شبکه گستر

فصلنامه شرکت مهندسی شبکه گستر

امنیت فناوری اطلاعات

سه ماهه اول سال ۱۳۹۶ / انتشار : مرداد ماه ۱۳۹۶

در این شماره می خوانید

Sorebrect؛ باج‌افزاری بدون فایل!

GPAA؛ باج‌افزاری برای نجات کودکان؟!

پرداخت باج یک میلیون دلاری توسط شرکت کره‌ای

جعل نشانی دامنه؛ روش شناسایی: تقریباً غیرممکن!

Industroyer؛ مخرب‌ترین بدافزار صنعتی پس از Stuxnet

کشف آسیب‌پذیری ۱۰ ساله در سیستم‌های عامل مبتنی بر Unix

شبکه گستر

در چهارمین فصلنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر، بدافزارهای جدید، حملات بااهیمت سایبری، گزارش‌های امنیتی و آمار تهدیدات سایبری در سه ماهه اول ۱۳۹۶ مورد بررسی قرار گرفته است.

در اردیبهشت امسال، انتشار باج افزار WannaCry با بهره‌جویی از یک آسیب‌پذیری شناخته شده در بخش SMB سیستم عامل Windows و آلودگی بیش از سیصدهزار دستگاه در ۲۰۰ کشور جهان به آن یکبار دیگر توجه کارشناسان صنعت فناوری اطلاعات را به خطر باج‌افزارها جلب کرد. در این شماره علاوه بر مرور این باج‌افزار، چندین باج‌افزار دیگر از جمله Sorebrect، GPAA، BitKangoroo، FrozrLock و Karmen که با عملکرد خاص خود کاربران را در فصل بهار هدف قرار دادند مورد بررسی قرار گرفته است.

یکی از اخبار قابل توجه در این دوره پرداخت باج یک میلیون دلاری توسط یک شرکت کره‌ای ارائه‌دهنده خدمات میزبانی وب در ازای بازگردانی فایل‌های رمز شده بر روی ۱۵۳ سرور با سیستم عامل لینوکس این شرکت بود که مشروح آن را می توانید در این شماره مطالعه کنید.

همچنین در خرداد ماه محققان امنیتی پرده از بدافزار مخربی با عنوان Industroyer برداشتند که هدف آن وارد ساختن آسیب قابل توجه به مراکز توزیع‌کننده برق معرفی شده است. این محققان، Industroyer را مخرب‌ترین بدافزار صنعتی پس از Stuxnet توصیف کرده‌اند که جزییات آن را در این شماره و در گزارش اختصاصی آن خواهید خواند.

بر اساس آمار ارائه شده، ۵۳ درصد دستگاه‌ها در سازمان‌ها از نسخه‌های آسیب‌پذیر نرم‌افزار Flash استفاده می‌کنند؛ این در حالی است که در سال گذشته میلادی این سهم ۴۲ درصد بوده است. این گزارش و گزارش‌های امنیتی دیگر را در این شماره مطالعه کنید.

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات 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 ٤

McAfee، دوباره McAfee شد ٥

حمله‌ای هوشمندانه که ظرف یک ساعت بی‌اثر شد! ٥

پرداخت باج یک میلیون دلاری توسط شرکت کره‌ای ٦

شناسایی حدود ۹ هزار سرور فرماندهی تبهکاران سایبری ٦

ساخت مخفیانه کامپیوتر توسط دو زندانی! ٧

ابزارهای نفوذ CIA، استفاده شده در حداقل ٤٠ حمله سایبری ٧

بدافزارها ٨

Sorebrect؛ باج‌افزاری بدون فایل! ٨

GPAA: باج‌افزاری برای نجات کودکان؟! ٩

WannaCry؛ تهاجمی‌ترین باج‌افزار تاریخ ١١

بدافزاری که با استفاده از چراغ‌های روتر، داده‌ها را سرقت می‌کند! ١١

این فایل PowerPoint، بدون ماکرو، بدافزار دانلود می‌کند! ١٢

BitKangoroo، در صورت عدم پرداخت باج، فایل‌ها را حذف می‌کند! ١٤

FrozrLock، نمونه‌ای جدید از باج‌افزار به‌عنوان سرویس ١٥

عرضه باج‌افزار Karmen RaaS در بازارهای سیاه نفوذگران ١٦

سایر تهدیدات ١٨

جعل نشانی دامنه؛ روش شناسایی: تقریباً غیرممکن! ١٨

گزارش‌ها ٢٠

Bitdefender، سپر دفاعی مؤثر در برابر WannaCry ٢١

Industroyer؛ مخرب‌ترین بدافزار صنعتی پس از Stuxnet ٢٢

استفاده ١٥ درصد کاربران IoT از گذرواژه پیش‌فرض ٢٢

استفاده از نرم‌افزارهای آسیب‌پذیر؛ معضلی جهانی ٢٣

نحوه راه رفتن، روشی مطمئن برای اصالت‌سنجی ٢٤

رونمایی Google از فناوری رفتارشناسی Play Protect ٢٦

تغییرات ضدباج‌افزاری در Android O ٢٨

پیشی گرفتن Android از Windows ٢٩

Pixel Tracking چیست؟ ٣٠

کشف آسیب‌پذیری ١٠ ساله در سیستم‌های عامل مبتنی بر Unix ٣١

آمار تهدیدات ٣٢

اخبار

McAfee،
دوباره McAfee شد

شرکت McAfee که نامی آشنا در صنعت امنیت فناوری اطلاعات است و در نزدیک به سه دهه امنیت بسیاری از کاربران و سازمان‌ها را تأمین کرده است اکنون با نشان، شعار و رویکردی جدید فعالیت خود را ادامه می‌دهد.

این شرکت در سال ۱۹۸۷ توسط بنیانگذار آن، John McAfee، تاسیس شد. بعدها، وی سهام خود را بطور کامل فروخت و از شرکت کناره‌گیری کرد. ولی نام McAfee همچنان با شرکت باقی ماند. البته برای مدت کوتاهی از اواخر دهه ۱۹۹۰ میلادی تا سال ۲۰۰۴، نام شرکت به Network Associates تغییر یافت ولی دوباره با تصمیم مدیران شرکت، نام McAfee انتخاب شد.

در سال ۲۰۱۰، شرکت Intel با پرداخت ۷/۷ میلیارد دلار، شرکت McAfee را بطور کامل خرید و در اختیار گرفت. در پی آن شرکت McAfee با حفظ ساختار، بعنوان یک شرکت تابعه متعلق به Intel تحت مجموعه بزرگ Intel Security به فعالیت خود ادامه داد.

در اواخر سال ۲۰۱۶ شرکت سرمایه گذاری TPG Capital اقدام به خرید ۵۱ درصد از سهام Intel Security از شرکت Intel نمود.

از ۱۴ فروردین ماه، این شرکت فعالیت رسمی خود را با منابع و سرمایه‌ای بیشتر اما به‌صورت مستقل از دو شرکت صاحب سهام خود – Intel و TPG Capital – با همان نام قدیمی McAfee و با شعار جدید "قدرت در با همدیگر بودن است" آغاز کرد.

Christopher Young، مدیر عامل اجرایی شرکت جدید، در نامه‌ای گفته:

به‌عنوان یک شرکت مستقل با یک هدف شفاف، McAfee چالاکی بیشتری در متحد و یکپارچه کردن مردم، فناوری و سازمان‌ها در نبرد با دشمنان مشترک و اطمینان از امن بودن آینده مبتنی بر فناوری خواهد داشت.

همچنین این شرکت اعلام کرده منابع و سرمایه‌های بیشتری را صرف تحقیقات در خصوص تهدیدات سایبری خواهد کرد. تمرکز اصلی این شرکت بر روی بدافزارهای پیشرفته، باج‌افزارها، کلاهبرداری‌های مالی، جرایم سایبری عمومی، جاسوسی سایبری، جنگ‌های سایبری و دست‌درازی به سیستم‌های کنترل صنعتی خواهد بود.

ضمن اینکه McAfee از مشارکت بیشتر با نهادهای قانونی و علمی به‌خصوص در زمینه انهدام شبکه‌ها و سرورهای تبهکاران سایبری خبر داده است.

یکی از اقدامات اخیر شرکت McAfee راه‌اندازی پورتال Threat Landscape Dashboard است که جدیدترین تهدیدات، بسته‌های بهره‌جو (Exploit Kit)، کارزارهای تبهکاران سایبری، باج‌افزارها و آسیب‌پذیری‌ها در آن ارائه و معرفی می‌شوند.

McAfee با بیش از ۷ هزار متخصص و اختراع ۱۲۰۰ فناوری ثبت شده یکی از بزرگترین و اصلی‌ترین تأمین‌کنندگان امنیت نقاط پایانی در جهان محسوب می‌شود.

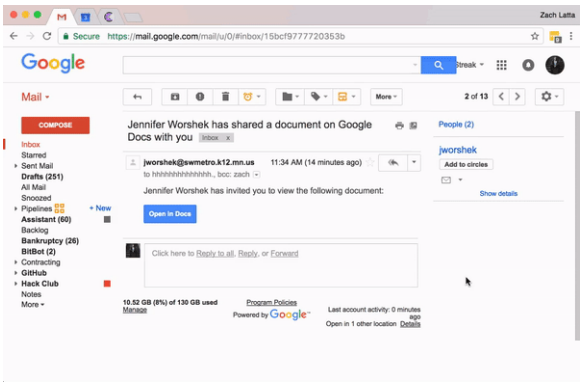
در حال حاضر، ۸۷ درصد از یکصد شرکت برتر آمریکا (موسوم به Fortune 100) از محصولات شرکت McAfee برای حفاظت سیستم‌های خود استفاده می‌کنند.

حمله‌ای هوشمندانه
که ظرف یک ساعت بی‌اثر شد!

یک حمله هوشمندانه فیشینگ در ۱۳ اردیبهشت که به‌سرعت در حال گسترش بود، به‌محض اطلاع یکی از کارشناسان شرکت گوگل، ظرف کمتر یک ساعت بی‌اثر شد.

بر اساس اطلاعات جمع‌آوری شده از منابع مختلف، اهداف اولیه این حمله، روزنامه‌نگاران، کسب‌وکارها و دانشگاه‌ها بوده‌اند. اما در مدتی بسیار کوتاه، تعداد فراوانی از کاربران دیگر نیز هدف قرار گرفتند.

گردانندگان این حمله، روش اجرا را به‌صورت هوشمندانه‌ای طراحی کرده بودند. قربانی ایمیلی حقیقی – و نه جعلی – را از یکی از دوستانش دریافت می‌کند؛ در ایمیل از کاربر خواسته می‌شود تا بر روی دگمه‌ای با عنوان Open in Docs به‌منظور دسترسی به یک سند Google Docs کلیک کند.



به گزارش شرکت مهندسی شبکه گستر، در صورتی که کاربر بر روی دگمه مذکور کلیک می‌کرد به یک صفحه واقعی انتخاب حساب کاربری گوگل هدایت می‌شد که در آن یک برنامه جعلی – و نه حقیقی – با عنوان Google Docs از کاربر درخواست دریافت مجوز دسترسی یافتن به اسناد به اشتراک گذاشته شده را می‌کرد. در حقیقت با این کار، برنامه جعلی به محتوای بخش Inbox ایمیل و فهرست Contact قربانی دست پیدا می‌کرد.

پس از دریافت مجوز دسترسی به این جزییات، برنامه جعلی فهرست Contactکاربر را کپی کرده و نسخه‌ای از خود را – از سمت ایمیل قربانی – به افراد موجود در فهرست ارسال می‌کرد. در بخش To این ایمیل‌ها نشانی hhhhhhhhhhhhhhhh@mailinator.com درج شده بود و ایمیل اهداف جدید در بخش BCC درج می‌شدند.

بدیهی است که با بهره‌گیری از این روش خاص و حرفه‌ای خودانتشاری، هر لحظه بر تعداد قربانیان افزوده می‌شد. چنین حملاتی یادآور انتشار کرم Samy در بستر MySpace در حدود یک دهه قبل هستند.

خوشبختانه، گزارش این حمله در یکی از تالارهای گفتگوی اینترنتی و اطلاع یک کارشناسان گوگل از این موضوع سبب گردید تا موضوع به‌سرعت به افراد مرتبط در این شرکت ارجاع داده شده و پس از گذشت یک ساعت از اولین گزارش آلودگی برنامه مخرب مسدود شود.

پس از گذشت چند ساعت و با انجام بررسی‌های بیشتر کارشناسان گوگل، اطلاعیه زیر صادر شد:

ما اقداماتی را برای حفاظت از کاربران در برابر ایمیل‌هایی که Google Docsرا جعل می‌کنند در نظر گرفته و حساب‌های کاربری خاطی را غیرفعال کرده‌ایم. ما صفحات جعلی را حذف کرده و به‌روز رسانی مربوطه را از طریق قابلیت Safe Browsing منتشر کرده‌ایم. ضمن اینکه یکی از تیم‌های ما در حال یافتن راهکاری به‌منظور جلوگیری از تکرار وقوع این اتفاقات است. به کاربران توصیه می‌کنیم که ایمیل‌های فیشینگ را از طریق Gmail اعلام کنند.

خبر خوش اینکه، هیچ یک از منابع، گزارشی از توزیع بدافزار در جریان این حمله منتشر نکرده‌اند. کاربرانی که بر روی دگمه Open in Docs کلیک کرده‌اند می‌توانند با مراجعه به https://myaccount.google.com/permissions دسترسی یافتن این برنامه مخرب به حساب کاربریشان را بررسی کنند. Google Docs واقعی در این بخش قرار ندارد؛ چرا که به‌عنوان یکی از برنامه‌های مجاز نیازی به دریافت چنین مجوزی از کاربر ندارد.

پرداخت باج یک میلیون دلاری توسط شرکت کره‌ای

به گزارش شرکت مهندسی شبکه گستر، Nayana، شرکت ارائه‌دهنده خدمات میزبانی وب که دفتر مرکزی آن در کره جنوبی قرار دارد اعلام کرده که در پی آلودگی سرورهایش به باج‌افزار، در حال پرداخت مبلغ ۱ میلیون دلار به باج‌گیران در ازای بازگردانی فایل‌های رمز شده است.

به نظر می‌رسد که این شرکت در ۲۰ خرداد ماه متوجه آلودگی سرورها به باج‌افزار شده باشد. دو روز پس از تاریخ مذکور این شرکت وقوع این اتفاق را بر روی سایت خود گزارش کرد.

مهاجمان این باج‌افزار، در ابتدا، مبلغ ۵۵۰ بیت‌کوین، معادل ۱٫۶۲ میلیون دلار اخاذی کرده بودند. اما ظاهراً پس از دو روز مذاکره با آنها، Nayana موفق به کاهش مبلغ باج به ۱ میلیون دلار و قسط‌بندی پرداخت آن در سه مرحله شده است!

روز شنبه، ۲۷ خرداد ماه، این شرکت از پرداخت دو قسط از باج ۱ میلیون دلاری خبر داد. همچنین این شرکت اعلام کرد که فرآیند رمزگشایی فایل‌ها با توجه به حجم بالای آنها ممکن است تا ۱۰ روز به طول بینجامد.

بر اساس توضیحات Nayana در جریان این حمله در مجموع ۱۵۳ سرور با سیستم عامل Linux که حاوی اطلاعات بیش از ۳،۴۰۰ مشتری این شرکت هستند به باج‌افزاری با نام Erebus آلوده شده‌اند.

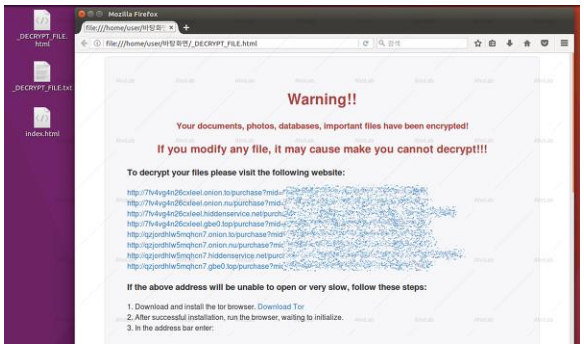
در سال گذشته نیز باج‌افزاری با همین نام دستگاه های با سیستم عامل Windows را هدف قرار داده بود. حال آنکه نمونه شناسایی شده بر روی سرورهای Nayana تنها کامپیوترهای با سیستم عامل Linux را هدف قرار می‌دهد.

هنوز مشخص نیست که هر دو نسخه این باج‌افزارها توسط یک فرد یا گروه نوشته شده باشد.

باج‌افزار Erebus از فایل‌های ذخیره شده در پوشه‌های با هر یک از نام‌های زیر صرف‌نظر می‌کند.

/bin, /boot, /dev, /etc, /lib, /lib64, /proc, /run, /sbin, /srv, /sys, /tmp, /usr, /var, /.gem, /.bundle, /.nvm, /.npm

به‌محض پایان رمزنگاری، دو اطلاعیه باج‌گیری با نام‌های _DECRYPT_FILE.html_و _DECRYPT_FILE.txt بر روی دسکتاپ کاربر کپی می‌شوند.



گفته می‌شود استفاده Nayana از نسخه‌های قدیمی و آسیب‌پذیر Linux، Apache و PHP، افراد پشت پرده این باج‌افزار را قادر به آلوده نمودن این سرورها کرده است.

شناسایی حدود ۹ هزار سرور فرماندهی تبهکاران سایبری

به گزارش شرکت مهندسی شبکه گستر، ۴ اردیبهشت ماه، اینترپل از شناسایی بیش از ۸،۸۰۰ سرور فرماندهی موسوم به Command & Control در ۸ کشور در جنوب شرق آسیا خبر داد که مهاجمان سایبری از آنها برای توزیع باج‌افزار، اجرای حملات از کاراندازی سرویس (DoS) و انتشار هرزنامه (Spam) بهره می‌برده‌اند.

چین، اندونزی، مالزی، میانمار، فیلیپین، سنگاپور، تایلند و ویتنام این ۸ کشور را تشکیل می‌دهند.

اینترپل داده‌های جمع‌آوری شده را در اختیار نهادهای قانونی این کشورها قرار داده است. انتظار می‌رود به زودی این سرورها منهدم شده و گردانندگان آنها در چنگال قانون گرفتار شوند. در صورت توقف این سرورها باید شاهد کاهش تعداد باج‌افزارها و هرزنامه‌ها طی روزها و هفته‌های آتی باشیم.

در شناسایی این سرورها چندین شرکت و مؤسسه خصوصی نیز نقش داشته‌اند.

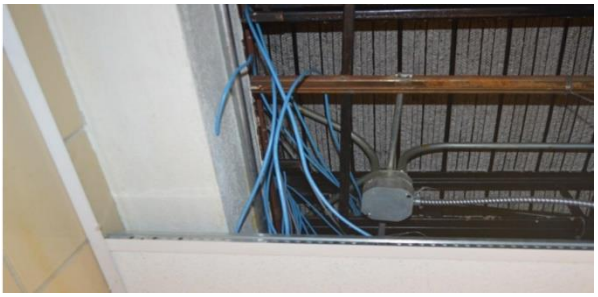
یکی از نکات قابل توجهی که اینترپل به آن اشاره کرده وجود صدها سایت دولتی است که بر اثر وجود آسیب‌پذیری و ضعف امنیتی در آنها مورد بهره‌جویی مهاجمان سایبری قرار گرفته‌اند.

به گزارش شرکت مهندسی شبکه گستر، مدتی پیش هم یوروپل از دستگیری سه فرد در اسپانیا و دو نفر در انگلیس خبر داده بود. این افراد مظنون به ساخت و توزیع بدافزارهایی از نوع Keylogger و Remote Access Trojan هستند.

سازمان جرایم ملی انگلیس (UK National Crime Agency) نیز در گزارشی ۱۷ صفحه‌ای با عنوان "Pathways Into Cyber Crime" منتشر به انگیزه نوجوانان در ورود به دنیای تبهکاران سایبری پرداخته است. یافته‌های این گزارش نشان می‌دهد که انگیزه اصلی بسیاری از این افراد نه مسائل مالی که کسب شهرت و احترام در دنیای مجرمان سایبری است.

ساخت مخفیانه کامپیوتر توسط دو زندانی!

به گزارش شرکت مهندسی شبکه گستر، دو زندانی در اوهایوی آمریکا با استفاده از زباله‌های الکترونیکی اقدام به ساخت کامپیوتر کرده و از طریق شبکه زندان به اینترنت متصل شدند!



هر چند این ماجرا به سال ۲۰۱۵ باز می‌گردد اما جزییات آن را دفتر بازرسی کل اوهایو بدنبال یک بررسی تقریباً یک ساله در گزارشی ۵۰ صفحه‌ای در فروردین ماه منتشر کرد.

بر اساس این گزارش این دو زندانی با مشارکت چند زندانی دیگر قطعات الکترونیکی مورد نیاز برای ساخت کامپیوتر را از یک کارگاه بازیافت زباله‌های الکترونیکی به‌صورت مخفیانه جمع‌آوری می کرده بودند.

آنها پس از ساخت دو کامپیوتر از طریق زباله‌های الکترونیکی جمع‌آوری شده، دستگاه‌ها را در سقف یک اتاق آموزشی مخفی کرده و سپس با اتصال به شبکه زندان به اینترنت متصل شده بودند.

این افراد به‌محض برخط شدن از مهارتشان برای نقض قانون استفاده کرده بودند. آنها به سوابق داخلی زندانیان دست یافته و اقدام به ایجاد مجوز عبور برای دسترسی به بخش‌های محدود شده که تردد در آنها تنها برای زندانیان دارای مجوز ممکن بوده کردند. همچنین با سوءاستفاده از مشخصات یکی از زندانیان درخواست صدور کارت اعتباری داده بودند.

ضمن اینکه به سایت‌هایی نظیر سایت‌های متعلق به سازندگان و توزیع‌کنندگان مواد مخدر، سلاح و مواد منفجره نیز مراجعه کرده بودند.

به گزارش شرکت مهندسی شبکه گستر، این برنامه مخفیانه زمانی لو می‌رود که کارمند فناوری زندان متوجه ترافیک بالای اینترنت با حساب کاربری پیمانکاری که در آن زمان حضور نداشته شده می‌شود.

در نهایت پنج زندانی در ارتباط با این نقشه شناسایی شدند. هر پنج زندانی از یکدیگر جدا شده و به زندان‌های دیگری منتقل شده‌اند.

ابزارهای نفوذ CIA، استفاده شده در حداقل ۴۰ حمله سایبری

گزارشی که در فروردین ماه شرکت Symantec آن را منتشر کرد نشان می‌دهد ابزارهای نفوذ CIA (سازمان اطلاعات مرکزی آمریکا) که جزییات آنها توسط WikiLeaks منتشر شده در حملات سایبری به سازمان‌ها در کشورهای مختلف که برخی از آنها از متحدان آمریکا هستند مورد استفاده قرار گرفته بوده.

به گزارش شرکت مهندسی شبکه گستر، فایل‌های فاش شده توسط WikiLeaks ابزارهایی برای نفوذ به گوشی‌های هوشمند، کامپیوترها و سایر ابزارهای الکترونیکی هستند که در برخی موارد کدهای برنامه‌نویسی را نیز شامل می‌شوند.

شرکت ضدویروس Symantec اعلام کرده که حداقل ۴۰ حمله به ۱۶ کشور در اروپا، خاورمیانه، آسیا و آفریقا توسط این ابزارها صورت گرفته است. تا پیش از درز فایل‌های CIA اجرای این حملات به گروهی موسوم به Longhorn نسبت داده می‌شد.

به گفته Symantec، سازمان‌های هدف قرار گرفته شده در این حملات در بخش‌های مالی، مخابرات و ارتباطات، انرژی، هوافضا، فناوری اطلاعات، آموزش و منابع طبیعی فعال بوده‌اند.

هدف این حملات ایجاد درب‌پشتی بر روی دستگاه و جمع‌آوری اطلاعات – و نه نابود کردن آنها – اعلام شده است.

همچنین یک مورد آلودگی نیز در آمریکا مشاهده شده بوده که ظرف چند ساعت پاکسازی آن صورت پذیرفته بوده. احتمالاً این دستگاه به‌صورت تصادفی و ناخواسته مورد آلودگی قرار گرفته بوده.

به گزارش شرکت مهندسی شبکه گستر به نقل از خبرگزاری Reuters، هر چند، CIA صحت فایل فاش شده را تایید نکرده اما سخنگوی این سازمان اعلام کرده هر درز اطلاعات صورت گرفته توسط WikiLeaks نه تنها کارکنان و عملیات‌های آمریکایی را به خطر می اندازد که دشمنان این کشور را نیز به ابزارها و اطلاعات مجهز می‌کند.

شهرت CIA به سبب جاسوسان انسانی آن و نه اجرای عملیات‌های سایبری است. اما به نظر می‌رسد سالهاست که این سازمان جاسوسی نیز متکی به ابزارهای هک و نفوذ شده است

.

بـدافـزارهـا

Sorebrect؛
باج‌افزاری بدون فایل!

به گزارش شرکت مهندسی شبکه گستر، محققان شرکت Trend Micro باج‌افزار پیشرفته‌ای با ویژگی Fileless (بدون فایل) شناسایی کرده‌اند که در بستر شبکه منتشر شده و پس از دسترسی یافتن از راه دور به دستگاه قربانی، کد مخرب خود را در یکی پروسه‌های سیستمی تزریق می‌کند. این باج‌افزار پس از پایان خرابکاری، با هدف پاکسازی ردپای خود، از روی سیستم حذف می‌شود.

بر اساس بررسی‌های انجام شده، این باج‌افزار که Sorebrect نامگذاری شده بر خلاف باج‌افزارهای رایج هر دو سیستم‌های سرور و ایستگاه کاری را هدف قرار می‌دهد.

Sorebrect در اولین مرحله با اجرای حملات سعی و خطا (Brute Force) و برخی روش‌های دیگر می‌کوشد تا با حق دسترسی Administrator به دستگاه قربانی متصل شود. در ادامه با بهره‌گیری از ابزار مجاز Sysinternals PsExec – که امکان اجرای از راه دور کد را فراهم می‌کند – کد مخرب خود را در یکی از پروسه‌های سیستمی نظیر svchost.exe تزریق کرده و فایل‌های بر روی دستگاه و فایل‌های ذخیره شده در پوشه‌های اشتراکی متصل شده به آن را که کاربر هک شده به آنها دسترسی نوشتن دارد رمزگذاری می‌کند.

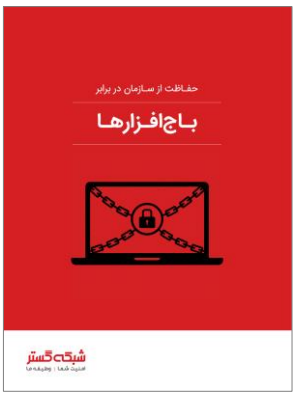
این باج‌افزار به فایل‌های رمزگذاری شده پسوند pr0tect. را الصاق می‌کند.

از دیگر اقدامات انجام شده توسط این باج‌افزار، حذف سوابق Event Logs و نسخه‌های Shadow Copy بترتیب با استفاده از پروسه‌های wevtutil.exe و vssadmin است.

Sorebrect با استفاده از شبکه مخرب Tor ارتباطات خود را با سرورهای فرماندهی مخفی می‌کند.

هر چند نخستین آلودگی‌ها به Sorebrect در منطقه خاورمیانه گزارش شده اما به نظر می‌رسد که آلودگی به این باج‌افزار به سرعت در نقاط دیگر جهان در حال گسترش است.

لازم به ذکر است، یکی از تکنیک‌های مورد استفاده بدافزارهای پیشرفته، استفاده از روشی موسوم به Fileless است. هدف، ماندگار کردن کد مخرب بدافزار بدون ذخیره آن به‌صورت فایل بر روی دیسک سخت است. با توجه به اینکه نرم‌افزارهای ضدویروس سنتی صرفاً اقدام به بررسی فایل‌ها در زمان نوشته شدن بر روی دیسک سخت و خوانده شدن از روی آن می‌کنند این روش می‌تواند براحتی این سد دفاعی را در هم بشکند. جزییات بیشتر در خصوص بدافزارهای Fileless در اینجا قابل دریافت و مطالعه است.



برای دریافت گزارش حفاظت از سازمان در برابر باج‌افزارها اینجا کلیک کنید.

GPAA:
باج‌افزاری برای نجات کودکان؟!

به گزارش شرکت مهندسی شبکه گستر، باج‌افزار جدیدی شناسایی شده که در اطلاعیه باج‌گیری (Ransom Note) آن با عنوان "Save Children" ضمن تبریک به قربانی به جهت عضویت در سازمان جهانی کمک به فقر (GPAA) گفته می‌شود که هدف از کارزار باج‌افزار جمع‌آوری ۱۰۰۰ بیت‌کوین برای نجات کودکان، با شعار هر کودک یک بیت‌کوین است.

مشخص است که هدف ویروس‌نویس یا ویروس‌نویسان این باج‌افزار فقط اخاذی بوده و از عنوان "نجات کودکان" و سازمان ساختگیGPAA صرفاً برای موفقیت بیشتر در تشویق قربانیان به پرداخت باج استفاده شده است.

با رمزگذاری فایل، نام آن تغییر یافته و عبارت cerber6. به عنوان پسوند جدید به آن الصاق می‌شود. برای مثال نام و پسوند فایل test.jpg پس از رمزگذاری به 2BiwaFbX6wlPaDSy.cerber6 تغییر می‌یابد.

بر خلاف بدافزارهای معمول، این باج‌افزار خود را در هر بار راه‌اندازی سیستم فراخوانی نکرده و فایل‌های اجرایی خود را نیز پس از پایان رمزگذاری از روی سیستم حذف می‌کند. همچنین هر پوشه ای که حداقل از فایل‌های آن رمزگذاری شده باشد فایل اطلاعیه باج‌گیری با نام !READ.htm کپی می‌شود.

بر اساس بررسی‌های انجام شده توسط یکی از محققان امنیتی، رمزگشایی رایگان فایل‌های رمزگذاری شده توسط این باج‌افزار، حداقل در حال حاضر، امکان‌پذیر نیست.

در زمستان ۹۵ نیز باج‌افزاری با نام Popcorn Time شناسایی شد که سازندگان آن ادعا می‌کردند باج دریافت شده را صرف تهیه غذا، دارو و پناهگاه برای سوری‌های آواره از جنگ خواهند کرد.

WannaCry؛
تهاجمی‌ترین باج‌افزار تاریخ

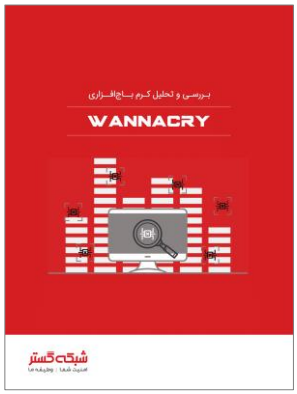
۲۲ اردیبهشت ماه، منابع متعدد از انتشار گسترده باج‌افزار جدیدی با عنوان WannaCry خبر دادند. باج‌افزاری که با خاصیت کرم گونه و با بهره‌جویی از یک ضعف امنیتی در بخش SMB سیستم عامل Windows از روی نخستین دستگاه آلوده شده، به‌سرعت خود را در سطح شبکه و اینترنت تکثیر می‌کرد.

ماجرای آسیب‌پذیری مورد استفاده WannaCry به حدود دو ماه قبل 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.

تنها در انگلیس، آلودگی تعداد زیادی از بیمارستان‌های این کشور به این باج افزار سبب تعطیلی برخی از بخش‌های این مراکز درمانی شد. در آن زمان، مرکز اصلی سلامت لندن به نام Barts Health به بیماران توصیه کرد که بیماران به مراکز درمانی دیگری مراجعه کنند. برخی دیگر از مراکز درمانی این کشور نیز مجبور به ترخیص زود هنگام بیماران و محدود کردن خدمات رادیولوژی خود شدند. حتی یکی از بیمارستان‌ها تصمیم گرفت تا بخش اورژانس خود را تعطیل کرده و فقط به موارد حیاتی رسیدگی کند.

در مدتی کوتاه، بیش از ۳۵۰ هزار دستگاه در ۲۰۰ کشور جهان به این باج‌افزار گرفتار شدند. به گزارش شرکت مهندسی شبکه گستر، در ایران نیز، تعداد قابل توجهی از سیستم‌ها به این باج‌افزار مخرب آلوده شدند.



جهت دریافت اطلاعات بیشتر در خصوص باج‌افزار WannaCry اینجا کلیک کنید.

بدافزاری که با استفاده از چراغ‌های روتر، داده‌ها را سرقت می‌کند!

مهاجم می‌تواند با ساخت یک بدافزار ویژه و نصب آن بر روی یک روتر یا سوییچ اقدام به دست‌درازی به چراغ‌های دستگاه کرده و داده‌های رد و بدل شده بر روی این تجهیزات را از شبکه قربانی – بدون نیاز به دسترسی به اینترنت – جمع‌آوری کند؛ سناریویی که توسط محققان دانشگاه بنگوریون در فلسطین اشغالی ارائه شده است.

به گزارش شرکت مهندسی شبکه گستر، این محققان بدافزاری آزمایشگاهی با نام xLED ساخته‌اند و در جریان بررسی‌هایشان، انتقال داده‌ها از روتر یا سوییچ آلوده شده را به این بدافزار، به حسگرهای نوری، دوربین‌های مداربسته، دوربین‌های گوشی‌های هوشمند، دوربین‌های پوشیدنی و سایر تجهیزات از این دست مورد آزمایش قرار داده‌اند.

یافته‌های آنها نشان می‌دهد که بهترین نتایج با حسگرهای نوری که قادر به نمونه‌برداری با نرخ بالا هستند حاصل شده است. ضمن اینکه هر چه تعداد چراغ‌های روتر یا سوییچ بیشتر باشد انتقال داده‌ها نیز با سرعت بالاتری انجام می‌شود.

مشخص است که در این سناریو، مهاجم باید قادر به رخنه به روتر یا سوییچ برای نصب بدافزار خود باشد. بدیهی است که در شرایط معمول، مهاجم می‌تواند از راه‌هایی بسیار مؤثرتر و به مراتب آسان‌تر اقدام به سرقت داده‌های رد و بدل شده بر روی این تجهیزات کند.

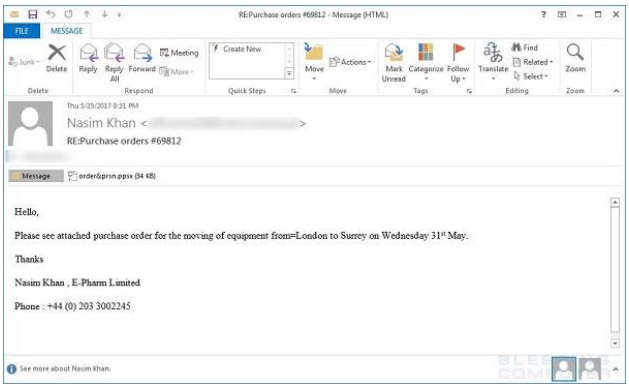
اما از سویی دیگر باید در نظر داشت در صورتی که روتر یا سوییچ قربانی در شبکه‌ای کاملاً مجزا از اینترنت قرار داشته باشد مهاجم گزینه‌های زیادی برای انتخاب نخواهد داشت.

شایان ذکر است که در طی چند سال گذشته این محققان مقالات متعددی را در خصوص سرقت داده‌ها از شبکه‌های غیر متصل به اینترنت موسوم به Air Gap ارائه کرده‌اند که به برخی از آنها در اتاق خبر شرکت مهندسی شبکه گستر نیز پرداخته شده است.

این فایل PowerPoint،
بدون ماکرو، بدافزار دانلود می‌کند!

به گزارش شرکت مهندسی شبکه گستر، محققان امنیتی نمونه فایل‌های PowerPoint مخربی را شناسایی کرده‌اند که بدون نیاز به هر گونه کد ماکرویی قادر به دریافت بدافزار از اینترنت و اجرای آن بر روی دستگاه قربانی است.

در نمونه‌های مشاهده شده روش اصلی انتشار و آلوده‌سازی هرزنامه‌ها بوده‌اند.



برخی عناوین گزارش شده از این هرزنامه‌ها به شرح زیر می‌باشد:

- RE:Purchase orders #69812
- Fwd:Confirmation

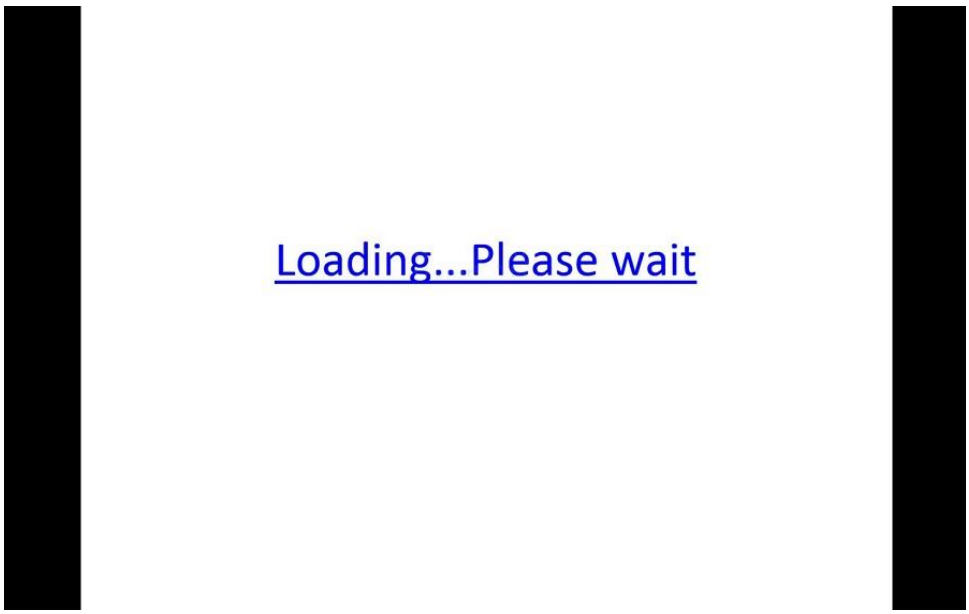
پیوست این هرزنامه‌ها نیز فایلی با یکی از نام‌های زیر بوده است:

- order&prsn.ppsx
- order.ppsx
- invoice.ppsx

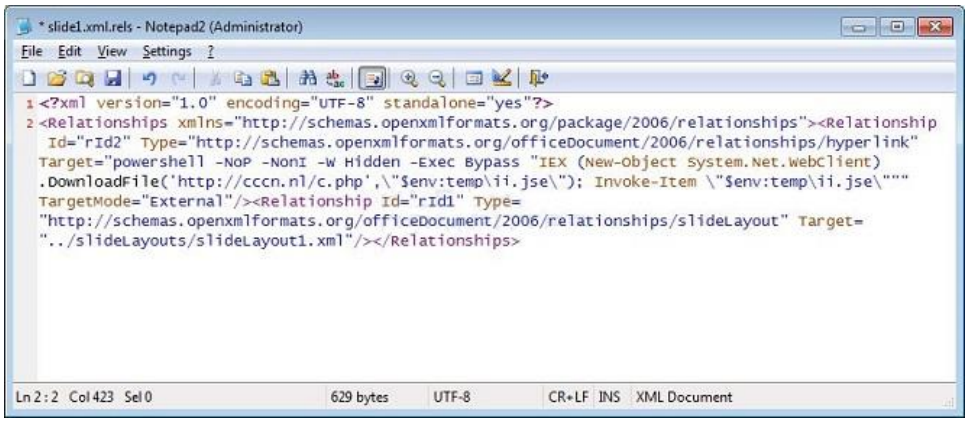
در برخی موارد نیز پیوست هرزنامه، یک فایل ZIP حاوی فایل مخرب PowerPoint با پسوند PPSX گزارش شده است.

بر خلاف فایل‌های PPTX که در حالت قابل ویرایش (Edit Mode) در نرم‌افزار PowerPoint باز می‌شوند، فایل‌های PPSX در نمای ارائه (Presentation Mode)اجرا می‌شوند.

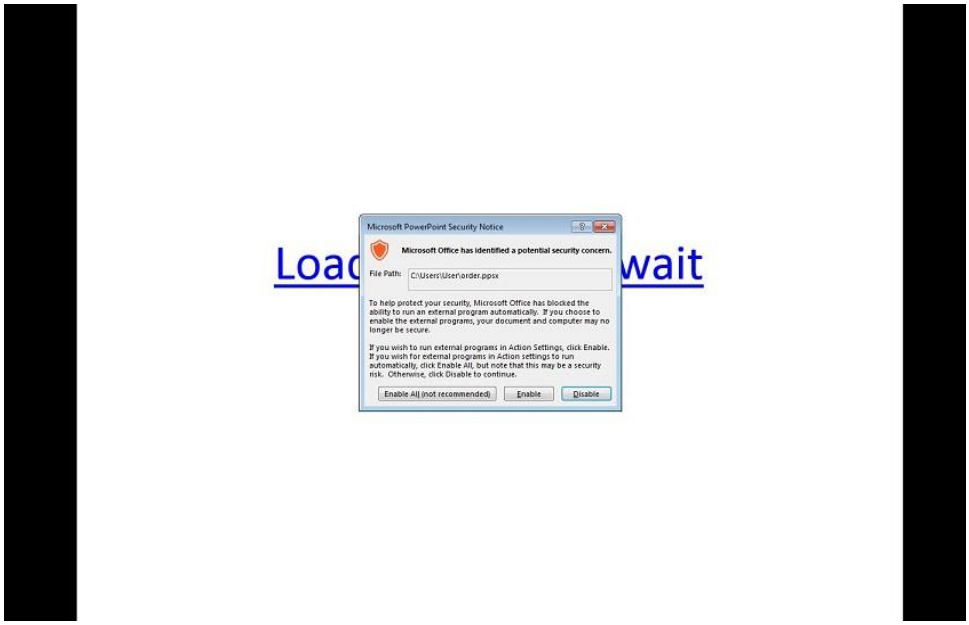
فایل PowerPoint مورد بررسی، تنها شامل یک اسلاید است که در آن یک لینک به چشم می‌خورد.



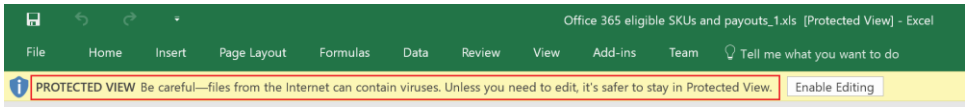
زمانی که اشاره‌گر بر روی این لینک قرار می‌گیرد کد مخرب زیر اجرا می‌شود. (این کدها از حالت مبهم‌سازی خارج شده‌اند.)



در صورتی که فایل در حالت Protected View اجرا شده باشد نرم‌افزار با نمایش پیامی مشابه شکل زیر از اجرای کد مخرب جلوگیری خواهد کرد.



به‌صورت پیش‌فرض، فایل‌های Office دریافت شده در مرورگرها یا پیوست‌های دریافت شده در نرم‌افزارهایی همچون Outlook در حالت Protected View باز می‌شوند. در این حالت کاربر عملاً تنها محتوای فایل را می‌بیند و کدهای تزریق شده در فایل که بالقوه می‌توانند سبب اجرای هر گونه کد مخرب گردند اجرا نمی‌شوند.



اما در صورت غیرفعال بودن Protected View یا زمانی که کاربر پیام هشدار این قابلیت حفاظتی را نادیده می‌گیرد، کد مخرب اقدام به برقراری ارتباط با نشانی hxxp://cccn.nl/c.php کرده و پس از دریافت بدافزار، آن را بر روی سیستم اجرا می‌کند.

بدافزار اجرا شده در نمونه بررسی شده با نام‌های زیر توسط ضدویروس‌هایMcAfee و Bitdefender شناسایی می‌شود:

McAfee:

RDN/Generic Downloader.x

Bitdefender:

Trojan.Downloader.JTNF

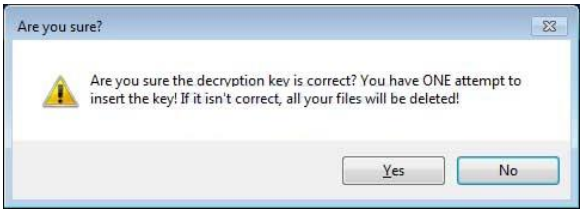
BitKangoroo،
در صورت عدم پرداخت باج، فایل‌ها را **حذف** می‌کند!

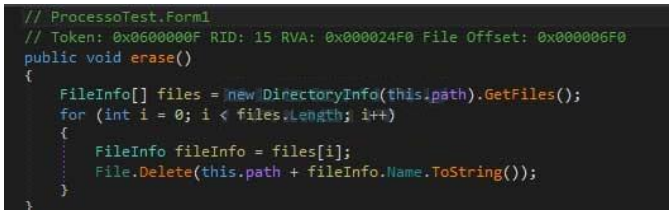
به گزارش شرکت مهندسی شبکه گستر، نمونه‌ای جدید از باج‌افزارها در حال انتشار است که در صورتی که قربانی آن باج را در مهلت مقرر شده پرداخت نکند، فایل‌های خود را یکی پس از دیگری از دست می‌دهد.

به‌طور خلاصه، این باج‌افزار فایل‌های قربانی را با استفاده از الگوریتم رمزگذاری AES-256 رمز کرده و به آنها پسوند bitkangoroo. را الصاق می‌کند. موضوعی که سبب معروفیت آن به BitKangoroo شده است. در ادامه پنجره‌ای نمایش داده می‌شود که بخشی از آن به یک شمارش‌گر معکوس ۶۰ دقیقه‌ای اختصاص دارد. با پایان مهلت ۶۰ دقیقه‌ای یکی از فایل‌های رمز شده قربانی حذف شده و مجدداً شمارنده به ۶۰ دقیقه باز می‌گردد.

به‌نظر می‌رسد این باج‌افزار در حال توسعه بوده و مراحل برنامه‌نویسی آن تکمیل نشده باشد. به‌خصوص آنکه در این نسخه، تنها فایل‌های در پوشه Desktop کاربر رمزگذاری می‌شوند.

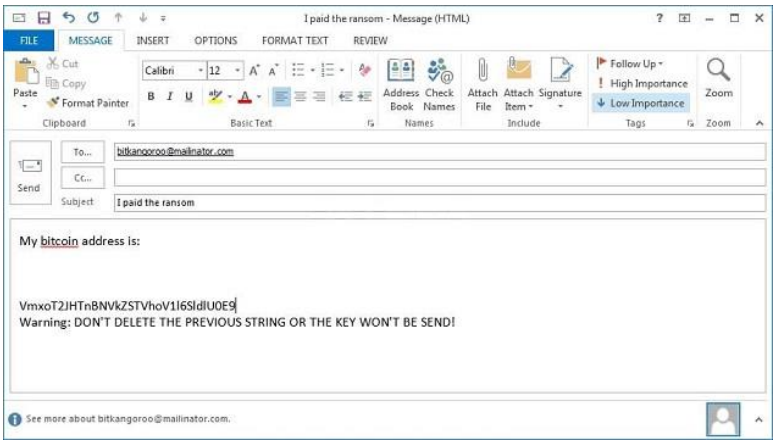
بررسی نمونه شناسایی شده نشان می‌دهد که در برنامه‌نویسی آن کدهایی بکار رفته که هدف آنها حذف کلیه فایل‌های کاربر در صورت وارد کردن کلید رمزگشایی نادرست توسط قربانی است.





```
// ProcessoTest.Form1
// Token: 0x0600000F RID: 15 RVA: 0x000024F0 File Offset: 0x000006F0
public void erase()
{
    FileInfo[] files = new DirectoryInfo(this.path).GetFiles();
    for (int i = 0; i < files.Length; i++)
    {
        FileInfo fileInfo = files[i];
        File.Delete(this.path + fileInfo.Name.ToString());
    }
}
```

در پنجره حاوی اطلاعیه باج‌گیری برچسبی وجود دارد که در صورت کلیک بر روی آن پنجره ارسال ایمیل باز می‌شود. در نمونه بررسی شده bitkangoroo@mailinator.com به‌عنوان نشانی گیرنده ایمیل درج شده است.



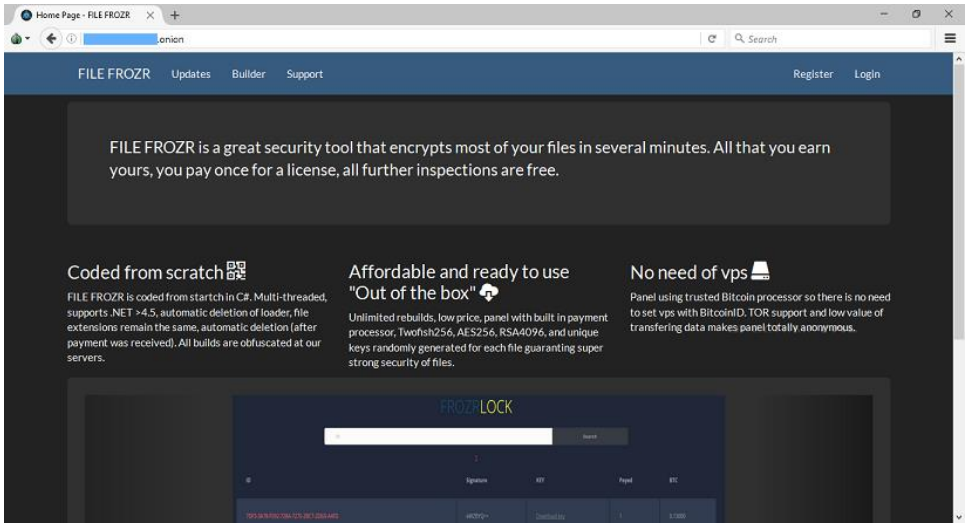
خوشبختانه فایل‌های رمز شده توسط نمونه مورد بررسی با استفاده از این ابزار بدون نیاز به پرداخت باج قابل رمزگشایی هستند.

FrozrLock،
نمونه‌ای جدید از باج‌افزار به‌عنوان سرویس

باج‌افزارهای رمزگذار را می‌توان یکی از مخرب‌ترین و همچنین رایج‌ترین تهدیدات سال های 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-Servicee 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، گونه جدیدی از باج‌افزارها با نام FrozrLock در قالب باج‌افزار به‌عنوان سرویس در Dark Web با قیمت ۰٫۱۴ بیت‌کوین (حدود ۲۲۰۰ دلار) به فروش می‌رسد.

گرداننده یا گردانندگان آن، FrozrLock را به‌عنوان یک ابزار امنیتی عالی برای رمزگذاری اکثر فایل‌ها در مدتی کوتاه توصیف می‌کنند.



گفته می‌شود اولین نمونه شناسایی شده از این باج‌افزار در کشور روسیه بوده که از طریق فایل‌های موسوم به JS Downloader به دستگاه راه یافته بود.

بر اساس توضیحات سایتی که FrozrLock در آن عرضه می‌شود، این باج‌افزار دارای ویژگی‌ها و قابلیت‌های زیر است:

- به زبان C# نوشته شده است.
- پسوند فایل‌های رمزگذاری شده را تغییر نمی‌دهد.
- در صورت پرداخت باج، می‌تواند خود را از روی سیستم قربانی حذف کند.
- امکان استفاده از الگوریتم‌های Twofish256، AES256 و RSA4096 را در خود دارد.
- در هر رمزگذاری از کلیدی یکتا و منحصربه‌فرد استفاده می‌شود.
- متقاضیان بدخواه این خدمت می‌توانند هر تعداد نسخه متفاوت از آن را داشته باشند.

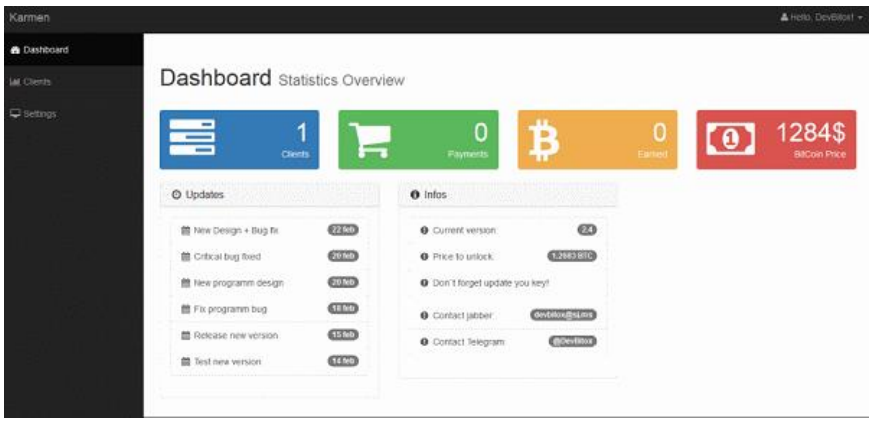
ابزاری نیز برای رمزگشایی فایل‌های رمز شده در اختیار مشتریان این سرویس قرار داده می‌شود تا در صورت پرداخت باج توسط قربانی آن را با توضیحاتی سفارشی به او ارسال کنند.

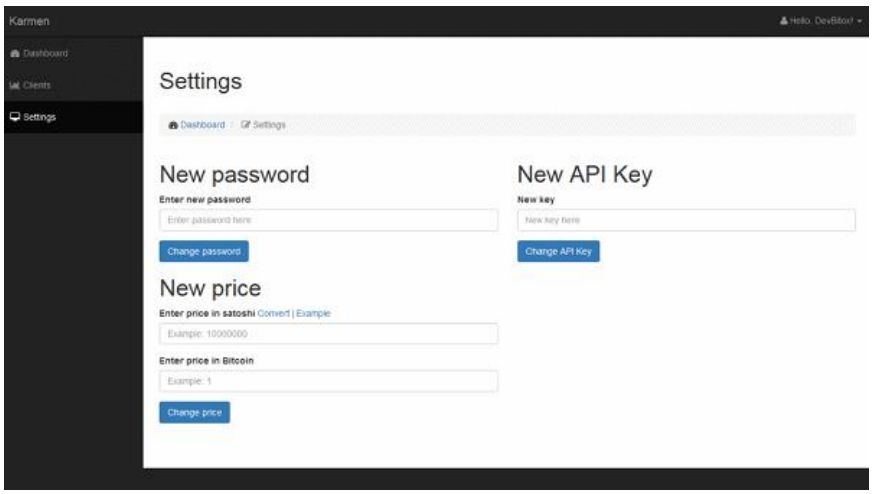
عرضه باج‌افزار Karmen RaaS
در بازارهای سیاه نفوذگران

به گزارش شرکت مهندسی شبکه گستر، سرویس خدمات باج‌افزاری Karmen در حال خرید و فروش شدن در حداقل یک تالار گفتگوی اینترنتی روسی زبان است.

باج‌افزار Karmen بر پایه HiddenTear که یک پروژه کد باز است توسط یک نفوذگر روسی زبان با نام DevBitox و با مشارکت یک برنامه‌نویس آلمانی در قالب RaaS توسعه داده شده است.

با خرید عضویت سرویس Karmen با قیمت ۱۷۵ دلار، یک دسترسی تحت وب به پورتال آن فراهم می‌شود و پرداخت‌کننده می‌تواند نسخه‌ای سفارشی شده از Karmen را ایجاد و دریافت کند.





با آلوده شدن دستگاه به Karmen، فایل های کاربر رمزگذاری شده و در پنجره‌ای ضمن اطلاع‌رسانی، به قربانی هشدار داده می‌شود که در صورت دست درازی به فرآیند رمزگذاری، ممکن است فایل‌ها برای همیشه از دست بروند.

باج‌افزار Karmen مجهز به قابلیت‌های ضد ماشین مجازی و ضد قرنطینه امن (Anti-Sandbox) بوده و در صورت شناسایی هر یک از این بسترها اجرای خود را متوقف می‌کند.

سازندگان Karmen ادعا می‌کنند که این باج افزار توسط اکثر محصولات ضدویروس قابل شناسایی نیست. این در حالی است که باج‌افزارهای مبتنی بر HiddenTearاز جمله Karmen بخوبی توسط بسیاری از محصولات ضدویروس شناسایی و متوقف می‌شوند.

خبر خوش اینکه فایل‌های رمز شده توسط باج‌افزار Karmen بدون نیاز به پرداخت باج و با استفاده از این ابزار قابل رمزگشایی هستند.

سـاير تهديدات

جعل نشانی دامنه؛
روش شناسایی: تقریباً غیرممکن!

یک محقق چینی روش جدیدی برای اجرای حملات فیشینگ کشف کرده که شناسایی آن توسط کاربران با روش‌های معمول تقریباً غیرممکن است.

به گزارش شرکت مهندسی شبکه گستر، بر اساس تحقیقات انجام شده توسط این محقق، مهاجم می‌تواند با بهره‌جویی از یک آسیب‌پذیری در مرورگرهای معروفی نظیر Chrome و Firefox یک دامنه جعلی را با نام یک دامنه حقیقی شرکت‌های مجازی نظیر Apple و Google نمایش داده و حتی محتاط‌ترین کاربران را وادار به ورود اطلاعات محرمانه در صفحه جعلی کند.

تا پیش از این تصور بر این بود که توجه به عبارت درج شده در نوار نشانی مرورگر و وجود پودمان SSL در آن می‌تواند کاربر را از گزند تهدیدات فیشینگ حفظ کند. اما در این روش کشف شده توجه به نوار نشانی کمکی به کاربر نمی‌کند.

قبل از بررسی بیشتر بهتر است نگاهی به این لینک انداخته شود.

اگر مرورگر مورد استفاده در نوار نشانی عبارت apple.com را با پودمان SSL نشان دهد در آن صورت مرورگر شما به این حملات آسیب‌پذیر است. نمونه‌ای دیگر نیز در اینجا قابل دسترس است که در آن نشانی سایت epic.com جعل شده است.

چند سال قبل مؤسسه ICANN تصویب کرد که در نامگذاری دامنه‌ها بتوان از نویسه‌های غیر ASCII استفاده کرد. همچنین در زمان ثبت دامنه از روشی موسوم به Punycode استفاده می‌شود تا نویسه‌های Unicode در قالب کدهای ASCII ثبت شوند. برای مثال در این روش نویسه چینی 短 به صورت xn—s7y ثبت می‌شود.

به گزارش شرکت مهندسی شبکه گستر، نویسه‌های متعددی وجود دارند که در زبان‌هایی نظیر یونانی، سیرلیک و ارمنی کاملاً مشابه نویسه‌های لاتین نوشته می‌شوند. برای مثال در استانداردUnicode ، نویسه سیریلیکی با شناسه U+0430 و نویسه لاتین با شناسهU+0041 هر دو، نویسه‌ای با شکل "aa" را نمایش می‌دهند.

اکنون مشخص شده که مهاجم می‌تواند با ثبت دامنه‌ای برای مثال با نام xn-pple-43d.com سبب نمایش apple.com در نوار نشانی مرورگرهای آسیب‌پذیر شود.

بررسی‌ها نشان می‌دهد مرورگرهای زیر به این حملات آسیب‌پذیرند:

- Chrome
- Firefox
- Opera
- Opera Neon

اما به‌نظر می‌رسد مرورگرهای زیر نویسه‌های نوار نشانی را به‌صورت Punycode نمایش داده و آنها را به Unicode تبدیل نمی‌کنند:

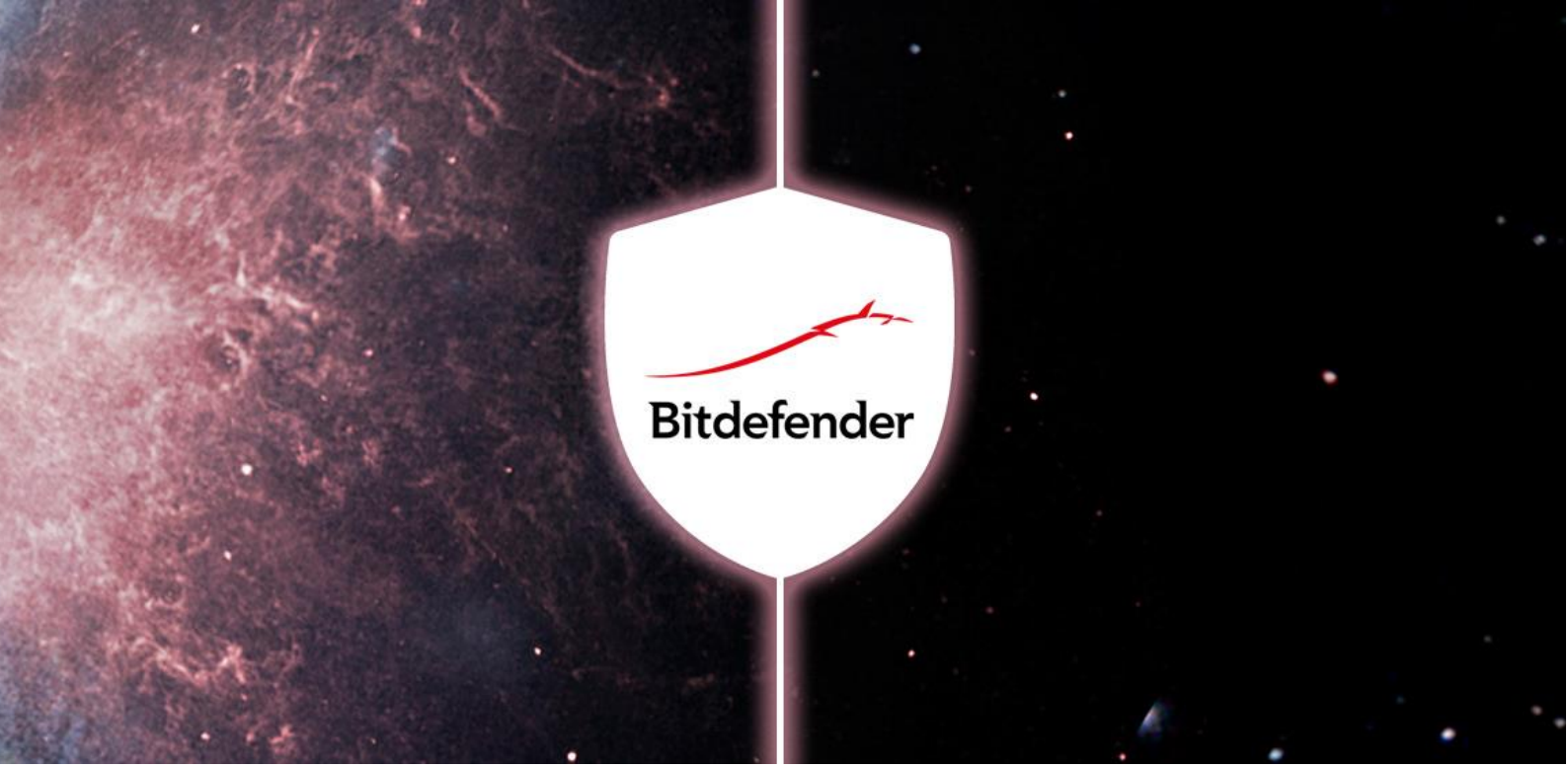
- IE
- Edge
- Vivaldi
- Brave

این محقق گفته که وجود این آسیب‌پذیری را در اول بهمن ماه به شرکت‌های Google و Mozilla اطلاع داده است. Google این آسیب‌پذیری را در نسخه Canary 59 ترمیم کرده است. اما به نظر می‌رسد که Mozilla هنوز به راه حل مشخصی نرسیده است. با این حال کاربران مرورگر این شرکت نیز می‌توانند با دنبال کردن مراحل زیر بخش آسیب‌پذیر را موقتاً حل کنند:

۱. در نوار نشانی عبارت about:config درج شود.
۲. در بخش جستجو، کلمه Punycode وارد شده و کلید Enter فشرده شود.
۳. با انجام مراحل فوق، پارامتر titled: network.IDN_show_punycode نمایش داده می‌شود. با دو بار کلیک بر روی آن مقدار آن به False تغییر داده شود.

شایان ذکر است مشاهده گواهینامه سایت نیز می‌تواند کاربران متخصص را نسبت به وجود این حملات آگاه کند.

گزارش‌ها



Bitdefender،
سپر دفاعی مؤثر
در برابر WannaCry

۲۲ اردیبهشت ماه، باج‌افزار WannaCry ده‌ها هزار کامپیوتر را در سراسر جهان آلوده کرد. تنها در ۲۴ ساعت نخست، تعداد آلودگی‌ها به این باج‌افزار به ۱۸۵ هزار دستگاه در بیش از ۱۰۰ کشور رسید.

آنچه که WannaCry را در مقایسه با سایر هم‌قطاران خود متمایز می‌کند انتشار خودکار آن در سطح شبکه و اینترنت با سوءاستفاده از ضعفی امنیتی موسوم به EternalBlue است.

WannaCry که با نام‌های WanaCrypt0r و WCRY نیز شناخته می‌شود، تهدیدی جدی برای سازمان‌هاست. تنها کافی است که دستگاه یک کاربر به این باج‌افزار آلوده شود؛ ظرف مدتی کوتاه، بدون نیاز به هر گونه دخالت کاربر، آلودگی به دستگاه‌های آسیب‌پذیر دیگر گسترش می‌یابد. بنابراین در صورت وجود یک دستگاه آلوده به این باج‌افزار در سطح شبکه، حتی دستگاه‌هایی که به اینترنت متصل نیستند نیز از گزند آن در امان نخواهند ماند.

فناوری‌های نسل بعدی یادگیری ماشین و بررسی حافظه Bitdefender سازمان‌ها را در برابر تهدیدات مخربی همچون WannaCry و بهره جوهایی نظیر EternalBlue ایمن نگاه خواهند داشت.

در جریان حمله اخیر نیز، سازمان‌های حفاظت شده توسط راهکار Bitdefender GravityZone و فناوری Bitdefender Hypervisor Introspection در برابر WannaCry، تهاجمی‌ترین باج‌افزار تاریخ در امان بوده‌اند.

فناوری یادگیری ماشین Bitdefender در تمامی نسخه‌های GravityZone فراهم است. این فناوری به نحوی طراحی شده که حملات از قبل دیده نشده در همان فاز اجرا شناسایی و خنثی شوند.

Industroyer؛
مخرب‌ترین بدافزار صنعتی پس از Stuxnet

در جریان یکی از حملات سایبری بر ضد اوکراین در سال ۲۰۱۶ میلادی، برق کی‌ف، پایتخت این کشور به مدت یک ساعت قطع شد. قطع برق در اواخر سال ۲۰۱۶ در کشور اوکراین از جهات بسیاری مشابه حمله‌ای بود که در سال قبل از آن منجر به قطع برق نزدیک به ۲۵۰ هزار خانه در چندین شهر این کشور شده بود. بررسی‌های بیشتر منجر به شناسایی بدافزاری موسوم به Industroyer گردید که کالبدشکافی و بررسی دقیق آن ماه‌ها به طول انجامید.

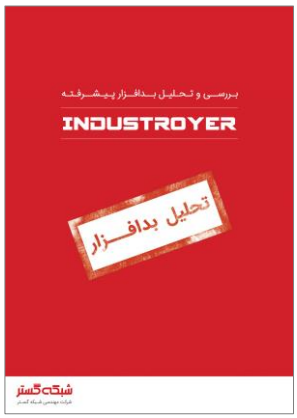
اکنون پس از بررسی‌های مفصل مشخص گردیده که بدافزار مذکور قادر به وارد ساختن آسیب قابل توجه به مراکز توزیع‌کننده برق بوده و حتی ارتقای آن برای هدف قرار دادن دیگر زیرساخت‌های حیاتی نیز امکان پذیر است.

با توجه به توانایی Industroyer در کنترل مستقیم سوییچ‌های برق و تجهیزات موسوم به مدارشکن، این بدافزار تهدیدی بسیار خطرناک محسوب می‌شود. Industroyer پودمان‌های ارتباطی صنعتی را که در زیرساخت‌های مراکز توزیع‌کننده برق، سیستم‌های کنترل حمل و نقل و زیرساخت‌های حیاتی دیگر در شبکه‌های تصفیه و انتقال آب و گازرسانی در سراسر جهان مورد استفاده قرار می‌گیرند مورد بهره‌جویی خود قرار می‌دهد.

سوییچ‌ها و مدارشکن‌های بکار گرفته شده در مراکز توزیع برق معادل دستگاه‌های آنالوگ سنتی هستند. از لحاظ فنی، این تجهیزات می‌توانند به‌نحوی مهندسی و طراحی شوند که توابع متعددی همچون خاموش کردن سیستم توزیع برق، از کاراندازی برخی تجهیزات و حتی اموری به مراتب خطرناک‌تر را در کسری از ثانیه اجرا کنند. بدیهی است که از کاراندازی چنین سیستم‌هایی خود می‌تواند صدمات مستقیم و غیرمستقیم غیر قابل جبرانی را بر روی سرویس‌های حیاتی هر کشور وارد کند.

بخصوص آنکه پودمان‌ها و استانداردهای مورد استفاده در تجهیزات صنعتی دهه‌ها قبل و در دوره‌هایی طراحی شده‌اند که اتصال به شبکه‌های قابل دسترس و اینترنت مفهومی نداشت و به عبارتی دیگر در این پودمان‌های ارتباطی خبری از تنظیمات و سیاست‌های امنیتی نیست.

هر چند Industroyer بدافزاری بسیار پیشرفته و قدرتمند توصیف شده و برخی محققان آن را پس از Stuxnet مخرب‌ترین بدافزار صنعتی معرفی کرده‌اند اما باید در نظر داشت که با وجود اشکالات پودمان‌های رایج فعلی، اجرای حملات مشابه کار چندان دشواری برای مهاجمان حرفه‌ای نخواهد بود.



جهت دریافت اطلاعات بیشتر در خصوص بدافزار Industroyer اینجا کلیک کنید.

استفاده ۱۵ درصد کاربران IoT
از گذرواژه پیش‌فرض

به گزارش شرکت مهندسی شبکه گستر، نتایج یک تحقیق انجام شده توسط شرکت Positive Technologies نشان می‌دهد ۱۵ درصد کاربران، گذرواژه پیش‌فرض دستگاه های موسوم به اینترنت اشیاء خود را تغییر نمی‌دهند.

این به معنای وجود ده‌ها میلیون‌ها دستگاه هایی است که می توانند به راحتی به تسخیر گردانندگان شبکه‌های مخرب (Botnet) در آیند.

چندین سال است که کارشناسان در خصوص امنیت ضعیف وسایل و تجهیزات متصل به اینترنت، موسوم به اینترنت اشیاء (IoT) هشدار داده‌اند.

امنیت ضعیف و پیکربندی آسیب‌پذیر این تجهیزات از یک سو و اتصال آنها به شبکه اینترنت از سویی دیگر، این تجهیزات را به هدفی بسیار مناسب و در عین حال آسان برای مهاجمان تبدیل کرده است.

یکی از اصلی‌ترین بهره‌جویی‌های تبهکاران سایبری از این وسایل و تجهیزات، تسخیر نمودن آنها برای اجرای حملات توزیع شده برای از کاراندازی سرویس (DDoS)است.

در جریان این حملات، لشکری از این تجهیزات هک شده با ارسال درخواست‌های همزمان به سرور قربانی آن را بمباران می‌کنند. دریافت همزمان درخواست، از هزاران و در برخی مواقع ده‌ها هزار دستگاه با نشانی‌های IP مختلف، در نهایت، منجر به کندی و یا حتی توقف خدمات‌دهی سرور به کاربران می‌شود.

بر اساس بررسی‌های انجام شده توسط محققان Positive Technologies، مهاجمان می‌توانند تنها با داشتن پنج ترکیب نام کاربری و گذرواژه زیر، تعداد قابل توجهی دستگاه اینترنت اشیاء را به کنترل خود در آورند:

- support/support
- admin/admin
- admin/0000
- user/user
- root/12345

بدیهی است که افزایش موارد این فهرست به معنای دستگاه‌های آسیب‌پذیر بیشتر است.

برای مثال بدافزار Mirai که شبکه مخرب آن در گسترده‌ترین حملات DDoS نقش داشته تنها از ۶۲ نام کاربری و گذرواژه پیش‌فرض و رایج استفاده می‌کرده است. Mirai بدافزاری است که با نفوذ به دستگاه با سیستم عامل Linux، آن را به عضوی از شبکه مخرب تبدیل می‌کند. دستگاه‌های قربانی این بدافزار عمدتاً رهیاب‌های خانگی و دوربین‌های اینترنتی با گذرواژه‌های ضعیف و تنظیمات آسیب‌پذیر هستند.

واقعیت آن است که دستگاه‌های متصل به اینترنت، صرفاً دستگاه‌هایی با منابع محدود نیستند. بلکه کامپیوترهایی هستند که اگر به‌طور صحیح پیکربندی و ایمن‌سازی نشوند، می‌توانند به ابزاری مخرب در دست نفوذگران تبدیل شوند.

رعایت موارد زیر آسان‌ترین راه برای حفاظت از دستگاه‌های موسوم به اینترنت اشیاء است:

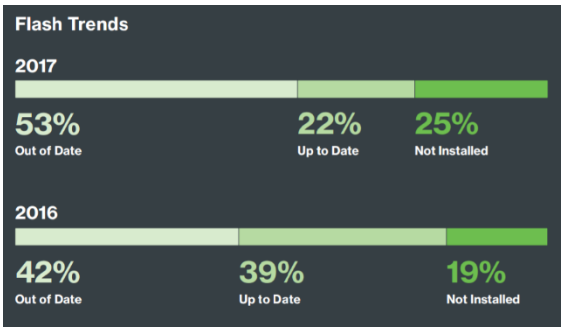
- گذرواژه‌های پیش‌فرض دستگاه به گذرواژه‌های پیچیده تغییر داده شده‌اند. نام‌های کاربری و گذرواژه‌های پیش‌فرض براحتی دستگاه را به تسخیر شبکه‌های مخرب در می‌آورند.
- دستگاه‌های اینترنت اشیاء به آخرین نسخه به‌روز شوند.
- پودمان‌های Telnet و SSH و همچنین پودمان‌های مرتبط با UPnP بر روی این دستگاه‌ها غیرفعال شود؛ مگر آنکه واقعاً به آن نیاز باشد.
- از دستگاه های متصل به اینترنت توسط دیواره های آتش کارآمد حفاظت شود.
- دستگاه‌های متصل به اینترنت حتی الامکان از شرکت‌های خوشنام خریداری شود.

استفاده از نرم‌افزارهای آسیب‌پذیر؛ معضلی جهانی

سالهاست که ویروس‌نویسان و نفوذگران به‌شدت به استفاده از نقاط ضعف سیستم‌های عامل – به ویژه سیستم عامل پرطرفدار Windows - و نرم‌افزارهای پر استفاده روی آورده‌اند. وجود یک نقطه ضعف (Vulnerability) خطرناک در سیستم عامل یا هر یک از نرم‌افزارهای پرکاربرد می‌تواند سبب دور زدن قوی‌ترین نرم‌افزارهای ضدویروس یا دیواره‌های آتش شود!

تاخیر در نصب اصلاحیه‌های امنیتی به منظور ترمیم این نقاط ضعف، سازمان را به‌شدت در برابر بدافزارها و حملات سایبری آسیب‌پذیر می‌کند.

به گزارش شرکت مهندسی شبکه گستر، بر اساس گزارشی که به تازگی شرکت امنیتی Duo Security آن را منتشر کرده، ۵۳ درصد دستگاه‌ها در سازمان‌ها از نسخه‌های آسیب‌پذیر نرم‌افزار Flash استفاده می‌کنند؛ این در حالی است که در سال گذشته میلادی این سهم ۴۲ درصد بوده است.

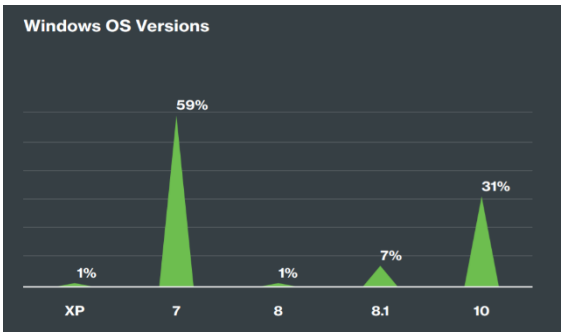


ضعف‌های امنیتی نرم‌افزار Flash همواره از اهداف مورد علاقه مهاجمان سایبری بوده است.

همچنین یافته‌های محققان Duo Security نشان می‌دهد که ۱۳ درصد دستگاه‌ها نیز از یکی از نسخه‌های از رده خارج مرورگر IE استفاده می‌کنند.

بر مبنای اطلاعات ارائه شده در گزارش مذکور، در بخش بهداشت و درمان، سهم دستگاه‌های با سیستم عامل Windows XPکه پشتیبانی از آن سالهاست توسط مایکروسافت متوقف شده از ۲ درصد در سال ۲۰۱۶ به ۳ درصد در سال ۲۰۱۷ افزایش یافته است. موضوعی که می‌تواند یکی از دلایل اصلی پرتعداد بودن دستگاه‌های آلوده به باج‌افزار WannaCry در این نوع سازمان‌ها بوده باشد.

در بخشی از این گزارش نیز اشاره شده که کمتر از یک سوم (۳۱ درصد) نقاط پایانی مبتنی بر یکی از سیستم‌های عامل مایکروسافت از Windows 10 استفاده می‌کنند.



جهت دریافت گزارش Trusted Access اینجا کلیک کنید.

نحوه راه رفتن،
روشی مطمئن برای اصالت‌سنجی

به گزارش شرکت مهندسی شبکه گستر، مقاله‌ای که به تازگی توسط سازمان پژوهش‌های علمی و صنعتی همسود استرالیا (CSIRO) منتشر شده نشان می‌دهد که نحوه گام برداشتن یا حرکات پاها و بدن در هنگام راه رفتن فرد می‌تواند به عنوان یک روش اصالت‌سنجی (Authenticationn) مطمئن مورد استفاده قرار گیرد.

در این فناوری اصالت‌سنجی، از شتاب‌سنج برای ضبط نحوه گام برداشتن فرد بر اساس دو مؤلفه حرکت و سرعت استفاده می‌شود.

بیش از یک دهه است که برخی محققان به امکان‌سنجی اصالت‌سنجی بر اساس راه رفتن افراد پرداخته‌اند. اشکال اصلی روش‌های پیشنهادی قبلی، مصرف بالای انرژی و در نتیجه عمر کوتاه فعال بودن باتری حسگرها بوده است.

اما در روش جدید محققان CSIRO از تکنیک جدیدی که آن را KEH – مخفف Kinetic Energy Harvesting به معنای استفاده از انرژی جنبشی – نامگذاری کرده‌اند بهره گرفته‌اند.

در KEH حرکات فرد به انرژی الکتریکی تبدیل شده و در نتیجه آن مدت زمان فعال بودن باتری استفاده شده در دستگاه‌ها و حسگرهای متصل به فرد افزایش یافته است.

به گفته محققان CSIRO، بررسی‌های انجام شده نشان‌دهنده دقت ۹۵ درصدی روش جدید بر روی سطوح مختلف نظیر موکت، آسفالت و چمن است. ضمن اینکه میزان مصرف توان باتری نیز در مقایسه با روش‌های پیشنهادی پیشین ۷۸ درصد کاهش یافته است.

همچنین در جریان بررسی‌ها مشخص شده که این سیستم قادر به شناسایی ۸۷ درصد حرکات جعلی که به تقلید از حرکات راه رفتن فرد دیگر انجام شده می‌باشد.

در مقایسه با روش‌های دیگر اصالت‌سنجی زیست‌شناسی (Biometrics)، می‌توان به دو مزیت خاص اصالت‌سنجی بر اساس راه رفتن اشاره کرد. نخست اینکه در روش جدید اگر نحوه راه رفتن فرد با گذشت زمان به تدریج تغییر کند سیستم تغییرات را شناسایی و آنها را در اصالت‌سنجی در نظر می‌گیرد.

دوم اینکه با توجه به داده‌های مختلف لحاظ شده در روش اصالت‌سنجی مبتنی بر نحوه راه رفتن، شکستن و هک آن در مقایسه با روش‌های زیست‌شناسی دیگر به مراتب دشوارتر خواهد بود. به خصوص اگر روند افزایش دقت آن همچنان ادامه یابد.

هر چند که همواره توصیه می‌شود که از ترکیب دو روش اصالت‌سنجی استفاده شود.

مقاله علمی این محققان در اینجا قابل دریافت و مطالعه است.

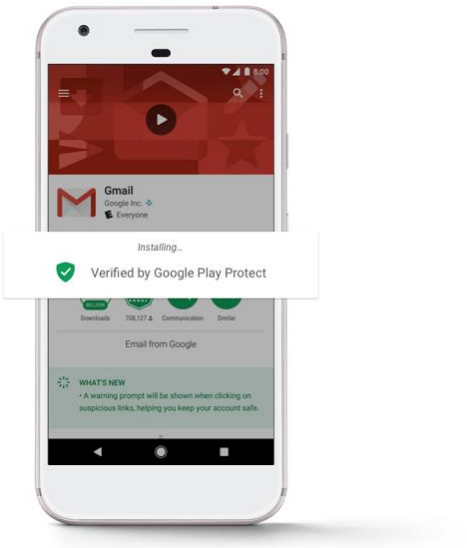
شایان ذکر است که در تحقیق پیشین گروه دیگری از محققان برای بررسی روش اصالت‌سنجی از حسگرهایی که بر روی زمین نصب شده بودند استفاده کرده بودند. در حالی که در روش جدید کاربر می‌بایست حسگرها را به نوعی به تن کند.

رونمایی Google
از فناوری رفتارشناسی Play Protect

به گزارش شرکت مهندسی شبکه گستر، شرکت Google اعلام کرده که با هدف حفاظت از دو میلیارد کاربر سیستم عامل Android خود، فناوری جدیدی تحت عنوان Play Protect را ارائه کرده است.

Play Protect به عنوان بخشی از برنامک Google Play Store بر روی دستگاه فعال می‌شود و بنابراین نیازی به انجام هیچ عملیات اضافی توسط کاربر نخواهد بود.

هدف این فناوری، بهره‌گیری از روش‌های یادگیری ماشین و تحلیل برنامک، به‌منظور کشف و شناسایی برنامک‌های مخرب است.



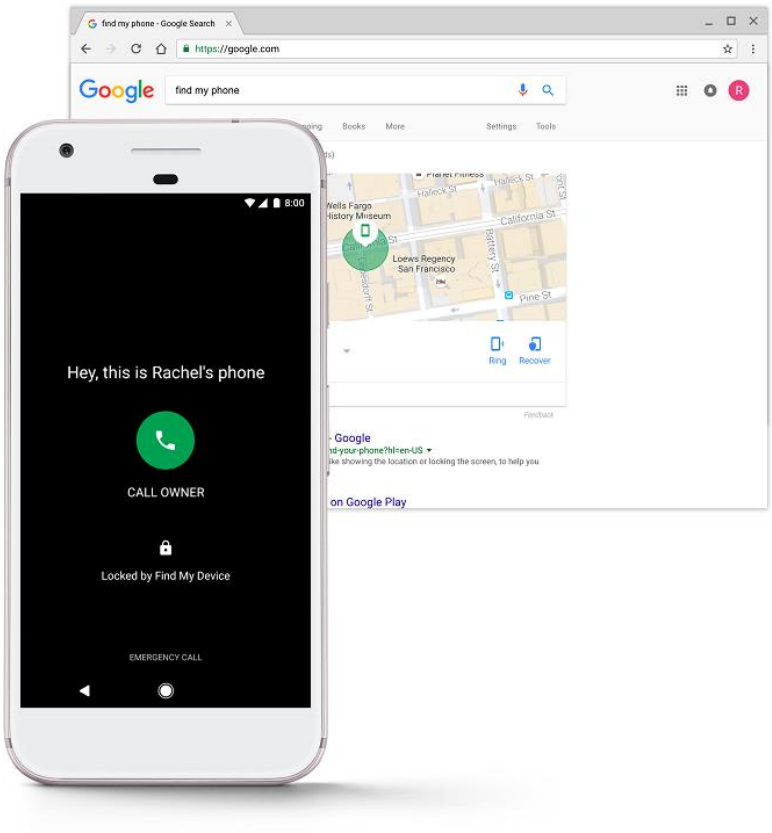
Google Play Protect یک سرویس همواره فعال است که به گفته شرکت Google روزانه بیش از ۵۰ میلیارد برنامک را بر روی دو میلیارد دستگاه با سیستم عامل Android پویش می‌کند.

پیش‌تر نیز این شرکت امکانات امنیتی همچون Verify Apps و سرویس Bouncer را بکار گرفته بود.

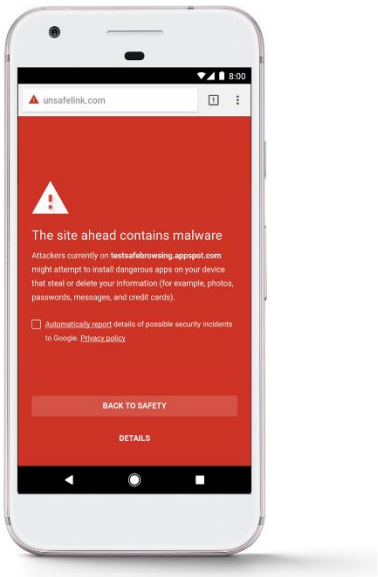
Play Protect، نه تنها برنامک‌ها را پیش از ظاهر شدن در Play Store – بازار توزیع دیجیتال رسمی شرکت Google – مورد تحلیل قرار می‌دهد، که پس از نصب شدن بر روی دستگاه نیز آنها را در پس‌زمینه رصد می‌کند. این رصد کردن شامل برنامک‌های نصب شده از طریق بازارهای توزیع دیجیتال ثالث نیز می‌شود.

برای این منظور، Play Protect با بهره‌گیری از الگوریتم‌های یادگیری ماشین به‌صورت خودکار رفتار برنامک را مقایسه کرده و رفتارهای غیرعادی را شناسایی می‌کند. این فناوری، در صورت برخورد با برنامک مخرب به کاربر هشدار داده یا حتی برنامک را غیرفعال می‌کند.

به گزارش شرکت مهندسی شبکه گستر، Play Protect حاوی قابلیت‌های ضدسرقت نیز می‌باشد. با استفاده از Play Protect کاربر قادر خواهد بود تا از طریق مرورگر یا دستگاهی دیگر، از راه دور با دستگاه خود ارتباط برقرار کرده، محل آن را شناسایی کند، آن را قفل کند و حتی داده‌های حساس خود را از روی آن حذف کند.



و در آخر اینکه Play Protect قابلیتی با عنوان Safe Browsing نیز به مرورگر Chrome اضافه می‌کند که هدف آن ایمن نگاه داشتن کاربران در زمان وبگردی است.



توضیح اینکه بدافزارهای تحت Android معمولاً در قالب برنامک بر روی دستگاه‌های با این سیستم عامل نصب می‌شوند.

تغییرات ضدباج‌افزاری در Android O

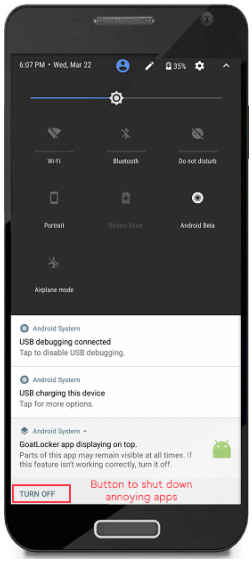
شرکت Google تغییراتی را در نسخه جدید Android اعمال می‌کند که کار را برای آن دسته از نویسندگان باج‌افزار که دستگاه‌های همراه با این سیستم عامل را هدف قرار می‌دهند بسیار دشوار می‌کند.

به گزارش شرکت مهندسی شبکه گستر، قرار است در Android O – یا همان نسخه ۸٫۰ – که احتمالاً در پاییز امسال عرضه خواهد شد به سطح دسترسی سه نوع پنجره زیر محدودیت‌هایی اعمال شود:

- TYPE_SYSTEM_ALERT
- TYPE_SYSTEM_ERROR
- TYPE_SYSTEM_OVERLAY

این سه، پنجره‌های سیستمی مخصوصی هستند که در صورت اجرا شدن بالاتر از هر پنجره دیگر قرار می‌گیرند. ناگفته پیداست که این نوع پنجره‌ها از ابزارهای مورد علاقه نویسندگان باج‌افزارهای موبایلی هستند تا از طریق آنها دسترسی کاربر را برای انجام عملیات‌های عادی مسدود کنند.

Google از نسخه ۶٫۰ سیستم عامل Android – موسوم به Marshmallow – این سه نوع پنجره را در گروه پنجره‌های "Above dangerous" طبقه‌بندی کرد. تا پیش از آن، در این سیستم عامل هر پنجره می‌توانست تنها در یکی از سطح‌های دسترسی "Normal" یا "Dangerous" قرار بگیرد. پنجره‌های Normal می‌توانند در زمان اجرا شدن برنامک مربوطه بدون نیاز به اخذ مجوز از کاربر اجرا شوند. حال آنکه اجرای پنجره‌های از نوع Dangerous مستلزم اخذ مجوز از کاربر است.



برای سطح دسترسی "Above dangerous"، لازم است که کاربر مجوز را با اعمال تغییراتی در بخش Settings دستگاه به برنامک مربوطه تخصیص دهد.

با این حال با توجه به استفاده از نسخه‌های سفارشی Android توسط سازندگان گوشی‌های همراه برخی از شرکت‌ها سیاست جدید را بر روی گوشی‌های ساخت خود اعمال نکردند. اما قرار است که در Android O، شرکت Google این اختیار را از این سازندگان سلب کند. این بدان معناست که بسیاری از نویسندگان باج‌افزار باید بدنبال راهی جدید برای مسدود کردن دسترسی قربانی به دستگاه باشند.

خبر خوب دیگر اینکه در Android O حتی در صورت قفل شدن دستگاه توسط یک برنامک، کاربر قادر خواهد بود تا با مراجعه به بخش Notifications اجرای آن برنامک را متوقف کند.

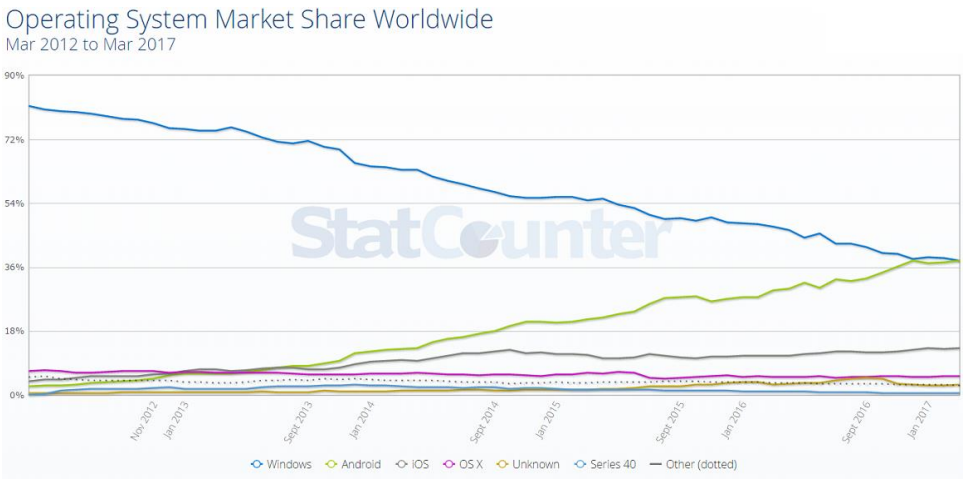
از این نکته نباید چشم‌پوشی کرد که متاسفانه بسیاری از کاربران باج‌افزارهای موبایلی از نسخه‌های قدیمی سیستم عامل Androidاستفاده می‌کنند.

پیشی گرفتن Android از Windows

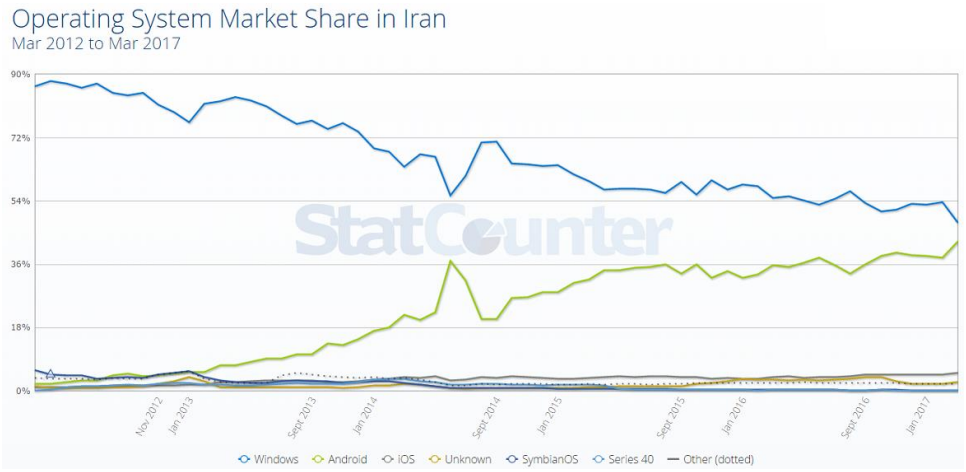
بر اساس آمار ارائه شده از سوی سایت StartCounter، در ماه گذشته میلادی، Android پراستفاده‌ترین سیستم عامل کاربران بر روی اینترنت بوده است.

با توجه به استفاده هر چه بیشتر کاربران از دستگاه‌های همراه که چیزی حدود ۹۰ درصد از آنها از این سیستم عامل استفاده می‌کنند پیش‌بینی وقوع این اتفاق چندان دشوار نبود.

به گزارش **شرکت مهندسی شبکه گستر**، بر اساس آمار StartCounter، سهم کاربران اینترنت با سیستم عامل Android در ماه مارس ۲۰۱۷، ۳۷/۹۳ درصد بوده است. سیستم عامل Windows با ۰/۰۲ درصد سهم کمتر در جایگاه دوم قرار گرفته است. در همین دوره، سهم سیستم‌های عامل iOS، OS X و Linux نیز به ترتیب ۱۳/۰۹، ۵/۱۷ و ۰/۷۵ درصد بوده است.



برای کاربران ایرانی این آمار اما کمی متفاوت است. در مارس ۲۰۱۷، ٤٧/٩٧ درصد کاربران ایرانی با دستگاه‌های با سیستم عاملWindows به اینترنت متصل شدند. این سهم برای سیستم عامل Adnroid، ٤٢/٣٤ درصد اعلام شده است.



این تغییرات در حالی روی می‌دهد که سهم جهانی سیستم‌های عامل Android و Windows در ۵ سال قبل به ترتیب ۲/٤ و ۸۱/٤ درصد بوده است.

Pixel Tracking چیست؟

Pixel Tracking یا ردیابی از طریق پیکسل، روش ساده‌ای است که تبلیغ‌کنندگان اینترنتی در ایمیل‌های ارسالی خود از آن بهره می‌گیرند. در این تکنیک، یک تصویر در اندازه یک پیکسل که معمولاً رنگ آن شفاف یا هم‌رنگ با پس‌زمینه ایمیل است در بدنه ایمیل درج می‌شود.

زمانی که ایمیل توسط کاربر باز می‌شود کد مربوط به تصویر با سرور ارسال‌کننده – در اینجا تبلیغ کننده – ارتباط برقرار می‌کند.

نمونه‌ای از این کدها در زیر قابل مشاهده است:

```
< img width=“1” height=“1” class=“beacon-o” src=“[SERVER_URL][TRACKING_CODE]” style=“float:left;margin-left:-1px;position:absolute;” >
```

TRACKING_CODEدر کد فوق می‌تواند هر چیزی، از ایمیل گرفته تا شناسه کارزار بازاریابی باشد.

به گزارش شرکت مهندسی شبکه گستر، همچون هر سرور دیگر، سرور ارسال‌کننده نیز می‌تواند به نحوی پیکربندی شود که اطلاعات زیر را جمع‌آوری کند:

- بررسی اینکه کاربر ایمیل را در مرورگر وب باز کرده یا ایمیل در یک نرم‌افزار مدیریت ایمیل باز شده است.
- نشانی ایمیل کاربر
- مرورگر کاربر
- نشانی IP دستگاه کاربر
- نام دستگاه کاربر
- سیستم عامل دستگاه کاربر
- تنظمیات استفاده از کوکی ها
- تاریخ و زمان باز شدن ایمیل

اما این روش و این جزییات در ظاهر کم اهیمت می‌توانند برای یک مهاجم بسیار باارزش باشند. به خصوص اگر ایمیل ارسالی مهاجم که حاوی ردیابی‌کننده پیکسلی است توسط چند نفر در سازمان هدف او باز شود .

استفاده از این روش، مهاجم سایبری را قادر خواهد کرد که نقشه‌ای از شبکه داخلی سازمان بدست آورد. اطلاعاتی که در مراحل بعدی حمله، او را در انتخاب بهره‌جوهای (Exploit) مناسب و کاربران آسیب‌پذیرتر یاری خواهند کرد.

خوشبختانه بسیاری از نرم‌افزارهای مدیریت ایمیل نظیر Outlook و Thunderbird به‌صورت پیش‌فرض دریافت خودکار تصویرهای درون ایمیل را مسدود می‌کنند. برخی افزونه‌های Chrome نظیر UglyEmail و PixelBlock نیز می‌توانند برای آن دسته از کاربرانی که ایمیل‌های خود را در این مرورگر مشاهده می‌کنند کمک‌کننده باشد. اما در کنار بکارگیری این روش‌ها آموزش کاربران نیز باید به‌عنوان اقدامی بسیار بااهمیت و مؤثر مد نظر مدیران شبکه قرار گرفته شود.

کشف آسیب‌پذیری ۱۰ ساله در سیستم‌های عامل مبتنی بر Unix

محققان امنیتی یک آسیب‌پذیری تقریباً ده ساله را در چندین سیستم عامل مبتنی بر Unix شامل Linux، OpenBSD، NetBSD، FreeBSD و Solaris شناسایی کرده‌اند که مهاجم با بهره‌جویی از آن قادر خواهد بود حق دسترسی خود را تا سطح root ترفیع داده و به صورت بالقوه کنترل کامل دستگاه را در اختیار بگیرد.

به گزارش شرکت مهندسی شبکه گستر، آسیب‌پذیری مذکور با شناسه CVE-2017-1000364 که نامگذاری شده از نحوه تخصیص حافظه پشته (Stack) به برنامه اجرا شده نشأت Stack Clash می‌گیرد.

در معماری سیستم عامل، به هر برنامه اجرا شده بخشی از حافظه اختصاص داده می‌شود که به حافظه پشته معروف است. کاربرد حافظه پشته ذخیره کوتاه مدت داده‌های مربوط به برنامه در حال اجراست که البته ممکن است در حین فعالیت برنامه افزایش نیز داده شود.

بر اساس توضیحات محققان Qualys که آسیب‌پذیری مذکور را شناسایی کرده‌اند یک برنامه مخرب می‌تواند با سوءاستفاده از این اشکال، مقدار پشته تخصیص داده شده به خود را افزایش داده و سبب بروز خطای سرریز پشته (Stack Overflow) شود.

ضمن اینکه بهره‌جوی Stack Clash می‌تواند از سد سیستم حفاظتی Stack Guard-Page نیز عبور کند.

هر چند اجرای بهره‌جوی Stack Clash مستلزم فراهم بودن دسترسی محلی (Local) مهاجم به دستگاه قربانی است اما یک مهاجم حرفه‌ای می‌تواند با ترکیب آن با تکنیک‌های دیگر یک حمله از راه دور را نیز مدیریت کند.

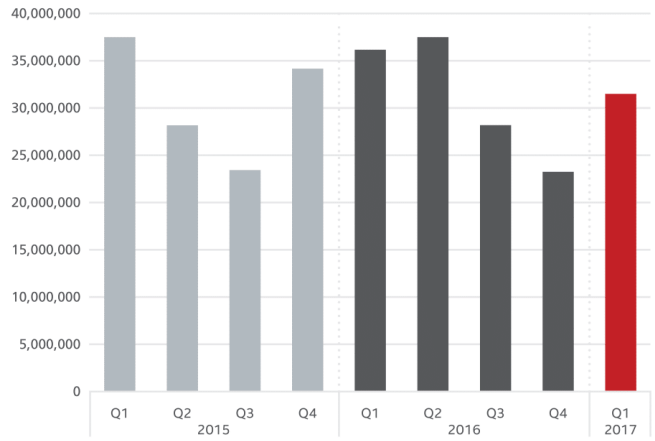
بسیاری از سازندگان سیستم‌های عامل اشاره شده اقدام به عرضه اصلاحیه برای ترمیم ضعف مذکور کرده‌اند که نصب آن در اولین فرصت توصیه می‌شود. راهبران آن دسته از نسخه‌هایی که هنوز اصلاحیه‌ای برای آنها عرضه نشده است نیز می‌توانند با اعمال محدودیت بر روی مقدار حافظه پشته این آسیب‌پذیری را موقتاً پوشش دهند

جهت دریافت و مطالعه مشروح گزارش Qualys، اینجا کلیک کنید.

آمار تهدیدات

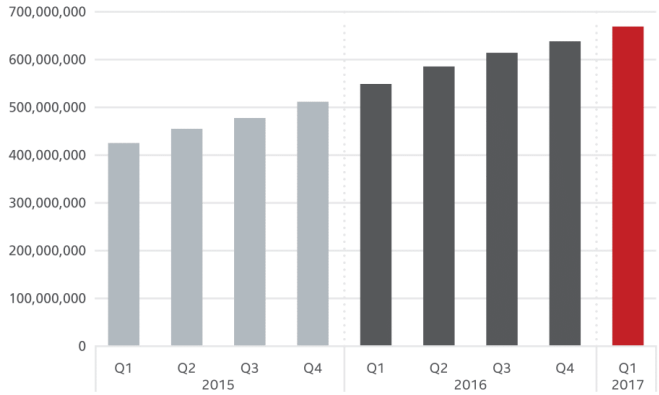
در سه ماهه نخست سال ۲۰۱۷ میلادی ۳۲ میلیون بدافزار منحصربفرد جدید منتشر شده است. تعداد کل بدافزارها نیز با ۲۲ درصد افزایش در مقایسه با سال قبل به ۶۷۰ میلیون نمونه رسیده است.

بدافزارهای جدید



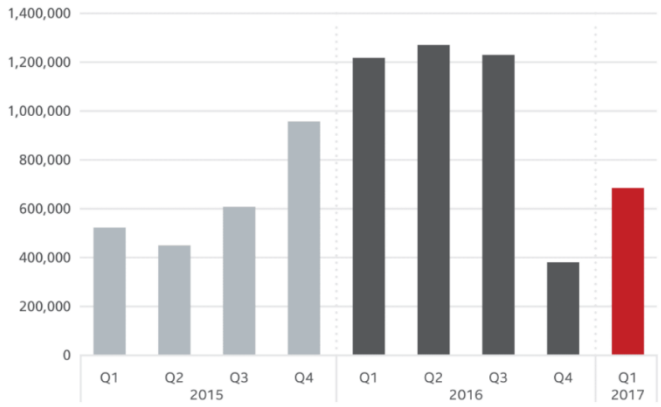
منبع: McAfee Labs، ژوئن ۲۰۱۷

تعداد کل بدافزارها



منبع: McAfee Labs، ژوئن ۲۰۱۷

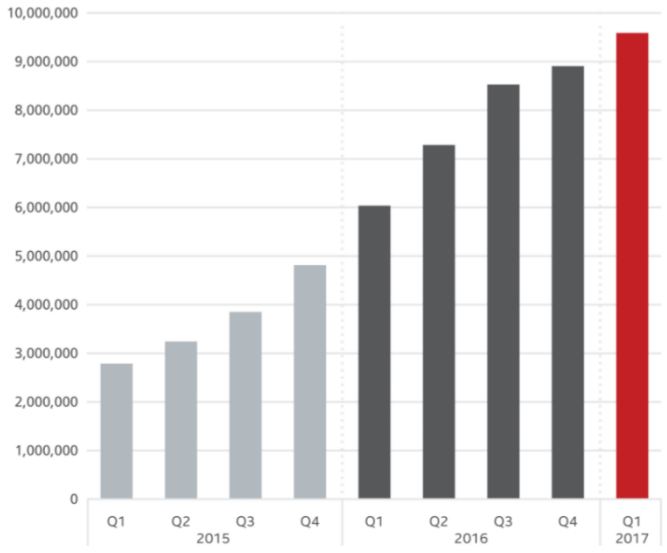
تعداد باج‌افزارهای جدید



منبع: McAfee Labs، ژوئن ۲۰۱۷

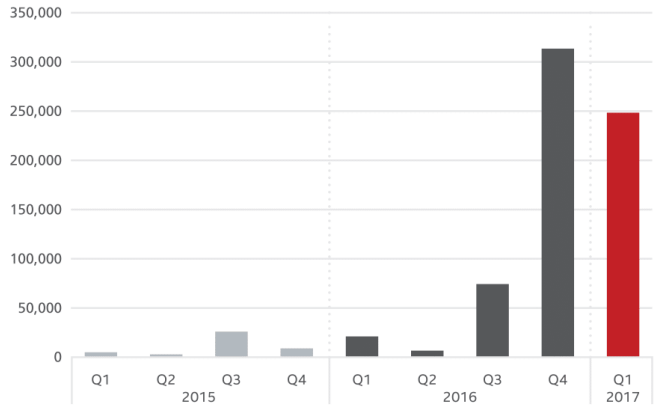
تعداد کل باج‌افزارها در یک سال گذشته با ۵۹ درصد افزایش به ۹٫۶ میلیون عدد رسیده است.

تعداد کل باج‌افزارها



منبع: McAfee Labs، ژوئن ۲۰۱۷

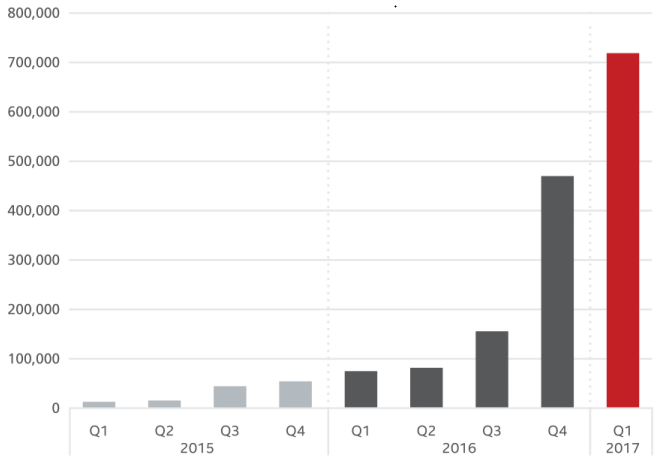
تعداد بدافزارهای جدید Mac OS



منبع: McAfee Labs، ژوئن ۲۰۱۷

در نتیجه انتشار گسترده یک تبلیغ‌افزار، تعداد بدافزارهای تحت Mac OS، ۵۳ درصد افزایش داشته است.

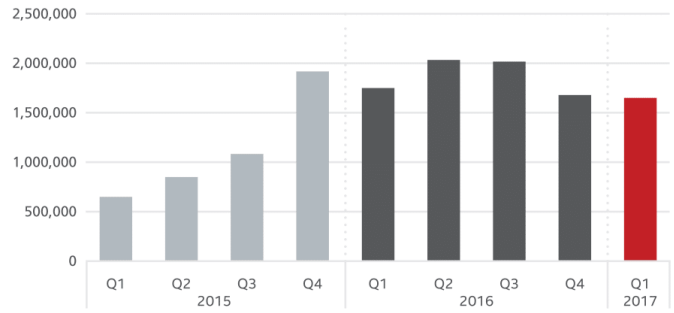
تعداد کل بدافزارهای Mac OS



منبع: McAfee Labs، ژوئن ۲۰۱۷

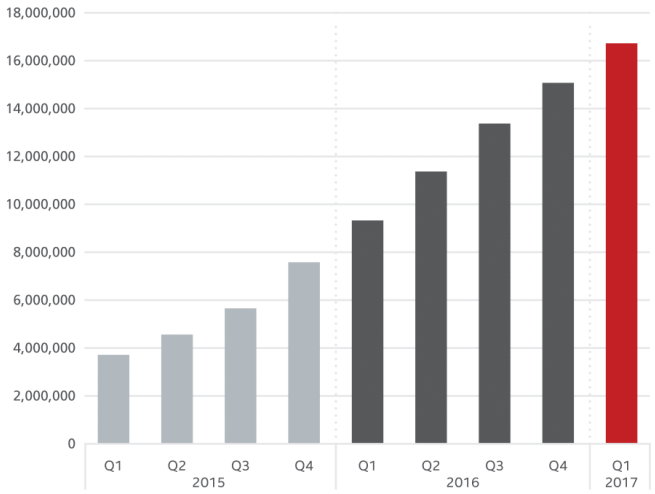
تعداد بدافزارهای موبایلی در منطقه آسیا در این سه ماهه نخست سال ۲۰۱۷ دو برابر شده و ۵۷ درصد سهم جهانی را به خود اختصاص داده است. تعداد کل بدافزارهای موبایلی نیز در یک سال گذشته با ۷۹ درصد افزایش به ۱۶٫۷ میلیون رسیده است.

تعداد بدافزارهای موبایلی جدید



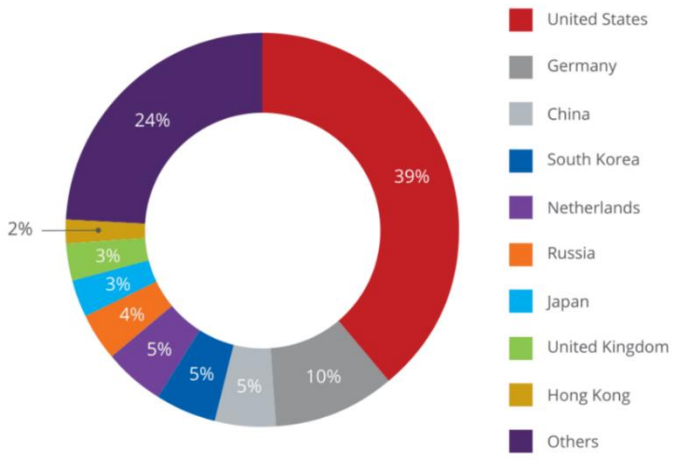
منبع: McAfee Labs، ژوئن ۲۰۱۷

تعداد کل بدافزارهای موبایلی



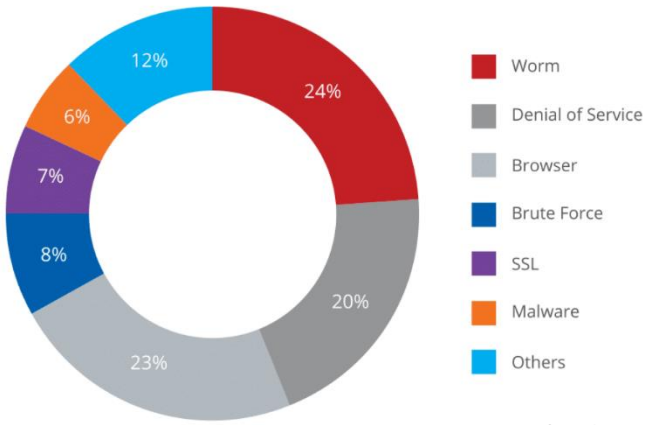
منبع: McAfee Labs، ژوئن ۲۰۱۷

سهم کشورهای میزبانی‌کننده سرورهای موسوم به C&C



منبع: McAfee Labs، ژوئن ۲۰۱۷

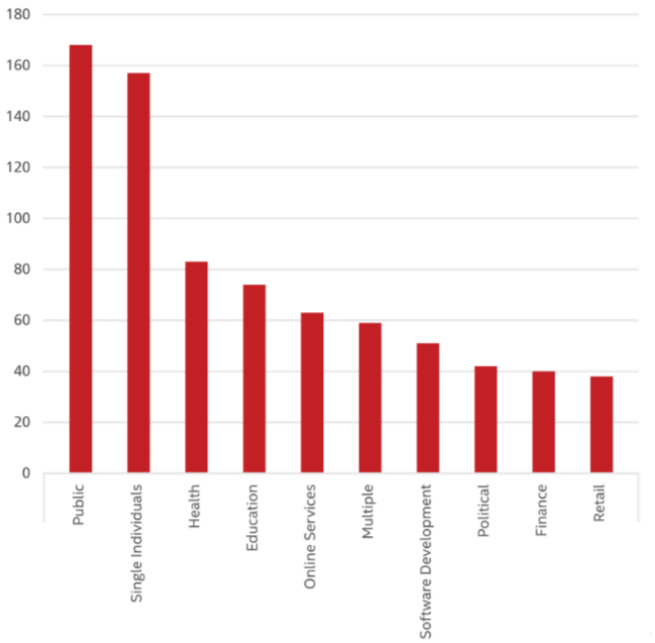
سهم بیشترین روش‌های حمله



منبع: McAfee Labs، ژوئن ۲۰۱۷

بیشترین بخش‌های هدف قرار گرفته در بین سال‌های ۲۰۱۶ و ۲۰۱۷

(بر اساس تعداد رخدادهایی که به صورت عمومی گزارش شده‌اند)



منبع: McAfee Labs، ژوئن ۲۰۱۷

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس 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 محبوب‌ترین 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 بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management) 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 با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید.

از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (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 بوده است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که 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 پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی 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.

ISO 9001:2008
Cert No 9150.C528

اتـــاق خـبـــر

newsroom.shabakeh.net

مـرکـز آمـــوزش

events.shabakeh.net

خدمات پس از فروش

my.shabakeh.net

خدمات پشتیبانی فنی

help.shabakeh.net

شبکه گستر

شرکت مهندسی شبکه گستر

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ – ۰۲۱

www.shabakeh.net

info@shabakeh.net