Man in the Cloud

[illegible]

[illegible] man in the cloud [illegible] MITC [illegible] (Password tokens) [illegible]

[illegible] man in the middle [illegible] man in the cloud [illegible] Black Hat [illegible] man in the cloud [illegible]

Synchronization Application	OneDrive	Box	Google Drive	Dropbox
Token Type	OAuth Refresh Token	OAuth Refresh Token	OAuth Refresh Token	Proprietary
Location	Windows Credential Manager	Windows Credential Manager	Encrypted in Registry	Encrypted SQLite file

3
6
2
1
4
5

نتایج کلیدی بهدست آمده از تحقیقات

تحقیقات انجام گرفته از سوی Imperva منجر به کشف چند حقیقت مهم شده است:

سرویسهای همسانسازی همچون واندرایو، دراپباکس، گوگلدرایو و باکس بهراحتی در زیرساختها دارای آسیبپذیری هستند، بهطوری که باعث ایجاد یک تونل برای استخراج دادهها، ایجاد یک کانال C&C و دسترسی از راه دور میشوند .

سرویسهای همسانساز فایلها میتوانند بدون استفاده از یک اعتبارنامه متنی شناسایی شوند .

بازگرداندن یک حساب کلاود یا دسترسی به فایلهای هک شده روی یک حساب ابری همیشه وجود ندارد . بهطوری که در بعضی مواقع تنها راه حل این مشکل بستن حساب است.

کارهایی که تاکنون در ارتباط با امنیت در نقاط پایانی و محیطهای کلاود انجام شده نه تنها کافی نبوده است، بلکه باعث کم شدن حجم حملات و تهدیداتی که از سوی کدهای مخرب وجود دارد، نیز نشده است، همچنین به دلیل عدم وجود هیچ کانال سیمی امکان مشاهده آشکار این حملات و یا شناسایی دقیق مبدأ در بعضی موارد وجود ندارد .

پیشنهاد **Imperva**

حتا اگر بسیاری از سرویسها سیستم احرازهویت دو عاملی را پیادهسازی کنند، باز هم امکان ترمیم آسیبپذیری حمله man in the cloud بهسادگی امکانپذیر نیست . این سرویسها یک پیغام هشدار را زمانی برای یک کاربر ارسال میکنند که حساب او از سوی یک کامپیوتر جدید یا مکان جدیدی مورد استفاده قرار گرفته باشد، اما بیشتر مردم در چنین زمانهایی از این هشدار صرفنظر کرده و آن را نادیده میگیرند .
برای محافظت در برابر اینگونه حملات، Imperva پیشنهاد کرده است شرکتها سرمایهگذاری بیشتری را برای نظارت و محافظت از منابع دادهای در سرویسهای کلاود اختصاص دهند . بر همین اساس، سازمانها لازم است اقدام به شناسایی الگوهایی که در آینده برای دسترسی و سوء استفاده از دادهها بر پایه نقصها مورد استفاده قرار میگیرند، اقدامات لازم را بهعمل آورند .

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
12:16 - 23/05/1394
برچسب:
امنیت - کلاود - man in the cloud - Password tokens