RedHelm

Security-First IT Management

Incident Response Case Study

THE PROBLEM

Our security team detected a sophisticated phishing campaign targeting both our employees and customers. The attack used polymorphic links that adapted based on the victim's browser, making traditional detection methods less effective. The scope of the attack appeared widespread, potentially affecting our entire customer base and beyond. This created an urgent need to **identify**, **analyze**, and **mitigate the threat** before significant damage could occur.

THE SOLUTION

We implemented a multi-faceted approach to address the threat:

- **Rapid Detection & Investigation:** Leveraged employee and customer reports to identify the emerging threat.
- **Technical Analysis:** Conducted forensic examination of suspicious emails, links, and attachments using sandbox environments to safely analyze the malicious content.
- **Pattern Recognition:** Identified common elements in the polymorphic phishing links, establishing reliable Indicators of Compromise (IOCs) across different iterations of the attack.
- **Enterprise-Wide Hunt:** Used established IOCs to proactively search for evidence of compromise across customer environments.
- **Customer Engagement:** Worked directly with affected customers to remediate identified compromises, particularly focusing on those without our EDR solution.
- **Broad Communication Strategy:** Distributed comprehensive threat intelligence, including all discovered IOCs, to our entire customer base across all business lines.

THE RESULTS

Through our coordinated response:

- We successfully **identified multiple customers** who had clicked malicious links but had not yet experienced full compromise.
- We **provided timely remediation assistance** to affected customers, preventing potential data breaches or network infiltration.
- Our proactive communication **empowered all customers with actionable intelligence** to protect their environments.
- We **demonstrated our commitment to security transparency** by openly sharing threat intelligence across our entire customer base.
- The incident **highlighted the value of our EDR solution**, as compromises were primarily identified in environments without this protection.

SUMMARY

This case study illustrates RedHelm's ability to rapidly detect, analyze, and respond to sophisticated phishing threats, while simultaneously supporting our customers through comprehensive threat intelligence and remediation assistance.

If you need help with incident response or preventative measures to minimize your risk exposure to scenarios like these, visit our website at **www.redhelm.com** and reach out for support.