Detecting Ransomware Lateral Movement in a Global Enterprise's Network

Executive Summary

A global enterprise with over 100,000 employees wanted to build post-breach detection capabilities to identify and stop in-network and insider threats before they could cause damage.

The team decided to add Zscaler Deception's deception-based active defense platform to their security stack with the objective of detecting lateral movement.

They chose deception over other threat detection solutions because of the tactical advantage that active defense provides in threat detection. They were interested to see how it played out in real life, especially in terms of operational compatibility and scale.

The Challenge

Operating a vast network brings its own set of challenges. A varied asset base, network configurations that vary from region to region, distributed applications, and a complex Active Directory setup. Achieving visibility in all parts of the network was a challenge. The company needed visibility into key segments without unjustifiable operational burdens. The primary concern was around the spread of ransomware. Any security initiative to address this challenge needed to maximize the chances of threat detection.

The Solution

The idea of planting decoy file shares in key segments was adopted as the primary strategy to detect ransomware in the lateral movement phase. In the event of a detection, the organization's internal incident response process would kick in.

The goal was to detect ransomware spreading on the network (preferably measured in seconds), quickly understand the nature of ransomware (measured in minutes), and allow established incident response processes to contain the threat (measured in hours).

INDUSTRY

Enterprise

NO. OF ASSETS

100,000+

EXISTING DEFENSES

- Firewall
- Network Segmentation
- Anti-Virus
- SIEM

DECEPTION COVERAGE

DC and DMZ+

DEPLOYMENT TIME

4 Weeks

HOW WE HELPED

- Decoy network services planted in the DMZ and DC detected ransomware spreading in the network when it encrypted the decoys.
- Valuable telemetry from the detection resulted in the identification of the ransomware strain and timely remediation.

The Deception Strategy

Considering the size of the organization and operational limitations, we recommended the team to deploy network decoys and concentrate them in the DMZ and DC.

The hypothesis behind this decision was that assets in the DMZ were at a high risk of infection and lateral movement activity would likely be recorded in those segments.

The decoys themselves were projecting a diverse set of network services ranging from decoy SMB file shares to FTP servers to SSH servers and decoy applications.

Zscaler Deception in Action

Zscaler Deception notified the team of an incident where suspicious activity was recorded on multiple network decoys. The decoys were the first to raise an alarm.

The Investigation

The analysis showed that all decoys masquerading as file shares had been encrypted within the DMZ segment. The decoy files hosted on these file shares had been encrypted and renamed, which allowed for easy identification of the ransomware strain.

Root cause analysis further revealed that the lateral movement phase of the ransomware attack was detected by Zscaler Deception less than a minute after it began encrypting assets.

Why Was Zscaler Deception Effective?

As a detection control, deception is technique and behavior-agnostic. Unlike some security products that flag specific signatures, IoCs, or behaviors; deception-based defenses serve as a catch-all for all bad activity.

It doesn't matter what the adversary does or how she does it. The very fact that someone accesses decoys is a high-confidence indicator of a breach and must be investigated swiftly.

For deception to be effective, only two things matter:

- There should be a varied set of decoys deployed in the environment.
- The deployment should be strategic to cover common attacker tactics.

Zscaler Deception's initial investment in strategically planning the deployment of network decoys paid-off. It ensured that decoys were present in key segments, enabling the security team to be alerted quickly to the spread of the ransomware.

After midnight, the attacker started targeting systems for encryption. A minute later, Zscaler Deception had raised a detection. In fact, Zscaler Deception was the first security control to raise an alarm.

Takeaways

Deception is a form of active defense and an effective one at that. However, you must think strategically about where you place the deception. This requires stepping into the adversary's shoes, anticipating her moves, and then planting traps on the path that she is most likely to take. Based on our experience, we highly recommend deploying:

- Deception in the network.
- Deception on the endpoints.
- Deception in the Active Directory.

We understand that organizations have numerous constraints. We encourage our customers to work through these by finding the best possible solution to ensure that all the key deception elements have been deployed.

Threat Detection and Active Defense With Deception Technology

Download the Whitepaper >

Defend Your Network, Endpoints, Cloud, and AD With Deception

Get a Demo >

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com