Colonial Pipeline Ransomware Attack

Overview

Colonial Pipeline, which is the owner of the largest pipeline system in the United States, recently fell victim to a ransomware attack that forced the company to halt its operations and pay a $5 million ransom. This incident exemplifies the evolving tactics used by ransomware groups that leverage the fact that most every organization now must support remote or hybrid work.

This incident provides more evidence of organized groups carrying out scalable campaigns that increase their success rate and enable them to reinvest in new tools and procedures. Doing so enables them to take advantage of organizations with distributed workforces where security teams don't have the same visibility they once did when everything was inside the corporate perimeter.

Lookout Analysis

In this situation, employees expect seamless access to all resources from unmanaged and personal devices on networks outside the traditional perimeter. To them, it doesn't matter where that resource resides as long as they can access it, but for security teams that means broadening access capabilities to ensure everyone can be productive.

In addition, employees want to be productive from any device including their personal smartphone or tablet. Attackers know this and target employees through personal apps to steal their login credentials. This enables attackers to discreetly enter the infrastructure using legitimate credentials that a traditional VPN solution would likely not detect. Since VPNs tend to give unlimited access to whoever connects, the attacker can then move freely around various apps and other components of cloud and on-prem infrastructure.

Recommendation for Lookout Admins

While there is no silver bullet against ransomware, combining Lookout Zero Trust Network Access, Modern Endpoint Protection, and Phishing & Content Protection will help mitigate the risk. By doing this, Lookout admins can continuously assess risk across endpoints, protect employees from account compromise, and modernize access policies to cloud and on-premises infrastructure. Adopting this strategy grounded in Zero Trust ensures that only authorized users can access resources and enables admins to give the right employees enough data access to do their jobs, but not so much that any account or device has access to everything.

Lookout Zero Trust Network Access (ZTNA)

Lookout ZTNA enables organizations to implement granular identity and context-aware access controls that deliver consistent security and user experience across on-premises, IaaS, and SaaS apps. Security teams can limit access only to those who need it, extend advanced security to legacy apps, and implement agentless access from any endpoint device.

Click here to learn more about Lookout ZTNA