Creating Private Threat Intelligence With Deception Ahead of a Business Launch

Executive Summary

One of the top 5 global banks by assets under management was launching a new business line.

The objective was to cater to a more progressive and younger generation of customers looking for innovative investment and banking solutions.

Operationally, this entailed integrating technology and processes at the new business line with their core banking systems.

These were uncharted waters, and the bank's security team wanted to build a threat model ahead of the launch so that they could defend the new business line against targeted threats.

The Challenge

Introducing state-of-the-art technology and a new class of investment assets to a traditional and storied banking set up came with a new set of processes and operational challenges.

The security team did not have any intelligence or research to understand the threat landscape before launching the new business line.

The bank was looking for a solution that could help them build a threat model beforehand. This solution had to meet two non-negotiable conditions:

- Under no circumstances were competitors to find out about the existence of the new business line.
- Any security control implemented to understand the threat landscape couldn't result in any reputational damage to the bank.

INDUSTRY

Banking & Finance

NO. OF ASSETS

78,000

EXISTING DEFENSES

- SIEM
- EDR
- IDS / IPS
- Firewall

DECEPTION COVERAGE

Perimeter

Endpoints

DEPLOYMENT TIME

3 Weeks

HOW WE HELPED

- Created a decoy replica of the new business line.
- The bank's security team was able to put this decoy business line out in the wild to gather threat intelligence and build a picture of the threat landscape that they would be encountering after launching the business.

The Solution

The idea of creating a decoy replica of the new business line and putting it out in the world emerged as the strategy for building the threat model and gathering intelligence beforehand.

The goal was to detect interest from targeted threat groups in the new business line. Additionally, the bank also wanted to catch any insider threats targeting the new initiative.

The Deception Strategy

Zscaler Deception's deception-based active defense platform generated a decoy entity and website complete with a customized network profile, user interface, and content that reflected the nature of the soon-to-be-launched business. The decoy replica was delinked from the bank to ensure that no threat actor could claim "hacking" it and malign their reputation. Any interaction with these Internet-facing assets would be considered malicious since no one knew of their existence.

In addition to the decoy website, our platform also created and hosted docker web applications patterned after the bank's custom apps that would be used as part of the new business line's operations. These docker decoys enabled the bank to gather intelligence on threat groups specifically seeking out those apps.

Decoy users masquerading as employees of the decoy entity were created to intercept phishing and social engineering attacks. These decoy users also had their very own social media profiles to make them look legitimate.

Decoy files alluding to the existence of this decoy entity were planted on employee laptops to detect any insiders that would attempt to access or exfiltrate this information. The decoy files were hidden from plain view to ensure that no legitimate user would be able to access them.

Zscaler Deception in Action

Over a six-month period, the decoy entity was targeted by several threat actors from Russia and North Korea among others. The security team was able to build out a threat model that informed their defense strategy. Post-launch, the private threat intelligence program was extended to the newly launched business line as well as the legacy banking business.

Why Was Zscaler Deception Effective?

Building a threat model and gathering intelligence before launching a new business is a unique problem to solve, and there aren't many solutions that can do this out-of-the-box. Zscaler Deception fit the bill perfectly.

Zscaler Deception's ability to ingest keywords and datasets to automatically generate everything from a decoy entity to websites, users and files made a project like this technically and operationally feasible in the first place.

Then there was the matter of efficacy. The intelligence generated from decoys is pretty accurate and local to the organization. Unlike traditional threat intel that tells you someone did something bad to someone, somewhere, deception-based private threat intelligence alerts you to adversaries targeting you in particular.

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 at the perimeter
- 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.

Useful Resources

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