محافظت در برابر باج افزار

پرسش و پاسخ برای مشتریان

۱. باج افزار چیست؟

باج افزار نوعی از تروجان باج خواهی است که عکس ها، ویدیو، موزیک و فایل های دیگر شما بر روی کامپیوتر را رمز نموده یا دسترسی به سیستم را به طور کامل مسدود می نماید. برای دستیابی دوباره به فایل ها و یا سیستم ، معمولا قربانیان باید مبلغی را به عنوان باج پرداخت نمایند.

۲. چه نوع باج افزارهایی وجود دارد؟

سه نوع باج افزار وجود دارد: باج افزار رمز کننده، که اطلاعات شما را رمز می کند (آنها را غیر قابل استفاده می نماید)؛ باج افزار قفل کننده صفحه، که یک عکس تمام صفحه نمایش داده و نمی گذارد به کامپیوتر خود دسترسی داشته باشید؛ و باج افزار master-boot-record ، که اولین سکتور پارتیشن سیستم های مبتنی بر BIOS را رمز می کند.

۳. باج افزار چه کاری انجام می دهد؟

باج افزار معمولا از طریق ایمیل و یا از طریق استخراج گسترش می یابد. در اولین نوع، مجرم سایبری یک ایمیل فیشینگ با ضمیمه خاص برای یک سازمان خاص می فرستد. به طور مثال، کاربر از همه جا بی خبر فایل ضمیمه (فایل Word و یا JavaScript) را باز کرده که متن ایمیل به صورت فریبکارانه ای برای کاربر درست شده است. هنگامی که فایل Word باز گردد، کاربر مطلع می گردد که برای نمایش درست متن باید ماکرو فعال گردد. فعال نمودن ماکرو به باج افزار اجازه می دهد که به صورت مخفیانه و توسط کدهای نوشته شده در فایل بر روی کامپیوتر دانلود شود.

۴. هنگامی که باج افزار کامپیوتر را آلوده کرد چه اتفاقی می افتد؟

فایل رمزکننده دانلود شده تمامی فایل ها شما مانند عکس ها، فیلم ها و فایل های آفیس شما را رمز می کند همچنین اگر در همان زمان فلش درایو به سیستم متصل بوده و یا به مراکز ذخیره سازی ابری نیز متصل باشد آنها را نیز مخدوش می نماید. حال که تمامی فایل ها با پسوندی خاص رمز شده اند، باج افزار در برابر باز پس دادن فایل ها درخواست باج می نماید. این باج، معمولا باید به صورت بیت کوین بر روی یک سایت خاص موجود در نت سیاه (darknet) پرداخت شود که می تواند چندین هزار یورو باشد. در مورد باج افزار قفل کننده صفحه، بدافزار صفحه اصلی را قفل کرده و دسترسی به دستگاه را مسدود می کند و مانند مثال قبل درخواست پول به صورت UKash و یا روش های دیگر می کند.

۵. وضعیت این تهدید چگونه است؟

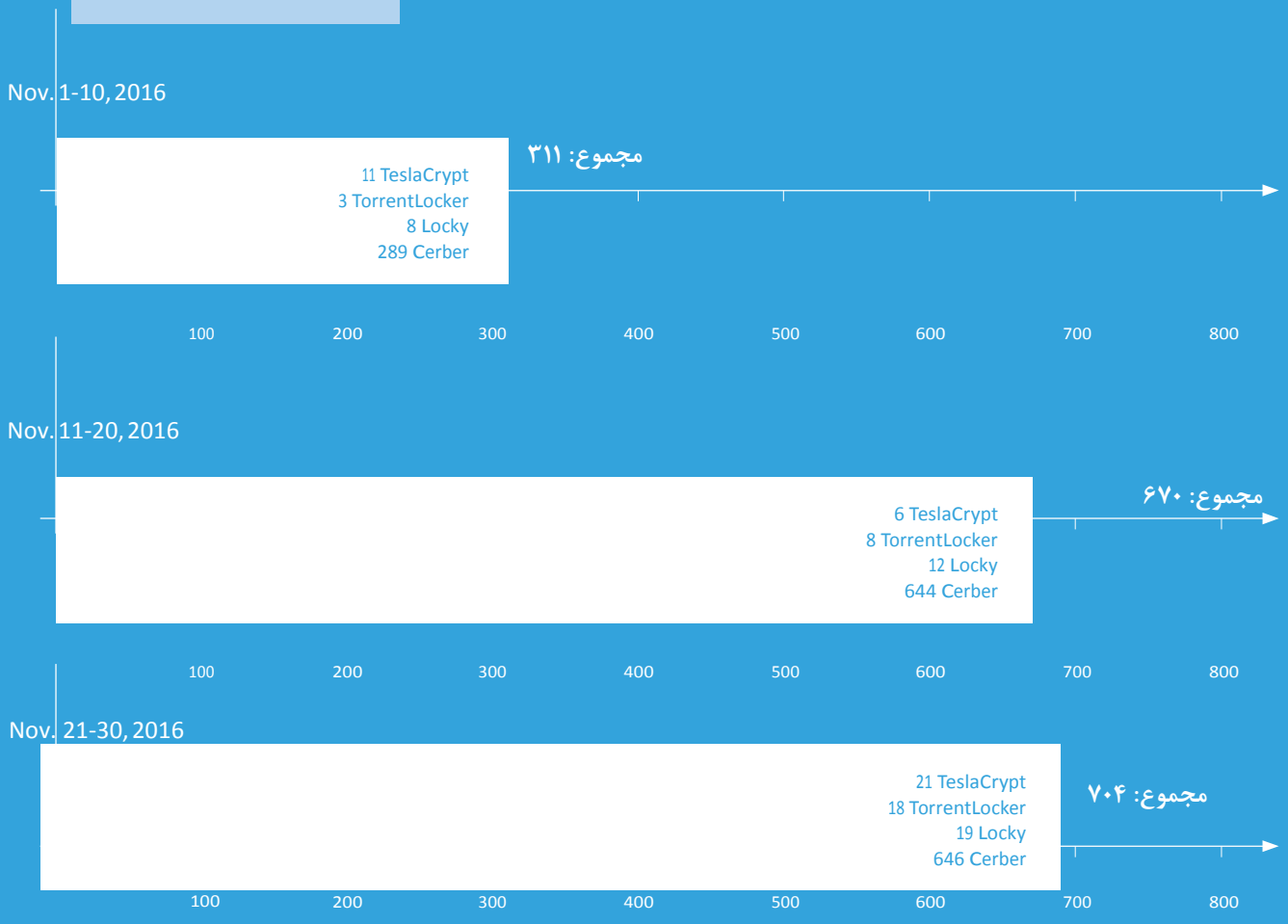
به دلیل آنکه این مدل کسب و کار مانند یک معدن طلا برای مجرمان سایبری است، حملات باج افزار ها ادامه خواهد داشت و بسیاری از افراد حاضر به پرداخت می شوند. مجرمان سایبری به صورت پیوسته این کسب و کار پر سود را گسترش می دهند. این بدان معنا است که نه تنها از برنامه های اجرایی ویندوز استفاده می کنند، بلکه با استفاده از زبان های اسکریپ - VBS، JavaScript، PowerShell – تشخیص و دسته بندی آن را نیز سخت تر می نمایند. باج افزارها بر روی دستگاه های اندروید نیز وجود دارند و دستگاه قفل شده تا زمانی که کاربر باج را پرداخت نماید. حتی کاربران Mac نیز تحت تاثیر باج افزار KeRanger قرار گرفته اند. مدل های معروف دیگر مانند Petya، FBI Ransomware و Locky میلیون ها کامپیوتر ویندوزی را تحت تاثیر قرار داده اند.

Cerber

خانواده Cerber یکی از خطرناک ترین باج افزارهای موجود می باشد، که به صورت ضمیمه های ایمیل منتشر می شوند. آخرین نسخه آن قادر است کل پایگاه داده را رمز کند.

باج افزار یک تهدید همیشگی

حجم باج افزار انتخاب شده
در نوامبر ۲۰۱۶ | منبع: ransomwaretracker.abuse.ch



۶. اویرا از چه تکنولوژی های امنیتی برای مقابله با باج افزار استفاده می نماید؟

یک استراتژی چند لایه امنیتی برای به حداقل رساندن و کاهش عوامل مرتبط با باج افزار نیاز می باشد. برای این منظور اویرا یک تکنولوژی موثر برای کشف و مقابله با نرم افزار های مخرب ایجاد نموده است. ما با استفاده از تکنولوژی هایی مانند یادگیری ماشین/ هوش مصنوعی، اعتبار، تشخیص مبتنی بر رفتار و آنالیز در زمان واقعی برای تشخیص فایل های ناشناخته استفاده می نماییم. و با تشکر از سرویس ابری مشتریان ما همیشه به آخرین اطلاعات دسترسی دارند. در آینده، استفاده از هوش مصنوعی نقش بزرگی در آنالیز و دسته بندی نرم افزار های مخرب گذشته خواهد داشت.

اویرا اقدامات زیر را برای مقابله با تروجان های اخاذی از طریق ایمیل توصیه می نماید:

۱. همیشه نرم افزار های امنیتی و برنامه های خود را به روز نگه دارید.

به روز رسانی و وصله های جدید را کنار نگذارید.

شبکه شرکت را قسمت بندی کنید.

۲. به صورت منظم کارمندان خود را در خصوص تهدیدات جدید (مانند باج افزار) آموزش دهید همچنین خصوصیات فردی آن ها را نیز ارتقاء دهید. هرچه در فواصل کمتری پشتیبان تهیه کنید بهتر است.

۳. این نسخه های پشتیبان باید جدا از یکدیگر و خارج از شبکه شما قرار داشته باشند زیرا یک پشتیبان رمز شده توسط یک تروجان به درد شما نخواهد خورد.

۷. شرکت ها باید از چه استراتژی امنیتی برای مقابله با حمله ها استفاده نمایند؟

امنیت IT باید قسمتی از استراتژی هر شرکتی برای آمادگی در برابر حملات سایبری باشد- فرقی نمی کند که یک شرکت کوچک با کارمندان کم باشد و یا شرکت بزرگ. این تنها راه برای جلوگیری از جاسوسی داده و از دست دادن آن و همچنین جلوگیری از خدشه دار شدن شهرت به دست آمده می باشد. در کل، شرکت ها باید نرم افزار های امنیتی را نصب نموده تا در هر زمان بتوانند از آنها در برابر نرم افزار های مخرب محافظت نمایند، مانند استفاده از تکنولوژی ابری و بعلاوه، تکنولوژی هوش مصنوعی که به شما اجازه می دهد فایل هایی را که هنوز به عنوان مخرب شناسایی نشده اند را شناسایی نمایید. برای این منظور، شرکت ها باید سیستم های امنیتی IT خود را تجهیز نموده و عملکرد این فن آوری ها را تضمین نمایند.

۴.

محدود کردن دسترسی کاربران: هر کاربر به سطح دسترسی متناسب با کار خود نیاز دارد.

لیست سفید: فقط برنامه های مجاز امکان اجرا شدن داشته باشند.

۵.

قوانینی برای دستگاه هایی که کارکنان با خود می آورند (BYOD) داشته باشید: شبکه سازمان را در برابر دستگاه های خارجی (مانند لپ تاپ، گوشی های هوشمند، و دیگر دستگاه های حمل کننده اطلاعات مانند فلش ها) محافظت نمایید.

۶.

از یک مرورگر امن استفاده نمایید تا شما را در برابر سایت ها مخرب و فیشینگ محافظت نماید.

اطلاعات تماس:

تهران، خیابان ولیعصر(ع)، نرسیده به توانیر،

برج طلوع، طبقه ۶، واحد ۶۰۱

تلفن: ۹۸۲۱۸۸۷۴۷۳۷۹+

www.ertebateamn.com

info@ertebateamn.com