خبرنامه الکترونیکی ۴۵

مرکز تخصصی آپا دانشگاه سمنان

شماره چهل و پنجم، سال چهارم، بهمن ۱۴۰۰ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

باج افزار چیست؟

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

مرکز آپا دانشگاه سمنان

"دنیای خود را امن کنید"

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

خبر

فیسبوک توکنی ارائه می‌دهد که باعث افشای اطلاعات می‌شود

این هفته Brave اعلام کرد که نصب افزونه محبوب کروم که L.O.C نام دارد را بلاک می‌کند، زیرا این افزونه داده‌های فیسبوک کاربران را در معرض خطر سرقت احتمالی قرار می‌دهد.

فرانسوا ماریر مهندس امنیت در Brave، در یک پست مشکلات گیت‌هاب می‌گوید: «اگر کاربری قبلاً وارد فیسبوک شده باشد، نصب این افزونه به طور خودکار به سرور شخص ثالث اجازه دسترسی به بعضی از داده‌های فیسبوک کاربر را می‌دهد. API استفاده شده توسط این افزونه باعث نمی‌شود که فیسبوک قبل از صدور توکن دسترسی به برنامه، درخواست مجوز را به کاربر نشان دهد.»

اما Loc Mai توسعه‌دهنده این افزونه گفت: که افزونه او همان طوری که در سیاست حفظ حریم خصوصی ذکر شده است اطلاعاتی جمع‌آوری نمی‌کند. این افزونه تاکنون حدود ۷۰۰۰۰۰ کاربر دارد.

در ادامه Mai توضیح داد که «افزونه داده‌های کاربران را جمع‌آوری نمی‌کند مگر اینکه کاربر به یک کاربر premium تبدیل شود و UID کاربر که برای هر شخص منحصر به فرد است، تنها چیزی است که جمع می‌کند.»

Mai گفت که افزونه توکن را به صورت محلی تحت localStorage.touch. ذخیره می‌کند. این نشان دهنده خطر امنیتی می‌باشد ولی دلیل بر تخلف نیست. L.O.C از طریق فروشگاه وب کروم همچنان در دسترس خواهد بود.

اما یک توسعه‌دهنده مخرب می‌تواند داده‌های فیسبوک را با استفاده از همین روش دسترسی جمع‌آوری کند زیرا فیسبوک یک توکن plain-text را ارائه می‌دهد که دسترسی بالایی را فراهم می‌کند، طوری که زک ادواردز، محقق امنیتی، نام آن را «حالت خدا[1]» می‌گذارد.

1-god mode

Mai در یک ایمیل به The Register توضیح داد که Graph API فیسبوک برای کار کردن نیازمند به توکن دسترسی کاربر است. برای به دست آوردن آن توکن - به طوری که کاربران افزونه بتوانند پردازش داده‌های فیسبوکشان را به طور خودکار انجام دهند (مانند دانلود پیام‌های خود) - افزونه یک درخواست GET را به Creator Studio برای فیسبوک ارسال می‌کند. این درخواست یک توکن دسترسی به افزونه را برای کاربر وارد شده در فیسبوک برمی‌گرداند و اجازه تعامل برنامه‌ای بیشتر با داده‌های فیسبوک را می‌دهد.

Mai در پاسخ به پست گیت‌هاب barve شرح داده است که «توکن دسترسی در HTML آن صفحه است. هر کاربر فیسبوک واقعاً می‌تواند به

view-source: https://business.facebook.com/creatorstudio/home

برود و توکن دسترسی را در آنجا مشاهده کند.»

ادواردز به The Register گفت: «فیسبوک در سال ۲۰۱۸ با رسوایی تقریباً مشابهی مواجه شد زمانی که ۵۰ میلیون حساب فیسبوک به دلیل افشای توکن حذف شدند. با این حال به نظر می‌رسد فیسبوک این توکن توزیع داده را یک ویژگی می‌داند نه یک اشکال.»

مای یک کپی از ایمیل ۹ آوریل ۲۰۱۹ را به The Register ارائه کرد که از که همان نوع دسترسی به داده‌ها را فعال می‌کرد. پاسخ امنیتی فیسبوک این بود: «در این مورد، مسئله‌ای که شما توضیح داده‌اید در واقع فقط عملکرد مورد نظر است و بنابراین واجد شرایط دریافت جایزه نیست.»

ادواردز می‌گوید: «به نظر می‌رسد فیسبوک از سال ۲۰۱۸ درس خود را نگرفته است و همچنان در حال افشای یک توکن plain-text god mode برای هر کاربر است، در صفحه‌ای که توسعه‌دهندگان خاص از آن اطلاع دارند. فیسبوک این ویژگی را یک ویژگی می‌نامد، اما آیا فیسبوک زمانی که اولین توسعه‌دهنده افزونه داده‌های صفحات و کاربران بی‌شماری را جمع‌آوری کرده و دزدیده باشد، اعتراف خواهد کرد که این یک باگ است دقیقاً مثل مشکلات سال ۲۰۱۸؟»

The Register از brave پرسید که آیا قصد دارد در ممنوعیت L.O.C تجدید نظر کند. بر اساس توضیح Mai از آنچه در حال وقوع است. یکی از سخنگویان Brave گفت: «ما در حال کار با نویسنده افزونه روی برخی تغییرات در افزونه هستیم تا بتوان آن را در Brave رفع انسداد کرد.»

افزونه نامناسب هنوز یک مشکل است

ادواردز گفت که شرایط خدمات فیسبوک در اینجا ناکافی است زیرا در حالی که شرکت اصرار دارد مردم از پلتفرم برنامه خود استفاده کنند، اما مانع از استفاده افراد از افزونه‌های مرورگر نمی‌شود و این شکافی که داده‌های کاربر را افشا می‌کند، با نحوه کار در حال حاضر افزونه‌های کروم تشدید می‌شود.

طبق توضیح ادواردز، برنامه‌های افزودنی کروم می‌توانند مجوزهایی را در دامنه‌ای که شما کنترل می‌کنید و دامنه‌ای دیگر که شما کنترل نمی‌کنید درخواست کند، هنگام نصب، یک برگه مرورگر را باز کند که فرصتی را فراهم می‌کند برای استخراج توکن API و session ID ها برای انواع مختلف برنامه‌ها.

ادواردز توضیح داد که «فیسبوک یک مجوز وب قدیمی کدگذاری شده در صفحه creator studio خودش دارد که برای کسی که یکی از این افزونه‌ها را کنترل می‌کند ممکن می‌سازد بدون ثبت‌نام در برنامه توسعه‌دهنده فیسبوک و با استفاده از ویژگی‌هایش، صدها هزار توکن فیسبوک را استخراج کند.»

او افزود: «اساساً، فیسبوک نمی‌تواند یک افزونه را تحریم کند، حتی اگر فیسبوک بداند که افزونه نباید اجازه درخواست مجوز در facebook.com را داشته باشد و اگر تیمشان فکر کند که این افزونه مخرب است.»

The Register از فیسبوک در مورد وضعیت سؤال کرده است و اینکه آیا همان طور که ادواردز پیشنهاد می‌کند، این شرکت قصد دارد تمام توکن‌های به دست آمده از نقطه پایانی Creator Studio خود را باطل کند یا خیر. یکی از سخنگویان meta ایمیلی ارسال کرد و گفت: «ما در حال بررسی این ادعاها هستیم و برای حفظ سیاست‌های خود و حفاظت از اطلاعات افراد، اقدامات لازم را انجام خواهیم داد.»

توصیه‌نامه حیاتی VMware: محصولات را به‌روز کنید

وی‌ام‌ور[1] برای رفع آسیب‌پذیری محصولات ESXi، Workstation و Fusion از جمله نسخه Cloud Foundation، به‌روزرسانی حیاتی منتشر کرده است. مهاجم با بهره‌گیری از این آسیب‌پذیری‌ها می‌تواند به کارهای جاری در محیط مجازی سازمان‌ها دسترسی پیدا کند.

امتیاز حساسیت این باگ‌ها در بازه بین ۵.۳ تا ۸.۴ در مقیاس CVSS قرار می‌گیرند که به معنی «متوسط» یا «مهم» بودن آنها است، اما طبق گفته وی‌ام‌ور، ترکیب این باگ‌ها می‌توانند منجر به نتایج بدتری شود: «ترکیب این اشکالات می‌تواند باعث حساسیت بالاتری شود، به همین دلیل، سطح حساسیت این [توصیه‌نامه]، بحرانی [یا حیاتی] قرار داده شده است.» وی‌ام‌ور خاطرنشان می‌کند که وصله کردن محصولات، سریع‌ترین راه برای حل مشکلات است. اما سازمان‌ها می‌توانند به عنوان یک راه حل موقت، کنترلرهای USB ماشین‌های مجازی را حذف کنند، هر چند ممکن است این کار در مقیاس بزرگ عملی نباشد، ضمن اینکه نمی‌تواند به خوبیِ به‌روزرسانی، مشکل را حل کند.

این آسیب‌پذیری‌ها عبارت اند از:

CVE-۲۰۲۱-۲۲۰۴۰: باگ استفاده پس از آزادسازی در کنترلر XHCI USB (CVSS 8.4)

CVE-2021-22041: آسیب‌پذیری واکشی مضاعف در کنترلر XHCI USB (CVSS 8.4)

CVE-2021-22042: آسیب‌پذیری دسترسی بدون مجوز در ESXi settingsd (CVSS 8.2)

CVE-2021-22043: آسیب‌پذیری از نوع TOCTOU (شرایط رقابتی در چک کردن یک شرط و استفاده از نتیجه این چک) در ESXi settingsd (CVSS 8.2)

CVE-2021-22050: باگ منع سرویس HTTP POST کُند (CVSS 5.3)

1-VMware

باگ‌های کنترلر USB

دو باگ اولی که دارای درجه حساسیت «مهم» هستند، به کنترلر یو اس بی ESXi، Fusion و Workstation مربوط می‌شوند. فرد بدخواه با داشتن دسترسی ادمین محلی روی یک ماشین مجازی می‌تواند در قالب پردازه VMX در حال اجرا روی هاست، کد اجرا کند. پردازه VMX در VMKernel قرار دارد و مسئول مدیریت ورودی/خروجی تجهیزاتی است که از لحاظ کارایی، نقش حیاتی ندارند.

مشکل امنیتی «settingsd»

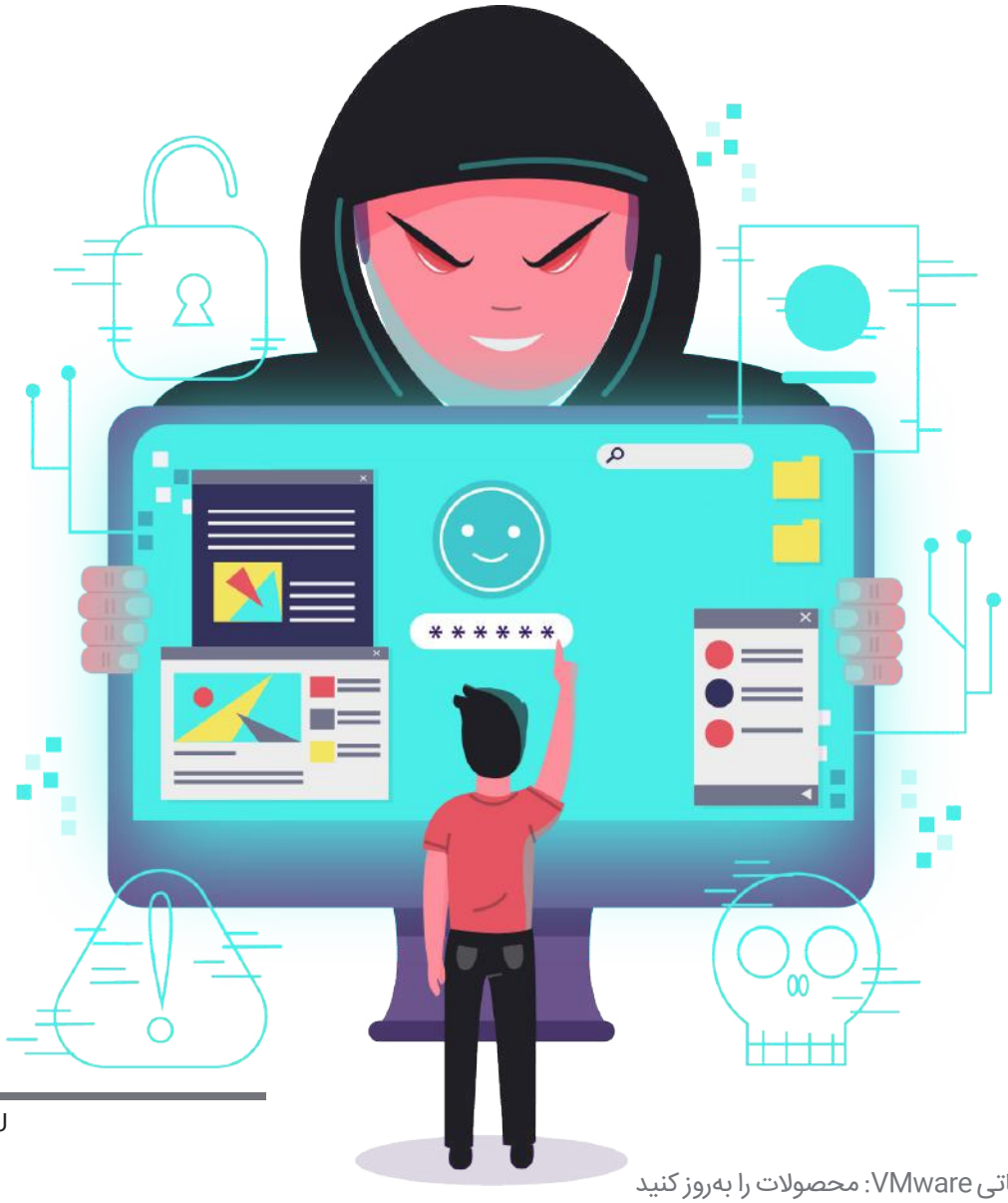
دو اشکال بعدی نیز از درجه مهم هستند. آنها دستور settingsd را تحت تأثیر قرار می‌دهند که مسئول تنظیمات، لاگ‌های هاست و ... است. باگ اول (CVE-2021-22042) به علت دسترسی بدون مجوز VMX به تیکت‌های مجازسنجی settingsd رخ می‌دهد.

باگ دوم، از نوع «زمان بررسی-زمان استفاده[1]» است و می‌تواند با اولی ترکیب شود. این باگ ناشی از نحوه مدیریت فایل‌های موقت است. مهاجمی که به settingsd دسترسی دارد، می‌تواند با استفاده از این باگ و با نوشتن فایل‌های دلخواه دسترسی خود را ارتقاء دهد.

اشکال سطح متوسط در ESXi

آخرین باگ، تنها پلتفرم ESXi را تحت تأثیر قرار می‌دهد و می‌تواند به مهاجم امکان ایجاد شرایط منع سرویس را بدهد. مهاجم می‌تواند با ارسال چند درخواست، سرویس rhttpproxy را تحت فشار قرار دهد. برای بهره‌برداری موفق، مهاجم باید از طریق شبکه به ESXi دسترسی داشته باشد.

هرچند به گفته وی‌ام‌ور در دنیای واقعی هیچ حمله‌ای مشاهده نشده است که این باگ‌ها را هدف بگیرد، اما تاریخ نشان می‌دهد که احتمال دارد شرایط به سرعت تغییر کند، بنابراین مدیران شبکه باید به سرعت وصله‌ها را اعمال کنند.



1-TOCTOU

مرکز آپا دانشگاه سمنان

آموزش

باج افزار چیست؟

باج افزارها نوعی از بدافزارهای مخرب هستند که به سیستم‌های را یانه ای (کامپیوتر، لپ تاپ، تلفن همراه و...) قربانی حمله کرده و دسترسی کاربر به اطلاعاتش را از بین می‌برند و در ازای باز کردن دسترسی درخواست پرداخت مبلغ به حساب طراح باج افزار می‌کنند. طراحان باج افزار به دلیل استفاده از روش دریافت پول‌های مجازی به راحتی قابل پیگیری و شناسایی نیستند. بسیاری از باج افزارها علاوه بر رمزگذاری فایل‌ها اقدام به قفل کردن هارددیسک نیز می‌کنند. بنابراین قربانی این نوع حمله یا باید قید اطلاعات خود را زده و اقدام به فرمت هارد دیسک خود نماید و یا اینکه مبلغ خواسته شده را به حساب هکر واریز نماید. هرچند که هیچ تضمینی وجود ندارد که حتی در صورت پرداخت باج خواسته شده، هکر کلید رمزگشایی را در اختیار کاربر قرار دهد.

چه کسانی هدف باج افزارها قرار میگیرند؟

به صورت تئوری، هر سیستم دیجیتال (شامل تمام رایانه‌ها، لپ تاپ‌ها، موبایل‌ها و...) ممکن است مورد حمله باج‌افزارها قرار گیرد. لیکن از آنجا که معمولا هدف اصلی طراحان باج‌افزار دریافت پول از قربانیان است، می‌بایست به سیستم‌هایی حمله شود که اطلاعات بسیار با ارزشی دارند مانند سازمان‌ها، شرکت‌ها، مراکز دولتی و درمانی و... چرا که بسیاری از کاربران عادی و خانگی ممکن است به راحتی قید اطلاعات خود را بزنند و اقدام به فرمت هارد دیسک دستگاه نمایند؛ این موضوع در خصوص سازمان‌ها و شرکت‌ها، احتمالا برعکس خواهد بود و معمولا آنها حاضرند در ازای دسترسی مجدد به اطلاعات خود هزینه‌های فراوانی را متحمل شوند. بنابراین به صورت کلی می‌توان اهداف باج‌افزارها را به صورت زیر دسته‌بندی کرد:

- شرکت‌های کوچک و متوسط
- سازمان‌های دولتی
- مراکز آموزشی
- مراکز درمانی
- موسسات مالی و بانکی (به دلیل دارا بودن سیستم بکاپ‌گیری پیشرفته احتمال پرداخت باج کاهش می‌یابد.)
- سایر کاربران

تاریخچه باج افزارها

در چند سال اخیر واژه باج‌افزار در رسانه‌ها بسیار بازتاب داشته است لیکن جالب است بدانید که این نوع از بدافزارها دارای سابقه تاریخی بسیار قدیمی‌تری هستند. در این قسمت به بیان تاریخچه کوتاهی از مهمترین باج‌افزارهای منتشر شده خواهیم پرداخت.

همانطور که در تصویر مقابل مشخص است، باج افزارها بسیار قدیمی‌تر از چیزی هستند که عموما تصور می‌شود. به عنوان مثال اولین بدافزار کشف شده، مربوط به سال ۱۹۸۹ میلادی و معادل ۱۳۶۸ هجری شمسی می‌باشد، که این موضوع نشان می‌دهد که این دسته از بدافزارها دارای سابقه تاریخی زیادی هستند.

باج افزار AIDS که درواقع یک تروجان بوده است پس از آلوده کردن سیستم، اقدام به رمزنگاری فایل‌ها و قفل کردن درایو C کامپیوتر کرده و سپس از قربانی درخواست می‌کرد که از طریق پست، مبلغ ۱۸۹ دلار را به یک آدرس در پاناما ارسال کند. جالب اینجاست که روش کلی عملکرد این باج افزار تقریبا مشابه، نسخه‌های امروزی است با این تفاوت که امروزه طراحان باج‌افزارها به جای پول نقد، درخواست رمز ارز می‌نمایند که همین امر باعث پیچیدگی و دشواری، پی‌جویی و ردیابی مجرمان شده است.

دو دلیل برای افزایش باج افزارها

۱. حملات باج‌افزارها هم اکنون از حملات نشت اطلاعات پیشی گرفته؛ و دلیل آن اجرای ساده و سودده‌بودن‌این‌حملات‌برای‌صاحبان‌آنهاست.
۲. سخت بودن و گاها ناممکن بودن امکان شناسایی باجگیران از طریق ردیابی مبالغ پرداختی، با توجه به استفاده آنها از پول‌های مجازی مانند بیت کوین

آینده باج افزارها

۱. هدفمندتر شدن حملات باج افزارها
۲. اضافه شدن قابلیت‌های پیشرفته فرار از سد امنیتی محصولات و در نتیجه دشوارتر شدن شناسایی آنها
۳. هدف قرار گرفتن دستگاه‌های همراه و اینترنت اشیا بیش از قبل

دسته‌بندی باج افزارها

تاکنون دسته‌بندی‌های متفاوتی از باج افزارها ارائه شده است که ما در اینجا به چند مورد آن اشاره می‌کنیم:

باج‌افزار رمزنگاری: این نوع از باج‌افزارها دارای ویژگی‌های کلی زیر هستند:

- پوشه‌ها و فایل‌های شخصی (اسناد، صفحات گسترده، تصاویر و ویدئوها) را رمزنگاری می‌کند.
- فایل‌های تحت تاثیر زمانی که رمزگذار ی شدند، حذف می‌شوند و کاربران عموما با یک فایل متنی حاوی دستورالعمل پرداخت پول درون فولدرهای حاوی‌فایل‌های‌غیرقابل‌دسترس،مواجه‌می‌شوند.
- قربانی ممکن است تنها زمانی این مسئله را متوجه شود که بخواهد یکی از این فایل‌ها را باز کند.

- اغلب نرم‌افزارهای رمزنگاری و البته نه همه آنها یک «صفحه قفل» مانند تصاویر زیر را نشان می‌دهند:

باج افزار قفل صفحه[1]: این دسته نیز دارای ویژگی‌های کلی زیر است:

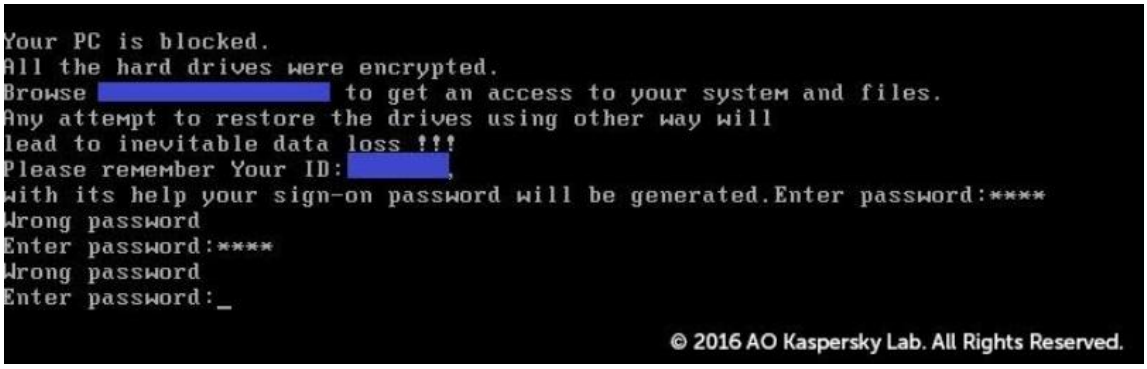
- این باج افزار صفحه کامپیوتر را قفل کرده و درخواست باج می‌کند.
- این باج افزار یک تصویر تمام صفحه را نشان داده و سایر پنجره‌ها را بلوکه می‌کند.
- هیچ فایل شخصی رمز نمی‌شود.

باج افزارهای ترس[2]: این باج افزار برخلاف نامش زیاد ترسناک نیست. این بدافزار امنیتی به نوعی از اطلاعات فنی رایانه کلاهبرداری می‌کند. ممکن است یک پیام پاپ آپ[3] دریافت کنید که ادعا می‌کند بدافزاری در رایانه کشف کرده و تنها راه خالص شدن از شر آن، رسیدگی و پرداخت آن است و اگر کاری انجام ندهید و به آن گوش نکنید به احتمال زیاد همچنان با پاپ آپ بمباران می‌شوید. در حالی که تمامی پرونده‌های شما در امنیت کامل هستند. درواقع این نوع باج افزار با ایجاد ترس، از قربانی باج‌گیری می‌کند.

1-WinLocker
2-Scareware
3-pop up

باج افزار MBR[1]: این دسته نیز دارای ویژگی‌های کلی زیر است:

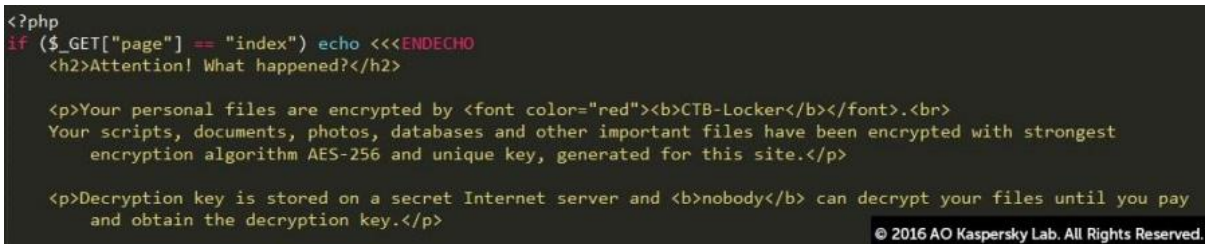
- MBR بخشی از حافظه رایانه است که به سیستم‌عامل اجازه بالا آمدن می‌دهد.
- باج افزار MBR، MBR کامپیوتر را تغییر می‌دهد به طوریکه فرآیند راه اندازی طبیعی دچار اختلال می‌شود.
- در عوض، پیغام درخواست باج بر روی صفحه نمایش داده می‌شود.



باج افزاری که سرورهای وب را رمزنگاری می‌کند:

این دسته نیز دارای ویژگی‌های کلی زیر است:

- این باج افزار سرورها را هدف قرار داده و تعداد زیادی از فایل‌های موجود بر روی آن را رمزگذاری می‌کند.
- آسیب‌پذیری‌های شناخته شده در سیستم‌های مدیریت محتوا[2]، اغلب برای گسترش باج افزار در وب سرویس‌ها استفاده می‌شوند.



باج افزار دستگاه موبایل (اندروید): این دسته نیز دارای ویژگی‌های کلی زیر است:

- دستگاه‌های موبایل (اکثرا اندروید) می‌توانند از طریق downloads by drive[3] آلوده شوند.
- همچنین آنها می‌توانند از طریق برنامه‌های جعلی آلوده شوند که به عنوان سرویس‌های مشهور مانند Adobe Flash یا آنتی ویروس خود را جا می‌زنند.

1-Record Boot Master

2-CMS - Systems Management Content

۳- برنامه‌هایی که به طور خودکار بدون رضایت یا آگاهی کاربر دانلود می‌شوند

آیا باید با باج‌گیرها همکاری کرد؟

اساسا چون تضمینی برای حل مشکل نیست، هرگز پرداخت باج پیشنهاد نمی‌شود. همچنین برخی موارد وجود دارند که می‌توانند به طور تصادفی ایجاد مشکل نمایند. برای مثال، اشکالاتی در بدافزار می‌تواند وجود داشته باشد که داده‌های رمز شده را حتی با وجود کلید درست، غیرقابل بازیابی می‌سازند. علاوه بر این اگر باج پرداخت شود، این کار به مجرمان سایبری اثبات می‌نماید که باج افزار موثر است. در نتیجه، مجرمان سایبری به فعالیت خود ادامه داده و به دنبال راه‌های جدید برای سوء استفاده از سیستم‌هایی خواهند بود که منجر به آلودگی‌های بیشتر و ورود پول بیشتر در حساب‌هایشان شود.

یک حمله باج‌افزاری چگونه کار می‌کند؟

در گذشته عموماً حملات باج‌افزاری از طریق پیوست ایمیل‌ها رخ می‌داد که فایل پیوست می‌توانست یک فایل اجرایی، آرشیو یا یک تصویر باشد. امروزه علاوه بر پیوست‌های ایمیل، موارد دیگری همچون فایل‌های موجود در شبکه‌های اجتماعی نیز به عنوان روشی برای آغاز حمله باج افزاری شناخته شده است. هنگامی که پیوست باز می‌شود، باج‌افزار در سیستم کاربر منتشر می‌شود. همچنین مجرمان سایبری می‌توانند بدافزار را در وب‌سایت‌ها جاسازی کنند و هنگامی که یک کاربر به طور ناخواسته از وب‌سایت بازدید می‌کند، بدافزار در سیستم کاربر منتشر می‌شود.

یکی از ویژگی‌هایی که معمولا باج‌افزارها دارند این است که، آلودگی بلافاصله برای کاربر آشکار نمی‌شود و بدافزار در سکوت و در پس زمینه عمل می‌کند تا زمانیکه مکانیزم قفل داده‌ها یا قفل سیستم مستقر شود. سپس پیغامی به کاربر نشان داده می‌شود و به کاربر می‌گوید که داده‌ها قفل شده‌اند و برای باز کردن مجدد آنها درخواست باج می‌کند. پس از آن دیگر خیلی دیر است که بخواهید داده‌ها را از طریق هرگونه اقدام امنیتی محافظت کنید.

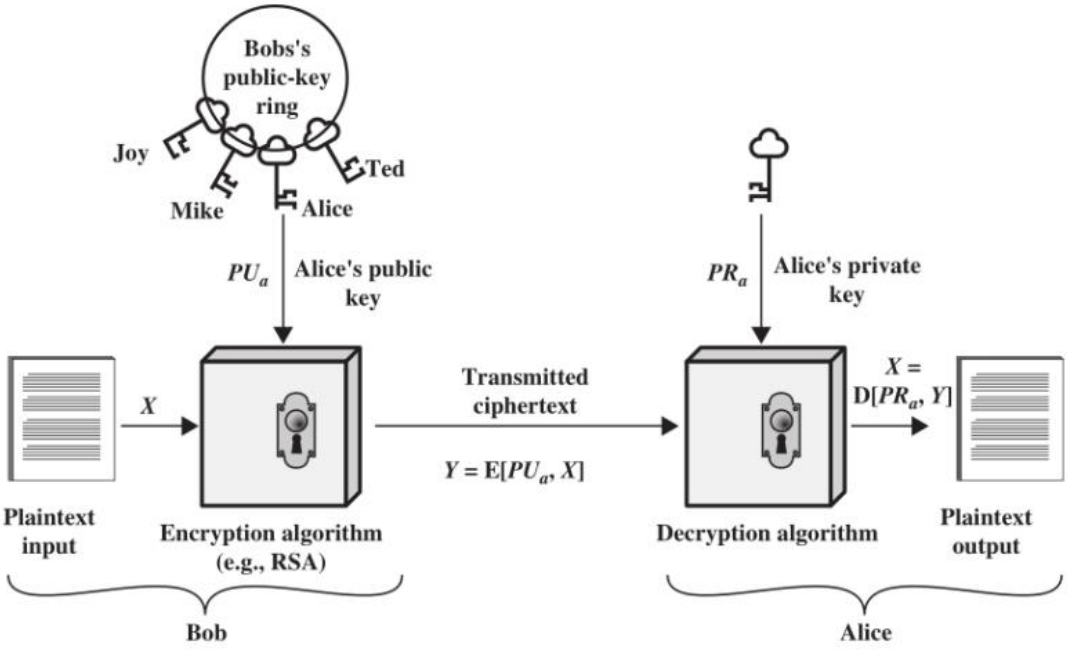
کلیات عملکرد باج‌افزارهای رمزکننده

بخش زیادی از حملات باج افزاری از نوع رمزکننده فایل است. حال این سوال مطرح می‌شود که این باج افزارها به چه صورت عملیات خود را اجرا می‌کنند که پس از رمز کردن فایل‌ها، امکان شکستن آن توسط دیگران به حداقل می‌رسد؟ در پاسخ باید گفت که طراحان باج‌افزار نهایت دقت خود را صرف استفاده از الگوریتم‌های رمزنگاری نوین خواهند کرد تا از قدرتمندترین آنها و یا حتی ترکیبی از چند الگوریتم رمزنگاری استفاده کنند و شانس رمزگشایی برای دیگران را به حداقل برسانند. در صورت کلی روش‌های مرسوم رمزنگاری که باج افزارهای شناخته شده تاکنون از آنها استفاده کرده‌اند را می‌توان به ۲ دسته کلی زیر تقسیم کرد:

۱. **رمزنگاری متقارن:** در رمزنگاری متقارن از یک کلید مشترک بین فرستنده و گیرنده استفاده می‌شود.

بنابراین افرادی که از طریق رمزنگاری متقارن در حال برقراری ارتباط هستند باید کلید مشترک را مبادله کنند تا در فرآیند رمزگشایی قابل استفاده باشد. این نوع رمزنگاری دارای سرعت بالایی است لیکن امنیت آن به اندازه سایر روش‌ها نیست. بنابراین باج افزارهایی که از این روش استفاده می‌کنند قادرند به سرعت فایل‌های قربانی را رمزنگاری کنند ولی متخصصان امنیتی با صرف زمان، قادر خواهند بود که کلید را کشف کرده و فایل‌ها را بازگردانند.

۲. **رمزنگاری نامتقارن:** برخلاف رمزنگاری متقارن در رمزنگاری به شیوه نامتقارن از یک جفت کلید عمومی[1] برای رمزگذاری و حفظ محرمانگی و کلید خصوصی[2] جهت رمزگشایی استفاده می‌شود که یک رابطه ریاضی بین آنها وجود دارد.



استفاده از الگوریتم های asymmetric پردازش زیادی را برای CPU در زمان رمزنگاری و رمزگشایی داده ایجاد می‌کند. به همین دلیل سرعت این رمزنگاری به مراتب کمتر از رمزنگاری متقارن است. روش رمزگذاری نامتقارن به سه زیر دسته تقسیم می‌شود:

سمت کاربر: در این روش کلید خصوصی در دستگاه قربانی ایجاد می‌شود و سپس به سرور اصلی ارسال می‌شود بنابراین اگر ارتباط شبکه قطع باشد و کلید خصوصی به سرور منتقل نشود فایل‌ها دیگر قابل رمزگشایی نخواهند بود.

سمت سرور: در این روش کلیدهایی عمومی و خصوصی، توسط سرور اصلی ایجاد می‌شود و پس از رمزنگاری فایل‌ها توسط باج افزار، برای بازگشایی آن باید هکر کلید خصوصی را از سرور به قربانی اهدا کند که البته

1-Public Key
2-Private Key

بدیهی است این اتفاق تنها در صورتی که باج پرداخت شود خواهد افتاد. گفتنی است این روش زیاد مورد استفاده قرار نمی گیرد چرا که در این حالت قربانی می‌تواند کلید را در اینترنت نشر دهد و عملا باج افزار کارآیی خود را از دست خواهد داد.

ترکیبی: این روش بسیار مدرن و پیشرفته است و برای رمزنگاری و رمزگشایی نیازی به ارتباط با سرور اصلی باج افزار وجود ندارد و از حداکثر امنیت برخوردار است به همین دلیل عموما باج افزارهای امروزی از این روش استفاده می‌کنند.

جمع بندی

همانطور که در بالا اشاره شد استفاده از پیشرفته‌ترین روش‌های رمزنگاری باعث شده است که هکرها و طراحان باج افزارها عموما دست بالا را داشته باشند و در صورت موفقیت در آلوده کردن یک سیستم، امکان رمزگشایی در بسیاری از مواقع وجود نخواهد داشت. بنابراین بهترین روش مقابله با باج افزارها، پیشگیری از آلودگی سیستم خواهد بود که در خبرنامه ماه بعد به آن می‌پردازیم.

" یک برنامه‌نویس خوب کسی است که

قبل از عبور از خیابان یک‌طرفه

هر دو طرف را نگاه می‌کند."

Doug Linder

استاد دانشگاه Missouri-Kansas

تلاش ما
حفظ امنیت
شماست...