SILVERSKY
Elevate your Cybersecurity

Case Study

Ransomware

CASE STUDY

SilverSky Discovered Ransomware

Introduction: The Incident

A global logistics company was the subject of a ransomware attack, but SilverSky's capabilities reduced the impact.

Incident Identification and Classification

During the customer's onboarding of SilverSky's Lightning Managed Endpoint Detection and Response (MEDR) service, several detections were identified in the Lighting Portal that were associated with potential ransomware during the deployment phase.

It was determined that this was a high-severity event. Multiple alerts were detected that indicated that executable files associated with a ransomware attack were present on computers in the network.

Incident Details and Description

Using advanced endpoint protection capabilities, the SilverSky service identified elements of a ransomware attack on computers within the customer's network. These devices had been previously protected by traditional antivirus services, which were not sophisticated enough to link the variables together to identify the ransomware. The Lightning MEDR technology quarantined the devices and blocked malicious communication across the network, preventing the further spread of the ransomware. The SilverSky onboarding team and SOC analysts team worked with the customer to take actions to clean infected systems and add advanced protections. These actions mitigated a potentially catastrophic event and enabled the business to remain operational throughout the evaluation, blocking, and cleanup phases.

linkedin.com/company/silversky
www.silversky.com

1-800-234-2175
learn@silversky.com

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560

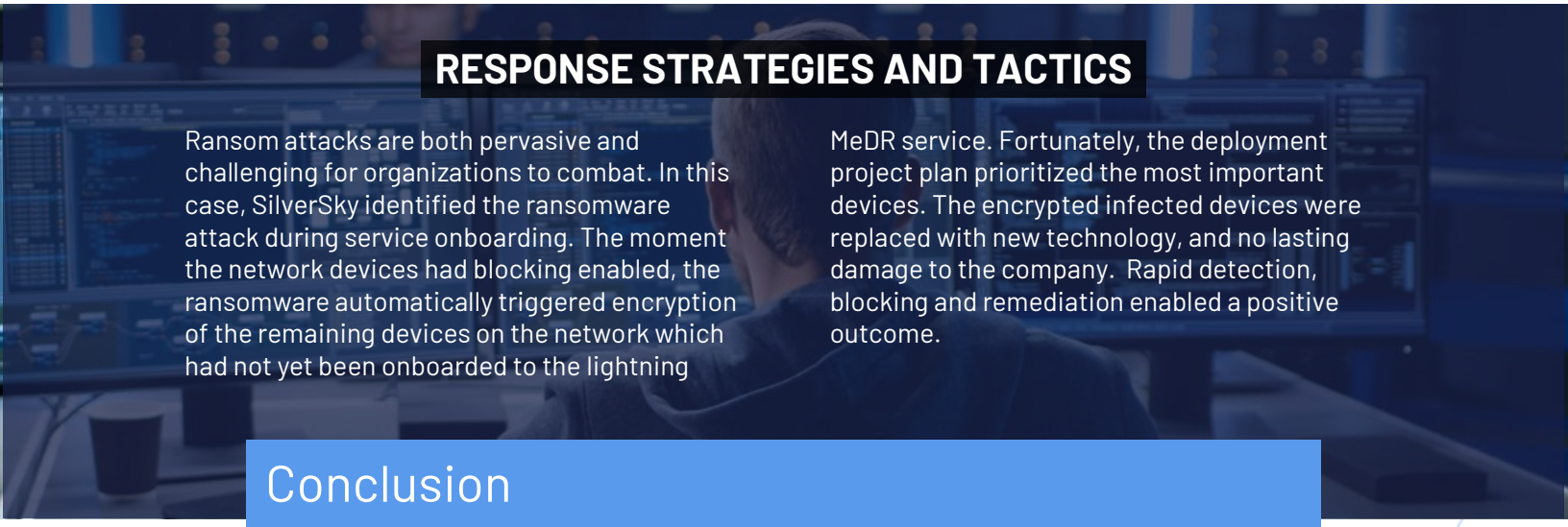
CASE STUDY

Operational Response Framework

The customer had just started onboarding SilverSky's Lighting MEDR service and had successfully pushed the services to roughly two-thirds of the business's devices. During deployment, these agents are typically deployed in a listening/learning state to enable SilverSky the ability to coordinate with the customer to define normal behavior on applications and processes.

Once the agent was successfully activated, the implementation engineer was immediately alerted to the threat lingering on some of these devices. The engineer immediately called the IT contact and was authorized to activate Lighting MEDR into an aggressive defensive posture to prevent these files from executing their encryption capabilities.

Unfortunately, in doing so, the hacker was made aware of these defensive moves and activated the remaining devices with encryption that had not been onboarded to the Lighting MEDR service. Thankfully, for the customer, these devices were not critical as they were the logistical driver's laptops used to support cellular devices.



RESPONSE STRATEGIES AND TACTICS

Ransom attacks are both pervasive and challenging for organizations to combat. In this case, SilverSky identified the ransomware attack during service onboarding. The moment the network devices had blocking enabled, the ransomware automatically triggered encryption of the remaining devices on the network which had not yet been onboarded to the lightning MeDR service. Fortunately, the deployment project plan prioritized the most important devices. The encrypted infected devices were replaced with new technology, and no lasting damage to the company. Rapid detection, blocking and remediation enabled a positive outcome.

Conclusion

Achievements and Future Directions

Once all the compromised devices had been reimaged, all Active Directory accounts had been evaluated and all devices were locked down to the new security posture. The client agreed to have SilverSky conduct a full business control assessment. Although this did not increase the services offered by SilverSky, it enabled the business to map out a 1-year plan on how they can improve business operations while also reducing their risk of future cybersecurity attacks.

linkedin.com/company/silversky
www.silversky.com

1-800-234-2175
learn@silversky.com

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560