بسمه تعالی

عنوان خبر:

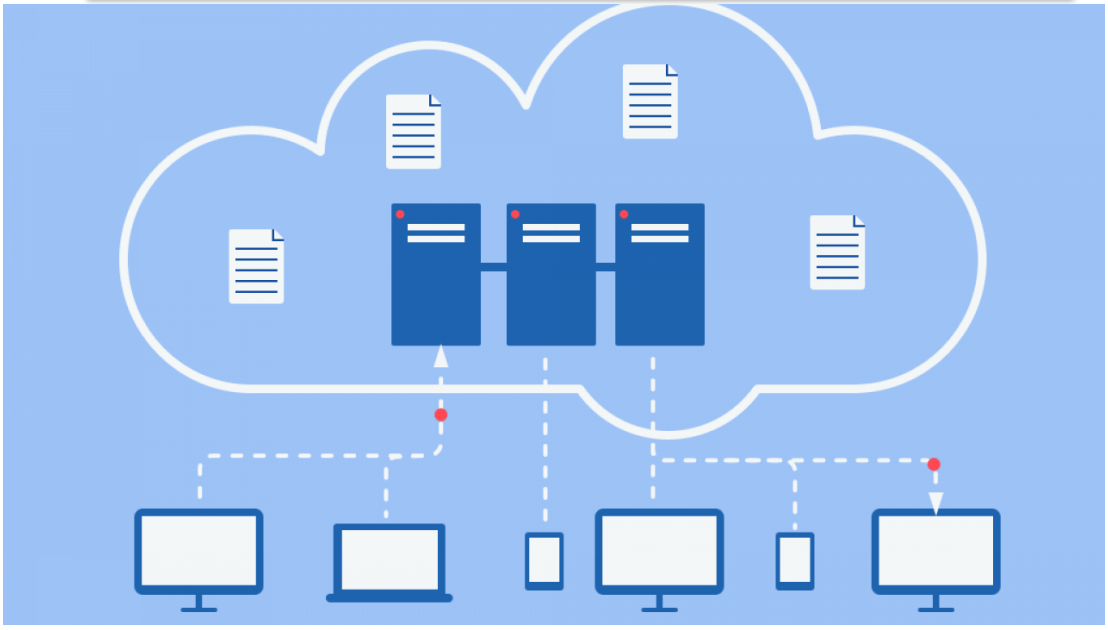
سوءاستفاده از نسخه‌های پشتیبان قرار گرفته در فضای ابری علیه خود کاربر توسط باج‌افزارها

گروه خبری:

آسیب‌پذیری

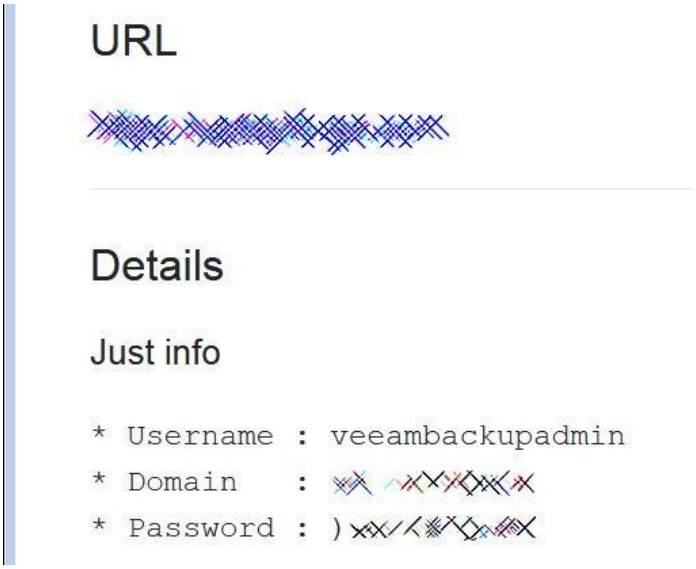
۱۶اسفند ۱۳۹۸

.



پشتیبان‌گیری یکی از مهم‌ترین راه‌حل‌های محافظت داده‌ها (حتی شاید مهم‌ترین) در برابر باج افزارها است، اما اگر به‌درستی از این شیوه استفاده نشود، مهاجمین از آن علیه شما استفاده می‌کنند.

اخیراً اپراتورهای DoppelPaymer Ransomware در سایت نشت اطلاعات خود، بدون پرداخت هزینه نرم افزار پشتیبان‌گیری Veeam، نام کاربری ادمین و رمزعبور متعلق به یک قربانی را منتشر کردند.



۱- حساب فاش‌شده Veeam

این امر نه به معنای افشای اطلاعات برای دیگران و حملات بیشتر، بلکه هشداری برای قربانی بود که اپراتورهای باج افزار به شبکه‌ی آن‌ها از جمله نسخه‌های پشتیبان آن‌ها، دسترسی کامل دارند.

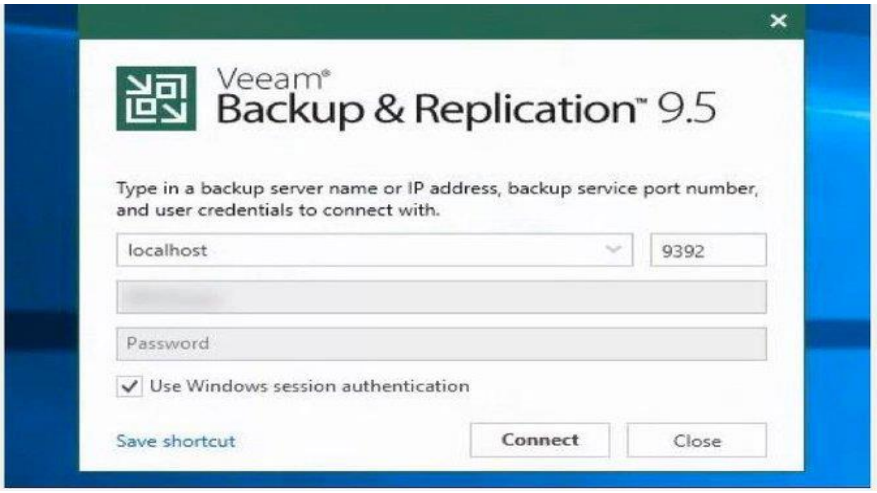
بعد از دیدن این اطلاعات، با اپراتورهای خانواده‌های DoppelPaymer و Maze Ransomware ارتباط برقرار شد تا چگونگی هدف قرارگرفتن پشتیبان‌های قربانی مشخص شود و نتایج بسیار تعجب‌آور بود.

لازم به ذکر است که در این مطلب به نرم‌افزار پشتیبان‌گیری Veeam پرداخته‌شده‌است. نه به این دلیل که نسبت به سایر نرم‌افزارها از امنیت کمتری برخوردار است، بلکه به این دلیل که یکی از محبوب‌ترین محصولات پشتیبان‌گیری است و توسط اپراتورهای باج‌افزار ذکر شده است.

مهاجمین ابتدا از نسخه‌ی پشتیبان ابری کاربر برای سرقت اطلاعات آنها استفاده می‌کنند.

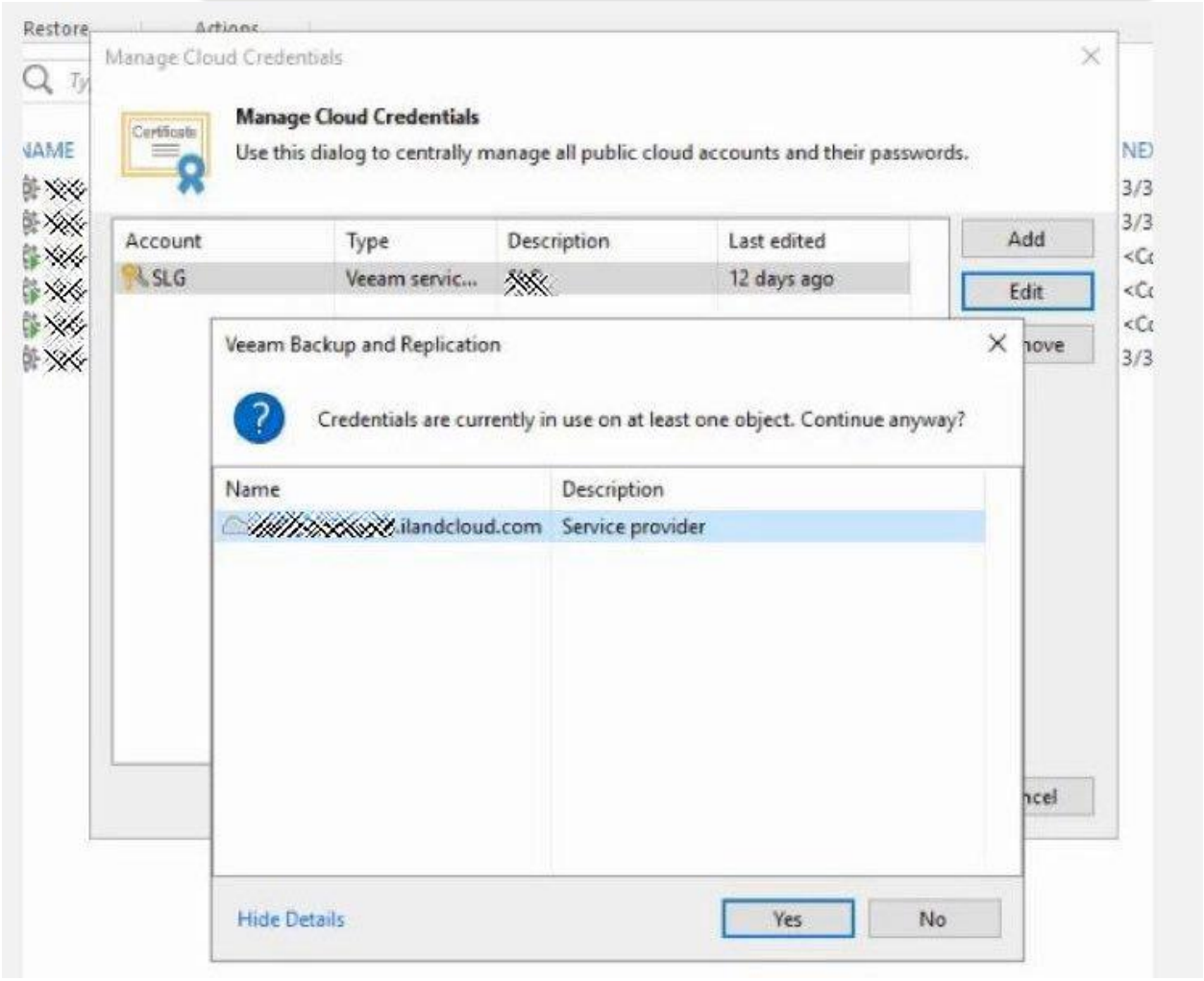
در طول حملات باج افزار، مهاجمین یک میزبان فردی را از طریق فیشینگ، بدافزار یا سرویس‌های کنترل از راه‌دور، در معرض خطر قرار می‌دهند. پس از بدست‌گرفتن دسترسی یک سیستم، به طور جانبی در سراسر شبکه گسترش می‌یابند تا اینکه به اعتبارنامه ادمین و کنترل‌کننده دامنه، دسترسی پیدا کنند. با استفاده از ابزاری مانند Mimikatz، اعتبارنامه‌ها را از active directory کپی می‌کنند.

طبق گفته Nero Consulting، یک شرکت مشاوره‌ی MSP و IT مستقر در اطراف نیویورک که در این مطلب نیز کمک کرده‌است، از آنجایی که برخی از ادمین‌ها Veeam را طوری پیکربندی می‌کنند که از احرازهویت ویندوز استفاده کند، به مهاجمین امکان می‌دهند که دسترسی نرم‌افزار پشتیبان‌گیری را بدست آورند.



۲- ورود به نرم‌افزار Veeam با استفاده از احرازهویت ویندوز

به گفته‌ی اپراتورهای Maze Ransomware، بدست‌آوردن دسترسی به پشتیبان‌های قرار گرفته در فضای ابری در سرقت داده‌های سیستم خود کاربر قربانی بسیار مفید بوده است.



۳- ارائه‌دهنده‌ی ابری پیکربندی شده

هنگامی که Maze پشتیبان‌های ذخیره شده در ابر را پیدا می‌کند، تلاش می‌کند تا اعتبارنامه‌های ذخیره‌سازی ابر را بدست آورد و سپس از آنها برای بازیابی اطلاعات قربانی به سرورهای تحت کنترل مهاجم استفاده کند. Maze در این خصوص می‌گوید: "بله، ما آن‌ها را بارگیری می‌کنیم، کار بسیار مفیدی‌ست. دیگر نیازی به جستجو برای اطلاعات حساس نیست چون قطعاً در نسخه‌ی پشتیبان وجود دارند. پشتیبان ابری حتی ساده‌تر است، فقط کافی‌ست وارد فضای ابری شوید و آن را از سرور خود بارگیری کنید، از دید نرم‌افزار تشخیص نشت داده نیز کاملاً نامرئی خواهید بود! هدف ابرها امنیت است، نه؟"

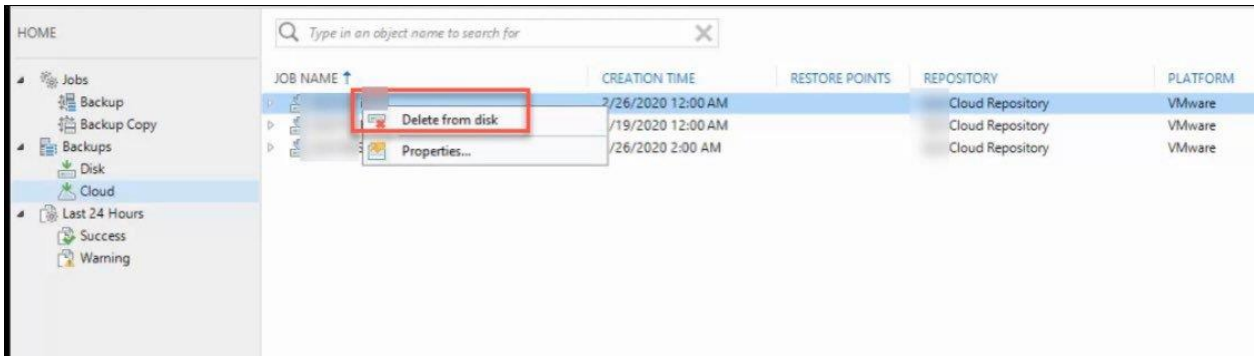
از آنجا که مهاجمین در حال بارگیری مستقیم از ابر به سرورهای خود هستند، هیچ هشداری برای قربانی ظاهر نمی‌شود زیرا به نظر می‌رسد سرورها کار عادی خود را انجام می‌دهند و هیچ‌گونه گزارشی در نرم‌افزار پشتیبان‌گیری آنها ایجاد نمی‌شود.

اپراتورهای Maze در مورد چگونگی دستیابی به مدارک ابری توضیح ندادند اما DoppelPaymer به ما گفت که آن‌ها از تمامی روش‌های ممکن استفاده می‌کنند. این می‌تواند شامل keylogger ها، حملات فیشینگ یا خواندن اسناد محلی ذخیره شده در سرورهای پشتیبان باشد.

حذف نسخه‌های پشتیبان قبل از حملات باج افزار

صرف نظر از این که از نسخه پشتیبان برای سرقت داده استفاده می‌شود، پیش از انجام فرآیند رمزنگاری فایل‌ها توسط باج‌افزار بر روی دستگاه‌های موجود در شبکه، مهاجمین ابتدا نسخه پشتیبان را حذف می‌کنند تا در بازیابی پرونده‌های رمزگذاری شده از آن‌ها استفاده نشود.

DoppelPaymer به BleepingComputer گفته است که اگرچه پشتیبان‌گیری ابری می‌تواند گزینه‌ی مناسبی برای محافظت در برابر باج افزارها باشد اما ۱۰۰٪ مؤثر نیست. DoppelPaymer از طریق ایمیل به ما گفت: "نسخه‌های پشتیبان ابری گزینه بسیار خوبی در برابر باج دادن است اما از آنجایی که این سیستم‌های ابری همیشه به درستی پیکربندی نمی‌شوند ،۱۰۰٪ مؤثر نیستند و پشتیبان آفلاین نیز اغلب تاریخ‌گذشته و منسوخ است. سیستم پشتیبان‌گیری واقعاً کارآمد و خوب است اما عامل‌انسانی برخی گزینه‌ها را باقی گذاشته‌است." مگر در مواردی که از سرویس‌هایی مانند پشتیبان‌های تغییرناپذیر استفاده کنید، زیرا عاملین دسترسی کاملی به نصب محلی نرم‌افزار پشتیبان دارند، آن‌ها می‌توانند به‌راحتی هرگونه پشتیبان موجود در ابر را حذف کنند.



۴- حذف نسخه پشتیبان ابری در Veeam

مهاجمین با سرقت اطلاعات قربانی و حذف نسخه پشتیبان آن‌ها، باج افزار خود را معمولاً خارج از ساعات کاری در سراسر شبکه‌ی قربانی با استفاده از PSExec یا PowerShell Empire، گسترش می‌دهند. این امر غالباً منجر به رویارویی شرکت قربانی با شبکه‌ای رمزگذاری شده در شروع روز کاری بعد، خواهد شد.

از نسخه‌های پشتیبان خود محافظت کنید

در ایمیل‌های ردوبدل شده با Vanover مدیر ارشد استراتژی محصول در Veeam، به ما گفته شد که فرقی نمی‌کند از چه نرم‌افزاری استفاده کنید، یک بار که یک مهاجم دسترسی سطح بالا به شبکه را کسب کند، همه چیز در معرض خطر است.

برای جلوگیری از نفوذ کامل مهاجمین باج‌افزار، Veeam توصیه می‌کند که شرکت‌ها هنگام پیکربندی نسخه پشتیبان از قانون ۱-۲-۳ پیروی کنند. این قانون می‌گوید که از داده‌ها حداقل سه پشتیبان در فضای‌های مختلف ذخیره‌سازی برای خود داشته باشید. مانند Veeam، Nero Consulting نیز به شدت توصیه می‌کند که کاربران در صورت استفاده از سرویس‌های ابری حتی‌الامکان یکی از گزینه‌های ذخیره‌سازی تغییرناپذیر (immutable storage) یا حفاظت ذخیره‌سازی (redundant storage protection) را خریداری کنند. با استفاده از این گزینه‌ها، حتی اگر داده‌ها از در فضای ذخیره‌سازی ابری حذف شوند، سرویس ذخیره‌سازی تغییرناپذیر، داده‌ها را برای مدت معینی بازیابی می‌کند. در مورد محافظت از شبکه در برابر استخراج داده‌ها، بهترین راه‌حل در وهله اول ممانعت از دسترسی مهاجمین به شبکه‌ی شما و نظارت بر

فعالیت‌های مشکوک است. این امر شامل استفاده از نرم‌افزار مانیتورینگ شبکه، سیستم‌های تشخیص نفوذ و کنترل دسترسی IP و مکانی برای ارائه‌دهندگان ذخیره‌سازی ابری است.

منبع:

https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/