ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

باج افزار

باج افزار چیست؟

باج افزار نوع خاصی از بدافزار است که بطور فعال در حال گسترش در اینترنت است، و قربانی را تهدید به از بین بردن مدارك و فایل هایش می کند. بدافزار نرم افزار است- یك برنامه کامپیوتری- که برای انجام کارهای مخرب استفاده می شود. در حالیکه باج افزار یکی از انواع مختلف بدافزار است ولی خیلی رایج شده است چون بسیار برای تبهکاران سود آور است. وقتی که باج افزار کامپیوترتان را آلوده می کند فایل های خاصی یا شاید همه هارد درایو را رمزگذاری می کند. در نتیجه به کل سیستم دسترسی نخواهید داشت یا به فایل های مهم تان نمی توانید دسترسی پیدا کنید، مثلا مدارك یا عکس هایتان. بدافزار سپس اطلاع می دهد تنها راهی که می توانید به فایل هایتان را رمزگشایی کنید و سیستم را دوباره بدست بیارید پرداخت پول به تبهکار سایبری (باج) است. بهمین خاطر باج افزار نامیده می شود. اغلب این باج باید بشکل پول دیجیتالی مثل بیت کویت پرداخت شود. باج افزار مثل همه انواع دیگر بدافزار گسترش پیدا می کند. رایج ترین روش شامل فرستادن ایمیل های مخرب به قربانیان است، جایی که تبهکار سایبری شما را به باز کردن ضمیمه ایمیل آلوده یا کلیك بر لینکی که شما را به سایت حمله کننده می برد می فریبانند.

سردبیر مهمان

لنی زلتسر بر حفاظت از عملیات IT مشتریان شرکت NCR تمرکز دارد و نبرد بدافزار در مؤسسه SANS تدریس می کند. لنی در توییتر با **@lennyzelster** فعال است و بلاگ مربوط به امنیت در **Zeltser.com** دارد.

آیا باید باج را بپردازید؟

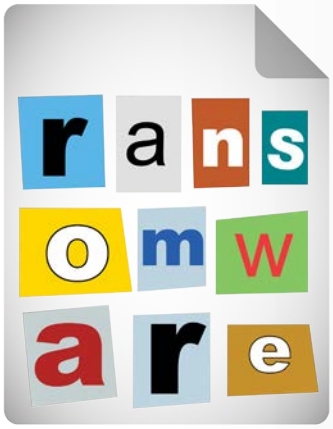
سوال سختی است. مشکل اینست هر چه موارد پرداخت باج به این تبهکاران بیشتر شود، این مجرمان با انگیزه بیشتری بقیه را مورد آلودگی قرار می دهند. از طرف دیگر ممکن است راه دیگری برای دوباره بدست آوردن فایل هایتان نداشته باشید. پس آگاه باشید حتی اگر باج را بپردازید هیچی تضمینی وجود ندارد که فایل هایتان را دوباره بدست بیاورید. شما با مجرمان معامله می کنید، ممکن است آنها فایل هایتان را رمزگشایی نکنند یا حتی ممکن است روش رمزگشایی را در ازای پول در اختیار شما بگذارند اما در طول فرایند رمزگشایی چیزی اشتباه شود و کامپیوترتان به بدافزار های دیگری آلوده شود.

پشتیبان گیری از فایل ها

شاید بهترین راه برای بهبودی از آلودگی باج افزار و نپرداختن باج افزار اینست که فایل هایتان را از نسخه پشتیبان بازیابی کنید. از این راه،

باج افزار

حتی اگر آلوده به باج افزار شوید، راهی برای درباره بدست آوردن فایل ها بعد از اینکه کامپیوترتان را بازسازی و پاکسازی کردید وجود دارد. در ذهن داشته باشید که اگر بتوان از طریق سیستم آلوده شده به نسخه پشتیبان دسترسی داشت، باج افزار ممکن است فایل های پشتیبان را هم پاك یا رمزگذاری کند. در نتیجه، بسیار مهم است که فایل های پشتیبان روی سرویس های خوشنام بر اساس ابر یا روی درایو های خارجی که همیشه به سیستم متصل نیست ذخیره شوند. بعلاوه، اشتباه رایجی که بسیاری از مردم در رابطه با پشتیبان مرتکب می شوند اینست که تصور می کنند این پشتیبان ها می توانند فایل ها را دوباره بازیابی کنند بدون اینکه امتحان کنند که آیا واقعا اینکار را می کنند. حتما بطور مرتب امتحان کنید که پشتیبان ها کار می کنند و مطمئن شوید که اگر سیستم آلوده شد می توانید فایل هایتان را از پشتیبان ها دوباره بدست بیاورید. پشتیبان ها از این جهت هم مهم هستند که اگر بطور تصادفی فایلی را پاك کردید یا هارد دیسك خراب شد می توانند کمك کنند فایل هایتان را دوباره بدست بیاورید.



باج افزار بدافزاری است که هنگامی که کامپیوترتان را آلوده کرد همه فایلهای کامپیوترتان را رمزگذاری می کند و مانع دسترسی شما به آن ها می شود.

اقدامات حفاظتی بیشتر

علاوه بر اینها، می توانید خودتان را از آلودگی باج افزار ها با همان راههایی که در برابر انواع دیگر بدافزار استفاده می کردید، در امان بدارید. آلوده نشوید. مطمئن باشید که نرم افزار آنتی ویروس بروز از یك سازنده مورد اعتماد دارید. اینگونه ابزار ها که گاهی نرم افزار ضد بدافزار نامیده می شوند، برای کشف و متوقف کردن بدافزار درست شده اند. اما آنتی ویرووس نمی تواند همه برنامه های مخرب را مسدود کند و بزداید. مجرمان سایبری بطور دائم در حال نوآوری کردن و و بهبود بدافزار های پیچیده ای هستند که ممکن است تشخیصشان ممکن نباشد. (نبرد آنتی ویرووس ها و بدافزار ها) با روش های زیادی تبدیل به یك مسابقه تسلیحاتی شده است. دو طرف تلاش دارند از طرف دیگر را شکست بدهند. متاسفانه، تبهکاران همیشه یك قدم جلو هستند، بهمین دلیل باید اطمینان داشته باشید که از فایل هایتان پشتیبان گرفته اید و این قدم های مکمل را برای حفاظت از خود بر می دارید.

- مجرمان سایبری اغلب کامپیوتر ها و دستگاهها را با بهره برداری کردن از نقاط آسیب پذیر در نرم افزارتان آلوده می کنند. هر چه نرم افزار تان جدیدتر باشد، سیستم نقاط آسیب پذیر شناخته شده کمتری دارد و آلوده کردنش برای مجرمان سایبری سخت تر است. بنابراین، حتما سیستم عامل، اپلیکیشن ها و دستگاههایتان قادر به نصب خودکار بروز رسانی ها باشند.

باج افزار

- در کامپیوتر ها، از حساب استانداردی که مزیت محدودی دارد بجای حساب خاص مثل «مدیر» یا «ریشه» استفاده کنید. اینکار باعث جلوگیری از اینکه بدافزار ها خودشان را روی کامپیوتر نصب کنند می شوند.
- مجرمان سایبری اغلب مردم را به نصب بدافزار برای آنها می فریبند. مثلا، ممکن است ایمیلی به شما بفرستند که بنظر قانونی بیاید و شامل یك ضمیمه یا لینك باشد. شاید ایمیل ظاهرا از دوست یا بانك تان رسیده است. اما، اگر فایل ضمیمه را باز کنید یا روی لینك کلیك کنید، ممکن است کد مخرب را فعال کنید که بدافزار را روی سیستم تان نصب می کند. اگر پیامی حس فوریت قوی ای را ایجاد می کند، گیج کننده است، بیش از حد خوب باشد، یا گرامر ضعیفی داشته باشد، ممکن است یك حمله باشد. مشکوك باشید، عقل سلیم اغلب بهترین دفاع است.

خودتان را از باج افزار با گوش بزنگی و هوشیاری هنگام باز کردن ضمیمه های ایمیل و یا کلیك بر روی لینك ها محافظت کنید. حتما از نرم افزار آنتی ویروس بروز استفاده کنید و از فایل هایتان مرتبا نسخه پشتیبانی که قابل بازگرداندن باشد بگیرید.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه !OUCH شوید و به آرشیو خبرنامه آگاهی از امنیت !OUCH دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: securingthehuman.sans.org/ouch/archives

منابع

فیشینگ: https://securingthehuman.sans.org//ouch/2015#december2015

بدافزار چیست: https://securingthehuman.sans.org/ouch/2016#march2016

رمز گذاری: https://securingthehuman.sans.org/ouch/2016#june2016

پشتیبان ها: https://securingthehuman.sans.org/ouch/2015#august2015

مقاله مایکروسافت: https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

SANS FOR610 Course-مهندسی معکوس بدافزار: https://sans.org/for610

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley

ترجمه شده توسط : سعید میرجلیلی