O ransomware ainda consegue atingir dados armazenados em serviços de nuvem como OneDrive ou Google Drive?

Resposta curta: Sim. Embora o armazenamento em nuvem já tenha estado fora do alcance do ransomware, os atacantes adaptaram os seus métodos e agora conseguem visar dados armazenados na nuvem através de técnicas como o mapeamento de unidades e, mais comummente hoje em dia, o roubo de chaves de API e tokens de sessão.

Como a abordagem do ransomware aos dados na nuvem mudou

Quando o trabalho remoto impulsionou uma rápida mudança para o armazenamento em nuvem, tanto as empresas como os cibercriminosos estavam a adaptar-se simultaneamente ao novo ambiente. Nas fases iniciais desta mudança, o ransomware normalmente não conseguia tocar em ficheiros armazenados em plataformas na nuvem — se os dados estivessem na nuvem em vez de num servidor local, os atacantes geralmente deixavam-nos em paz, pois não tinham um caminho direto até eles.

Isso mudou à medida que os atacantes aprenderam a ligar manualmente o armazenamento na nuvem, como uma conta da Amazon, OneDrive ou Google Drive, a um sistema infetado. Fizeram isto ao montar o armazenamento na nuvem como uma letra de unidade local, de forma semelhante a como um dispositivo USB aparece como a sua própria unidade num computador. Uma vez montados desta forma, os ficheiros baseados na nuvem tornavam-se tão expostos à encriptação quanto os ficheiros num disco rígido local.

A maior ameaça de hoje: chaves e tokens roubados

À medida que a utilização da nuvem amadureceu, as táticas dos atacantes voltaram a mudar. Em vez de montar unidades manualmente, muitos vão agora atrás de chaves de API e tokens de

sessão — credenciais que concedem acesso direto, a nível de programa, a contas e dados na nuvem. Obter uma destas é comparável a roubar uma palavra-passe, exceto que frequentemente proporciona um acesso mais amplo e rápido aos recursos na nuvem do que apenas uma palavra-passe roubada.

Esta mudança é importante porque a mesma velocidade e escalabilidade que tornam a computação em nuvem valiosa para equipas de TI legítimas estão agora também disponíveis para os atacantes. Entre os clientes da Cyber Crucible no último ano, mais de metade sofreu uma tentativa de roubo de um token de sessão na nuvem com o objetivo de sequestrar a sessão ativa de um utilizador, enquanto menos de 9% sofreram algum comprometimento real de dados. Isto sugere que os atacantes estão a priorizar o roubo de credenciais e tokens como o seu principal ponto de entrada, sendo o roubo de dados um objetivo secundário.

Os dados na nuvem estão automaticamente seguros?

O armazenamento na nuvem não garante proteção contra ransomware ou roubo de dados. Simplesmente altera o método que os atacantes têm de usar para chegar a esses dados — deslocando o risco principal para o comprometimento de credenciais e tokens de sessão em vez da encriptação direta de ficheiros.

https://player.vimeo.com/video/1047006345

Ver no Vimeo · Legendas: Inglês, Francês, Espanhol, Árabe

Revision #1
Created 2026-07-24 06:10:21 UTC by Dennis Underwood
Updated 2026-07-24 06:10:21 UTC by Dennis Underwood