پیش بینی حوادث
سایبری
در سال ۱۳۹۷

شبکه گستر

خلاصه مدیریتی

وابستگی بشر به صنعت فناوری اطلاعات هر روز بیشتر و بیشتر می‌شود. وابستگی بیشتر، یعنی ارزشمندتر شدن داده‌های راه یافته به آن و حیاتی‌تر شدن بسیاری از خدمات الکترونیکی؛ در این میان آنچه که بیش از هر زمانی دیگر اهمیت پیدا می‌کند امنیت این داده‌ها و خدمات است. مساله‌ای که همواره چالشی برای کاربران و سازمان‌ها و صد البته فرصتی برای تبهکاران بوده است.

حدود سه دهه قبل، ویروس‌ها اصلی‌ترین تهدید برای سیستم‌ها و شبکه‌های کامپیوتری محسوب می‌شدند. برنامه‌های مخربی که معمولاً توسط افرادی ماجراجو و صرفاً با هدف جلب توجه کاربران به مهارت ویروس‌نویس نوشته می‌شدند.

اما سالهاست که دامنه تهدیدات کامپیوتری از ویروس‌های پر سروصدا فراتر رفته است. گردانندگان این تهدیدات نیز دیگر محدود به آن جوانان کنجکاو نیست. کم نیستند ویروس‌نویسان و هکرهایی که سالانه میلیون‌ها دلار را از راه انتشار بدافزارهای مخرب یا اجرای حمات سایبری به جیب می‌زنند.

در این ویژه‌نامه تلاش شده تا بر اساس رویدادها و تجارب کسب شده در گذشته و مرور و بررسی بدافزارها، حملات و تهدیدات سایبری در سال ۹۶، دورنمایی از مهمترین موضوعات و چالش‌های حوزه امنیت فناوری اطلاعات در سال ۹۷ ترسیم شود.

بطور خلاصه انتظار می‌رود که موارد زیر اصلی‌ترین موضوعات سال ۹۷ در دنیای امنیت فناوری اطلاعات باشند:

- افزایش شمار باج‌افزارها در پی گسترش خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware as a Service - به اختصار RaaS) و ظهور نسخه‌هایی با عملکرد کرم (Worm)
- ظهور هر چه بیشتر باج‌افزارهای فارسی
- استقبال تبهکاران سایبری از ابزارهای موسوم به استخراج‌کننده پول‌های دیجیتال (Cryptocurrency Miner) و توزیع آنها بر روی ایستگاه‌های کاری و سرورها از طریق بدافزارها
- افزایش بدافزارهای سیستم عامل Android نه فقط در بازارهای توزیع دیجیتال غیررسمی که حتی بر روی بازار رسمی Google Play
- ادامه روند رو به رشد بدافزارهای تحت سیستم عامل Mac
- ظهور تهدیدات جدید برای سیستم عامل Windows و افزایش بهره‌جویی از آسیب‌پذیری‌ها و ضعف‌های امنیتی نرم‌افزار پراستفاده Microsoft Office

در سال ۹۶، فعالیت گسترده باج‌افزار Cerber و انتشار وسیع و غیرمنتظره باج‌افزارهای WannaCry و Petya - که با نام NotPetya نیز شناخته می‌شود - را شاهد بودیم. با نگاهی به آمار، خواهیم دید که در سالی که گذشت، WannaCry با عبور از Cerber به عنوان پرسودترین عضو خانواده باج‌افزارها، موفق به تصاحب سهم بیشترین آلودگی‌ها به باج‌افزار شد.

Ransoware-as-a-service

باج‌افزار به عنوان سرویس (RaaS) یا به عبارتی بسته‌های ساخت باج‌افزار برای همه - صرف‌نظر از میزان توانائیشان در برنامه‌نویسی - به مشکلی روزافزون تبدیل شده که بهترین مثال برای آن، همین باج‌افزار نام آشنای Cerber است. در سال ۹۶ نویسندگان Cerber توانستند که مدیران شبکه بسیاری از سازمان‌ها، بیمارستان‌ها و دانشگاه‌ها را به زانو در آورده و مبالغ هنگفتی از آنها اخاذی کنند.

همچنین در سالی که گذشت، باج‌افزارها نه فقط سیستم عامل Windows که بطور گسترده کاربران با دستگاه‌های تحت Android را هدف قرار دادند.

نکته نگران‌کننده انتشار برنامک‌های ناقل باج‌افزار از طریق بازار رسمی توزیع دیجیتال Google Play Store است. هر چند که Google این بازار را همواره تحت رصد و کنترل داشته و دارد اما به نظر نمی‌رسد که سال ۹۶ پایانی بر دور زدن سیاست‌های امنیتی این شرکت توسط نویسندگان انواع بدافزارها از جمله باج‌افزارها باشد.

در سال ۹۶، تهدیدات پرکاربرترین سیستم عامل دستگاه‌های همراه تنها محدود به باج‌افزارها نبودند. انواع بدافزارهای دیگر با اهداف مختلف از ارسال ناخواسته پیامک گرفته تا سرقت داده‌ها، از غیرفعال کردن برنامک‌های امنیتی و ضدویروس گرفته تا نصب برنامک‌های بالقوه ناخواسته (Potentially Unwanted Program) و جاسوس‌افزارها (Spyware) نیز موفق به آلوده‌سازی سهم قابل توجهی از دستگاه‌های همراه با سیستم عامل Android شدند. کاربران دستگاه‌های با سیستم عامل Mac و Linux نیز چندان از این نوع بدافزارهای مخرب آسوده خاطر نبودند و گزارش‌های متعدد، از آلوده شدن این دستگاه‌ها به باج‌افزار حکایت داشته است.

در سالی که گذشت شاهد انتشار پرسروصدای دو باج‌افزار فارسی نیز بودیم. فارسی بودن اطلاعیه باج‌گیری (Ransom Note) این دو باج‌افزار نمایانگر تمرکز نویسندگان آنها بر روی کاربران و سازمان‌های ایرانی بود.

Ransomware

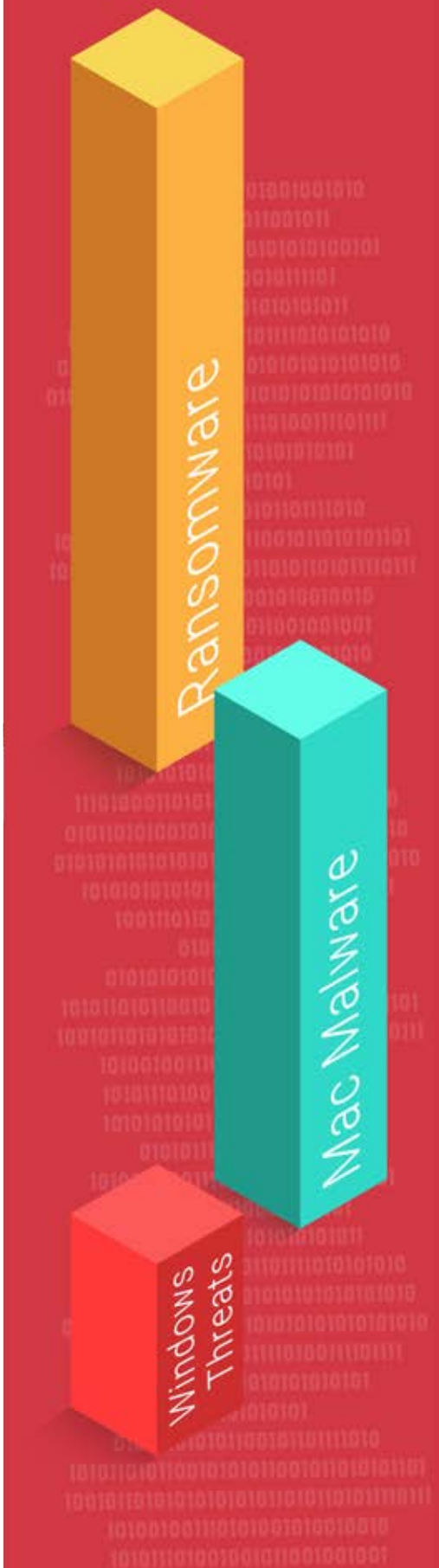
در سال ۹۷، باج‌افزارها همچنان یکی از دغدغه‌های اصلی مدیران شبکه سازمان‌ها باقی خواهند ماند. ضمن اینکه پیش‌بینی می‌شود که تعداد باج‌افزارهای فارسی نیز روندی صعودی به خود گرفته و تبعات آن بیش از قبل گریبانگیر کاربران و سازمان‌های ایرانی بی‌توجه به توصیه‌های امنیتی شود.

در سال ۹۶، برنامه‌های ناخواسته و سایت‌هایی که نصب یا فراخوانی آنها منجر به اجرای ابزارهای موسوم به استخراج کننده پول‌های دیجیتالی همچون Monero بر روی دستگاه کاربر می‌شود گسترش فراوانی داشتند. در برخی موارد مهاجمان با بکارگیری بهره‌جوها (Exploit) و روش‌های پیشرفته اقدام به آلوده نمودن سرورهای با سیستم عامل Windows و Linux کرده و از آنها برای استخراج پول دیجیتالی بهره‌گیری کردند. با توجه به سود فراوان توسعه و توزیع این برنامه‌های ناخواسته، انتظار می‌رود که دامنه اهداف گردانندگان آنها به سرعت گسترش یابد.

در این ویژه نامه مروری هم خواهیم داشت بر بدافزارهای تحت سیستم عامل Mac؛ بدافزارها و حملات بر ضد سیستم عامل Apple در مقایسه با رقیب آن ناچیز است؛ اما همانطور که در ادامه خواهیم خواند این سیستم عامل هم بدخواهان خود را دارد.

در نهایت نیز مروری خواهیم داشت بر بدافزارهای ویژه‌ای که با بهره‌جویی از آسیب‌پذیری‌ها و ضعف‌های امنیتی مجموعه نرم‌افزاری Microsoft Office دستگاه کاربران را به کنترل خود در می‌آورند.

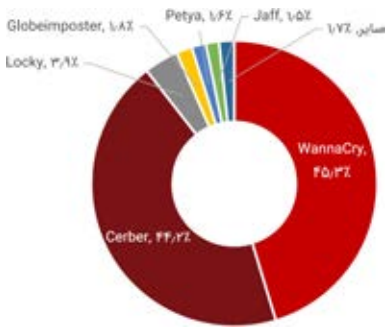
شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب این ویژه‌نامه که حاصل تحقیق و پژوهش کارشناسان این شرکت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



باج افزارها

WannaCry: تصویری متفاوت از باج‌افزارها

برای مدتی طولانی، Cerber فعال‌ترین عضو خانواده باج‌افزارها بود؛ اما برای چند ماه این باج‌افزار در پس طوفان عظیم WannaCry که با بهره‌جویی از یک آسیب‌پذیری و با رفتاری مشابه کرم‌های کامپیوتری یک دهه قبل منتشر می‌شد به حاشیه رانده شد.

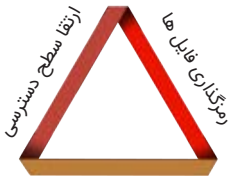


WannaCry باج‌افزاری معمولی مشابه باج‌افزارهای دیگر که از طریق ایمیل و در قالب لینک و پیوست مخرب منتشر می‌شوند نبود. بلکه با خاصیت کرم گونه و با بهره‌جویی از یک ضعف امنیتی در بخش SMB سیستم عامل Windows از روی نخستین دستگاه آلوده شده، به‌سرعت خود را در سطح شبکه و اینترنت تکثیر می‌کرد. در مدتی کوتاه، بیش از ۳۵۰ هزار دستگاه در ۲۰۰ کشور جهان از جمله ایران به این باج‌افزار گرفتار شدند.

ماجرای آسیب‌پذیری مورد استفاده WannaCry به اوایل سال ۹۶ و انتشار اسناد محرمانه‌ای باز می‌گردد که در جریان آن فایل‌های سرقت شده از یک گروه نفوذگر حرفه‌ای با نام Equation که وابستگی اثبات شده‌ای به "سازمان امنیت ملی" دولت آمریکا (NSA) دارد توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. در بین این فایل‌ها، بهره‌جوهایی به چشم می‌خوردند که از یک ضعف امنیتی روز صفر در بخش سیستم عامل Windows که به EternalBlue موسوم شد سوءاستفاده می‌کردند. یک ماه پیش از درز این اطلاعات شرکت مایکروسافت اقدام به عرضه اصلاحیه‌ای با شناسه MS17-010 به‌منظور ترمیم آسیب‌پذیری مذکور نموده بود.

نویسنده یا نویسندگان WannaCry نیز با استفاده از بهره‌جوی این آسیب‌پذیری باج‌افزار خود را به کرمی بسیار مخرب تبدیل کرده بودند.

بررسی دقیق‌تر این باج‌افزار ما را به حمله‌ای سه مرحله‌ای می‌رساند. کار با اجرای از راه دور کد شروع شده و باج‌افزار سطح دسترسی خود را ارتقاء می‌دهد. از آنجا به بعد، کدهای مورد نیاز استخراج شده و به اجرا در می‌آیند. پس از آن فایل‌های کاربر رمزگذاری شده و اطلاعیه باج‌گیری ظاهر می‌شود.



WannaCry از یک الگوریتم رمزگذاری قدرتمند برای رمز کردن فایل‌هایی همچون اسناد، تصاویر و ویدئوها استفاده می‌کند. ضمن اینکه فایل‌های پایگاه داده SQL و فایل‌های اطلاعاتی Exchange بر روی سرورها نیز از گزند این باج‌افزار در امان نیستند.

انتشار WannaCry در ماه‌های اخیر روندی نزولی داشته که از نصب شدن اصلاحیه توسط کاربران حکایت دارد.

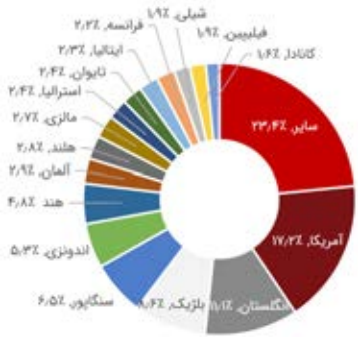
متأسفانه با توجه به انتشار مستمر بهره‌جوهای روز صفر (Zero-day Exploit) توسط سایت‌ها و گروه‌هایی همچون WikiLeaks و Shadow Brokers و بی‌توجهی بسیار از کاربران به لزوم نصب اصلاحیه‌های امنیتی باید انتظار اجرای چنین حملاتی را در سال ۹۷ داشته باشیم.

Cerber، همچنان قدرتمند

هر چند در سال ۹۶، Cerber با ٤٤ درصد در مقام دوم باج‌افزارهای با بیشترین قربانی قرار گرفت اما این چیزی از میزان مخرب بودن این باج‌افزار پیشکسوت کم نمی‌کند. Cerber از جمله باج‌افزارهایی است که مجهز به قابلیت‌هایی برای عبور از سد نرم‌افزارهای ضدویروس و ابزارهای موسوم به قرنطینه امن (Sandbox) است. Cerber باج‌افزاری است که گردانندگان آن به طور مستمر در حال به‌روزرسانی و ارتقای آن هستند و به نظر نمی‌رسد که این روند در سال ۹۷ متوقف شود.

پراکندگی در سطح جهان

شرکت Sophos در گزارشی میزان انتشار باج‌افزارها را به تفکیک کشورها در فاصله ۱۲ فروردین تا ۱۱ مهر ۹۶ بررسی کرده؛ بر اساس این بررسی آمریکا و پس از آن انگلستان و بلژیک در مقام‌های اول تا سوم قرار داشته‌اند.



در سالی که گذشت، گزارش‌های متعددی در خصوص آلوده شدن شبکه سازمان‌های ایرانی به انواع باج‌افزارها به شرکت مهندسی شبکه گستر واصل شد. نکته قابل توجه در خصوص بسیاری از این آلودگی‌ها، نفوذ مهاجمان به شبکه سازمان از طریق پودمان RDP و سپس اجرای فایل مخرب باج‌افزار بر روی دستگاه‌ها - و متاسفانه در بسیاری موارد بر روی سرورها - بوده است.

باج‌افزار به عنوان سرویس

تجارت باج‌افزار در شبکه تاریک (Dark Web) عظیم است. صاحبان این بدافزارهای مخرب درک کرده‌اند که نه فقط با اخاذی از قربانیان خود که با فروش بسته‌های باج‌افزار می‌توانند به ثروتی هنگفت دست پیدا کنند.

بهترین مثال برای باج‌افزارهایی که با این ساختار عرضه می‌شوند باج‌افزار Cerber است. نمونه‌ای دیگر Karmen است که به محض اجرا شدن بر روی Windows، فایل‌ها را رمزگذاری کرده و در ازای ارائه یک ابزار رمزگشایی از کاربر اخاذی می‌کند.

در روش "باج‌افزار به عنوان سرویس" صاحب 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.

پیش‌بینی می‌شود که در سال ۹۷ نیز عرضه باج‌افزار در قالب چنین سرویس‌هایی همچنان ادامه یافته و با تنوع هر چه بیشتر به بدخواهان سایبری عرضه شود.

واحد پول اخاذی

تقریباً از زمان ظهور نخستین گونه از باج‌افزارهای رمزگذار، بیت‌کوین (Bitcoin)، واحد پول مبلغ اخاذی شده از قربانیان بود.

ارزش بیت‌کوین هر چند در نمایی کلی روندی صعودی داشته اما در چند ماه گذشته بالا و پایین‌های فراوانی داشته است.

کاهش سریع ارزش این واحد پولی می‌تواند ضررهای فراوانی را متوجه صاحبان باج‌افزارها کند.

هزینه نقل و انتقال در این واحد پولی نیز از چند سنت در سال‌های گذشته به ده‌ها دلار در ماه‌های اخیر رسیده که این خود یکی دیگر از مشکلات استفاده از این واحد پولی است.

در سال ۹۶، نمونه‌هایی از باج‌افزارها مشاهده شدند که علاوه بر بیت‌کوین از پرداخت از طریق واحد دیجیتال مونرو (Monero) هم پشتیبانی می‌کردند.

در بهمن ماه نیز نسخه‌ای از باج‌افزار HC7 مشاهده شد که از ویژگی‌های خاص آن پذیرفتن واحد پول دیجیتال اِتیریم (Ethereum) علاوه بر پشتیبانی از پرداخت از طریق بیت‌کوین و مونرو بود.

ایراداتی که در نقض حریم شخصی و فاش شدن میزان نقل و انتقال به کیف پول دیجیتال بیت‌کوین مطرح می‌شود متوجه پول‌های دیجیتال مونرو و اتیریم نیست.

ضمن اینکه اتیریم مجهز به قابلیتی موسوم به Smart Contracts نیز می‌باشد.

بطور کلی تضمینی نیست که در صورت پرداخت باج توسط قربانی، نویسنده باج‌افزار کلید رمزگشایی را در اختیار قربانی قرار دهد. در صورت استفاده نویسنده باج‌افزار از قابلیت Smart Contracts این امکان فراهم خواهد بود که تنها در صورت ارسال کلید رمزگشایی، عملیات پرداخت تکمیل شود. هر چند که بکارگیری این قابلیت در فرآیند دریافت باج بسیار پیچیده بوده و برخی کارشناسان استقبال نویسندگان باج‌افزار از آن را دور از انتظار می‌دانند.

البته روش اخاذی، خود، تنوع فراوانی دارد. برای مثال باج‌افزار Spora خدمات خود را در قالب بسته‌های "بازگردانی کامل"، "مصونیت در برابر حملات آتی باج‌افزار"، "حذف باج‌افزار" و "بازگردانی فقط فایل" به قربانیان ارائه می‌دهد!

جالب اینکه سایت این باج‌افزار که پس از پایان رمزگذاری فایل‌ها، قربانی به آن هدایت می‌شود مجهز به بخشی برای گفتگوی زنده قربانیان با تبهکاران صاحب Spora است!

گسترش باج‌افزارهای ایرانی

در پائیز سال ۹۶، باج‌افزاری موسوم به Tyrant که بر اساس یک باج‌افزار کد باز (Open Source) توسعه داده شده بود موفق به آلوده‌سازی برخی از دستگاه‌ها در سطح کشور شد.
با توجه به فارسی بودن اطلاعیه باج گیری آن کاملاً مشخص است که این باج‌افزار برای هدف قرار دادن کاربران فارسی زبان طراحی شده است.

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر)، روش انتشار این باج‌افزار را استفاده از پوشش فیلترشکن سایفون گزارش کرده است. به این ترتیب که از طریق شبکه‌های اجتماعی با فریفتن کاربران، آنها را تشویق به دریافت و اجرای فایلی اجرایی با ظاهر سایفون می کند که در حقیقت حاوی بدافزار می‌باشد.
برخی منابع دیگر نظیر سایت sensorstechforum.com به انتشار این باج‌افزار از طریق هرزنامه‌ها و ایمیل‌های با پیوست مخرب اشاره کرده‌اند.
شرکت Enigma Software Group نیز در گزارشی Tyrant را مبتنی بر باج‌افزار DUMB اعلام کرده که پیش‌تر کاربران ترک زبان را هدف قرار داده بود.
در مدت کوتاهی پس از انتشار خبر Tyrant، باج‌افزاری دیگر موسوم به WannaSmile شناسایی شد که فایل‌های پراستفاده و بااهمیت را با الگوریتم‌های AES/RSA رمزگذاری کرده و در ازای بازگرداندن آنها بحالت قبل، از کاربر مبلغ ۲۰ بیت‌کوین را اخاذی می‌کرد.
اطلاعیه باج‌گیری WannaSmile نیز همانند Tyrant، فارسی است که نمونه‌ای از آن در تصویر زیر نمایش داده شده است:

در اطلاعیه مذکور از کاربر خواسته می‌شود تا ظرف پنج روز مبلغ ۲۰ بیت‌کوین را به نشانی کیف بیت‌کوین درج شده در اطلاعیه واریز کرده و موضوع را از طریق ایمیل wannasmile@tuta.io به گردانندگان این باج‌افزار اطلاع دهد. در این اطلاعیه هشدار داده شده که در صورت عدم پرداخت باج در مهلت تعیین شده هر روز یک بیت‌کوین به مبلغ اصلی افزوده خواهد شد.

در زمان نگارش این ویژه‌نامه ارزش هر بیت‌کوین، حدود هشت هزار دلار است که با احتساب هر دلار ۴۵۰۰ تومان مبلغ اخاذی شده توسط این باج‌افزار، به مبلغ ۷۲۰ میلیون تومان می‌رسیم که مبلغی غیرمعمول در میان باج‌افزارها محسوب می‌شود.

همچنین در اطلاعیه مذکور نشانی چند سایت اینترنتی نیز برای خرید بیت‌کوین در ایران معرفی شده است.

این باج‌افزار که به نظر می‌رسد نسخه‌ای برگرفته شده از باج‌افزار ZCrypt باشد به فایل‌های رمزگذاری شده پسوند WSmile. را الصاق می‌کند.

انتظار می‌رود که در سال آینده شاهد ظهور تعداد بیشتری از چنین باج‌افزارهایی که به باج‌افزارهای فارسی معروف شده‌اند باشیم.

قـربانیـــان

حملات باج‌افزارها در سال ۹۶ بر روی سازمان‌هایی همچون مراکز درمانی، دولتی، زیرساخت‌های حساس، آموزشی و کسب‌وکارهای کوچک متمرکز شدند. سازمان‌هایی که احتمال پرداخت باج توسط آنها بیشتر از سایر سازمان‌ها به نظر می‌رسد.

برای مثال، در بهمن ماه، بیمارستان آمریکایی Hancock که دستگاه‌های آن آلوده به باج‌افزار شده بودند، در ازای رمزگشایی فایل‌ها، اقدام به پرداخت ۵۵ هزار دلار به مهاجمان کرده است. آلوده شدن بیمارستان‌ها و مراکز درمانی به باج‌افزار موضوع جدیدی نیست و در طی دو سال گذشته به کرات اتفاق افتاده است. اما آنچه که این رویداد را با سایر رخدادهای قبلی متفاوت می‌کند پرداخت باج به مهاجمان با وجود فراهم بودن نسخه پشتیبان از فایل‌های رمزگذاری شده است. مدیریت این بیمارستان در گفتگو با یکی از رسانه‌های محلی دلیل اتخاذ این تصمیم را زمانبر بودن فرآیند برگرداندن نسخه پشتیبان دانسته و گفته این کار می‌توانست روزها و شاید هفته‌ها به درازا بیانجامد. به همین خاطر، پرداخت باج به نفوذگران را به بازگرداندن نسخه پشتیبان (Backup) ترجیح داده‌اند.

پیش‌بینی می‌شود که مراکز درمانی و کسب و کارهای کوچک همچنان اصلی‌ترین اهداف باج‌افزارها باشند.

راه‌های پیشگیری و مقابله

- از ضدویروس قدرتمند و به‌روز استفاده شود.
- از اطلاعات سازمانی به‌صورت دوره‌ای نسخه پشتیبان تهیه شود. پیروی از قاعده ۱-۲-۳ برای داده‌های حیاتی توصیه می‌شود. بر طبق این قاعده، از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه به عنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود.
- از نصب فوری آخرین اصلاحیه‌های امنیتی اطمینان حاصل شود.
- پودمان RDP غیرفعال شده یا حداقل تنها کاربران محدود با گذرواژه‌های پیچیده مجاز به استفاده از آن باشند.
- دسترسی به پوشه‌های اشتراکی در حداقل سطح ممکن قرار داده شود.
- سطح دسترسی کاربران محدود شود. بدین ترتیب حتی در صورت اجرا شدن فایل مخرب توسط کاربر، دستگاه به باج‌افزار آلوده نمی‌شود.

برنامه‌های ناخـواسته استخراج‌کننده پول دیجیتال

نویسندگان برنامه‌های ناخواسته موسوم به استخراج کننده پول‌های دیجیتالی به سرعت در حال گسترش اهداف خود هستند.

در پول‌های دیجیتال، فرآیندی با عنوان استخراج (Mining) وجود دارد که یکی از اصلی‌ترین وظیفه آن تایید اطلاعات تبادل شده در شبکه این واحدهای پولی است. فرآیند استخراج مستلزم فراهم بودن توان پردازشی بسیار بالاست. در نتیجه شبکه واحد دیجیتال نیز در قبال تلاشی که برای این پردازش‌ها انجام می‌شود به استخراج‌کنندگان پاداشی اختصاص می‌دهد.

با توجه به نیاز به توان پردازش بالا، انجام استخراج می‌تواند یک سرمایه‌گذاری هزینه‌بر برای استخراج‌کننده باشد. اما برنامه های ناخواسته موسوم به Cryptocurrency Miner با بهره‌گیری از توان پردازشی دستگاه‌های آلوده به خود از آنها به‌منظور سودرسانی به نویسنده یا نویسندگان برنامه سوءاستفاده می‌کنند.

در حالی که ابزارهای استخراج کننده متنوعی در دسـترس هستند، اما Coinhive یکی از پراستفاده‌ترین ابزارهای استخراج کننده محسوب می‌شود.

ابزار Coinhive شامل کتابخانه‌ای از کدهای JavaScript است که در زمان عرضه آن در اواسط سال ۹۶، سازندگانش آن را به عنوان جایگزینی برای تبلیغات سنتی صاحبان سایت معرفی کردند.

به این ترتیب که مدیران سایت می‌توانند با بکارگیری این ابزار در صفحات خود سبب استخراج پول دیجیتال با استفاده از منابع پردازشگر دستگاه کاربر بازدید کننده از صفحات سایت شوند.

هر چند که بخش قابل توجهی از کامپیوترها دارای ضدویروس‌هایی هستند که توانایی مسدودسازی این نوع اسکریپت‌ها را در خود دارند اما این موضوع در مورد کاربران گوشی‌های هوشمند چندان صادق نیست. چیزی که سبب توجه بیشتر نویسندگان این برنامه‌های ناخواسته بر روی دستگاه‌های همراه شده است.

برای مثال، بتارگی شرکت Trend Micro از کشف دو برنامکی که در پشت صحنه اقدام به اجرای اسکریپت استخراج کننده می‌کنند خبر داده است. در زمان باز بودن این برنامک‌ها، اسکریپت استخراج کننده فعال شده و با استفاده از منابع دستگاه اقدام به استخراج به نفع صاحبان برنامک مخرب می‌کند. مشکل اصلی اینجاست که این نوع اسکریپت‌ها برای اجرا شدن بر روی دستگاه همراه نیازی به کسب اجازه از کاربر ندارند و ممکن است کاربر برای مدتها از تحت تسخیر بودن دستگاه خود آگاه نباشد.

همچنین شرکت Sucuri و بنیاد Wordfence، هر دو، نسبت به افزایش شمار آن دسته از سایت‌های مبتنی بر سامانه مدیریت محتوای WordPress خبر داده‌اند که مهاجمان با هک کردن آنها اقدام به تزریق ابزارهای استخراج کننده پول دیجیتال کرده‌اند.

انتظار می‌رود با توجه به درآمدزا بودن استفاده از این ابزارها، در آینده‌ای نزدیک نویسندگان ویروس و مهاجمان بیشتری به سمت استفاده از آنها در بدافزارها و سایت‌های هک شده رو بیاورند.

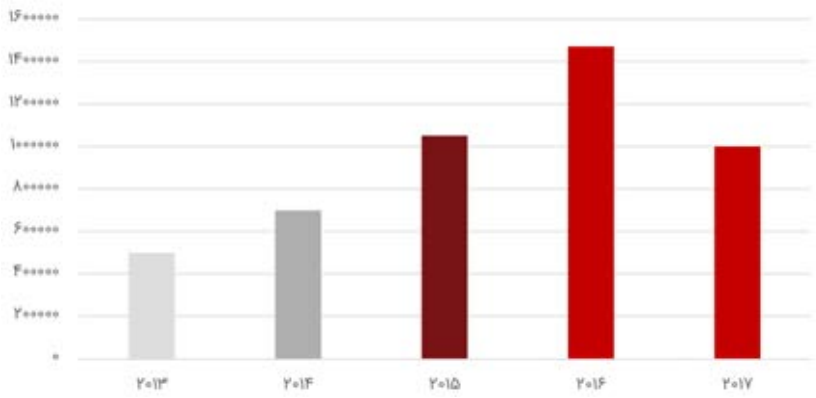
استفاده از ضدویروس قدرتمند، نصب آخرین اصلاحیه‌های امنیتی و دقت و حساسیت بالا در زمان کلیک بر روی لینک‌ها یا پیوست ایمیل‌ها همگی در کنار یکدیگر می‌توانند احتمال آلوده شدن کامپیوتر به این نوع برنامه‌های ناخواسته را به حداقل برسانند.

بدافـزارهـا و برنامک‌های ناخواسته تحت Android

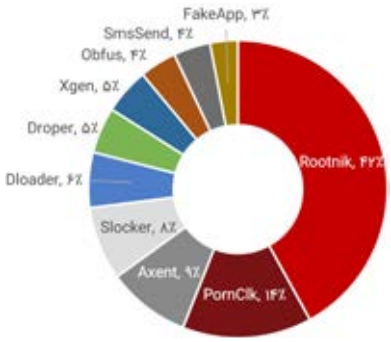
در سال ۹۶، بدافزارها یکی از مشکلات اصلی کاربران دستگاه‌های با سیستم عامل Android بودند. همانطور که در ادامه خواهیم دید کدهای مخرب در پس عناوین برنامک‌های معروف و معتبر مخفی شده و کاربران را برای نصب آنها بر روی دستگاه فریب می‌داده‌اند.

در مجموع تعداد برنامک‌های مخرب در طی چهار سال گذشته روندی نسبتاً ثابت صعودی داشته است. در سال ۲۰۱۳ تعداد برنامک‌های مخرب Android نیم میلیون مورد اعلام شده بود. در سال‌های ۲۰۱۵ و ۲۰۱۷ این تعداد بترتیب ۲/۵ و ۳/۵ میلیون عدد گزارش شد.

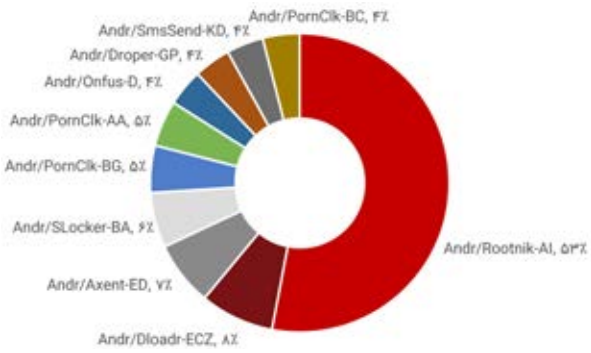
در عین حال تعداد برنامک‌های بالقوه ناخواسته که در بین سال‌های ۲۰۱۳ تا ۲۰۱۶ روندی صعودی داشته در سال گذشته میلادی کاهش یافته و از ۱/٤ میلیون در سال ۲۰۱۶ به ۱ میلیون در سال ۲۰۱۷ رسیده است.



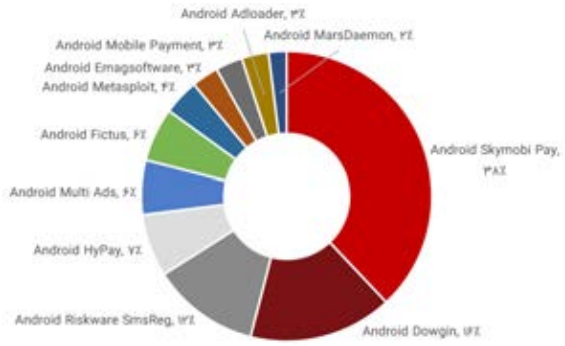
در سال ۲۰۱۷، Rootnik با اختصاص ٤۲ درصد از کل آلودگی‌های دستگاه‌های تحت Android، فعال‌ترین بدافزار این سیستم عامل اعلام شد.



در سال ۹۶، نسخه‌های مختلف بدافزار Rootnik در ظاهر تعداد قابل توجهی از برنامک‌های معروف بر روی Play Store کاربران را هدف قرار دادند. بر اساس آمار شرکت Sophos نسخه‌های مختلف این بدافزار بیش از نیمی از کل آلودگی‌های Android در سال ۲۰۱۷ را به خود اختصاص دادند.



همچنین در سال گذشته میلادی Android Skymobi Pay با ۳۸ درصد، بیشترین سهم از برنامک‌های بالقوه ناخواسته را از آن خود کرد.



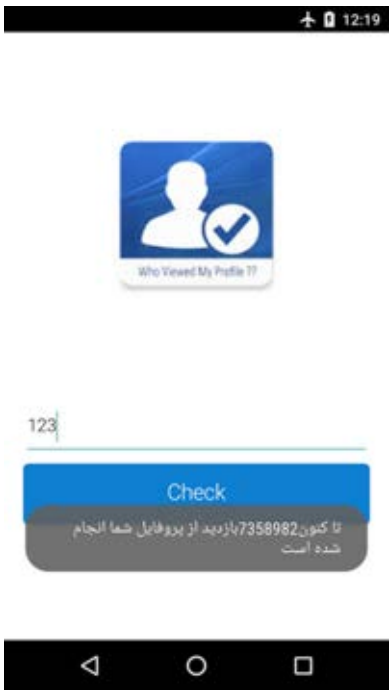
هر چند برنامک‌های بالقوه ناخواسته در دسته کدهای مخرب طبقه‌بندی نمی‌شوند اما انجام اقداماتی همچون نمایش تبلیغات ناخواسته سبب اشغال شدن منابع دستگاه و آزار کاربر می‌شوند.

بررسی یک نمونه: جاسوس‌افزار ایرانی

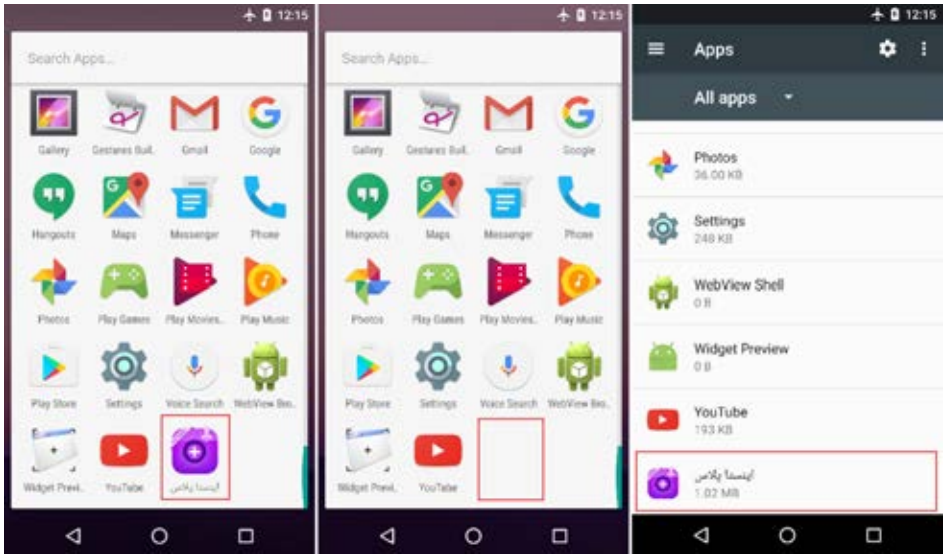
در سال ۹۶، جاسوس‌افزاری تحت سیستم عامل Android شناسایی شد که حجم قابل توجهی از داده‌های شخصی کاربر را از روی دستگاه جمع‌آوری کرده و آنها را به یک سرور در ایران ارسال می‌کرد.

این جاسوس‌افزار در قالب چندین برنامک مختلف منتشر شده بود. یکی از این برنامک‌ها با عنوان «اینستا پلاس» ادعا می‌کند که تعداد بازدیدکنندگان نمایه Telegram کاربر را نمایش می‌دهد. چند نمونه دیگر از این جاسوس‌افزار نیز در قالب برنامک‌های Cleaner Pro و Profile Checker کاربر را تشویق به نصب آن می‌کنند.

عملکرد کد مخرب جاسوس‌افزار، تقریباً در همه این برنامک‌ها یکسان بوده و هدف آن سرقت داده‌های شخصی قربانی از روی دستگاه Android آلوده شده است. مکانیزم ارتباط این جاسوس‌افزار با سرور فرماندهی خود نیز از طریق توابع Telegram Bot صورت می‌گیرد و بنابراین نویسنده یا نویسندگان آن عملاً خود سیستمی برای این منظور برنامه‌نویسی و پیاده‌سازی نکرده‌اند.
به محض دریافت برخی از برنامک‌های مذکور از کاربر خواسته می‌شود تا اطلاعات اصالت‌سنجی حساب Telegram خود را وارد کند. برنامک دلیل این درخواست را اعلام تعداد کاربرانی که نمایه آن کاربر را مشاهده کرده‌اند بیان می‌کند. اما در حقیقت این برنامک فقط یک عدد تصادفی را به کاربر نشان می‌دهد!



برنامک برای مدتی فعالیت خود را متوقف کرده و نشان خود را هم مخفی می‌کند. تا جایی که ممکن است بسیاری از کاربران تصور کنند که برنامک از روی دستگاه حذف شده است. اما پس از مدتی کد مخرب در پشت صحنه فعالیت خود را از سر می‌گیرد.



یکی از کارهایی که این برنامک انجام می‌دهد گرفتن عکس با استفاده از دوربین جلوی دستگاه است. اما جاسوسی آن محدود به انجام این کار نیست. اطلاعات تماس، پیامک‌های دریافتی و ارسالی (شامل شماره تماس فرستنده یا گیرنده و متن پیامک)، اطلاعات حساب Google و موقعیت دستگاه همگی در فایل‌هایی جداگانه ذخیره شده و سپس به سرور مهاجم ارسال می‌شوند.

این جاسوس افزار قادر است که هر یک از فرامین زیر را از سرور فرماندهی دریافت کرده و آنها را بر روی دستگاه اجرا کند:

- برقراری تماس یا ارسال پیامک
- ارسال اطلاعات در خصوص برنامک‌های نصب شده و فایل‌های در دسترس
- ارسال هر فایل به سرور یا حتی حذف آنها

باج‌افزارهای Android

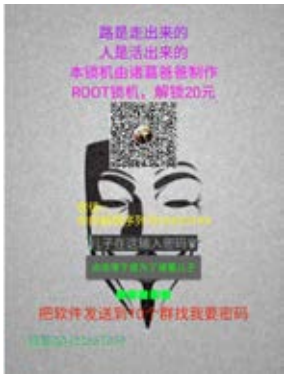
باج‌افزار تحت سیستم عامل Android را می‌توان در دو دسته زیر تقسیم‌بندی کرد:

- باج‌افزارهای قفل کننده صفحه نمایش (Lock Screen ransomware)
- باج‌افزارهای رمزگذار (Crypto ransomware)

باج‌افزارهای دسته نخست هر چند دسترسی کاربر را به دستگاه محدود می‌کنند اما فایل های کاربر را رمزگذاری نمی کنند. برخی گونه‌های این نوع باج‌افزارها کد PIN را تغییر می‌دهند. برخی هم اعمال مخرب دیگری همچون موارد زیر را انجام می‌دهند:

- برقراری ارتباط با سرور فرماندهی
- ارسال پیامک
- سرقت داده های حساس
- غیرفعال کردن ضدویروس دستگاه
- نصب یا حذف برنامک ها

شکل زیر نمونه ای از تصویر بکار رفته در قفل کردن دستگاه را نشان می‌دهد.



اما باج‌افزارهای دسته دوم اقدام به رمزگذاری فایل‌های ذخیره شده بر روی دستگاه نیز می‌کنند.

بررسی یک نمونه: DoubleLokcer

در سال ۹۶، باج‌افزاری با عنوان DoubleLokcer با سوءاستفاده از سرویس Accessibility دستگاه‌های با سیستم عامل Android را به تسخیر خود در می‌آورد.

سرویس Accessibility بخشی برای آسان کردن دسترسی کاربران با ناتوانی‌های جسمی به دستگاه تحت Android است.

نویسنده یا نویسندگان DoubleLokcer برای آلوده ساختن دستگاه‌های همراه به این باج‌افزار با بکارگیری تکنیک‌های مهندسی اجتماعی کاربر را تشویق به نصب یک برنامک مخرب - البته در ظاهر نرم‌افزار Flash Player - می‌کنند. در زمان نصب شدن برنامک مذکور از کاربر خواسته می‌شود تا مجوز دسترسی برنامک به سرویس Accessibility را صادر کند.

با دسترسی یافتن برنامک، کد مخرب با حق دسترسی Admin قادر به اجرای کامل خرابکاری‌ها و دست‌درازی‌ها به دستگاه می‌شود.

از جمله اینکه دسترسی به دستگاه با نمایش یک اطلاعیه باج‌گیری مسدود می‌شود، کد PIN با کدی تصادفی جایگزین می‌گردد و تمامی فایل‌های موجود بر روی حافظه اصلی با الگوریتم AES رمزگذاری می‌شود. DoubleLokcer پسوند cryeye را به فایل‌های رمزگذاری شده الصاق می‌کند.

کد جدید PIN و کلید رمزگذاری نیز به گرداننده یا گردانندگان این باج‌افزار ارسال می‌شود.

همچنین DoubleLokcer با تخصیص خود به عنوان برنامک پیش‌فرض اجرا شونده بر روی دستگاه، در هر بار فشرده شدن دگمه Home توسط کاربر مجدداً فعال می‌شود. در حقیقت، هدف این مکانیزم ناتوان ساختن کاربر در دسترسی یافتن به برنامک‌های بر روی دستگاه است.

DoubleLokcer از محدود باج‌افزارهای تحت سیستم عامل Android است که فایل‌های بر روی دستگاه را رمزگذاری می‌کند. اکثر باج‌افزارهای Android صرفاً دسترسی به دستگاه را با فعال کردن دائمی یک برنامک بر روی برنامک‌های دیگر مسدود می‌کنند.
بدیهی است که دسترسی به دستگاه قفل شده توسط DoubleLokcer با انجام عملیات بازگردانی کارخانه‌ای (Factory Rese) امکان‌پذیر است. ضمن اینکه در دستگاه‌های Root شده بازگشایی دسترسی در حالت موسوم به Debugging Mode و بدون نیاز به انجام عملیات بازگردانی کارخانه‌ای ممکن است. اما متاسفانه در زمان نگارش این گزارش، راهکاری برای بازگردانی فایل‌های رمزگذاری شده توسط DoubleLokcer، بدون در اختیار داشتن کلید رمزگشایی فراهم نمی‌باشد.

دو برابر شدن تهدیدات بر روی Play Store

Play Store بازار توزیع دیجیتال رسمی سیستم عامل Android است. سیاست‌های کنترلی شرکت Google در این بازار ورود برنامک‌های مخرب را نه غیرممکن که دشوار می‌کند.

بر طبق اعلام Google، این شرکت در سال ۲۰۱۷ بیش از ۷۰۰ هزار برنامک مخرب را از Play Store حذف کرده که افزایشی ۷۰ درصدی را در مقایسه با سال قبل از آن نشان می‌دهد. همچنین این شرکت مدعی است که ۹۹ درصد این برنامک‌های مخرب را در پروسه بررسی و پیش از آنکه توسط کسی از Play Store دریافت و بر روی دستگاه او اجرا شود شناسایی و مسدود کرده است.

بر طبق گزارشی از شرکت Sophos نیز در سال ۲۰۱۷ حداقل ۳۲ تهدید مختلف بر روی Play Store شناسایی شد که در مقایسه با سال قبل از آن دو برابر شده است.

برای مثال، Judy به عنوان یکی از این تهدیدات، تنها در مدت یک ماه، بیش از ۳۵ میلیون دستگاه را به خود آلوده کرد.

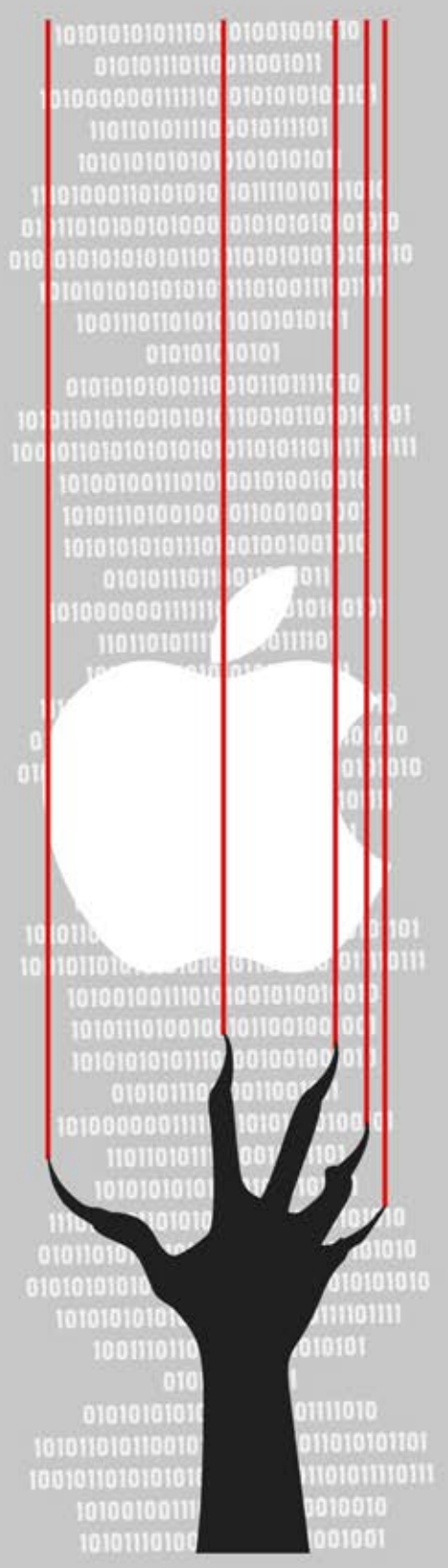
برخی نمونه‌ها نظیر Lipizzan نقش جاسوس‌افزار داشته و فعالیت کاربر بر روی دستگاه را رصد و داده‌های برنامک‌های معروف را سرقت می‌کنند. تعداد کل آلودگی‌ها به Lipizzan تنها ۱۰۰ مورد گزارش شده که تعداد بسیار ناچیزی در مقایسه با دیگر بدافزارها محسوب می شود.

محققان بر این باور بودند که دلیل اندک بودن تعداد آلودگی‌ها، ناشی از محدود بودن اهداف مهاجمان بوده است. در کد Lipizzan نشانه‌هایی دیده می‌شد که به شرکتی با عنوان Equus Technologies اشاره داشت. شرکتی که عرضه‌کننده سلاح‌های سایبری است و راهکارهای سفارشی برای نهادهای قانونی و اطلاعاتی و سازمان‌های امنیتی ارائه می‌کند. این جاسوس‌افزار در Play Store در ظاهر برنامک‌های بی‌خطری همچون Cleaner، Backup و Notes به اشتراک گذاشته شده بود.

Google این تهدیدات را مسدود کرد و Google Play Protect نیز آنها را از روی دستگاه‌های آلوده شده حذف کرد؛ اما قطعاً حذف این تهدیدات پایانی بر انتشار بدافزارها در بازار توزیع دیجیتال Play Store نخواهد بود.

راه‌های پیشگیری و مقابله

- سیستم عامل و برنامک‌های نصب شده بر روی دستگاه همراه همیشه به آخرین نسخه ارتقاء داده شود.
- برنامک‌ها فقط از بازار توزیع دیجیتال Play Store یا حداقل بازارهای مورد اعتماد معروف دریافت شود. 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 حاصل شود. با غیر فعال بودن گزینه نخست، از اجرا شدن فایل‌های APK میزبانی شده در بازارهای ناشناخته بر روی دستگاه جلوگیری می‌شود. وظیفه گزینه دوم نیز پویش دوره‌ای دستگاه است.
- پیش از نصب هر برنامک امتیاز و توضیحات کاربران آن مرور شده و به نکات منفی توضیحات کاربران توجه شود.
- به حق دسترسی‌های درخواستی برنامک در زمان نصب توجه شود. اگر فهرست آن بطور غیرعادی طولانی بود از نصب آن اجتناب شود.
- از راهکارهای امنیتی قدرتمند برای حفاظت از دستگاه‌های همراه سازمان بهره گرفته شود.



بدافـزارهـای Mac

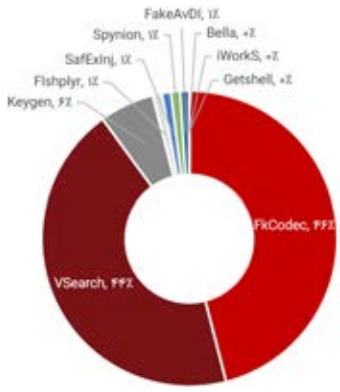
برای بیش از یک دهه تصور عموم کاربران و حتی باور برخی متخصصان فناوری اطلاعات بر این بود که سیستم عامل Mac در مقایسه با Windows در برابر بدافزارها امن‌تر و ایمن‌تر است.

همانطور که در سال‌های اخیر که بدافزارهای بیشتری سیستم‌های Mac را هدف قرار می‌دهند طرفداران Windows این باور را زیر سئوال می‌برند. هر چند که هواداران Mac هم همچنان مثال‌های بی‌شماری از بدافزارها و تهدیدات تحت Windows را در چنته دارند.

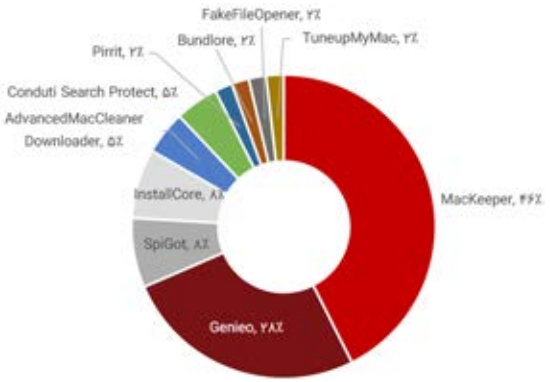
در سال ۹۶ تعداد قابل توجهی از بدافزارهای مخرب از جمله چند باج‌افزار دستگاه‌های با سیستم عامل Mac را هدف قرار دادند. MacRansom و MacSpy دو نمونه از این باج‌افزارها هستند.

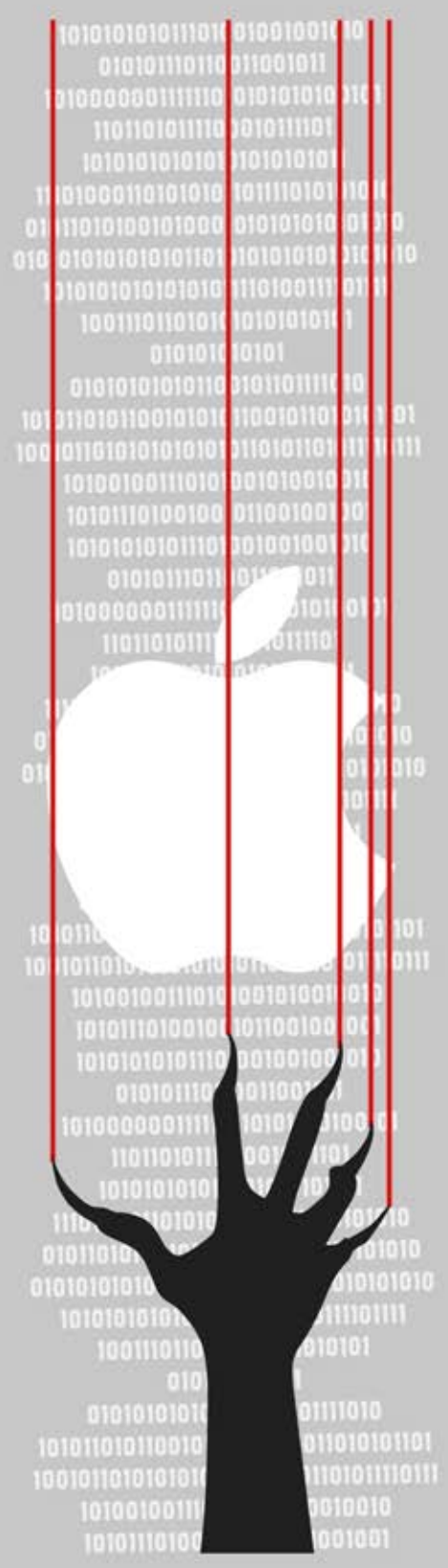
همچنین تعداد بسیار زیادی برنامه‌های ناخواسته تحت این سیستم عامل با عناوین فریبنده‌ای همچون Advanced Mac Cleaner، MacKeeper و TuneUpMyMac شناسایی شد که انتظار می‌رود روند صعودی آن در سال ۹۷ نیز ادامه داشته باشد.

در سال ۲۰۱۷، بدافزارهای بدافزارهای FkCodec، VSearch و Keygen بترتیب با ٤٦٪، ٤٤٪ و ٦٪ بیشترین سهم از آلودگی‌های سیستم عامل Mac را داشتند.



در همین دوره، MacKeeper با ٤٦ درصد، Genieo با ۲۸ درصد و SpiGot با ۸ درصد بیشترین سهم از برنامه‌های بالقوه ناخواسته را به خود اختصاص دادند.

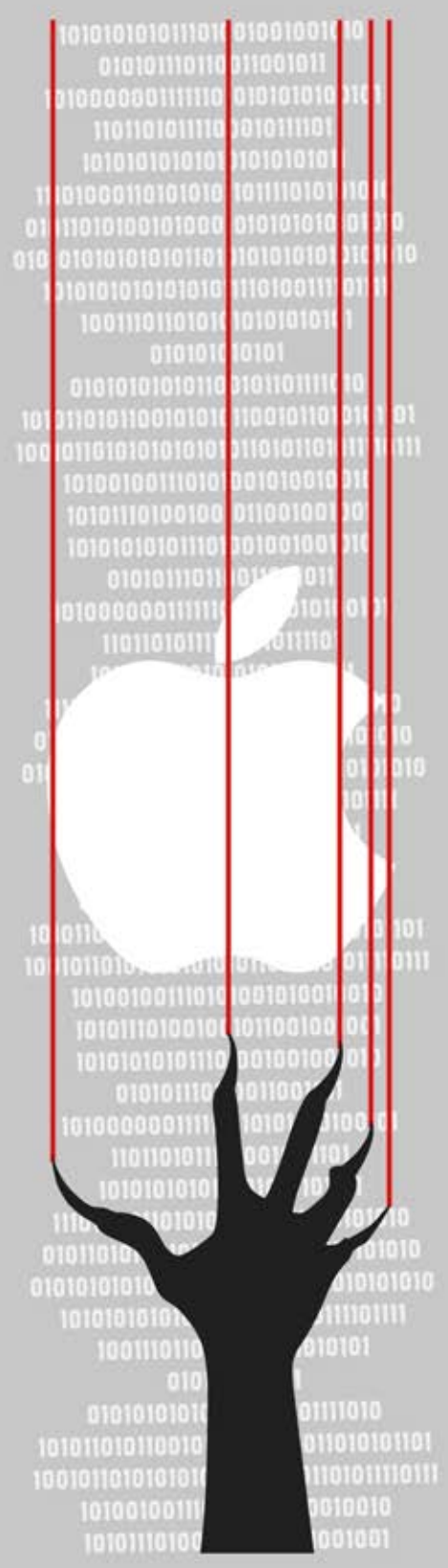


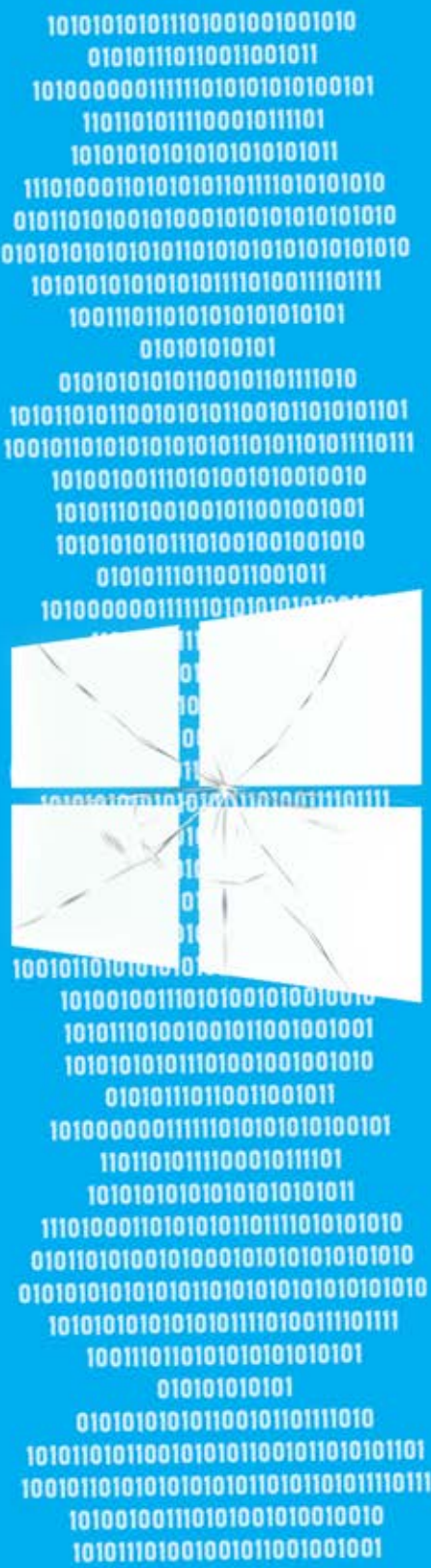


همانطور که در تصویر بالا نشان داده شده است بیشترین تهدیدات Mac در آمریکا و اروپا گزارش شده است.

راه‌های پیشگیری و مقابله

- از ضدویروس قدرتمند و به‌روز استفاده شود.
- از نصب فوری آخرین اصلاحیه‌های امنیتی اطمینان حاصل شود.

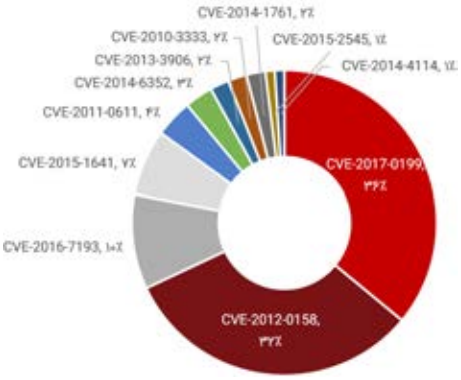




تهـدیـدات
Windows

هر چند روند تهدیدات سیستم عامل پراستفاده Windows در سال ۹۶ تغییرات چندانی با سال‌های پیش از آن نداشت اما بهره‌جویی هر چه بیشتر مهاجمان از ضعف‌های امنیتی مجموعه نرم‌افزاری Microsoft Office جلب توجه می‌کند.

در سال ۲۰۱۷، برای نخستین بار طی نیم دهه گذشته، CVE-2012-0158 جایگاه آسیب‌پذیری با بیشترین بهره‌جو را از دست داد. این آسیب‌پذیری بیش از پنج سال است که در اصلاحیه MS12-027 توسط مایکروسافت ترمیم شده است. اما با توجه به نصب نبودن این اصلاحیه بر روی بسیاری از سیستم‌ها بطور مستمر مورد بهره جویی مهاجمان قرار گرفته است.



در عوض، در سال ۲۰۱۷، آسیب‌پذیری CVE-2017-0199 با ۳۶ درصد، بیشترین سهم از موارد بهره‌جویی را کسب کرد. سوءاستفاده از این آسیب‌پذیری مهاجم را قادر می‌سازد تا کد مخرب مورد نظر خود را از راه دور و از طریق یک فایل دستکاری شده Word بر روی دستگاه قربانی به اجرا در آورد. لازمه اجرای موفقیت‌آمیز این بهره‌جو باز شدن فایل Word دستکاری شده توسط قربانی است که کار چندان دشواری نیست. تنها کافی است که فایل مخرب با نامی جذاب به یک ایمیل با عنوان و محتوای فریبنده پیوست شده و به قربانی ارسال شود.

این آسیب‌پذیری بطور گسترده در حملات هدفمند مورد بهره‌جویی قرار گرفته که در برخی حملات از تکنیک‌هایی همچون فرار از سد محصولات ضدویروس استفاده شده است. همچنین افزوده شدن آن در بسته‌های بهره‌جو (Exploit Kit) رایگان نشانه‌ای از افزایش بکارگیری آن توسط مهاجمان و تبهکاران سایبری است.

انتظار می‌رود در سال ۹۷ تعداد بهره‌جوهای عرضه شده در وب تاریک افزایش یابد. بطور معمول، یک ماه پس از فاش شدن هر آسیب‌پذیری، بهره‌جوی آن نیز در دسترس قرار می‌گیرد.

در سالی که گذشت علاوه بر سوءاستفاده از قابلیت ماکرو (Macro) در Microsoft Office از چندین امکان و قابلیت دیگر این مجموعه نرم‌افزاری بهره‌جویی شد.

برای مثال، در مهر ماه مشخص شد که برخی از مهاجمان سایبری موفق به کشف راهی برای رخنه به دستگاه‌ها شده‌اند که در آن با سوءاستفاده از قابلیت مجاز Dynamic Data Exchange - به اختصار DDE - در مجموعه Office، فایل مخرب دریافت شده و بر روی دستگاه به اجرا در می‌آید.

انتظار می‌رود بسیاری از نویسندگان و گردانندگان بدافزارها نیز به سوءاستفاده از قابلیت DDE رو آورند.

راه‌های پیشگیری و مقابله

- از ضدویروس قدرتمند و به‌روز استفاده شود.
- از نرم‌افزارها و ابزارهای نفوذیاب استفاده شود.
- از نصب فوری آخرین اصلاحیه‌های امنیتی اطمینان حاصل شود.
- نسبت به پیکربندی صحیح تنظیمات بخش DDE در مجموعه نرم‌افزاری Office اقدام شود.
- تنظیمات امنیتی ماکرو بنحو مناسب پیکربندی شود.
- ایمیل‌های دارای پیوست ماکرو در درگاه شبکه مسدود شود. بدین منظور می‌توان از تجهیزات دیواره آتش پیشرفته بهره گرفت.
- سطح دسترسی کاربران محدود شود.

نتیجه‌گیری

پیش‌بینی تحقق رویدادها در آینده با دقتی ۱۰۰ درصد امری غیرممکن است؛ بخصوص در حوزه امنیت فناوری اطلاعات که روند آن دائماً در حال تغییر و تحول است. در این گزارش تلاش شد تا با بررسی تهدیدات سایبری سال ۹۶ با آمادگی بیشتری به استقبال سال ۹۷ رویم. علاو بر راهکارهای اشاره شده در گزارش، آموزش و آگاهی‌رسانی به کاربران نیز از جمله مؤثرترین اقدامات در مقابله با بدافزارها و حملات سایبری است که مدیران امنیت سازمان ها می‌بایست همواره به آن توجه خاص داشته باشد.

منـــابـع

SophosLabs 2018 Malware Forecast

https://www.sophos.com/en-us/en-us/medialibrary/PDFs/technical-papers/malware-forecast-2018.pdf?la=en

بررسی و تحلیل باج‌افزار WannaCry

https://newsroom.shabakeh.net/18625/wannacry-analysis.html

بررسی و تحلیل باج‌افزار Petya

https://newsroom.shabakeh.net/18681/petya-analysis.html

HC۷: اولین باج‌افزار پذیرنده اتریوم

https://newsroom.shabakeh.net/19376/hc7-is-first-of-its-kind-ransomware-to-accept-ethereum-payments.html

Spora؛ باج‌افزاری با خدمات پس از آلودگی عالی!

https://newsroom.shabakeh.net/18295/spora-with-excellent-customer-service.html

کاربران ایرانی هدف یک باج‌افزار فارسی

https://newsroom.shabakeh.net/19143/tyrant.html

باز هم یک باج‌افزار فارسی دیگر

https://newsroom.shabakeh.net/19238/wannasmile-targeting-iranian-users.html

پرداخت باج ۵۵ هزار دلاری، با وجود داشتن نسخه پشتیبان!

https://newsroom.shabakeh.net/19390/hospital-pays-55k-ransomware-despite-having-backups.html

گسترش روزافزون برنامه‌های ناخواسته استخراج‌کننده

https://newsroom.shabakeh.net/19185/coinhive-miners.html

راهنمای شناسایی اسکریپت‌های استخراج‌کننده در مرورگر Chrome

https://newsroom.shabakeh.net/19485/google-chrome-task-manager.html

برنامکی که از طریق Telegram Bot از کاربران ایرانی جاسوسی می‌کند

https://newsroom.shabakeh.net/18747/telegram-bot-spyware.html

باج‌افزاری تحت Android، با توانایی‌های مخرب

https://newsroom.shabakeh.net/19133/doublelokcer.html

حذف بیش از ۷۰۰ هزار برنامک مخرب از Play Store در سال ۲۰۱۷

https://newsroom.shabakeh.net/19426/google-removed-over-700-000-android-apps-from-the-play-store.html

پیکربندی تنظیمات امنیتی ماکرو

https://newsroom.shabakeh.net/19265/securing-office-macros.html

حملات از طریق پودمان DDE

https://newsroom.shabakeh.net/19222/dde-attacks.html


شبکه گستر
shabakeh.net
my.shabakeh.net
events.shabakeh.net
newsroom.shabakeh.net