستورالعمل Factory Rest دستگاه، موفق به حذف این باج‌افزار شده است. هر چند که کاملاً مشخص است اجرای این عملیات سبب پاک شدن تمامی تنظیمات پیکربندی شده غیرپیش‌فرض دستگاه نیز می‌شود.



# انتشار تلفنی باج‌افزار!

به گزارش شرکت مهندسی شبکه گستر، مؤسسه انگلیسی Action Fraud با صدور اطلاعیه‌ای به مؤسسات آموزشی این کشور نسبت به اجرای حملات کلاهبرداری تلفنی هشدار داده است. در جریان این حملات مهاجمان با برقراری تماس تلفنی، مقامات ارشد مؤسسه را مجاب به باز کردن ایمیل با فایل مخربی می‌کنند که با اجرا شدن آن در نهایت دستگاه به نمونه‌ای باج‌افزار آلوده می‌شود.

بر اساس اطلاعیه صادر شده، مهاجمان این حملات خود را نماینده یک سازمان دولتی با عنوان "Department of Education" معرفی کرده و از پاسخ‌دهنده تلفن می‌خواهند که شماره تماس و ایمیل مدیر یا مسئول مالی مؤسسه آموزشی را در اختیار آنها قرار دهد. این در حالی است که "Department for Education"، نام صحیح این سازمان انگلیسی است.

برای متقاعد کردن فرد پاسخ‌دهنده تماس، مهاجمان اعلام می‌کنند که قصد ارسال ایمیلی حاوی اطلاعات حساس را داشته و می‌خواهند مطمئن شوند که این اطلاعات تنها به دست این مقامات مؤسسه آموزشی رسیده و در صندوق‌های پست الکترونیکی عمومی مؤسسه برای افراد غیرمجاز قابل دسترس نباشد.

در بسیاری موارد، مهاجمان، این اطلاعات حساس را شامل دستورالعمل امتحان یا روال ارزیابی سلامت روان معرفی می‌کنند.

با دریافت اطلاعات درخواستی، مهاجمان اقدام به ارسال ایمیلی با پیوست فایل فشرده شده ZIP می‌کنند. فایل فشرده شده خود حاوی یک فایل Word یا Excel است که با باز شدن آن توسط کاربر دستگاه او به باج‌افزار آلوده می‌شود.

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 برخی نمونه‌ها مبلغ اخاذی شده حدود ۸ هزار پوند (حدود ۳۹۰ میلیون ریال) اعلام شده است.

به گزارش شرکت مهندسی شبکه گستر، اجرای حملات کلاهبرداری (Phishing) از طریق تماس تلفنی موضوعی بی‌سابقه نیست. برای مثال، مهاجمان گروه Carbanak با برقراری تماس تلفنی با مدیران شبکه سازمان‌های بزرگ، با بکارگیری روش‌ها و ترفندهای مهندسی اجتماعی، آنها را وادار به نصب بدافزار می‌کردند.

آگاهی‌رسانی به کاربران، نقشی بسیار بااهمیت در مقابله با ترفندهای مهندسی اجتماعی تبهکاران سایبری دارد.

# شبکه گستر
## کارگاه‌های 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 |

## دیواره‌های 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.

## دوره‌های 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 |

# وجود آسیب‌پذیری‌های متعدد در سرورهای پنتاگون

وجـــود ســـرورهای آســـیب‌پذیر در وزارت دفـــاع آمریـــکا بـــه راحتـــی مهاجمـــان ســـایبری را قـــادر بـــه بهره‌جویـــی از آنهـــا می‌کنـــد. ایـــن نتیجـــه بررســـی محققـــی اســـت کـــه در پـــروژه "Hack the Pentagon" (پنتاگـــون را هـــک کنیـــد) شـــرکت داشـــته اســـت.

وزارت دفـــاع آمریـــکا، از ســـال گذشـــته میـــلادی، در جریـــان ایـــن پـــروژه از نفوذگـــران خواســـته کـــه وضعیـــت امنیتـــی ســـایت defense.gov و هـــر ســـایت بـــا دامنـــه اینترنتـــی mil. را بررســـی کـــرده و اشـــکالات یافـــت شـــده را گـــزارش کننـــد.

بـــه نظـــر مـــی رســـد پـــروژه "Hack the Pentagon" از برنامه‌هـــای "Bug Bounty" الگوبـــرداری شـــده اســـت. در ایـــن برنامه‌هـــا شـــرکت‌های ســـازنده نرم‌افـــزار و توســـعه‌دهنده ســـایت بـــه نفوذگرانـــی کـــه وجـــود ضعف‌هـــای امنیتـــی را در محصـــولات ایـــن شـــرکت‌ها گـــزارش کننـــد پـــاداش اعطـــا می‌کننـــد.

بـــه گـــزارش شـــرکت مهندســـی شـــبکه گســـتر، ایـــن محقـــق در گفتگـــو بـــا ســـایت ZDNet گفتـــه:

"ســـرورهایی بـــوده کـــه پیکربنـــدی امنیتـــی آنهـــا دارای اشـــکالات اساســـی اســـت و بســـادگی یـــک مهاجـــم در داخـــل خـــاک آمریـــکا و یـــا خـــارج از ایـــن کشـــور می‌توانـــد از آنهـــا بهره‌جویـــی کنـــد."

بـــرای مثـــال، مهاجـــم می‌توانـــد بـــا سوءاســـتفاده از ایـــن اشـــکالات از ســـوی ایـــن ســـرورها اقـــدام بـــه اجـــرای حملـــه کنـــد. بـــه ایـــن ترتیـــب اجـــرا کننـــده حملـــه نـــه آن مهاجـــم کـــه وزارت دفـــاع آمریـــکا بـــه نظـــر خواهـــد رســـید.

ایـــن محقـــق توضیـــح داده کـــه بـــدون هـــر گونـــه مشـــکل و دشـــواری موفـــق بـــه شناســـایی ایـــن آســـیب‌پذیری‌ها شـــده اســـت.

هـــر چنـــد گفتـــه می‌شـــود شـــبکه‌های وزارت دفـــاع آمریـــکا حـــاوی اطلاعـــات محرمانـــه و ســـری نبـــوده و نفـــوذ بـــه ایـــن سیســـتم‌ها مهاجـــم را بـــه اطلاعـــات حساســـی نظیـــر سیســـتم‌های دفـــاع موشـــکی نمی‌رســـاند امـــا عـــدم ترمیـــم ایـــن آســـیب‌پذیری‌ها بـــا وجـــود گـــزارش شـــدن آنهـــا بـــه ایـــن وزارتخانـــه موضوعـــی ســـئوال برانگیـــز بـــه نظـــر می‌رســـد.

# ارسال اشتباه ایمیل و وارد آمدن خسارت چندمیلیون دلاری به بوئینگ

به گزارش شرکت مهندسی شبکه گستر، یکی از کارکنان شرکت بوئینگ با ارسال فایلی به همسرش با هدف حل یک مساله قالب‌بندی فایل، سهواً سبب نشت اطلاعات شخصی ۳۶ هزار نفر از همکاران خود شده است.

خبر این درز اطلاعات زمانی عمومی شد که نامه ارسالی معاون بخش حریم خصوصی بوئینگ به دادستانی واشنگتن بر روی یک سایت منتشر شد.

قوانین ۴۷ ایالت آمریکا از جمله واشنگتن شرکت‌ها و سازمان‌های دولتی را ملزم می‌کند وقوع هر گونه نشت داده شامل اطلاعات شخصی را اعلام کنند. بر طبق قوانین واشنگتن در صورتی که نشت داده مربوط به بیش از ۵۰۰ شهروند این ایالت شود، موضوع می‌بایست به دفتر دادستانی گزارش شود. ۷,۲۸۸ نفر از این ۳۶ هزار نفر شهروندان این ایالت بوده‌اند.

بر اساس نامه مذکور، ارسال فایل در ۱ آذر ۱۳۹۵ صورت گرفته بوده. بر طبق توضیحات این نامه، قصد این کارمند از این ارسال صرفاً حل مساله‌ای در خصوص قالب‌بندی یک فایل صفحه‌گسترده بوده است.

فایل مذکور شامل اطلاعاتی نظیر نام و شماره ملی ۳۶ هزار کارمند این شرکت بوده است.

به گزارش شرکت مهندسی شبکه گستر، شرکت بوئینگ در ۲۰ دی ۱۳۹۵ متوجه وقوع این نشت داده شده و بررسی‌های قانونی خود را بر روی کامپیوترهای کارمند و همسر او برای اطمینان از حذف شدن این اطلاعات آغاز می‌کند.

این کارمند و همسرش هر دو گفته‌اند که اطلاعات ثبت شده در فایل را توزیع نکرده و از آنها هیچ استفاده‌ای نکرده‌اند.

بوئینگ نیز اعلام نموده که معتقد است که از این داده‌ها به شکلی نادرست استفاده نشده و نخواهد شد.

در پی این حادثه، شرکت بوئینگ، بزرگترین پیمانکار دفاعی جهان پس از Lockheed Martin، حق دسترسی به سرویس حفاظت در برابر سرقت هویت را برای مدت دو سال به‌صورت رایگان به کارکنان خود داده است.

همچنین این شرکت خبر داده که برنامه‌های آموزشی بیشتری را برای کارکنان خود برگزار خواهد کرد و کنترل‌های جدیدی را در آینده‌ای نزدیک پیاده‌سازی خواهد نمود.

منظور از نشت داده، دست یافتن عمدی یا غیرعمدی شخص، گروه یا سازمانی غیرمجاز به داده خصوصی یا محرمانه است.

نتایج یک تحقیق نشان می‌دهد که میانگین خسارت ناشی از هر نشت داده در سال ۲۰۱۶ حدود ۴ میلیون دلار بوده است. اما The Register خسارت وارد شده به شرکت بوئینگ در جریان این ارسال نادرست ایمیل را ۵/۷ میلیون دلار اعلام کرده است.


# حمله باج‌افزارها به سرورهای ایرانی

به گزارش شرکت مهندسی شبکه گستر به نقل از مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر)، به تازگی، گزارش‌های متعددی از حمله باج‌افزارها به سرورهای با سیستم عامل Windows در کشور به این مرکز واصل شده است.

بررسی‌های فنی این مرکز نشان داده که در این حملات مهاجم یا مهاجمان با سواستفاده از دسترسی‌های حفاظت نشده به سرویس Remote Desktop (پودمان RDP)، وارد شده و با انتقال فایل باج‌افزار اقدام به رمزگزاری فایل‌های سرور می‌نماید.

در این حملات مهاجم با سواستفاده از نسخه‌های آسیب‌پذیر سرویس Remote Desktop و یا گذرواژه ضعیف وارد سرور می‌گردد.

استفاده از ضدبدافزار به‌روز و قدرتمند، مسدود نمودن سرویس‌های غیرضروری Remote Desktop، کنترل پودمان RDP بر روی دیواره آتش، بکارگیری گذرواژه‌های پیچیده با طول مناسب و اطمینان از نصب بودن آخرین بسته‌ها و اصلاحیه‌های امنیتی توصیه می‌شود.

بدافزارها

# صنعت دفاعی آمریکا هدف بدافزاری جدید؛ کاشفان آن: بدافزار کار ایران است

به گزارش شرکت مهندسی شبکه گستر، دو محقق امنیتی در مقاله‌ای از انتشار بدافزاری خبر داده‌اند که دستگاه‌های با سیستم عامل Windows یا macOS را در صنعت دفاعی آمریکا هدف قرار داده است. این محققان بدافزار مذکور را محصول ایران می‌دانند.

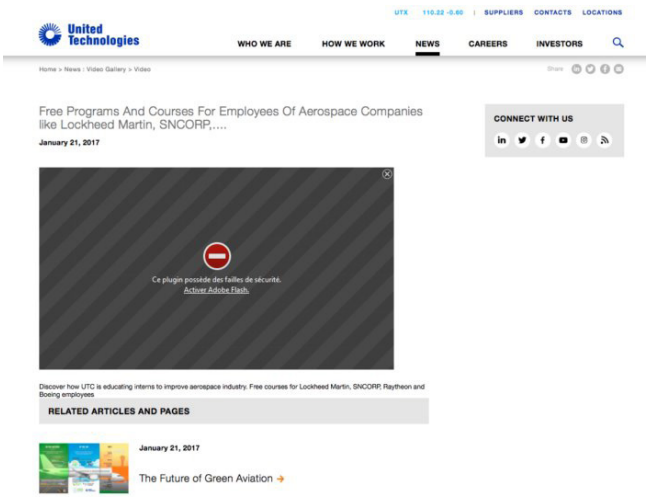
بدافزار بررسی شده که با نام MacDownloader شناخته می‌شود بر روی سایتی که نام و نشان یک شرکت فضانوردی آمریکایی با عنوان United Technologies را جعل کرده کشف شده است.

از این سایت جعلی پیش‌تر نیز برای اجرای حملات Phishing و انتشار بدافزار تحت سیستم عامل Windows استفاده شده بود.

این محققان ادعا می‌کنند که این سایت توسط هکرهای ایرانی مدیریت می‌شود.

بازدیدکنندگان از این سایت با صفحه‌ای روبرو می‌شوند که در ظاهر در آن برنامه‌ها و دوره‌های ویژه کارکنان شرکت‌های معروف هوافضای آمریکایی نظیر Raytheon، Lockheed Martin و Boeing به رایگان قابل دریافت است.

در صفحه مذکور در کادری مشابه افزونه‌های Adobe Flash به زبان فرانسوی گفته می‌شود که افزونه دارای اشکالات امنیتی است. در زیر آن نیز لینکی قرار دارد که در آن از کاربر خواسته می‌شود تا با کلیک بر روی آن Adobe Flash را فعال کند.




در صورت کلیک کاربر بر روی لینک مذکور، بر اساس سیستم عامل دستگاه، نسخه تحت سیستم عامل Windows یا macOS بر روی دستگاه قربانی دانلود می‌شود. فایل دریافت شده بر روی دستگاه با سیستم عامل macOS در برخی نمونه‌ها addone flashplayer.app و در برخی دیگر Bitdefender Adware Removal Tool نام دارد که با اجرای آن دستگاه آلوده می‌شود. این محققان وجود نویسه e پس از کلمه addon را نشانه‌ای دیگر از فارسی زبان بودن نویسنده یا نویسندگان بدافزار می‌دانند.

بدافزار در دستگاه با سیستم عامل macOS با نمایش پنجره‌های دروغین ورود به سیستم و سرقت بانک‌های داده Apple Keychain اطلاعات اصالت‌سنجی قربانی را جمع‌آوری کرده و در ادامه آنها را به سرور فرماندهی بدافزار ارسال می‌کند.

به گزارش شرکت مهندسی شبکه گستر، این محققان این

بدافـزار را محصـول کار یـک برنامه‌نویـس آماتـور دانسـته‌اند. ضمـن اینکـه وجـود اشـکالات تایپـی و گرامـری در پیام‌هـای نمایـش داده شـده را نشـانه‌ای از عـدم اعمـال روالـی بـرای کنتـرل کیفیـت در زمـان برنامه‌نویسـی آن معرفـی کرده‌انـد. همچنیـن یـک از قابلیت‌هـای در نظـر گرفتـه شـده توسـط نویسـنده یـا نویسـندگان ایـن بدافـزار امـکان دانلـود فایل‌هـای مخـرب دیگـر بـر روی دسـتگاه macOS آلـوده شـده اسـت. قابلیتـی کـه حداقـل در نسـخه بررسـی شـده توسـط ایـن محققـان بـه طـور صحیـح عمـل نمی‌کنـد. بـا ایـن حـال، همانطـور کـه ایـن محققـان اشـاره کرده‌انـد در زمـان بررسـی، بدافـزار توسـط هیـچ یـک از محصـولات ضدویـروس قابـل شناسـایی نبـوده. در زمـان نـگارش ایـن خبـر نیـز تنهـا تعـداد محـدودی از نرم‌افزارهـای ضدویـروس قـادر بـه شناسـایی آن شـده‌اند. موضوعـی کـه آماتـور بـودن نویسـنده را بشـدت نقـض می‌کنـد.


ایـن دو محقـق، در جریـان بررسـی‌ها بـه دو شـبکه بی‌سـیم بـا نام‌هـای Jok3r و mb_1986 رسـیده‌اند. بـه ایـن نام‌هـا پیش‌تـر نیـز در چندیـن حملـه سـایبری کـه اجراکننـدگان آن نفوذگـران ایرانـی معرفـی شـده بودنـد اشـاره شـده بـود. مشـروح گـزارش بررسـی ایـن محققـان در اینجـا قابـل مطالعـه اسـت.


# انتشار نسخه جدید باج‌افزار CryptoMix

نسخه‌ای جدید از باج‌افزار CryptoMix - که با نام‌های CrypMix و CryptoShield نیز شناخته می‌شود - از طریق سایت‌های مخرب و تسخیر شده اقدام به آلوده کردن سیستم‌ها و رمزگذاری فایل‌های آنها می‌کند.

در زمان مراجعه کاربر به این سایت‌ها، کد مخرب تزریق شده در صفحه اینترنتی با سوءاستفاده از ضعف‌های امنیتی موجود در سیستم عامل Windows و نرم‌افزارهایی نظیر Adobe Reader، Adobe Flash و Oracle Java که بر روی دستگاه کاربر نصب شده‌اند، باج‌افزار را بر روی سیستم نصب می‌کند.

نویسنده این باج‌افزار از بسته‌های بهره‌جوی EITest و RIG برای این منظور استفاده می‌کند. بسته بهره‌جو (Exploit Kit) امکان سوءاستفاده از آسیب‌پذیری‌های موجود را برای ویروس‌نویس یا مهاجم فراهم می‌کند. بنابراین نصب بودن آخرین اصلاحیه‌های امنیتی می‌تواند دستگاه را از گزند آلوده شدن به این نسخه خاص از CryptoMix مصون نگاه دارد.

پس از دریافت و اجرای باج‌افزار بر روی سیستم شناسه‌ای منحصربه‌فرد و یک کلید رمزگذاری بر روی سیستم ایجاد شده و به سرور فرماندهی (Command & Control) ارسال می‌شود. در ادامه باج‌افزار اقدام به شناسایی و رمزگذاری فایل‌های با پسوندهای رایج می‌کند.

CryptoMix از الگوریتم‌های AES-256 و ROT-13 به ترتیب برای رمزگذاری فایل و تغییر نام و پسوند فایل استفاده می‌کند. برای مثال، فایلی با نام test.jpg پس از رمز شدن به grfg.wct.CRYPTOSHIELDD تغییر می‌کند.

بازگرداندن نام و پسوند فایل به حالت اولیه از طریق ابزارهای رمزگشایی ROT-13 نظیر سایت rot13.com امکان‌پذیر است. اما متأسفانه حداقل در زمان نگارش این خبر امکان رمزگشایی محتوای فایل بدون پرداخت باج ممکن نیست.

همچنین در هر پوشه‌ای که حداقل یکی از فایل‌های آن رمزگذاری شده است اطلاعیه باج‌گیری (Ransom Note) با نام‌های # RESTORING FILES #.HTML و # RESTORING FILES #.TXT نیز کپی می‌شود.

این باج‌افزار به‌منظور غیرفعال کردن امکان بازگردانی از طریق بخش Windows Startup و حذف نسخه‌های Windows Shadow Volume از فرامین زیر استفاده می‌کند:

cmd.exe /C bcdedit /set {default} recoveryenabled No

cmd.exe /C bcdedit /set {default} bootstatuspolicy ignoreallfailures

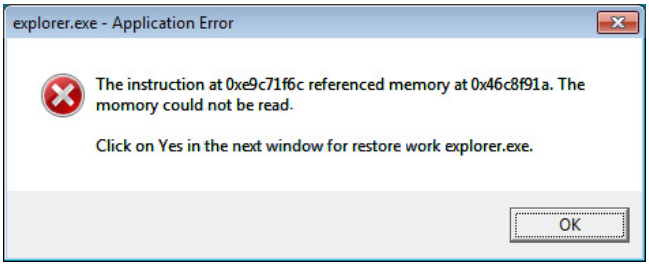
“C:\Windows\System32\cmd.exe”

/C vssadmin.exe Delete Shadows /All /Quiet

“C:\Windows\System32\cmd.exe”

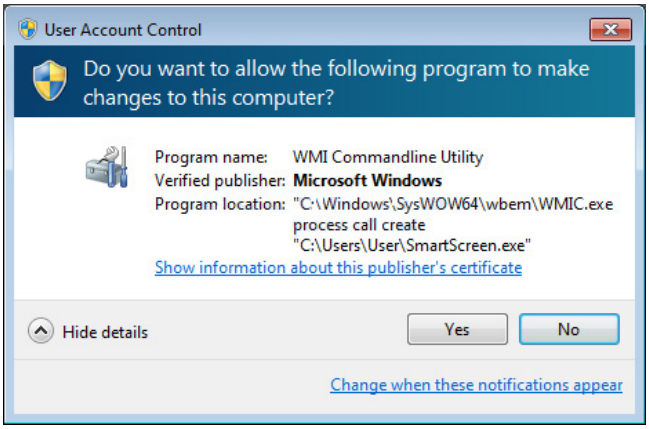
/C net stop vss

در ادامه یک پنجره خطای جعلی مشابه شکل زیر نمایش داده شده و از کاربر خواسته می‌شود در پنجره‌ای که در مرحله بعد ظاهر می‌شود بر روی دکمه Yes کلیک کند.

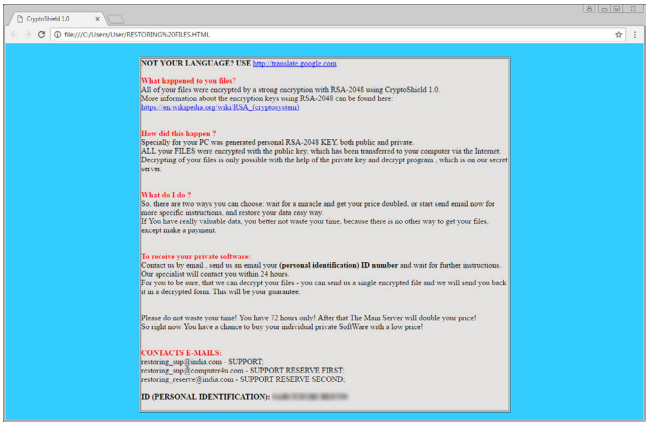



نکته قابل توجه در این پنجره املای نادرست کلمه memory است که در بخشی از پیام به صورت momory درج شده است.


با کلیک بر روی دگمه OK بخش UAC سیستم عامل از کاربر جهت ایجاد پروسه SmartScreen.exe اجازه می‌گیرد. در اینجا دلیل نمایش پنجره قبلی مشخص می‌شود.




با کلیک بر روی دگمه Yes اطلاعیه باج‌گیری مطابق شکل زیر ظاهر می‌شود.




باج‌گیر در این اطلاعیه باج‌افزار را با عنوان CryptoShield 1.0 معرفی کرده است.

در این اطلاعیه از کاربر خواسته می‌شود با برقراری تماس با نویسنده باج‌افزار دستورالعمل پرداخت باج را دریافت کند.

restoring_sup@india.com

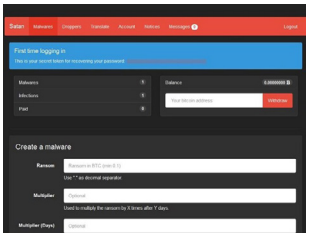
restoring_sup@computer4u.com

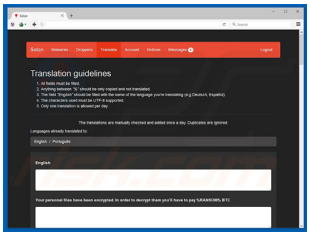
restoring_reserve@india.com

از جمله نشانی‌های ایمیل استفاده شده در این نسخه از CryptoMix هستند.

## Satan، نمونه‌ای از باج‌افزار به‌عنوان سرویس

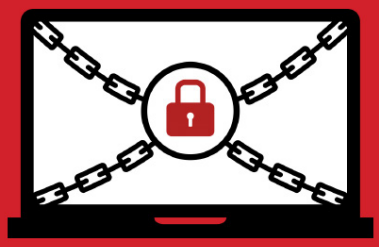
باج‌افزارهای رمزگذار را می‌توان یکی از مخرب‌ترین و همچنین رایج‌ترین تهدیدات دو سال اخیر قلمداد کرد. یکی از عوامل نگران‌کننده که انتظار می‌رود سبب افزایش انتشار و گسترش این نوع بدافزارها شود عرضه باج‌افزار در قالب خدماتی موسوم به Ransomware-as-a-Service است. در این روش، نویسنده باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به نویسنده و بخشی دیگر به متقاضی می‌رسد. به گزارش شرکت مهندسی شبکه گستر به نقل از سایت PCrisk.com، گونه جدیدی از باج‌افزارها با نام Satan در قالب باج‌افزار به‌عنوان سرویس در بازار زیرزمینی سایبری Dark Web ارائه شده است. این باج‌افزار پسوند فایل‌های رمز شده را به stn. تغییر می‌دهد. در فایل HTML اطلاعیه باج‌گیری (Ransom Note) ادعا می‌شود که فایل‌های کاربر رمز شده و برگرداندن آنها به حالت اولیه بدون پرداخت باج عملاً غیرممکن است؛ ادعایی که با در نظر گرفتن استفاده این باج‌افزار از الگوریتم‌های رمزگذاری RSA-2048 و AES-256 و نگهداری کلید خصوصی بر روی سرور فرماندهی ویروس‌نویسان حداقل در حال حاضر صحیح به نظر می‌رسد. متقاضی بدخواه با مراجعه به سایت نویسنده یا نویسندگان Satan بر روی شبکه Dark Web پس از معرفی یک کیف بیت‌کوین (Bitcoin Wallet) و مقدار مبلغ باج - بر اساس بیت کوین - می‌تواند فایل مخرب را دریافت کند. همچنین متقاضی قادر است تا اطلاعیه باج گیری را سفارشی کرده و حتی آن را به زبانی غیرانگلیسی درج کند. پس از دریافت فایل مخرب، متقاضی می‌تواند با هر روش اقدام به آلوده نمودن دستگاه‌های قربانی کرده و در صورت پرداخت باج توسط قربانی ۷۰ درصد مبلغ اخاذی شده را از آن خود کند. ۳۰ درصد مبلغ نیز به جیب نویسنده یا نویسندگان باج‌افزار می‌رود. تخمین زده می‌شود تنها در سال ۲۰۱۶ میلادی باج‌افزارها مسبب وارد آمدن ۱ میلیارد خسارت شده باشند.




بـررسـی و تحلیل بـاج‌افـزار

VIRLOCK



# DynA-Crypt؛ رمزگذار سارق

محققان از انتشار نسخه جدیدی از باج‌افزار DynA-Crypt خبر داده‌اند که از طریق یک ابزار ساخت بدافزار به چند قابلیت مخرب جدید مجهز شده است. به گزارش شرکت مهندسی شبکه گستر، نسخه جدید نه تنها فایل‌ها را رمزگذاری می‌کند بلکه انبوهی از اطلاعات را از روی دستگاه قربانی سرقت می‌کند. بدین‌منظور DynA-Crypt از پنجره‌های فعال تصویربرداری کرده و صدا را با بهره‌گیری از میکروفون دستگاه ضبط می‌کند. همچنین کلیدهای فشرده شده بر روی صفحه کلید نیز توسط این نسخه از باج‌افزار DynA-Crypt ثبت می‌شود. اطلاعات فوق و داده‌های حساس نرم‌افزارهای متعددی از جمله Skype و Chrome در مسیر %LocalAppData%\dyna\loot کپی می‌شوند. اطلاعات جمع‌آوری شده در زمان مقرر با پسوند ZIP فشرده شده و به نویسنده یا نویسندگان باج‌افزار ارسال می‌شود. به گزارش شرکت مهندسی شبکه گستر، این نسخه از باج‌افزار DynA-Crypt فایل‌های با پسوند زیر را شناسایی کرده و به آنها پسوند crypt الصاق می‌کند.

.jpg, .jpeg, .docx, .doc, .xlsx, .xls, .ppt, .pdf, .mp4, .mp3, .mov, .mkv, .png, .pst, .odt, .avi, .pptx, .msg, .rar, .mdb, .zip, .m4a, .csv, .001

هچنین نسخه‌های Shadow Volume نیز از روی دستگاه قربانی حذف می‌شود. در نهایت نیز باج‌افزار صفحه را با نمایش تصویری مشابه شکل زیر قفل می‌کند. در تصویر از کاربر خواسته می‌شود تا مبلغ ۵۰ دلار را به بیت‌کوین پرداخت کند تا دسترسی به داده‌ها و دستگاه مجدد برقرار شود. خبر خوش اینکه روش رمزنگاری استفاده شده در نسخه بررسی شده قدرتمند نبوده و داده‌ها را می‌توان بدون نیاز به پرداخت باج بازگشایی کرد.



بررسی و تحلیل باج‌افزار

## Sage 2.0


# Spora؛ باج‌افزاری با خدمات پس از آلودگی عالی!

همانطور که در خبر مربوط به انتشار نخستین نسخه از باج‌افزار Spora در دی ماه در اتاق خبر شرکت مهندسی شبکه گستر اشاره شد از جمله خدمات ارائه شده توسط تبهکاران صاحب این باج‌افزار پورتال ویژه‌ای است که قربانیان می‌توانند از طریق شناسه آلودگی درج شده در اطلاعیه باج‌افزار به آن متصل شوند. پورتالی که علاوه بر امکانات منحصربه‌فرد خود مجهز به بخشی برای گفتگوی زنده قربانیان با صاحبان باج‌افزار Spora است.

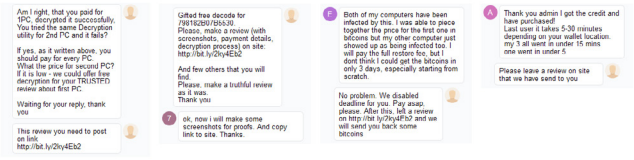
به گزارش شرکت مهندسی شبکه گستر، محققان گروه MalwareHunter موفق شده‌اند که با تغییر شناسه یک نمونه آلودگی، به پورتال چندین قربانی این باج‌افزار متصل شده و ارتباطات بین این قربانیان و صاحبان Spora را رصد کنند.

آنچه که مشخص است صاحبان این باج افزار توجه‌ای خاص به پشتیبانی از مشتریان یا بهتر بگوییم قربانیان خود دارند.

به گزارش شرکت مهندسی شبکه گستر، صاحبان Spora پشتیبانی را به دو زبان انگلیسی و روسی ارائه کرده و به سئوالات و ابهامات مشتریان عصبانی در نهایت ادب و احترام و با صرف زمان کافی پاسخ می‌دهند.

در خصوص قربانیانی که قادر به پرداخت باج در مهلت تعیین شده نیستند صاحبان Spora با ملایمت و خوش‌رویی این مهلت را برای این قشر از مشتریان خود یا تمدید کرده یا به طور کامل غیرفعال می‌کنند.

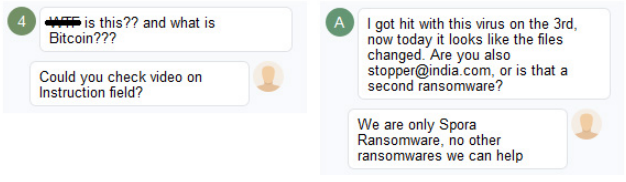
همچنین صاحبان Spora به آن دسته از قربانیانی که تجاربشان را از کیفیت پشتیبانی این باج‌افزار در تالار گفتگوی اینترنتی سایت Bleeping Computer که به بررسی باج‌افزارها شهرت دارد به اشتراک بگذارند تخفیف رمزگشایی و یا حتی امکان رمزگشایی رایگان ارائه می‌دهند.



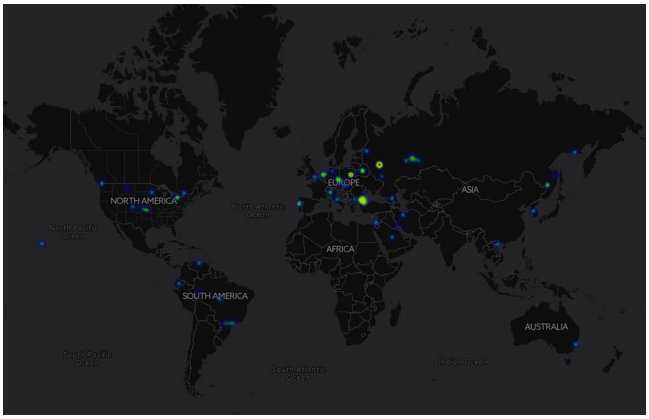
به گزارش شرکت مهندسی شبکه گستر به نقل از سایت Bleeping Computer، تا تاریخ ۱۸ بهمن ماه هیچ کاربری نسبت به درج چنین توضیحی بر روی این تالار گفتگو اقدام نکرده است. در طی دو سال گذشته نمونه‌هایی از باج‌افزارها بوده‌اند که حتی در صورت پرداخت باج توسط قربانی عملیات رمزگشایی را انجام نمی‌دادند. برای اینگونه باج‌افزارهای کلاهبردار که از ابتدا قصد برگرداندن اطلاعات قربانی را ندارند و فقط سعی در گرفتن پول از قربانی دارند، از اصطلاح Ranscamm که خلاصه شده Ransome Scam است، استفاده می‌شود. به‌نظر می‌رسد هدف صاحبان Spora از این پیشنهاد، اطمینان خاطر دادن به قربانیان خود در خصوص رمزگشایی شدن فایل‌ها با پرداخت باج بوده باشد.

در نمونه‌ای دیگر این افراد به شرکتی که بیش از ۲۰۰ دستگاه آن به این باج‌افزار آلوده شده بود تخفیف ۱۰ درصدی دادند.

گروه MalwareHunter پشتیبانی صاحبان Spora را از بخش



پشـتیبانی بسـیاری از شـرکت‌های فنـاوری کاربرپسـندتر و کمک‌کننده‌تـر توصیـف کـرده اسـت. صاحبـان ایـن باج‌افـزار خدمـات خـود را در قالـب بسـته‌های "بازگردانـی کامـل"، "مصونیـت در برابـر حمـلات آتـی باج‌افـزار"، "حـذف باج‌افـزار" و "بازگردانـی فقـط فایـل" بـه قربانیـان خـود ارائـه می‌دهنـد. بررسـی‌های انجـام شـده نشـان می‌دهـد کـه در صـورت خریـد بسـته "مصونیـت در برابـر حمـلات آتـی باج‌افـزار" ابـزاری در اختیـار کاربـر قـرار می‌گیـرد کـه بـا اجـرای آن در مسـیر ٪appdata٪ فایلـی بـا شـماره سـریال Volume دسـتگاه ایجـاد می‌شـود. هـر چنـد تعـداد آلودگـی بـه این باج‌افـزار فاصلـه زیـادی بـا دامنـه گسـترده آلودگـی بـه باج‌افزارهـای معروفـی نظیـر Cerber و Locky دارد امـا ارائـه خدمـات پشـتیبانی حرفـه‌ای و مبتکرانـه توسـط صاحبـان ایـن باج‌افـزار نشـانه‌ای از قصد ایـن تبهـکاران بـرای توسـعه هـر چـه بیشـتر ایـن کسـب و کار کثیف اسـت.




## باج‌افزارهای رمزکننده Master Boot Record

# بدافزار مخرب KillDisk هم باج‌افزار شد

به گزارش شرکت مهندسی شبکه گستر، بدافزار مخرب و معروف KillDisk که تا اندکی پیش، سیستم عامل کامپیوترها را با حذف فایل‌های سیستمی و اصلی آنها از کار می‌انداخت اکنون با قابلیت جدید باج‌افزاری خود مبلغ کلانی را از قربانیان اخاذی می‌کند. KillDisk، بدافزاری برای اجرای عملیات جاسوسی و خرابکاری (Cyber Espionage & Sabotage) سایبری بوده و اهداف اصلی آن معمولاً بخش‌های صنعتی است. گردانندگان این بدافزار با دو نام Sandworm و TeleBots شناخته می‌شوند. گروه Sandworm در سال ۲۰۱۴، سیستم‌های کنترل صنعتی (ICS) و تجهیزات سامانه‌های سرپرستی و گردآوری داده (SCADA) آمریکا را هدف قرار داده بودند. به نظر می‌رسد گروه TeleBots همان گروه Sandworm است که بدافزاری از نوع درب‌پشتی (Backdoor) و همچنین بدافزار KillDisk را توسعه داده‌اند. گروه دیگری نیز با نام BlackEnergy در دو سال اخیر از KillDisk برای حمله به شرکت‌های اوکراینی فعال در حوزه‌های انرژی، معدن و رسانه استفاده کرده است. هر چند ارتباط گروه BlackEnergy که مشخصاً وابسته به یک دولت است با TeleBots به اثبات نرسیده، اما چیزی که مشخص است گروه TeleBots در چندین عملیات هدفمند خرابکارانه دخالت داشته است. به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت ضدویروس ESET، در یکی از جدیدترین نمونه‌ها، این گروه، سیستم‌های کارکنان بانک‌های اوکراین را با سوءاستفاده از قابلیت ماکرو (Macro) در نرم‌افزار Office که به ایمیل هرزنامه (Spam) پیوست شده بودند به درب‌پشتی آلوده کردند. در جریان این حمله پس از جمع‌آوری داده‌های مهمی همچون گذرواژه (Password) از روی سیستم‌های آلوده شده، ویروس KillDisk بر روی آنها نصب شده و با حذف و رونویسی فایل‌های حساس سیستمی، سیستم عامل این دستگاه‌ها غیرقابل راه‌اندازی می‌شدند. اکنون به‌نظر می‌رسد گروه TeleBots تصمیم گرفته که خرابکاری خود را با اضافه کردن قابلیت باج‌افزار به این بدافزار تکمیل کند. به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت CyberX، در جدیدترین نسخه KillDisk، با نمایش پیام زیر در ازای باز گرداندن داده‌ها، از قربانی مبلغ ۲۲۲ بیت کوین (Bitcoin) معادل حدود ۲۲۰ هزار دلار اخاذی می‌شود.


رمزگذاری فایل‌ها در نسخه جدید KillDisk، با یک کلید مبتنی بر الگوریتم AES صورت می‌گیرد. ضمن اینکه این کلید نیز خود با الگوریتم RSA-1028 رمزگذاری و در حقیقت حفاظت می‌شود. محققان CyberX، معتقدند نسخه باج‌افزاری KillDisk نیز از طریق هرزنامه‌های با پیوست ماکروی مخرب در حال انتشار است. در پیام نمایش داده شده از قربانی خواسته می‌شود با برقراری ارتباط با مهاجمان از طریق ایمیل درج شده در پیام، مبلغ باج را پرداخت کرده و کلید خصوصی (Private Key) رمزگشایی RSA را دریافت کند. دامنه ایمیل (lelantos.org) متعلق به یک سرویس‌دهنده امن و ناشناس است. هر چند مبلغ باج در این نسخه KillDisk - در مقایسه با باج‌افزارهای رایج - بسیار زیاد به‌نظر می‌رسد اما اخاذی مبالغ بالا در حملات هدفمند، موضوعی عادی محسوب می‌شود.

بررسی و تحلیل بـدافـزار

**KillDisk**

# باج‌افزارهای رمزگذار

## مراحل اخاذی تبهکاران سایبری

باج‌افزارهای رمزگذار یکی از پرطرفدارترین و متأسفانه مخرب‌ترین بدافزارهایی هستند که در چند سال اخیر مورد استفاده تبهکاران سایبری قرار گرفته‌اند. محدود کردن دسترسی به داده‌های حساس از طریق رمزنگاری، ارعاب کاربر و بدنبال آن اخاذی در ازای بازگرداندن این داده‌ها، هدف اصلی این نوع باج‌افزارها است. رمزگشایی فایل‌هایی که با طراحی زیرکانه به این روش رمزنگاری می‌شوند، در بسیاری مواقع غیرممکن است.

## ۱. توزیع

### نفوذ به دستگاه برای اجرای باج‌افزار

**هرزنامه**

ایمیل‌های با عنوان و محتوای فریبنده که فایل‌های در ظاهر بی‌خطر نظیر ZIP و Office به آنها پیوست شده است. با اجرای پیوست، فایل مخرب بر روی دستگاه اجرا می‌شود. در برخی نمونه‌ها بجای پیوست، از لینک‌های مخرب در درون ایمیل استفاده می‌شود که با کلیک بر روی آن کاربر به یک سایت مخرب هدایت می‌شود.

**سوءاستفاده از ضعف‌های امنیتی**

وجود یک نقطه ضعف خطرناک در سیستم عامل یا نرم‌افزار نصب شده بر روی دستگاه می‌تواند سبب دور زدن قوی‌ترین نرم‌افزارهای ضدویروس یا دیواره‌های آتش شود! بسیاری از ضعف‌های امنیتی بدون دخالت کاربر قابل بهره‌جویی هستند.

**برنامک‌های مخرب**

باج‌افزار در برنامک‌های معروف و پراستفاده تزریق شده و در بازارهای توزیع دیجیتال غیررسمی به اشتراک گذاشته می‌شود. با دریافت و نصب برنامک، دستگاه به باج‌افزار آلوده می‌شود.

**راهکارهای دفاعی شبکه گستر**

- آموزش و راهنمایی کاربران سازمان به صرف‌نظر کردن از فایل‌های مشکوک و باز نکردن آنها
- نصب مستمر اصلاحیه‌های امنیتی و ترجیحاً استفاده از نرم‌افزارهای WSUS یا SCCM
- بکارگیری ابزارهای ضدهرزنامه در درگاه شبکه
- استفاده از ابزارهای کنترل وب
- استفاده از ضدویروس قدرتمند و به‌روز
- مسدود کردن ایمیل‌های با پیوست ماکرو

## ۲. نصب

باج‌افزار خود را بر روی ماشین قربانی نصب کرده و حضور خود را بر روی سیستم ماندگار می‌کند.

**راهکارهای دفاعی شبکه گستر**

- استفاده از نام‌های کاربری با سطح دسترسی محدود
- بکارگیری ابزارهای کنترل برنامه برای جلوگیری از اجرای برنامه‌های غیرمجاز

## ۳. خلع سلاح دستگاه

در برخی نمونه‌های باج‌افزار رمزگذار، تنظیمات امنیتی غیرفعال شده و نسخه‌های کپی شده سیستمی حذف می‌شوند.

**حذف Shadow Copy**

باج افزار اقدام به حذف نسخه‌های Shadow Copy از طریق پروسه vssadmin.exe برای غیرممکن کردن بازگرداندن فایل‌ها از طریق این قابلیت می‌کند.

**حذف System Restore**

به‌منظور جلوگیری از بازگشت سیستم به حالت قبل، سوابق System Restore حذف می‌گردد.

**راهکارهای دفاعی شبکه گستر**

- تهیه نسخه‌های پشتیبان؛ پیروی از قاعده ۳-۲-۱ برای داده‌های حیاتی توصیه می‌شود. بر طبق این قاعده، از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه بعنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها نیز می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود.

## ۴. اعلام به سرور فرماندهی

با برقراری ارتباط با سرور فرماندهی شناسه‌ای منحصربه‌فرد ایجاد شده و به دستگاه تخصیص داده می‌شود.

**راهکارهای دفاعی شبکه گستر**

- معمولاً باج‌افزارها پیش از برقراری ارتباط با سرور فرماندهی فایل‌های کاربر را رمزگذاری نمی کنند؛ بنابراین استفاده از دیواره آتش و ابزارهای کنترل اینترنت بسیار کمک‌کننده خواهد بود.

## ۵. به گروگان رفتن داده‌های بااهمیت

### رمزگذاری مستندات، تصاویر و به‌طور کلی فایل‌های پراستفاده

**رمزگذاری قدرتمند**

در باج افزارهای رمزگذار، محدودسازی به دستگاه از طریق رمزگذاری فایل‌های بااهمیت کاربر انجام می‌شود. 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 بکار رفته در ساخت کلید است. هرچه تعداد این بیت‌ها بیشتر باشد شانس یافتن آن هم دشوارتر و در تعداد بیت بالا عملاً غیرممکن می شود.

**هدف قرار دادن پسوندهای پراستفاده**

بسته به نوع باج‌افزار، فایل‌های با پسوندهای خاص و معمولاً رایج رمزگذاری می‌شوند.

**در امان نبودن پوشه‌های اشتراکی و حافظه‌های متصل به دستگاه**

علاوه بر فایل‌های موجود بر روی دیسک سخت دستگاه، باج‌افزار پوشه‌های اشتراکی که کاربر دستگاه آلوده شده به آنها دسترسی نوشتنی دارد و همچنین حافظه‌های جانبی نظیر حافظه‌های حذف شدنی را نیز هدف قرار می‌دهد.

**راهکارهای دفاعی شبکه گستر**

- تهیه نسخه‌های پشتیبان؛ پیروی از قاعده ۳-۲-۱ برای داده‌های حیاتی توصیه می‌شود. بر طبق این قاعده، از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه بعنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود.

## ۶. اخاذی

### باج‌افزار پیامی را به قربانی نمایش داده و در آن کاربر در خصوص مبلغ باج و روش پرداخت راهنمایی می‌شود.

**پرداخت بیت کوین**

اکثر باج افزارها از بیت کوین استفاده می‌کنند. بیت کوین نوعی پول دیجیتال بر پایه اصل اثبات دانایی صفر است. بدان معنا که فرستنده و گیرنده ضمن اطلاع از انتقال پول، از هویت یکدیگر مطلع نمی‌شوند.

**پشتیبانی**

برخی گردانندگان باج‌افزار دارای سامانه‌هایی برای ارائه خدمات پشتیبانی به قربانیان خود هستند! قربانیان می‌توانند در خصوص مسائلی نظیر نصب Tor خرید بیت کوین از باج‌گیران راهنمایی بگیرند.

**رمزگشایی رایگان اما محدود**

در برخی باج‌افزارها به قربانی این امکان داده می‌شود تا یک یا چند فایل را به رایگان و به عنوان اثبات توانایی باج‌افزار در رمزگشایی به حالت قبل باز گرداند.

## ۷. رمزگشایی

## بهترین راهکار برای مقابله باج افزارهای رمزگذار، پیشگیری از آلوده شدن است.

هر چند که در اکثر نمونه‌ها با پرداخت باج کار رمزگشایی انجام می‌شود، اما انجام این کار به دلایل مختلف از جمله تشویق تبهکاران سایبری به ادامه این فعالیت‌های مخرب و همچنین عدم وجود تضمینی برای بازگشت فایل‌ها به حالت قبل به هیچ وجه توصیه نمی‌شود.

## آیا شما آماده اید؟

کارشناسان شبکه گستر در کنار شما هستند.


شبکه گستر

www.shabakeh.net

۰۲۱ - ۴۲۰۵۲

# انتشار گسترده بدافزار Tordow

به گزارش شرکت مهندسی شبکه گستر، محققان شرکت Comodo از انتشار گسترده نسخه دوم بدافزار پیشرفته Tordow که دستگاه‌های با سیستم عامل Android را هدف می‌دهد خبر داده‌اند.

ویژگی اصلی این بدافزار، توانایی آن در روت کردن (Rooting) دستگاه‌های مبتنی بر سیستم عامل Android است. کاری که حداقل در تئوری، بدافزار را قادر به اجرای هر فرمان مخربی می‌کند. این نسخه Tordow، شامل ۹ روش مختلف، برای اطمینان از فراهم شدن حق دسترسی Root است.

بر طبق توضیحات محققان Comodo، نسخه دوم بدافزار Tordow قادر به اجرای خرابکاری‌های زیر بر روی دستگاه‌های Android است:

- برقراری تماس‌های تلفنی
- مدیریت پیامک (SMS)
- دانلود و نصب برنامک
- دسترسی به دفترچه تلفن دستگاه
- رمزنگاری فایل‌ها
- دسترسی از راه دور به نشانی URL
- سرقت اطلاعات اصالت‌سنجی برنامک‌ها
- سرقت داده‌ها از مرورگر Chrome
- جاسوسی از برنامک‌های بانکی
- راه‌اندازی مجدد دستگاه
- دسترسی و تغییر نام فایل‌ها
- جمع‌آوری مشخصات دستگاه
- جمع‌آوری اطلاعات مربوط به موقعیت جغرافیایی داده‌ها

به گفته این محققان، گردانندگان Tordow، در اکثر مواقع، از این بدافزار برای سرقت اطلاعات اصالت‌سنجی مشتریان بانک‌های روسی استفاده می‌کنند.

همچنین قابلیت رمزنگاری نسخه جدید، فایل‌ها را با الگوریتم AES رمزگذاری می‌کند. عملیات رمزگذاری با کلید MIIxxxxCgAwIB که در کد بدافزار درج شده انجام می‌شود. با توجه به کلید متقارن بودن الگوریتم AES، با اطلاع از این کلید، امکان رمزگشایی فایل‌ها ممکن می‌شود و بنابراین نمی توان آن را یک باج‌افزار پیشرفته دانست.

گردانندگان Tordow، با تزریق کد این بدافزار در برنامک‌های معروفی نظیر Telegram و Pokemon و با اشتراک‌گذاری آنها در بازارهای توزیع دیجیتال (Store) غیررسمی، کاربران را هدف قرار داده‌اند.

نسخه اول این بدافزار، نخستین بار در سپتامبر ۲۰۱۶ شناسایی شد. اما بررسی‌های بعدی نشان داد که این بدافزار از حدود یک سال قبل فعال بوده است.

برای ایمن ماندن از گزند این نوع بدافزارها، رعایت موارد زیر توصیه می‌شود:

- 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 رسمی شرکت گوگل (Play Store) یا حداقل بازارهای مورد اعتماد معروف دانلود کنید. همچنین از غیرفعال 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 غیرفعال بودن گزینه نخست، از اجرا شدن فایل‌هایAPK میزبانی شده در بازارهای ناشناخته بر روی دستگاه جلوگیری می‌شود. وظیفه گزینه دوم نیز پایش دوره‌ای 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 دستگاه‌های همراه خود یا سازمانتان استفاده کنید. توضیح اینکه نمونه‌های بررسی شده توسط


بررسی و تحلیل بدافزارهای

## Fileless

تحلیل بدافزار

شرکت مهندسی شبکه گستر توسط راهکارهای ضدبدافزار McAfee، Bitdefender و ESET با نام‌های زیر شناسایی می‌شوند:

**McAfee**

- Artemis!2A6EF3539913
- Artemis!5B3203816953
- Artemis!965A5E5D237C
- Artemis!6865D4FAA9A1
- Artemis!5A4E9A8E3903

**Bitdefender**

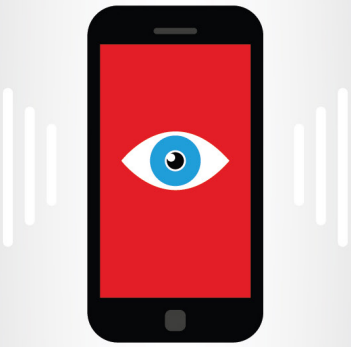
- Android.Riskware.Agent.gXZIO
- Android.Trojan.Carnooc.F
- Android.Riskware.Agent.gXZIB

**ESET**

- a variant of Android/Agent.TS
- a variant of Android/Spy.Banker.ES

حملات سایبری

# جاسوسی از نیروهای اسراییلی از طریق برنامک Android



به گزارش شرکت مهندسی شبکه گستر، تماس‌ها و اطلاعات ذخیره شده بر روی گوشی بیش از ۱۰۰ عضو نیروهای دفاعی رژیم صهیونیستی از طریق برنامک‌های Android سرقت شده است.

شرکت Kaspersky که با بخش امنیت اطلاعات نیروهای دفاعی اسراییل مشارکت می‌کند آغاز این حملات را جولای سال گذشته میلادی اعلام کرده است.

در جریان این حملات سربازان رژیم اشغالگر قدس از طریق شبکه‌های اجتماعی نظیر Facebook در گفتگو با فردی در ظاهر یک زن کانادایی و در برخی حملات آلمانی و در برخی دیگر سوییسی، تشویق به اجرای یک برنامک Android مخرب شده بودند. این برنامک پس از نصب شدن اقدام به پویش دستگاه کرده و برنامک مخرب دیگری را در ظاهر به‌روزرسانی یکی از برنامک‌های ثبت شده بر روی دستگاه اجرا می‌کند. برای مثال، در یکی از نمونه‌ها نام فایل مخرب اجرا شده WhatsApp_Update اعلام شده است.

برنامک مخرب مهاجمان را قادر به اجرای فرامین متعدد می‌کند. ضمن اینکه اطلاعات زیر را جمع‌آوری کرده و به سرور فرماندهی مهاجمان ارسال می‌کند:

- اطلاعات کلی در خصوص دستگاه آلوده شده
- پیامک‌ها و بانک داده پیام‌رسان WhatsApp
- سوابق سایت‌های مشاهده شده و جستجوهای انجام گرفته
- فایل‌های با پسوند خاص نظیر doc که حجم آنها کمتر از ۲ مگابایت است
- تصاویر گرفته شده
- فهرست تماس‌ها و سوابق تماس‌های برقرار شده
- ضبط و شنود تماس‌ها

این نخستین بار نیست که از برنامک مخرب برای جاسوسی از نیروهای نظامی استفاده می‌شود. برای نمونه، بتازگی نیز یک بدافزار تحت سیستم عامل Android نیروهای توپخانه اوکراین را که در درگیری‌های منطقه دنباس نقش داشته‌اند هدف قرار داده بود.


# سوءاستفاده گسترده از آسیب‌پذیری اخیر WordPress

از بهمن ماه بیش از ۲۰ مهاجم و گروه نفوذگر اقدام به تغییر ظاهر سایت‌های مبتنی بر یکی از نسخه‌های آسیب‌پذیر سامانه مدیریت محتوای WordPress کرده‌اند.

به گزارش شرکت مهندسی شبکه گستر، وجود یک آسیب‌پذیری در بخش REST API این سامانه، نفوذگران را قادر به اجرای این حملات کرده است. مهاجم می‌تواند با سوءاستفاده از ضعف امنیتی مذکور، بدون اصالت‌سنجی، محتوای صفحه اینترنتی را به دلخواه خود تغییر دهد. به حملاتی که در جریان آن محتوای یک صفحه اینترنتی توسط هکر تغییر داده می‌شود Website Defacement گفته می‌شود.

WordPress در هفتم بهمن ماه، آسیب‌پذیری مذکور را با عرضه نسخه 4.7.2 ترمیم کرد. بنیاد WordPress در روز ۱۳ بهمن ماه نیز جزییات این آسیب‌پذیری را منتشر کرد.

با وجود تأخیر یک هفته‌ای در اعلام وجود این آسیب‌پذیری، بسیاری از مدیران سایت اقدام به نصب اصلاحیه نکرده بودند. موضوعی که سبب اجرای این حملات گردید.

شرکت امنیتی Sucuri، ۲۱ بهمن ماه گزارش داد که محتوای حدود ۶۷ هزار صفحه اینترنتی توسط چهار گروه مهاجم تغییر کرده است.

در همان روز شرکت Feedjit نیز از تغییر محتوای بیش از ۱/۵ میلیون صفحه اینترنتی توسط ۲۰ مهاجم و گروه سایبری خبر داد و گفت طی ۴۸ ساعت گذشته بیش از ۸۰۰۰ هزار حمله برای سوءاستفاده از این آسیب‌پذیری را کشف و شناسایی کرده است.

تصاویر زیر نیز دو نمونه از صفحات هک شده را نمایش می‌دهند.



جالب اینکه مهاجمان این حملات توانسته‌اند راهی برای عبور از سد قواعد مسدودکننده سیستم‌های موسوم به Web Application Firewall یافته و آنها را دور بزنند.

به گزارش شرکت مهندسی شبکه گستر، شرکت Google نیز اقدام به ارسال هشدارهای امنیتی به مدیران سایت‌هایی کرده که سایت مبتنی بر WordPress خود را بر روی Google Search Console ثبت کرده‌اند. موضوعی که سبب سردرگمی آن دسته از مدیرانی شده که پیش از دریافت هشدار نسخه 4.7.2 را نصب کرده بودند.

به تمامی مدیران سایت‌های مبتنی بر سامانه WordPress توصیه اکید می‌شود از نصب بودن آخرین نسخه از این سامانه اطمینان حاصل کنند.

گزارش‌ها

# مراقب باج‌افزارهای جعلی باشید!

نتایج یک تحقیق نشان می‌دهد که برخی تبهکاران سایبری بدون نوشتن کدهای پیچیده و حرفه‌ای، تنها با ادعای رمزگذاری شدن اطلاعات دستگاه، موفق به اخاذی از بسیاری از سازمان‌های بزرگ می‌شوند.

به گزارش شرکت مهندسی شبکه گستر، بر اساس یافته‌های این تحقیق که توسط شرکت Citrix و با مصاحبه با ۵۰۰ سازمان انگلیسی با حداقل ۲۵۰ کارمند حاصل شده، ۳۹ درصد سازمان‌ها به دام باج‌افزارهای در ظاهر رمزگذار افتاده‌اند که از این تعداد ۶۱ درصد آنها اقدام به پرداخت مبلغ اخاذی شده در ازای رمزگشایی فایل‌های رمز نشده کرده‌اند.

میانگین پرداخت باج به گردانندگان باج‌افزارهای جعلی بیش از ۱۳ هزار پوند اعلام شده است. حتی در ۲۰ درصد این موارد مبلغ پرداختی بیش از ۲۵ هزار پوند گزارش شده است.

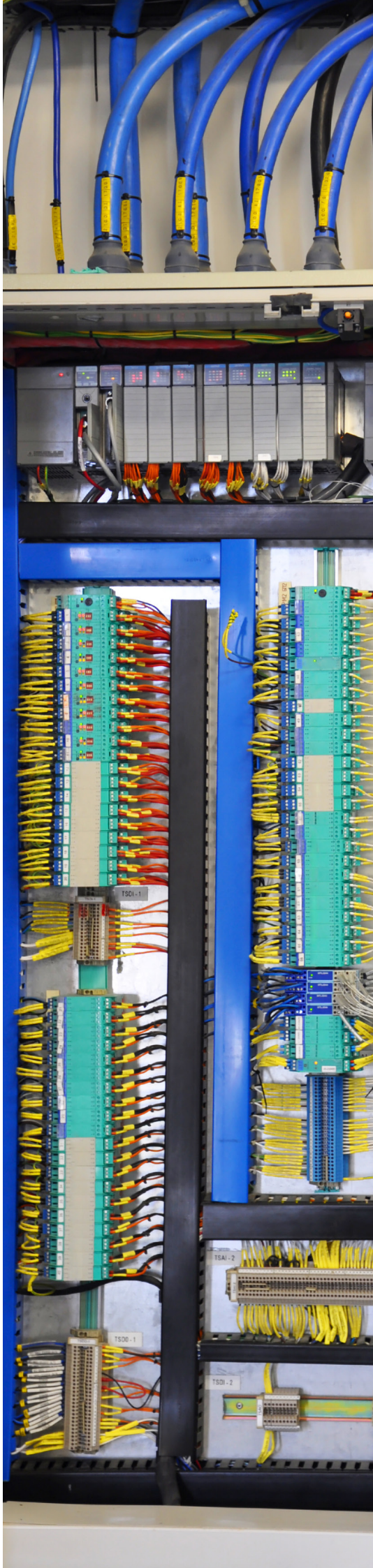
شرکت Citrix به اشتراک‌گذاری و گزارش اخاذی سایبری به سازمان‌ها و نهادهای مسئول نظیر پلیس را عاملی مؤثر در جلوگیری از به دام افتادن در این تهدیدات در ظاهر مخرب دانسته است. ضمن اینکه خوشبختانه بر اساس یافته‌های این تحقیق ۴۵ درصد سازمان‌های انگلیسی که هدف این تهدیدات قرار گرفته‌اند به سایت‌هایی نظیر «اخاذی بس است» مراجعه کرده بودند.

بر خلاف باور نادرست بسیاری از کاربران و حتی مدیران شبکه که در نتیجه اثرات مخرب باج‌افزارهای رمزگذار در سال‌های اخیر ایجاد شده، تنها راهکار در زمان آلوده شدن به هر گونه باج‌افزار پرداخت مبلغ اخاذی شده یا صرف‌نظر کردن از اطلاعات نیست. برای مثال، در سال گذشته باج‌افزاری شناسایی شد که بدون اعمال هر نوع رمزنگاری تنها پسوند فایل‌ها را به crypted تغییر می‌داد.

هر چند که تحقیق اخیر چیزی از اهمیت بکارگیری اقدامات پیشگیرانه در مقابله با باج‌افزارهای حرفه‌ای، به‌عنوان یکی از مخرب‌ترین تهدیدات سایبری دو سال اخیر کم نمی‌کند، اما لزوم گزارش آلودگی به افراد متخصص و نهادهای مسئول را بیش از پیش پر رنگ می‌کند.

مشروح گزارش شرکت Citrix در اینجا قابل مطالعه است.

# تجهیزات PLC؛ هدف بعدی باج‌افزارها؟



به گزارش شرکت مهندسی شبکه گستر، دو محقق از مؤسسه فناوری جورجیا، باج‌افزاری آزمایشی ساخته‌اند که قادر است ضمن قطع دسترسی به دستگاه PLC تنظیمات آن را نیز تغییر دهد. این محققان این نمونه باج‌افزار را ۲۵ بهمن در کنفرانس RSA ارائه کردند. در دنیای واقعی تجهیزات PLC دریچه‌ها، موتورها، پمپ‌ها، حسگرها، آسانسورها، پله‌های برقی، ورودی‌های ولتاژ، زمان‌سنج‌ها، سیستم‌های تهویه و بسیاری از سیستم‌های مکانیکی دیگر را کنترل می‌کنند. تجهیزات PLC که در موقعیت های مختلف پراکنده‌اند خود نیز از طریق نرم‌افزارهای SCADA که معمولاً بر روی یک کامپیوتر معمولی نصب شده‌اند توسط راهبر یا بصورت خودکار کنترل و پیکربندی می‌شوند. در حقیقت تجهیزات PLC، قلب تپنده سیستم‌های کنترل صنعتی (ICS) و سامانه‌های SCADA هستند. PLC داده‌ها را از روی دستگاه متصل به آن جمع‌آوری کرده و آنها را به کامپیوتر و نرم‌افزار کنترل‌کننده نصب شده بر روی آن ارسال می‌کند. همچنین PLC فرامین دریافت شده از نرم‌افزار کنترلی را نیز بر روی دستگاه اعمال می‌کند. به گزارش شرکت مهندسی شبکه گستر، اکنون این دو محقق نشان داده‌اند که چطور یک باج‌افزار می‌تواند با اجرا شدن بر روی دستگاه با نرم‌افزار SCADA دسترسی به PLC را مسدود کرده و حتی در پشت صحنه تنظیمات آن را هم بنحوی مخرب تغییر دهد. حمله باج‌افزار به مرکز تصفیه آب می‌تواند یک سناریوی احتمالی باشد. مهاجم دسترسی به تجهیزات PLC را مسدود کرده و در عین حال مقدار ترکیبات کلردار اضافه شده به آب را نیز به میزان خطرناکی افزایش می‌دهد. این مهاجم در ازای بازگشایی دسترسی به تجهیزات PLC مبلغ بسیار هنگفتی را اخاذی می‌کند. بسته به تعداد دستگاه‌های PLC قفل‌شده ممکن است سازمان هدف قرار گرفته شده پرداخت باج را به Reset کردن هر دستگاه و پیکربندی مجدد آن که ممکن است ساعت‌ها زمان ببرد ترجیح دهد. در یک دهه اخیر به کنترل در آوردن تجهیزات PLC توسط بدافزار عمدتاً از سوی مهاجمان دولتی انجام می‌شده است. یکی از معروف‌ترین نمونه‌های آن بدافزار پیشرفته Stuxnet است که در آن دستگاه‌های PLC مدل SIMATIC S7-3000 شرکت زیمنس به کنترل بدافزار در می‌آمدند. این محققان باج‌افزار را به‌عنوان عاملی برای مخفی نمودن و پوشش قصد و نیت اصلی مهاجمان معرفی کرده‌اند. باید در نظر داشت که آلوده شدن سامانه SCADA به باج‌افزار مستلزم اجرا شدن فایل مخرب بر روی این سامانه است. بنابراین عدم اتصال این سامانه‌ها به اینترنت و شبکه عمومی سازمان در کنار استفاده از ابزارهای موسوم به Device Control می‌توانند به‌نحوی مؤثر چنین حملاتی را خنثی کنند.

# ضربان قلب به‌عنوان گذرواژه؛ روشی خلاقانه یا ایده‌ای احمقانه؟!

به گزارش شرکت مهندسی شبکه گستر، محققان دانشگاه Binghamton University در نیویورک در مقاله‌ای به استفاده از الگوی نوار قلب افراد به‌عنوان گذرواژه‌ای برای رمزگذاری و رمزگشایی داده‌های هر فرد پرداخته‌اند. این محققان گفته‌اند که هر فرد یک نوار قلب (ECG) منحصربه‌فرد و خاص خود را دارد. ثبت نوار قلب پروسه‌ای است که از طریق الکترودهای قرار داده شده بر روی پوست امواج الکتریکی محرک قلب در بازه‌ای از زمان ضبط می‌شود. این الکترودها تغییرات ریز ماهیچه‌های قلب را شناسایی می‌کنند. این محققان بر این باورند که می‌توان سیستم‌هایی را راه‌اندازی کرد که در آنها از الگوی نوار قلب هر فرد به‌عنوان کلیدهای رمزگذاری و رمزگشایی - بجای کلیدهای با مقدار تصادفی - استفاده شود. هدف از رمز کردن، تغییر ساختار فایل با استفاده از گذرواژه‌ای موسوم به کلید است؛ به‌نحوی که تنها با داشتن کلید رمزگشایی بتوان به محتوای فایل دسترسی پیدا کرد. به گزارش شرکت مهندسی شبکه گستر، این محققان گفته‌اند که روش‌های فعلی رمزگذاری نیاز به منابع کامپیوتری نسبتاً بیشتری در مقایسه با این روش پیشنهادی دارند. در حالی که منابع مورد نیاز برای انجام چنین پردازش‌هایی در کامپیوترهای خانگی و سرورها به‌راحتی قابل چشم‌پوشی است، بسیاری از دستگاه‌های موسوم به اینترنت اشیاء (IoT) فاقد توان لازم برای این چنین پردازش‌هایی هستند. بنابراین در بسیاری از آنها از رمزگذاری استفاده نشده و داده‌ها در خطر قرار می‌گیرند. اما این روش پیشنهادی با چالش‌هایی جدی روبرو است. نخست اینکه نوار قلب در نتیجه افزایش سن، بروز بیماری یا ایجاد جراحت در فرد تغییر می‌کند. دوم اینکه اگر از الگوی نوار قلب هر فرد برای رمزگذاری اطلاعاتی همچون اطلاعات درمانی بیمار استفاده شود؛ پس از مرگ فرد چه اتفاقی برای داده‌ها می‌افتد؟

سوم اینکه در صورت فاش شدن الگوی نوار قلب فرد، چگونه می‌توان آن را به‌نحوی تغییر داد که دست یافتن افراد غیرمجاز به اطلاعات رمز شده توسط آن ناممکن شود؟

مقاله مذکور در کنفرانس IEEE Global Communications Conference ۲۰۱۶ که در شهر واشنگتن برگزار گردید ارائه شد.

# Android، آسیب‌پذیرترین نرم‌افزار سال ۲۰۱۶

با پایان سال ۲۰۱۶، سیستم عامل Google Android به‌عنوان آسیب‌پذیرترین نرم‌افزار و شرکت Oracle به‌عنوان تولیدکننده نرم‌افزار با بیشترین آسیب‌پذیری در این سال میلادی شناخته شده‌اند.

این رده‌بندی‌ها بر مبنای تعداد آسیب‌پذیری‌های گزارش شده توسط محققان در سال گذشته میلادی صورت گرفته است. به هر یک از آسیب‌پذیری‌های ثبت شده یک شناسه CVE اختصاص داده می‌شود.

| | Product Name | Vendor Name | Product Type | Number of Vulnerabilities |
|---|---|---|---|---|
| 1 | Android | Google | OS | 523 |
| 2 | Debian Linux | Debian | OS | 319 |
| 3 | Ubuntu Linux | Canonical | OS | 278 |
| 4 | Flash Player | Adobe | Application | 266 |
| 5 | Leap | Novell | OS | 259 |
| 6 | Opensuse | Novell | OS | 228 |
| 7 | Acrobat Reader Dc | Adobe | Application | 227 |
| 8 | Acrobat Dc | Adobe | Application | 227 |
| 9 | Acrobat | Adobe | Application | 224 |
| 10 | Linux Kernel | Linux | OS | 216 |
| 11 | Mac Os X | Apple | OS | 215 |
| 12 | Reader | Adobe | Application | 204 |
| 13 | Chrome | Google | Application | 172 |
| 14 | Windows 10 | Microsoft | OS | 172 |
| 15 | Iphone Os | Apple | OS | 161 |
| 16 | Windows Server 2012 | Microsoft | OS | 156 |
| 17 | Windows 8.1 | Microsoft | OS | 154 |
| 18 | Windows Rt 8.1 | Microsoft | OS | 139 |
| 19 | Edge | Microsoft | Application | 135 |
| 20 | Windows 7 | Microsoft | OS | 134 |

**آسیب‌پذیرترین نرم‌افزار**

به گزارش شرکت مهندسی شبکه گستر، بر اساس آمار ارائه شده در سایت CVE Details که جزییات هر ضعف و اشکال امنیتی CVE را ثبت می‌کند، در سال ۲۰۱۶ محققان در مجموع ۵۲۳ باگ امنیتی را در سیستم عامل Android گزارش کرده‌اند. پس از Android، دو نرم‌افزار Debian Linux با ۳۱۹ و Ubuntu Linux با ۲۷۸ آسیب‌پذیری در جایگاه‌های بعدی قرار گرفته‌اند.

Adobe Flash Player با ۲۶۶، openSUSE Leap با ۲۵۹، openSUSE با ۲۲۸، Adobe Acrobat DC با ۲۲۷، Adobe Acrobat Reader DC با ۲۲۷، Adobe Acrobat با ۲۲۴ و Linux Kernel با ۲۱۶ باگ، سایر ۱۰ نرم‌افزار با بیشترین آسیب‌پذیری در سال ۲۰۱۶ بوده‌اند.

Mac OS X، آسیب‌پذیرترین محصول سال ۲۰۱۵، در فهرست جدید در جایگاه یازدهم قرار گرفته است.

فهرست زیر آسیب‌پذیرترین نرم‌افزار را در هر یک از سال‌های گذشته میلادی نشان می‌دهد:

- در سال ۲۰۱۵، Apple Mac OS X با ۴۴۴ باگ
- در سال ۲۰۱۴، Internet Explorer با ۲۴۳ باگ
- در سال ۲۰۱۳، Linux Kernel با ۱۸۹ باگ
- در سال ۲۰۱۲، Google Chrome با ۲۴۹ باگ
- در سال ۲۰۱۱، Google Chrome با ۲۶۶ باگ
- در سال ۲۰۱۰، Google Chrome با ۱۵۲ باگ
- در سال ۲۰۰۹، Mozilla Firefox با ۱۲۶ باگ
- در سال ۲۰۰۸، Mozilla Firefox و Apple OS X هر کدام با ۹۶ باگ
- در سال ۲۰۰۷، PHP با ۱۱۴ باگ
- در سال ۲۰۰۶، Apple OS X با ۱۰۶ باگ
- در سال ۲۰۰۵، Linux Kernel با ۱۳۳ باگ
- در سال ۲۰۰۴، Internet Explorer با ۵۹ باگ
- در سال ۲۰۰۳، Solaris OS با ۴۴ باگ

- در سال ۲۰۰۲، Internet Explorer با ۵۴ باگ
- در سال ۲۰۰۱، RedHat Linux با ۴۷ باگ
- در سال ۲۰۰۰، RedHat Linux با ۴۷ باگ
- در سال ۱۹۹۹، Windows NT با ۶۴ باگ

**آسیب‌پذیرترین شرکت نرم‌افزاری**

در بین شرکت‌های تولیدکننده نرم‌افزار که مجموع آسیب‌پذیری‌های محصولات آنها بیش از سایر تولیدکنندگان نرم‌افزار بوده، شرکت Oracle با مجموع ۷۹۸ آسیب‌پذیری در جایگاه اول قرار گرفته است. اکثر این آسیب‌پذیری‌های این شرکت مربوط به محصولاتی نظیر Solaris، MySQL و نسخه سفارشی سیستم عامل Linux آن بوده است. در مقام بعدی شرکت Google با ۶۹۸ آسیب‌پذیری قرار دارد که بیشترین موارد آنها مربوط به محصولات Android و Chrome بوده است. جایگاه سوم متعلق به شرکت Adobe با ۵۴۸ آسیب‌پذیری است که بسیاری از آنها مربوط به نرم افزارهای Acrobat، Reader و Flash Player است. Microsoft با ۴۹۲، Novell با ۳۹۴، IBM با ۳۸۲، Cisco با ۳۵۳، Apple با ۳۲۴، Debian Project با ۳۲۰ و Canonical با ۲۸۰ باگ سایر شرکت‌هایی هستند که نام آنها در فهرست ۱۰ تولیدکننده نرم‌افزار با بیشترین آسیب‌پذیری در سال ۲۰۱۶ ثبت شده است. شرکت‌هایی که در سال‌های گذشته میلادی بیشترین آسیب‌پذیری‌ها به نام آنها ثبت شده نیز به‌شرح زیر است:

- در سال ۲۰۱۵، Apple با ۷۰۰۸ باگ
- در سال ۲۰۱۴، IBM با ۴۵۵ باگ
- در سال ۲۰۱۳، Oracle با ۴۹۶ باگ
- در سال ۲۰۱۲، Oracle با ۳۸۰ باگ
- در سال ۲۰۱۱، Google با ۲۹۵ باگ
- در سال ۲۰۱۰، Microsoft با ۳۱۷ باگ
- در سال ۲۰۰۹، Microsoft با ۲۳۶ باگ
- در سال ۲۰۰۸، Microsoft با ۲۳۶ باگ
- در سال ۲۰۰۷، Microsoft با ۲۵۵ باگ
- در سال ۲۰۰۶، Microsoft با ۲۶۷ باگ
- در سال ۲۰۰۵، Microsoft با ۱۶۶ باگ
- در سال ۲۰۰۴، Microsoft با ۱۴۸ باگ
- در سال ۲۰۰۳، Microsoft با ۱۰۳ باگ
- در سال ۲۰۰۲، Microsoft با ۲۴۳ باگ
- در سال ۲۰۰۱، Microsoft با ۱۷۳ باگ
- در سال ۲۰۰۰، Microsoft با ۱۴۳ باگ
- در سال ۱۹۹۹، Microsoft با ۱۷۱ باگ

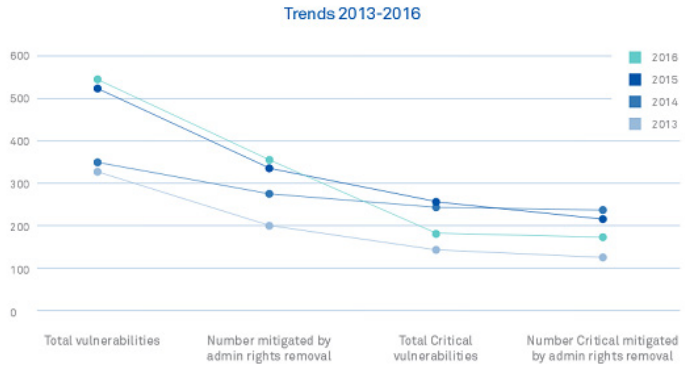
| | Vendor Name | Number of Vulnerabilities |
|---|---|---|
| 1 | Oracle | 793 |
| 2 | Google | 698 |
| 3 | Adobe | 548 |
| 4 | Microsoft | 492 |
| 5 | Novell | 394 |
| 6 | IBM | 382 |
| 7 | Cisco | 353 |
| 8 | Apple | 324 |
| 9 | Debian | 320 |
| 10 | Canonical | 280 |
| 11 | Redhat | 252 |
| 12 | Linux | 217 |
| 13 | Mozilla | 143 |
| 14 | Fedoraproject | 121 |
| 15 | HP | 116 |
| 16 | PHP | 107 |
| 17 | Apache | 103 |
| 18 | Huawei | 100 |
| 19 | Wireshark | 95 |
| 20 | Suse | 90 |

# حفاظت مؤثر از ضعف‌های حیاتی تنها با کنترل سطح دسترسی

با جلوگیری از عدم ورود کاربران به سیستم با نام کاربری با حق دسترسی Administrator، مدیر شبکه نه تنها می‌تواند نصب هر برنامه‌ای را بر روی سیستم‌ها تحت رصد داشته باشد که اکثر آسیب‌پذیری‌ها و ضعف‌های امنیتی حیاتی در محصولات مایکروسافت نیز به‌نحوی مؤثر پوشش داده می‌شوند.

به گزارش شرکت مهندسی شبکه گستر، این نتیجه مطالعه شرکت Avecto بر روی اصلاحیه‌های عرضه شده مایکروسافت در سال ۲۰۱۶ است. بر اساس یافته‌های این مطالعه، ۹۴ درصد آسیب‌پذیری‌های حیاتی ترمیم شده توسط مایکروسافت در سال میلادی مذکور، تنها در زمان ورود کاربر با حق دسترسی Administrator قابل بهره‌جویی بوده‌اند. گزارشی نیز که سال گذشته این شرکت منتشر کرده بود نشان می‌داد که ۸۶ درصد آسیب‌پذیری‌های حیاتی اصلاح شده در سال ۲۰۱۵ با عدم استفاده از نام‌های کاربری با حق دسترسی Administrator غیرقابل بهره‌جویی بوده‌اند. افزایش از ۸۶ درصد در سال ۲۰۱۵ به ۹۴ درصد در سال ۲۰۱۶ به معنای بهبود امنیت محصولات مایکروسافت البته به شرط اعمال سیاست محدود کردن سطح دسترسی کاربران است.

جالب‌تر آنکه بر اساس گزارش Avecto در صورتی که کاربران در سال گذشته میلادی برای اجرای کارهای معمول با حق دسترسی غیر Administrator به سیستم وارد می‌شدند، سوءاستفاده از ۱۰۰ درصد آسیب‌پذیری‌های حیاتی مرورگرهای Internet Explorer و Edge و همینطور نرم‌افزار Office ۲۰۱۶ غیرممکن می‌شد.




عدم تخصیص سطح دسترسی Administrator به کاربران یکی از مؤثرترین توصیه‌های امنیتی به مدیران شبکه است. تحقیق Avecto تایید می‌کند که دستگاه‌های با سیستم عامل Windows سازمان‌ها و کاربران از آلوده شدن به بسیاری از بدافزارها و حملات شبکه‌ای در امان خواهند بود اگر مشابه سیستم عامل Linux حساب کاربری پیش‌فرض دارای حق دسترسی Administrator نباشد.

# Bitdefender®

## افتخارات جدید برای Bitdefender

به گزارش شرکت مهندسی شبکه گستر، مؤسسه معتبر AV-Test، نشان "بهترین کارایی" (Best Performance) در سال ۲۰۱۶ را به ضدبدافزار سازمانی Bitdefender اعطا کرده است. Bitdefender این نشان را در نتیجه کسب بالاترین امتیاز از لحاظ اثرگذاری کم بر روی سرعت دستگاه حفاظت‌شده در شش آزمون برگزار شده توسط این مؤسسه در سال ۲۰۱۶ کسب کرده است.


Bitdefender در سال‌های ۲۰۱۵ و ۲۰۱۴ نیز موفق به کسب این نشان از این مؤسسه مستقل ارزیابی‌کننده محصولات ضدبدافزار شده بود.

در آزمون‌های AV-Test محصولات ضدبدافزار در سه بخش حافظت (Protection)، کارایی (Performance) و قابلیت استفاده (Usability) مورد ارزیابی قرار می‌گیرند که شرکت Bitdefender به‌طور پیوسته امتیازات بالایی در هر سه بخش کسب کرده است. برای نمونه در تمامی آزمون‌های بررسی ضدبدافزارهای سازمانی بر روی سیستم عامل Windows 10 که در سال ۲۰۱۶ توسط این مؤسسه برگزار شد، Bitdefender موفق به کسب امتیاز کامل در هر سه بخش شد.

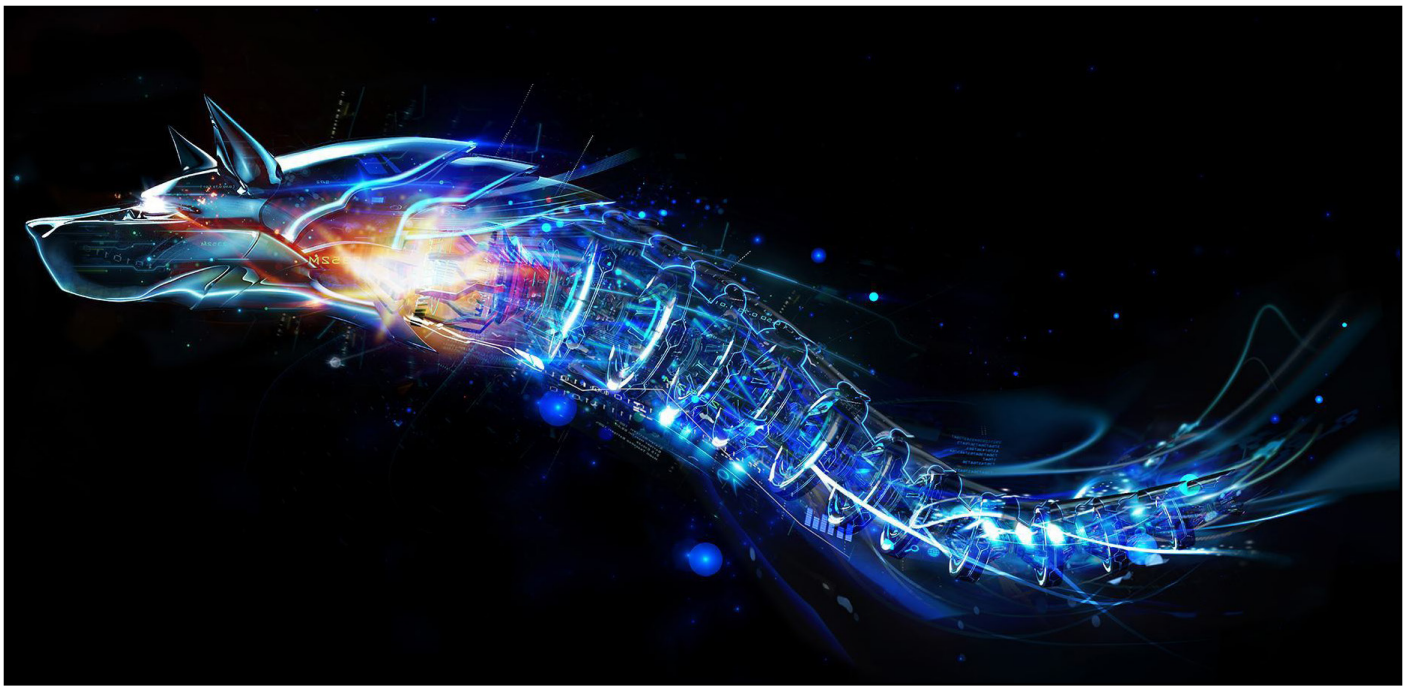
**December 2016**

| Name | Protection | Performance | Usability |
|---|---|---|---|
| Bitdefender Endpoint Security 6.2 | | | |
| F-Secure Client Security 12.20 | | | |
| Kaspersky Lab Endpoint Security 10 | | | |
| Kaspersky Lab Small Office Security 5 | | | |
| Symantec Endpoint Protection 14.0 | | | |
| Trend Micro Office Scan 11.0 | | | |
| G Data AntiVirus Business 14.0 | | | |
| Intel Security McAfee Endpoint Security 10.2 | | | |
| Seqrite Endpoint Security 17.00 | | | |
| Microsoft System Center Endpoint Protection 4.10 | | | |
| Sophos Endpoint Security and Control 10.6 | | | |
| AVG Antivirus Business 2016 | | | |

**April 2016**

| Name | Protection | Performance | Usability |
|---|---|---|---|
| Bitdefender Endpoint Security 6.2 | | | |
| F-Secure Client Security 12.0 | | | |
| Kaspersky Lab Endpoint Security 10 | | | |
| Kaspersky Lab Small Office Security 4 | | | |
| Sophos Endpoint Security and Control 10.6 | | | |
| Symantec Endpoint Protection 12.1 | | | |
| Trend Micro Office Scan 11.0 | | | |
| AVG Antivirus Business 2016 | | | |
| G Data AntiVirus Business 13.2 | | | |
| Intel Security McAfee Endpoint Security 10.0 | | | |
| Microsoft System Center Endpoint Protection 4.8 | | | |
| Seqrite Endpoint Security 16.00 | | | |

به گزارش شرکت مهندسی شبکه گستر، مؤسسه AV-Comparatives، دیگر مؤسسه ارزیابی‌کننده مستقل و



معتبر نیز در گزارشی به جمع‌بندی آزمون‌های مختلف خود در سال ۲۰۱۶ که بر روی انواع محصولات ضدویروس انجام داده پرداخته است. بر اساس این گزارش، ضدویروس Bitdefender مشترکاً با ضدویروس Kaspersky به‌عنوان محصول "ممتاز" (Outstanding) در سال ۲۰۱۶ معرفی شده است.


همچنین در بخش "محافظت در دنیای واقعی" (Real-World Protection) نیز Bitdefender نشان طلایی را از این مؤسسه دریافت کرده و بالاتر از ضدویروس‌هایی نظیر Kaspersky، Avira و ESET قرار گرفته است. این آزمون یکی از آزمون‌های مهم AV-Comparatives به شمار می‌آید. در این آزمون از تمام امکانات و قابلیت‌های ضدویروس برای مقابله با انواع تهدیدات، مشابه آنچه که هر روز در دنیای واقعی رخ می‌دهد، استفاده می‌شود. ضدویروس‌ها باید بدون نیاز به دخالت مکرر کاربر و با حداقل درصد خطا، عملکرد مناسبی نشان دهند.

در بخش های "شناسایی بدافزار" و "خطا در شناسایی" نیز Bitdefener موفق به دریافت نشان‌های "نقره‌ای" شده است.

شرکت Bitdefender در سال ۲۰۰۱ میلادی در کشور رومانی تاسیس شد و در زمانی اندک، به یکی از سازندگان مطرح نرم‌افزارهای ضدویروس تبدیل شد. شرکت Bitdefender سازنده یکی از سریع‌ترین و کارآمدترین نرم‌افزارهای ضدبدافزار در دنیا است.

محصولات متنوع Bitdefender صدها میلیون کاربر خانگی و سازمانی را در اقصی نقاط جهان در برابر تهدیدات سایبری محافظت می‌کنند. محصولات Bitdefender توسط نمایندگان محلی این شرکت در بیش از ۲۰۰ کشور دنیا توزیع و پشتیبانی می‌شوند.

شرکت‌های متعددی از جمله Bullguard، Qihoo، GData، F-Secure eScan و IBM از فناوری‌های Bitdefender در شناسایی بدافزارها بهره می‌گیرند.


Bitdefender


Avira, Kaspersky Lab


ThreatTrack VIPRE, AVG

# آسیب پذیری های امنیتی

# کشف بیش از ۲۰۰ آسیب‌پذیری در محصولات Trend Micro


به گزارش شرکت مهندسی شبکه گستر به نقل از سایت Forbes دو محقق امنیتی در مدت ۶ ماه بیش از ۲۰۰ آسیب‌پذیری را در محصولات Trend Micro کشف و گزارش کرده‌اند.

این دو هکر کلاه سفید نخستین باگ را در ۱۱ تیر ماه ۹۵ به شرکت Trend Micro گزارش کردند. بررسی‌های بعدی این محققان منجر به کشف ۲۲۲ آسیب‌پذیری دیگر در ۱۱ محصول این شرکت گردید. ۱۹۴۴ مورد از این آسیب‌پذیری‌ها، به‌صورت از راه دور و بدون نیاز به دخالت کاربر قابل بهره‌جویی هستند.

یکی از مخرب‌ترین این آسیب‌پذیری‌ها در ابزار جلوگیری از از دست رفت داده‌های Trend Micro شناسایی شده است. سوءاستفاده از این آسیب‌پذیری مهاجم را قادر به در اختیار گرفتن کنترل سروری که این نرم‌افزار بر روی آن اجرا شده می‌کند.

از آسیب‌پذیری‌های قابل توجه دیگر ضعفی از نوع Cross-site Scripting به اختصار - XSS - است که در نرم‌افزار InterScan این شرکت شناسایی شده است.

قرار است در کنفرانس Hack In The Box در فروردین ۱۳۹۶ این دو هکر کلاه سفید جزییات بیشتری در خصوص این آسیب‌پذیری‌ها که ممکن است تا آن زمان تعداد آنها بیشتر نیز شود ارائه کنند.

هر چند که بر اساس توضیحات سایت Forbes، این شرکت به این محققان پاسخگو بوده و اصلاحیه‌هایی را برای ترمیم این آسیب‌پذیری‌ها عرضه کرده اما این اصلاحیه‌ها ناکافی اعلام شده‌اند.

به گزارش شرکت مهندسی شبکه گستر به نقل از سایت SC Magazine یکی از مدیران ارشد شرکت Trend Micro گفته که نشانه‌ای مبنی بر سوءاستفاده از این ضعف‌ها یافت نکرده‌اند. این مقام شرکت Trend Micro وعده داده که با مشارکت تیم‌های تحقیق و توسعه این شرکت پروسه توسعه نرم‌افزارها بهبود داده خواهد شد.

کشف آسیب‌پذیری در محصولات امنیتی محدود به محصولات شرکت Trend Micro نیست؛ برای نمونه در ماه‌های اخیر یکی از محققان شرکت Google ضعف‌هایی امنیتی را در محصولات شرکت‌های Kaspersky و Symantec کشف و به این شرکت‌ها گزارش کرده است.

# لغو عرضه اصلاحیه‌های ماه فوریه مایکروسافت

۲۶ بهمن ماه در حالی که قرار بود شرکت مایکروسافت اصلاحیه های ماه فوریه خود را عرضه کند، این شرکت اعلام کرد که ارائه آنها در تاریخ مذکور را به دلیل آنچه که مایکروسافت آن را بروز یک مساله لحظه آخری خوانده لغو کرده است.

مایکروسافت توضیحی در خصوص این مساله لحظه آخری نداده است.

بر اساس یک سنت قدیمی شرکت مایکروسافت در سه‌شنبه دوم هر ماه میلادی، اصلاحیه‌های امنیتی جدید خود را عرضه می‌کند.

این اقدام مایکروسافت در حالی صورت گرفت که حدود دو هفته قبل از آن جزییات وجود یک ضعف امنیتی روز صفر علنی شد.

این آسیب‌پذیری مربوط به پودمان SMBv3 است که چندین نسخه از سیستم عامل Windows از جمله 8.1، 10، Server 2012 و Server 2016 را تحت تأثیر قرار می‌دهد. مهاجم با بهره‌جویی از این آسیب‌پذیری قادر به ایجاد اشکال و حتی اجرای کد بر روی دستگاه هدف قرار گرفته شده است.

محقق کاشف این آسیب‌پذیری، این اشکال را در پاییز به مایکروسافت گزارش کرده بود اما تعلل این شرکت در ارائه اصلاحیه سبب شد که این محقق اقدام به انتشار عمومی جزییات آن کند.

مدتی کوتاه پس از آن نیز، گروه Project Zero شرکت Google جزییات وجود یک آسیب‌پذیری امنیتی را در مرورگرهای IE و Edge به‌صورت عمومی منتشر کرد.

بر اساس توضیحات ارائه شده توسط گروه Project Zero مهاجم می‌تواند با نوشتن کمتر از ۲۰ خط کد HTML در زمان مراجعه کاربر به سایت حاوی آن کد، از این آسیب‌پذیری بهره‌جویی کرده و ضمن از کارانداختن مرورگر، در پشت صحنه فایل مخرب را بر روی دستگاه اجرا کند.

هدف Project Zero، شناسایی ضعف‌های امنیتی پیش از مورد سوءاستفاده قرار گرفتن توسط تبهکاران سایبری است.

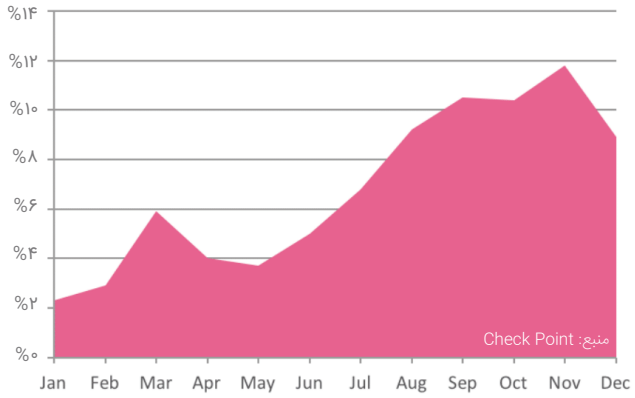
این آسیب‌پذیری در ۵ آذر ۹۵ به شرکت مایکروسافت اعلام شده بود.

بر اساس سیاست‌های Project Zero پس از اعلام وجود آسیب‌پذیری به سازنده نرم‌افزار، مهلتی ۹۰ روزه برای ترمیم آن به سازنده داده می‌شود. احتمالاً شرکت مایکروسافت قصد داشته که این آسیب‌پذیری را در اصلاحیه‌های ماه فوریه خود برطرف کند.

آمـــار

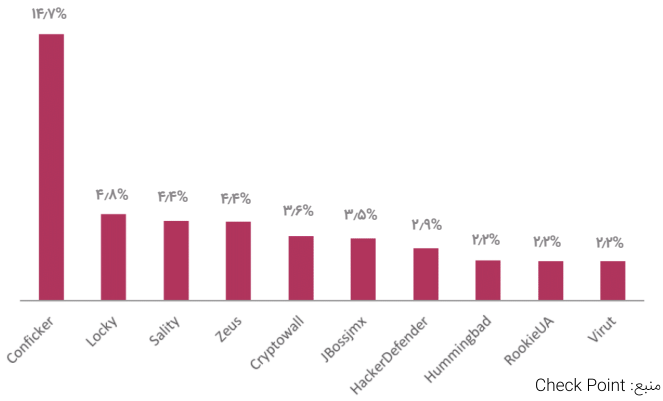
**سهم حملات باج افزارها از تمامی حملات سایبری اجرا شده در شش ماهه دوم ۲۰۱۶**

سـهم حمـلات بـاج افزارهـا از تمامی حملات سـایبری اجرا شـده در شـش ماهه دوم ۲۰۱۶ در مقایسـه بـا شـش ماهه قبـل از آن تقریباً دو برابر شـد.

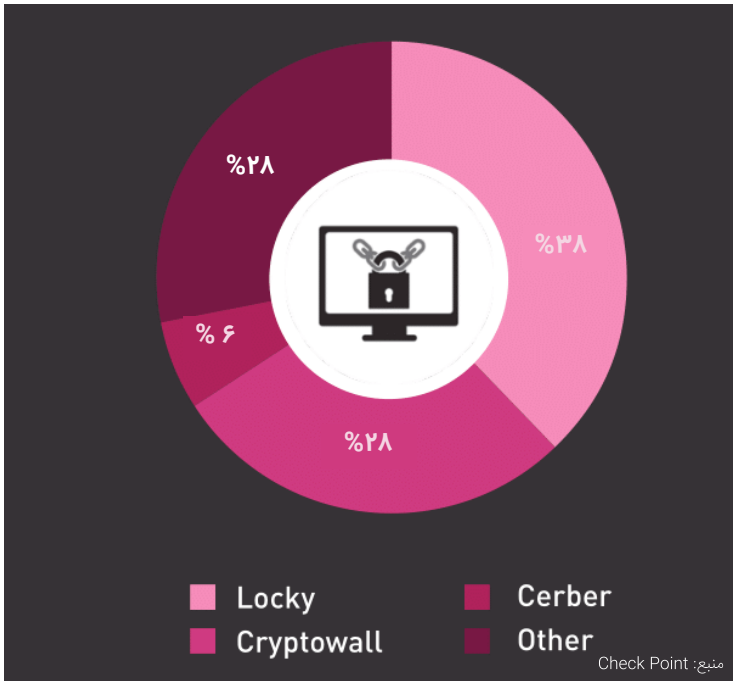



**۱۰ آلودگی اول در شش ماهه دوم ۲۰۱۶ در منطقه اروپا، خاورمیانه و آفریقا**

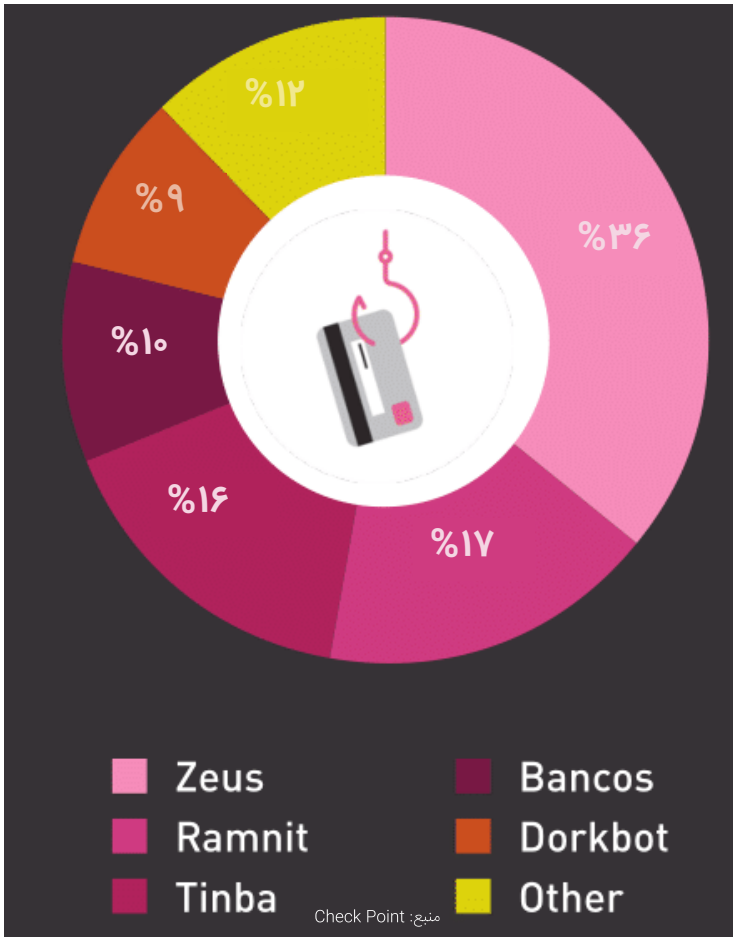
بدافزارهـای Sality، Locky، Conficker و Zeus بیشـترین سـهم از آلودگی‌ها را در نیمـه دوم سـال ۲۰۱۶ در منطقـه اروپـا، خاورمیانه و آفریقا داشـته‌اند. جالب اینکـه بدافزار قدیمـی Conficker همچنان در صدر قـرار دارد.



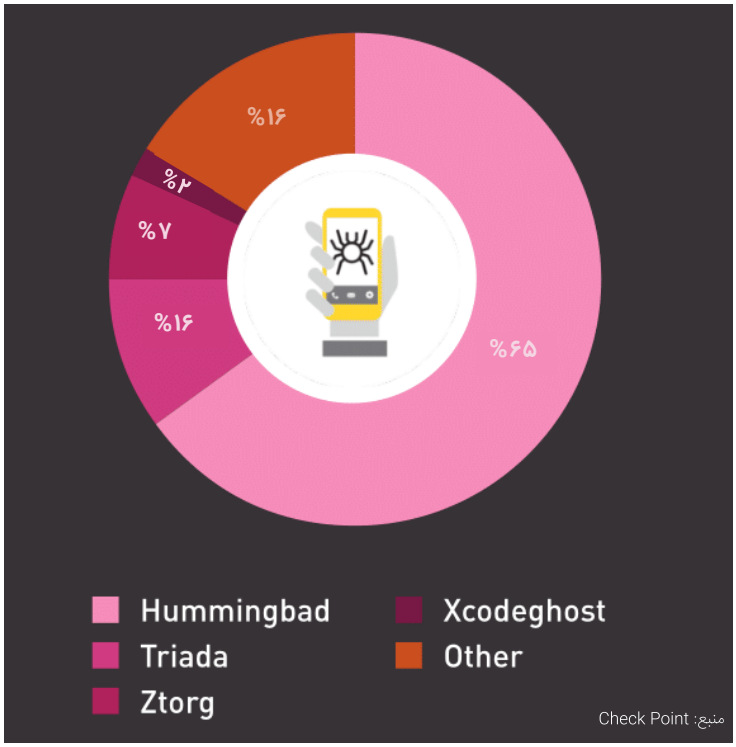

**سه باج‌افزار اول در شش ماهه دوم ۲۰۱۶ در منطقه اروپا، خاورمیانه و آفریقا**



**پنج بدافزار بانکی اول در شش ماهه دوم ۲۰۱۶ در منطقه اروپا، خاورمیانه و آفریقا**




**چهـــار بدافـــزار اول دســـتگاه‌های همـــراه در شـــش ماهـــه دوم ۲۰۱۶ در منطقـــه اروپـــا، خاورمیانـــه و آفریقـــا**



## 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.


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