Plume Security

RansomStop for Google Drive Overview

Background

Ransomware has become one of the most prolific and impactful risks for almost every organization today. While most people think ransomware only affects your computer, it can also encrypt network-based storage like file servers, and even cloud-based storage like Google Drive. Computers are often configured to sync or backup data from their laptops to Google Drive. If the laptop is encrypted, the encrypted files are automatically uploaded to the Google Drive in the background. This means the copies of data you thought were safe in Google Drive, become encrypted as well. This makes recovering the files difficult or impossible, and can affect shared Drives across your organization, multiplying the impact of the ransomware attack.

Solution

RansomStop for Google Drive can monitor user and shared Drives in your organization and monitor the files for any signs of ransomware activity, i.e. maliciously encrypted files. Once ransomware activity is detected, RansomStop will disable the stolen account used by the attacker, and disable access to not only Google Drive, but all Google services such as Gmail, Calendar and Docs to limit any damages by the attacker. This happens in just a few seconds from the start of the attack.

Technical

RansomStop for Google Drive runs in your Google Cloud environment, so there is no need for any software to be installed on your endpoints. Installation takes about 10 minutes. Detection and response are all automated and run in real time. Policy and Alerts can easily be managed in the RansomStop Admin Portal, but this is an automated, set-it-and-forget-it solution.

Free Trial

Plume Security is offering free trials of RansomStop for Google Drive to interested organizations for 15 days. To find out more, get a demo or start your free trial, please contact sales@plumesecurity.com