اهرم باج افزار

اهرم باج افزار: اپراتورهای باج افزار گاهی اوقات برای جبران خسارت قربانیان خود به تهدیدهای غیر متعارف متوسل می‌شوند.
در چند سال گذشته، مجرمان سایبری به طور قابل توجهی تغییر کرده اند. تا همین چند سال پیش، آن‌ها معمولاً تروجان‌ها را بطور دسته جمعی اعزام می‌کردند و بی سر و صدا منتظر می‌ماندند تا کسی هزینه آن را پرداخت کند، زیرا به خوبی می‌دانست که اکثر اهداف، تقاضا را نادیده می‌گیرند. اکنون به نظر می‌رسد که آن‌ها رویکرد متفاوتی را اتخاذ کرده‌اند و به اصطلاح بیشتر مشتری مدار شده‌اند.

مهاجمان از آلودگی‌های دسته جمعی به آلودگی‌های هدف تبدیل شده‌اند، بدون شک منطقه پوشش خود را کاهش داده و از این رو عزم خود را برای فرار از دیگران افزایش داده‌اند. اکنون هر هدفی نشان دهنده یک جایزه بزرگ است و مجرمان سایبری به دنبال نفوذ بیشتر هستند. به عنوان مثال، یک ایمیل اخیر را که هنگام تحقیق در مورد گروه مجرمان سایبری به نام Darkside با آن برخورد کردیم، در نظر بگیرید.

پیامی از باج خواهان

ماجرای اصلی
این ایمیل اساساً می‌گوید که مهاجمان سازمانی را که خدمات عکاسی برای مدارس انجام می‌دهد و داده‌های دانش آموزان و کارکنان مدرسه را ذخیره می کند، آلوده کرده‌اند. مقامات فدرال این سازمان را از پرداخت باج منع کرده‌اند، ظاهرا مجرمان سایبری آسیب دیده را مجبور کرده است تا از اهرم‌های اضافی استفاده کنند.

بازی‌های فکری Darkside
مجرمان سایبری مستقیماً به مدارسی روی آوردند که اطلاعات دانش آموزان آن‌ها در معرض خطر قرار گرفته بود و به دنبال راه اندازی هرچه بیشتر اقدامات کلاسی علیه شرکت آسیب دیده بودند. مجرمان سایبری از مدارس خواستند تا مطبوعاتی تهیه کنند و با والدین دانش آموزان تماس بگیرند تا وضعیت را توضیح دهند. در غیر این صورت، آنها گفتند نمی‌توانند تضمین دهند که داده‌های مدرسه، از جمله داده‌های شخصی کودکان، در وب تاریک به سرانجام نرسد. آن‌ها همچنین تأکید کردند که داده‌ها شامل عکس‌های کارکنان و جزئیاتی است که می‌تواند به پدوفیل‌ها در ایجاد کارت‌های جعلی مدرسه کمک کند و در نتیجه کودکان را در معرض خطر بیشتری قرار دهد.

بنابراین، مهاجمان نه تنها تهدید کردند که اعتبار قربانی را خراب می‌کنند، بلکه مشتریان و شرکای وی را نیز تحت تأثیر قرار می‌دهند تا از طریق پیامدهای بالقوه مخرب قانونی خسارت‌های بیشتری به بار آورند.

اهرم باج افزار

چه باید کرد
همانطور که یوجین کسپرسکی اخیراً اشاره کرده است: درک این نکته مهم است که در حقیقت، برآوردن خواسته‌های مجرمان سایبری باعث برطرف شدن مشکل نمی‌شود. شما به هیچ وجه نمی توانید بفهمید که آیا آن‌ها داده‌های سرقت شده را حذف کرده‌اند یا خیر.

بنابراین، ما به همه سازمان‌ها و شرکت‌ها، به ویژه آن‌هایی که داده‌های شریک یا مشتری را ذخیره می‌کنند، توصیه می‌کنیم که از قبل برای حمله احتمالی آماده شوند:

ماهیت تهدید را برای همه کارکنان توضیح دهید و آن‌ها را در تشخیص اقدامات مزاحم آموزش دهید.
مجهز کردن تمام رایانه‌ها و دستگاه‌ها به راه حل‌های امنیتی قابل اطمینان که می‌توانند تروجان‌های باج افزار را شکست دهند.

(پیگیری به روزرسانی‌های نرم افزاری موجود و نصب آن‌ها به طور منظم) حملات باج افزار از طریق آسیب پذیری‌ها به خصوص اخیراً مخرب بوده است.

منبعkaspersky

لطفا جهت مشاوره در انتخاب آنتی ویروس مناسب خود با این شماره **09224971053** تماس بگیرید.

مارو در شبکه های اجتماعی خودتان به اشتراک بگذارید.