شماره هشتم - شهریور ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

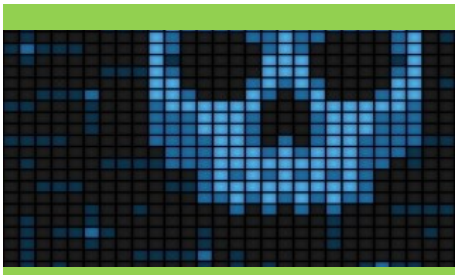
در این شماره خواهید خواند:

D-Link و آپدیت سیستم عامل روتر DIR-850L

پیش از این ماه، محققی به نام pierre Kim، جزییات چندین نقص امنیتی موثر روتر D-Link DIR-850L و کمپانی D-Link راکه قابلیت سرویس دهی دارد را افشا نمود. - صفحه ۲

حمله هکرها به شرکت‌های بخش انرژی آمریکا و اروپا

طبق گزارش محققان مرکز امنیتی Symantec، به تازگی شرکت‌های بخش انرژی اروپا و آمریکا، طی یک سری عملیات جاسوسی سایبری از سوی هکرها مورد هدف و حمله قرار گرفته‌اند. تعدادی از این حملات، سیستم‌های مرکزی کنترل عملیات این شرکت‌ها را دچار آسیب کرده‌اند. - صفحه ۵



حمله هکرها به شرکت‌های بخش انرژی آمریکا و اروپا

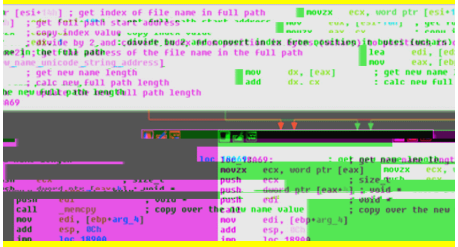
طبق گزارش محققان مرکز امنیتی Symantec، به تازگی شرکت‌های بخش انرژی اروپا و آمریکا، طی یک سری عملیات جاسوسی سایبری از سوی هکرها مورد هدف و حمله قرار گرفته‌اند. تعدادی از این حملات، سیستم‌های مرکزی کنترل عملیات این شرکت‌ها را دچار آسیب کرده‌اند. - صفحه ۵

نرم افزار CCleaner برای انتشار بدافزار، هک شد!

اگر شما نرم افزار محبوب CCleaner را در رایانه شخصی خود در بازه زمانی ۲۴ مرداد تا ۲۱ شهریور سال جاری از وب سایت رسمی شرکت سازنده این نرم افزار دانلود نموده یا آن را به روز کرده اید، توجه داشته باشید که رایانه شما در معرض خطر است. - صفحه ۳ و ۴

هکرهای چینی در حال استفاده از جاسوس افزار xRAT

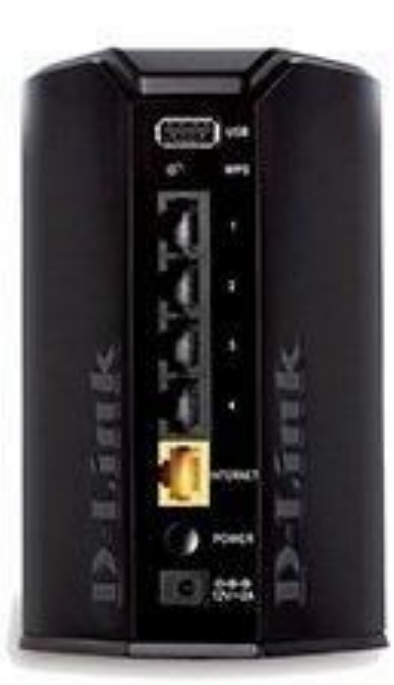
این بدافزار جاسوسی موبایل با نام xRAT که بخاطر هدف قرار دادن گروه‌های سیاسی با طیف وسیعی از راهکارهای جمع آوری اطلاعات همراه است، آن را تبدیل به ابزاری موثر برای گروه هکرهای جاسوس کرده است. - صفحه ۶



باگ در کرنل PsSetLoadImageNotifyRoutine ویندوز

توسعه دهندگان بدافزارها می‌توانند از یک خطای برنامه نویسی در هسته ویندوز برای جلوگیری از تشخیص آنان توسط برنامه‌های امنیتی سو استفاده کنند و ماژول‌های مخرب را در هنگام اجرا بارگذاری کنند. - صفحه ۷

D-Link و آپدیت سیستم عامل روتر DIR-850L



پیش از این ماه، محققی به نام pierre Kim، جزییات چندین نقص امنیتی موثر روتر D-Link DIR-850L و کمپانی D-Link راکه قابلیت سرویس دهی دارد را افشا نمود. وی یافته های خود را بدون دادن فرصتی به D-Link به منظور رفع اشکالات افشا کرد. D-Link در حال حاضر به روز رسانی هایش را برای هردونسخه A و B دستگاه های DIR-850L منتشر نموده است. این شرکت دستورالعمل های دقیقی برای به روز رسانی سیستم عامل ارائه نموده است که می گوید فرآیندی دومرحله ای است. آسیب پذیری های یافت شده به وسیله ی Kim، شامل عدم پشتیبانی از سیستم عامل، XSS، عدم پذیرش سرویس (Dos) و نقاط ضعفی است که می تواند برای اجرای دستورات دلخواه مورد سوء استفاده قرار بگیرد.

نقصی که در mylink وجود دارد می تواند در سرویسی باشد که اجازه می دهد تا کاربران برای دسترسی به دستگاه های D-Link از هرجایی از طریق اینترنت، به وسیله ی یک فرد مهاجم از راه دور و غیرقابل شناسایی، موردسوءاستفاده قرار بگیرند.

Kim به روز رسانی های سیستم عامل را تجزیه و تحلیل کرده است و به این نتیجه رسیده است که اکثر معایبی که اوشناسایی کرده ، رفع شده اند. درمجموع۱۸ شناسه CVE توسط MITER برای آسیب پذیری ها در روتورهای DIR-850L اختصاص داده شده است.

گردآورنده: حسین علیمرادی

نرم افزار CCleaner برای انتشار بدافزار، هک شد!

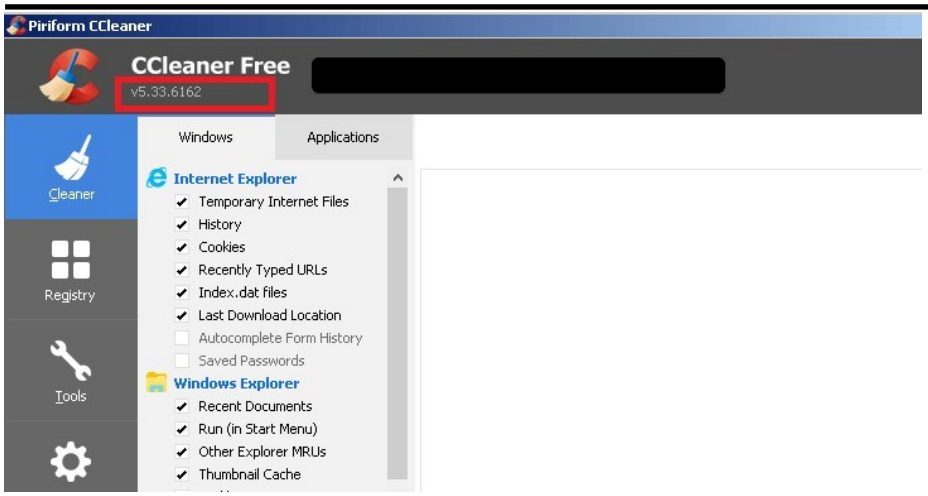
اگر شما نرم افزار محبوب CCleaner را در رایانه شخصی خود در بازه زمانی ۲۴ مرداد تا ۲۱ شهریور سال جاری از وب سایت رسمی شرکت سازنده این نرم افزار دانلود نموده یا آن را به روز کرده اید، توجه داشته باشید که رایانه شما در معرض خطر است.

نرم افزار CCleaner یک برنامه کاربردی محبوب است که به کاربران اجازه می دهد تا سیستم خود را برای بهینه سازی و افزایش کارایی، پاکسازی کنند و تاکنون بیش از ۲ میلیارد بار توسط کاربران دانلود شده است. شرکت Piriform، سازنده این نرم افزار است که به تازگی امتیاز این شرکت توسط کمپانی امنیتی Avast خریداری شد.

به گفته محققان امنیتی گروه Cisco Talos، سرورهای دانلود این نرم افزار که Avast آنها را میزبانی می‌کند؛ توسط برخی از هکرهای ناشناس مورد حمله قرار گرفتند. آنها نسخه اصلی نرم افزار را با یک بدافزار جایگزین نموده و به مدت یک ماه در بین میلیونها کاربر توزیع کرده اند.

این حادثه نمونه دیگری از حملات موسوم به زنجیره تامین است. در اوایل سال جاری، سرورهای به‌روزرسانی یک شرکت اوکراینی به نام MeDoc نیز به همین شیوه مورد تهاجم قرار گرفت که منجر به انتشار بدافزار Petya Ransomware در سرتاسر جهان شد.

Avast و Piriform هر دو تأیید کردند که نسخه ۵.۳۳.۶۱۶۲ پلتفرم ویندوز ۳۲ بیتی این نرم افزار و نسخه ۱.۰۷.۳۱۹۱ پلتفرم



Cloud آن تحت تاثیر این حمله قرار گرفته اند.

روز ۲۲ شهریور مشخص شد که نسخه آلوده CCleaner حاوی یک بدافزار چندلایه مخرب است که داده‌ها را از رایانه های آلوده سرقت نموده و آنها را به سرورهای کنترل و فرمان از راه دور مهاجم، علاوه بر این، هکرهای ناشناس، نسخه آلوده قابل نصب (۵.۳۳) را با استفاده از گواهینامه معتبر صادر شده توسط Symantec و الگوریتم DGA ، امضای دیجیتال نموده اند. به طوری که حتی اگر سرور مهاجم از دسترس خارج شود؛ الگوریتم DGA می تواند دامنه های جدیدی برای دریافت و ارسال اطلاعات سرقت شده، ایجاد کند.

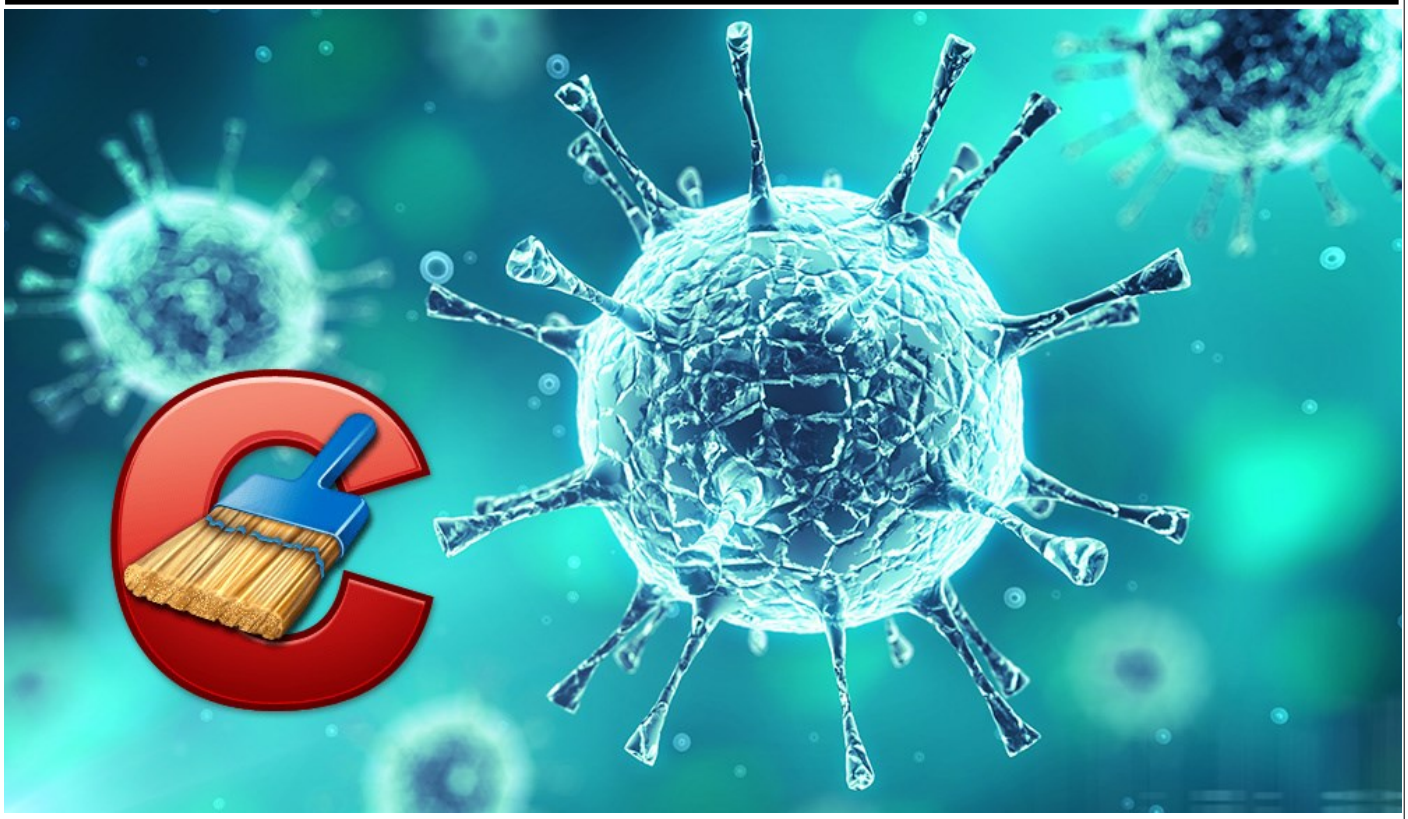
پل یانگ مدیر محصول Piriform می گوید: "تمامی اطلاعات سرقت شده، توسط الگوریتم base64 و با الفبای سفارشی؛ رمزگذاری و کد گذاری می‌شود. سپس اطلاعات کدگذاری شده به آدرس IP خارجی 216.216.x.x از طریق درخواست HTTPS POST ارسال می‌شود."

نرم افزار آلوده برای جمع آوری تعداد زیادی از داده‌های کاربر، نوشته شده است، از جمله: نام کامپیوتر (Computer Name)فهرست نرم افزارهای نصب شده، از جمله به‌روزرسانی ویندوز فهرست تمام فرآیندهای در حال اجرا در ویندوز آدرس IP و MAC سیستم قربانی اطلاعات اضافی مانند این که آیا فرایند با امتیازات مدیر اجرا می شود و اینکه آیا سیستم ۶۴ بیتی است یا خیر.

ادامه مطلب در صفحه بعد.

گردآورنده: محمدحسین خدامی

نرم افزار CCleaner برای انتشار بدافزار، هک شد! (ادامه...)



چگونه بدافزار را از رایانه حذف کنیم؟

طبق گفته محققان Talos، حدود ۵ میلیون نفر هر هفته CCleaner یا Crap Cleanerرا دانلود می‌کنند، بنابراین انتظار می‌رود بیش از ۲۰ میلیون نفر می توانند با نسخه مخرب این برنامه آلوده شده باشند.

گروه Talos گزارش داد: "تاثیر این حمله می تواند با توجه به تعداد بسیار زیاد سیستم‌های احتمالًا آلوده شده، چشمگیر باشد. بنابر ادعای شرکت سازنده، CCleaner ؛ بیش از ۲ میلیارد بار از نوامبر سال گذشته در سراسر جهان دانلود شده است، همچنین نرخ ۵ میلیون دانلود در هفته توسط کاربران جدید را نیز باید به این تعداد اضافه کرد"

با این حال، شرکت Piriform برآورد کرده است که تا ۳ درصد از کاربران آن (حدود ۲.۲۷ میلیون نفر) براثر نصب مخرب تحت تأثیر قرار گرفته باشند.

به کاربران آسیب دیده قویاً توصیه می شود تا نرم افزار CCleaner خود را به نسخه ۵.۳۴ یا بالاتر ارتقا دهند تا رایانه هایشان از این بدافزار در امان بماند. آخرین نسخه برای دانلود اینجا در دسترس است.

https://www.piriform.com/ccleaner/download

گردآورنده: محمدحسین خدامی

حمله هکرها به شرکت‌های بخش انرژی آمریکا و اروپا

طبق گزارش محققان مرکز امنیتی Symantec، به تازگی شرکت‌های بخش انرژی اروپا و آمریکا، طی یک سری عملیات جاسوسی سایبری از سوی هکرها مورد هدف و حمله قرار گرفته‌اند. تعدادی از این حملات، سیستم‌های مرکزی کنترل عملیات این شرکت‌ها را دچار آسیب کرده‌اند.

چهارشنبه ۶ آگوست ۲۰۱۷، Symantec گزارش داد که برای نفوذ به سازمان‌های فعال بخش انرژی در کشورهای آمریکا، ترکیه و سوئیس، از ایمیل‌های مخرب استفاده شده است؛ البته احتمال آسیب کشورهای دیگر نیز از این طریق، محتمل است.

طبق گزارش Eric Chien، از محققان امنیتی شرکت Symantec، این حملات سایبری که در اواخر سال ۲۰۱۵ میلادی آغاز شده و در آوریل سال جاری به بالاترین تعداد خود رسیده، به احتمال بسیار زیاد توسط دولت‌های خارجی پشتیبانی شده و البته برخی آن را به گروه هک Dragonfly نسبت می‌دهند.

تحقیقات مزبور همچنین به این نکته هشدار می‌دهند که مراکز صنعتی همچون تامین‌کنندگان برق و سایر خدمات حوزه انرژی، براحتی در معرض هجوم حملات سایبری قرار دارند. این حملات، در صورت وقوع یک اختلاف بزرگ ژئوپلتیک، می‌توانند برای مقاصد مخرب به کار گرفته شوند.

در ژوئن سال جاری دولت آمریکا به شرکت‌های صنعتی هشدار داد که بخش‌های انرژی و هسته‌ای این کشور در معرض حمله هکرها قرار دارند. این هشدار که خبرگزاری رویترز نیز به آن اشاره کرد به این نکته اشاره می‌کرد که هکرها با ارسال ایمیل‌های فیشینگ، سعی در دسترسی به شبکه‌های موردنظرشان در بخش انرژی داشته‌اند.

Chien می‌نویسد: "عقیده من این است که در هشدارهای داده شده توسط دولت آمریکا نیز، ردپای Dragonfly دیده می‌شود. ده‌ها شرکت فعال بخش انرژی هدف این حمله قرار گرفته‌اند. این سطح از دسترسی، به این معناست که هدف از این حمله سایبری، خرابکاری گسترده در شبکه توزیع برق بوده است."

در نقطه مقابل، برخی دیگر از محققان نسبت به یافته‌ها و گفته‌های Chien مردّداند. به طور مثال Robert M.Lee موسس Dragos، شرکت امنیتی زیرساخت‌های حیاتی، می‌گوید: "حملات صورت گرفته آنقدری جدی نبودند که بتوانند بر شبکه برق خانگی تاثیرگذار باشند، در نتیجه نیازی به اعلان خطر و هشدار نیست."

Dragonfly از سال ۲۰۱۱ تا ۲۰۱۴ فعالیت می‌کرد. در سال ۲۰۱۴ پیرو انتشار اخبار حملات آنها از سوی چندین کمپانی سایبری، فعالیت این گروه ظاهرا متوقف شد. این گروه که با نام‌های Energetic Bear یا Koala نیز شناخته می‌شود، به زعم متخصصین حوزه امنیت، تحت نظر دولت روسیه فعالیت می‌کند. در گزارشی که توسط Symantec ارائه شده، صراحتا از نام و نقش دولت روسیه یاد نشده است، اما به این مساله اشاره شده که هکرها از رشته کدهایی به زبان روسی استفاده کرده‌اند. هرچند که از کدهایی در زبان‌هایی غیر از زبان روسی مانند فرانسوی نیز، احیانا برای ایجاد دشواری در فرآیند شناسایی آنها، استفاده شده است.

گردآورنده: شیوا بهادری

هکرهای چینی در حال استفاده از جاسوس افزار xRAT

ابزار جاسوسی جدیدی که احتمال می‌رود توسط هکرهای چینی توسعه و استفاده می‌شود توسط محققان امنیتی شناسایی شده است. این بدافزار جاسوسی موبایل با نام xRAT که بخاطر هدف قرار دادن گروه‌های سیاسی با طیف وسیعی از راهکارهای جمع آوری اطلاعات همراه است، آن را تبدیل به ابزاری موثر برای گروه هکرهای جاسوس کرده است.

از ماه آپریل بیش از ۶۰ نمونه یکتا از xRAT توسط محققان امنیتی شرکت LookOut کشف شده است. بدافزار xRAT شباهت‌های زیادی با بدافزارهای Xsser/mRAT دارد که در سال ۲۰۱۴ در هنگ کنگ بر علیه طرفداران دموکراسی مورد استفاده قرار گرفت.

در چند ماه اخیر، محققان امنیتی یک ورژن جدید از نسخه‌ی اندروید بدافزار mRAT را کشف کردند. این کشف نشان می‌دهد که همچنان هنوز هم خانواده‌ی این بدافزار در حال توسعه و استفاده در پروژه‌های مختلف است.

محققان امنیتی شرکت LookOut در بلاگ خود بیان کردند: "شباهت‌های زیاد بین mRAT و xRAT نشان می‌دهد که این بدافزار توسط یک مجموعه، توسعه داده می‌شود. سرورهای کنترل و فرمان بدافزار xRAT همچنان با بدافزار سیستم عامل ویندوز مرتبط است و شامل عملگرهای مخربی در پشت این تهدیدات همانند حملات چند پلتفرمی بر علیه کامپیوترها و موبایل می‌باشد."

Michael Flossman به Cyberscoop اعلام کرد که: "در ابتدا هنگامی که ما شروع به تحقیق در خصوص xRAT کردیم، ارجاعات ما با توجه به ترکیبی از کامنت‌ها در کد، انواع برنامه‌های تروجان و اطلاعات مربوط به محل و whois سرور کنترل و فرمان، نشان داد که عامل اصلی در پشت این موارد به احتمال زیاد چین می‌باشد. تحقیقات بعدی، ارتباط قوی با بدافزار mRAT را نشان داد. این دست آورد نظریه‌ی ما را درباره‌ی کسانی که در پشت mRAT قرار دارند را تقویت کرد."

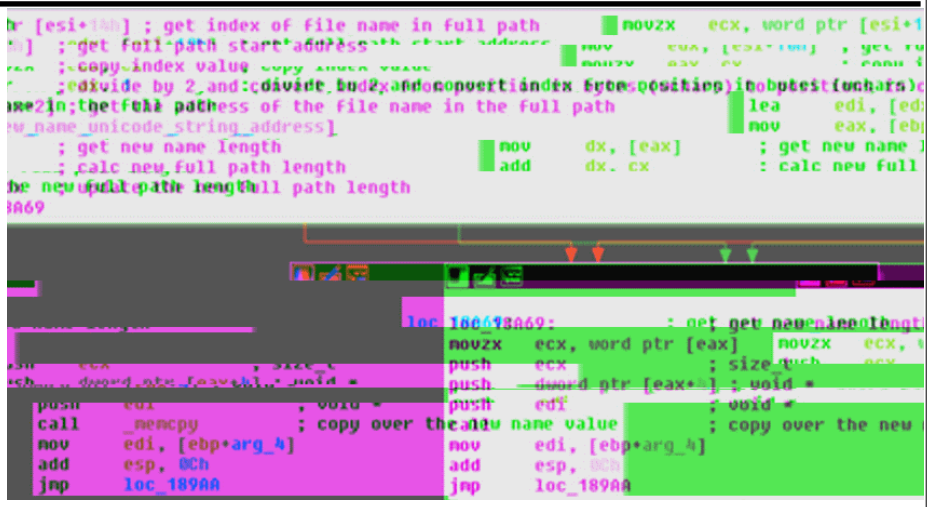
بدافزار xRAT دارای طیف وسیعی از ویژگی‌های سرقت اطلاعات می‌باشد. این بدافزار همچنین اطلاعات موجود در برنامه-های چت چینی همانند QQ و WeChat را جستجو می‌کند. این برنامه قابلیت سرقت اطلاعات مرورگر، ابرداده‌های دیوایس‌ها (شامل مدل، ID، شماره سیم کارت و سازنده)، پیام‌های متنی، مخاطبین، تاریخچه-ی تماس‌ها، اطلاعات Wi-Fi، اطلاعات احراز هویت ایمیل، موقعیت جغرافیایی دیوایس، اطلاعات سیم کارت و غیره را دارد.

این بدافزار همچنین قابلیت اجرای تابع خودکشی را دارد. در صورت اجرای تابع خودکشی این بدافزار قادر است تا پوشه نصب خود را به طور کامل حذف نماید و از تشخیص جلوگیری کند. هکرها می‌توانند این بدافزار را با کنترل از راه دور هدایت کنند و تصاویر و فایل‌های صوتی موجود در حافظه‌ی SD را حذف نمایند. همچنین این بدافزار قابلیت پاک کردن کامل دیوایس و بیشتر را نیز دارد.

Flossman بیان نمود: "بدافزار mRAT همچنان در تلفن‌های همراه فعال می‌باشد. باوجود اینکه دارای ظرفیت مراقبتی از خود می‌باشد، از سه سال پیش در کانون توجه قرار گرفته است... توسعه دهندگان این بدافزار به وضوح بی‌رحم هستند. این امر مشابه چیزی است که آن‌ها در طول توسعه‌ی mRAT یادگرفته‌اند و آن را در توسعه‌ی xRAT گنجانده‌اند."

گردآورنده: محمد مرتضوی

باگ در کرنل PsSetLoadImageNotifyRoutine ویندوز



توسعه دهندگان بدافزارها می‌توانند از یک خطای برنامه نویسی در هسته ویندوز برای جلوگیری از تشخیص آنان توسط برنامه‌های امنیتی سو استفاده کنند و ماژول‌های مخرب را در هنگام اجرا بارگذاری کنند. باگی که برروی PsSetLoadImageNotifyRoutine تاثیر می‌گذارد، یکی از مکانیسم‌های سطح پایین می‌باشد که برخی از راه حل‌های امنیتی برای شناسایی زمانی که کد در کرنل ویا فضای کاربر بارگذاری می‌شود مورد استفاده قرار می‌دهند.

مشکل این است که حمله کننده می‌تواند از این باگ در زمانی که PsSetLoadImageNotifyRoutine یک نام ماژول نامعتبر را بر می‌گرداند، سو استفاده کند. این باگ اجازه می‌دهد که مهاجم بدافزار را به یک عملیات قانونی تبدیل کند.

این باگ تمامی ویندوزهایی را که در ۱۷ سال گذشته انتشار یافته‌اند را تحت تاثیر قرار می‌دهد.

زمانی که محققان enSilo کد کرنل ویندوز را بررسی می‌کردند این موضوع را در اوایل امسال کشف کردند. Omri Misgav محقق امنیتی این شرکت و کسی که پرده از این باگ برداشت می‌گوید که این باگ تمامی نسخه‌های ویندوز را از ویندوز ۲۰۰۰ به بعد تحت تاثیر قرار می‌دهد.

آزمایش های Misgav نشان داد که این خطای برنامه نویسی تا آخرین نسخه‌ی ویندوز ۱۰ همچنان باقی است.

مایکروسافت مکانیسم اطلاع رسانی PsSetLoadImageNotifyRoutine را به عنوان راهی برای اطلاع رسانی به توسعه دهندگان اپلیکیشن‌ها از درایورهای تازه ثبت شده معرفی کرده است. این سیستم همچنین می‌تواند هنگامی که یک تصویر PE در حافظه مجازی بارگذاری می‌شود را تشخیص دهد، این مکانیزم نیز با نرم افزار آنتی ویروس به عنوان راهی برای شناسایی برخی از انواع عملیات مخرب، یکپارچه شده است.

مایکروسافت به این موضوع به عنوان یک موضوع امنیتی نگاه نمی‌کند.

در حال حاضر، بزرگترین مشکل این است که نرم افزارهای امنیتی به این روش متکی هستند تا بتوانند برخی از انواع عملیات مخرب را شناسایی کند.

Misgav با ایمیل برای Bleeping Computer بیان نمود که: "ما هیچ نرم افزاری امنیتی خاص را آزمایش نکرده‌ایم. ما آگاه هستیم که بعضی از فروشندگان از این مکانیزم استفاده می کنند، با این حال در این زمان نمی‌توانیم بگوییم چگونه استفاده از اطلاعات معیوب [PsSetLoadImageNotifyRoutine] بر آنها تاثیر می گذارد."

ما همچنین با MSRC (واحد پاسخگویی مایکروسافت) در خصوص این مشکل در ابتدای سال ارتباط برقرار کردیم. برخی از منابع آنلاین نشان می دهد که این اشکال تا حدودی شناخته شده است، اما ما تنها می‌توانیم دلیل اصلی آن را توضیح دهیم و مفاهیم کامل تاکنون به طور جزئی توضیح داده نشده‌اند.

برای دستیابی به توضحیات فنی و جزئیات پست وبلاگ enSilo به آدرس زیر می‌توان مراجعه نمود.

گردآورنده: محمد مرتضوی

Kharazmi CERT Coordinator Center

مرکز آپا دانشگاه خوارزمی

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

رییس مرکز:

دکتر امید مهدی عبادتی

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

وب سایت:

http://cert.khu.ac.ir/

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن یزدی نژاد