SILVERSKY
Elevate your Cybersecurity

Case Study

Malware Attack - Financial Services

CASE STUDY

SilverSky Discovered Banking Trojan

Introduction: The Incident

The company was subject to a credential-scraping malware attack.

Incident Identification

New customer deployment of Managed extended Detection and Response (MxDR) services for a customer whose security environment currently uses Meraki firewalls, Proofpoint Email, and a basic anti-virus agent for their computers and servers. Once deployed, SilverSky's Lightning MxDR analytics detected low and slow unauthorized communications to Russia, Latvia, and Cyprus created by a credential-scraping malware attack.

It was determined that this was a high-severity event. The malware generated hundreds of event logs, five alerts, and a single case. This enabled the SilverSky Security Operations Center (SOC) to notify the customer and devise a game plan to remediate the threat.

Incident Details and Description

After the root cause analysis, it was determined that before SilverSky was engaged, the customer was subjected to a phishing attack with an email with a URL embedded. The URL tricked one of the users into downloading a file that installed the malware. Because the company's security technology heavily relied on traditional signature-based examination and the variant of malware was unknown, this attack was successful enough to be installed.

At the time of detection, the hackers prepared to use the malware to send unauthorized wire transfers. But thanks to the quick hast and intelligence available to the SilverSky SOC, the analyst could determine the means of the attack and work with the customer to stop the event.

CASE STUDY

Operational Response Framework

The SilverSky analyst conducting this analysis was able to collaborate on the case generated. Still, additional research was required due to the customer's lack of data and the previous security tools. They informed the customer of the investigation and began further analysis. They could correlate the traffic to the Techniques, Tactics, and Procedures (TTPs) associated with a new variant of malware that had also been seen within other financial customers supported by SilverSky.

Upon confirmation, the analyst reengaged the customer and identified a malicious agent running on several hosts within the customer's environment. This was not detected due to the lack of technical capabilities in the customer's antivirus, which relied heavily on signature detection. Since this was a new variant of malware, no signatures had been updated to enable detection.

The analyst was able to work with the customer to reimage all impacted hosts and confirm that no persistent threats existed. Throughout the investigation, SilverSky's Lighting MxDR continuously analyzed and protected the organization.

RESPONSE STRATEGIES AND TACTICS

SilverSky's goal is to meet customers wherever they are within their security journey. During the sales process, SilverSky discussed with the customer the deficiencies of their traditional security tools. It was understood that after switching to SilverSky Lightning MxDR, they would be able to enhance their security posture and work on a strategy to grow it over time.

Due to the quick actions of the SilverSky SOC and subsequent education of the customer, SilverSky strategically aligned with the customer to implement a better security posture utilizing their tools and SilverSky Lightning MxDR. This meant that the customer could improve their security and use the investments already made and stopped paying for technology that had been proven to provide little worth.

Conclusion

Achievements and Future Directions

Post-incident, the customer enhanced their security posture through SilverSky's education, enabling them to improve security prevention capabilities. They were also able to demonstrate to the organization's Board of Directors the value the partnership created and how they were able to reduce the company's risk, create operational efficiencies, and save money while doing all this.

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

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

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560