Lepide

How Lepide Would Have Helped to Prevent the Colonial Pipeline Attack

CASE STUDY

ABOUT THIS CASE STUDY

This is a case study of how Lepide would have helped prevent a real-world cyber-attack. It is theoretical. The Colonial Pipeline Company were not asked to participate in the case study, and the information on the attack was gathered from publicly available sources.

HIGHLIGHTS

HOW IT HAPPENED

- Hackers gained access to the network through an exposed password for an account within their Active Directory network
- This account was likely not intended for regular use and is thought to have belonged to an inactive employee.
- The password for this account was breached in a separate incident and leaked on the dark net. Attackers matched the breached credentials with social media data, this allowed them to understand they had a password to an administrator's account for Colonial Pipeline.

THE IMPACT

- The attackers gained access to Colonial Pipeline's systems and used ransomware to encrypt critical infrastructure data. This forced the company to shut down operations for six days, leading to fuel shortages and price hikes.
- Controversially, Colonial Pipeline opted to pay the ransom demand of 75 Bitcoin (around $4.4 million at the time) to regain access to their systems.

WHAT HAPPENED

The attack unfolded on May 7, 2021, targeting Colonial Pipeline, the largest refined products pipeline in the United States. Hackers affiliated with the DarkSide ransomware group gained access to the company's IT systems through an outdated VPN account. Here's the breakdown:

- **Access**: DarkSide exploited a vulnerable VPN login to infiltrate Colonial's network.
- **Data Theft**: They exfiltrated over 100GB of corporate data within two hours.
- **Ransomware Deployment**: They deployed ransomware, encrypting critical business systems.
- **Pipeline Shutdown**: As a precaution to contain the attack, Colonial shut down the entire pipeline, halting fuel transportation across the Eastern Seaboard.

THE IMPACT

The impact of the Colonial Pipeline attack was significant, leading to widespread disruptions in the fuel supply chain along the East Coast of the United States. Colonial Pipeline temporarily shut down its operations as a precautionary measure to contain the ransomware attack and assess the extent of the breach. This disruption caused shortages and panic buying of gasoline in various states, leading to fuel shortages at gas stations and a spike in fuel prices.

The incident highlighted the vulnerability of critical infrastructure, such as energy supply chains, to cyberattacks. The U.S. government and private sector entities have since increased efforts to enhance cybersecurity measures and resilience to protect against similar attacks in the future. The Colonial Pipeline attack also raised awareness about the importance of proactive cybersecurity measures and collaboration between public and private sectors to mitigate the impact of cyber threats on critical infrastructure.

SOLUTION

How the Lepide Data Security Platform Could Have Helped

With the benefit of hindsight, there were several ways in which Lepide could have helped Colonial Pipeline Company reduce the likeliness of the attack and speed up detection/response. These include:

1. **Reducing Active Directory Threat Surface**: The attack started with a breached active directory account. Later investigation discovered the account was inactive. With a solution like Lepide, inactive accounts can have passwords automatically reset, or shut down entirely as part of an automated process.

2. **Alerting / Anomaly Analysis / Response**: When an inactive account suddenly logs in and starts making changes that have never been seen before, Lepide's anomaly analysis would flag this up as a potential threat by sending alerts. It's possible to trigger actions off the back of these alerts such as ending a user session or even shutting down a server. This would have minimized damage attackers were able to do.

3. **Investigation**: When Colonial Pipeline noticed the attack, they shut down their infrastructure systems themselves, because they didn't know how far the attackers had gone. A system like Lepide may have enabled them to identify the scope of the attack and isolate affected areas of infrastructure.

1. Cleaning Up Inactive Accounts in Active Directory

Regularly cleaning up inactive Active Directory (AD) accounts is a crucial cybersecurity practice that aids in preventing ransomware attacks. Active Directory, integral to Windows OS, manages user accounts and access permissions within a network. By eliminating inactive accounts, the attack surface is reduced, thwarting potential entry points for hackers who often target forgotten accounts with weak passwords. Inactive accounts, if compromised, can serve as a starting point for lateral movement within a network during ransomware attacks. Cleaning up and deactivating such accounts limits pathways for attackers, preventing unauthorized access and privilege escalation.

Ransomware attacks frequently exploit stolen or compromised credentials, and inactive accounts may have outdated security configurations. Regular cleanup ensures that compromised credentials from inactive accounts cannot be utilized in launching ransomware attacks. Additionally, maintaining an accurate inventory of active users through regular AD cleanup facilitates better monitoring, detection, and response to unusual or suspicious activities. This proactive approach aligns with security best practices, compliance requirements, and enhances the network's overall resilience against cyber threats. Efficient incident response becomes possible with a well-maintained AD environment, focusing on active and authorized accounts during security incidents, thus minimizing the impact of potential ransomware attacks.

2. Alerting / Anomaly Analysis / Response

In the context of the Colonial Pipeline cyberattack, implementing a system like Lepide's anomaly analysis could have significantly enhanced threat detection and response capabilities. If an inactive Active Directory (AD) account suddenly logged in and initiated unusual changes, Lepide's system would promptly flag this as a potential threat and generate alerts. These alerts serve as early warnings, enabling security teams to swiftly respond to anomalous activities.

The anomaly analysis feature could have detected the unauthorized access and unusual behavior associated with the ransomware attack on Colonial Pipeline. Immediate alerts would have provided security personnel with real-time awareness of the threat, allowing them to take rapid actions, such as terminating the compromised user session or shutting down affected servers. This proactive response could have minimized the damage inflicted by the attackers, potentially preventing the widespread disruption of fuel supply chains along the East Coast.

In essence, integrating alerting, anomaly analysis, and threat response mechanisms into the cybersecurity infrastructure could have played a pivotal role in early detection and containment, fortifying the resilience of critical infrastructure systems like Colonial Pipeline against ransomware threats.

3. Investigation

Enhanced investigation capabilities, facilitated by a system like Lepide, could have significantly benefited Colonial Pipeline during the cyberattack in 2021. When the attack was detected, the company proactively shut down its infrastructure to prevent further damage, reflecting the uncertainty about the extent of the breach. Lepide's advanced capabilities, including detailed event logs and real-time reporting, could have provided crucial insights into the scope and progression of the attack.

With comprehensive event logs, Colonial Pipeline's security teams would have been able to conduct a more granular analysis, understanding the specific actions taken by the attackers. This detailed information could aid in isolating affected areas of the infrastructure, allowing for a more targeted and strategic response. Better investigation capabilities would enable a deeper understanding of the attack vectors, compromised systems, and potential points of lateral movement within the network.

Furthermore, real-time reporting offered by Lepide could have allowed Colonial Pipeline to make informed decisions promptly. Understanding the attackers' movements and tactics would have empowered the company to implement more effective containment measures, potentially reducing the overall impact and downtime. In summary, improved investigation capabilities would have provided Colonial Pipeline with the insights needed to make informed decisions during the early stages of the attack, enhancing their ability to mitigate and recover from the cyber incident more efficiently.

Lepide

Get peace of mind that your identities and data are secure with Lepide.

Take a look at our interactive demo to see how Lepide can help your business achieve your security and compliance goals.

Launch Interactive Demo