Deception in action

The top ten real-world threats captured by Zscaler Deception

Deception-based Active Defense against targeted attacks

Deception is one of the most effective strategies to detect human-driven attacks that usually bypass predictable defenses. Its goal is to disrupt adversary tactics and force the adversary to make mistakes which lead to detection.

Our Deception platform is deployed with a strategy that considers how the adversary might move in your environment. This has allowed us to detect serious threats impacting global organizations.

This document looks at some of the top attacks from our global decoy mesh.

Top 10 in-the-wild real world detections

01 North Korean APT

02 Human-operated ransomware tactics (pre-infection)

03 Internal recon and scanning

04 Credential stuffing

05 MikroTik Router exploitation

06 Distributed brute force attack

07 X-ray machine controller compromise

08 MedusaLocker ransomware spread

09 Early warning against ransomware

10 Shadow RDP

CASE STUDY 1

North Korean APT Attack on a Large Global Conglomerate

The Incident

SMB port scan on decoy triggers a detection

- NTLM username captured
- Context revealed this was a compromised user

Triage and investigation

- C2 domain similar to legitimate domain
- Our investigation isolated two DLLs with no known signatures
- DLLs contained hardcoded credentials and loader code to receive further commands
- Offline confirmation from team about targeted attempt from North Korea by group “Hidden Cobra”

Deception Strategy

- Identified critical parts of the infrastructure most likely to be attacked and placed decoys in those segments
- Zscaler Threat Hunting support for endpoint investigation and triage

Outcome

- Zscaler Deception was the only solution to raise an alarm in the environment

Takeway

A deception strategy tailored to environmental constraints and desired outcomes is one of the most important factors that drive Active Defense success

CASE STUDY 2

Pre-infection detection of a ransomware operator targeting a retailer

The Incident

Decoy service account triggered by Patient Zero

- A system scanned Active Directory decoys for property Service Principal Name (SPN) on 8th May, 2021

Lateral Movement to a decoy over SMB from Patient Zero

- NTLM authentication revealed SYSTEM account compromise on May 13th,2021

Ransomware propagation via WinRM

- Decoys capture port scan on port 5985 on June 10th,2021

Ransomware deployed via WinRM on June 13th

- Unfortunately, due to a lack of timely response, Ransomware infected multiple servers on the network

Deception Strategy

- Active Directory decoys to detect account compromise
- Network decoys in the DC and DMZ to detect lateral movement

Outcome

- Zscaler Deception gave an early warning of an imminent ransomware attack a month before the incident

Takeway

Active Directory decoys are one of the most reliable sources of an imminent infection warning in a ransomware attack. Security teams must prioritise these for investigation

CASE STUDY 3

Internal recon and scanning at a large bank

The Incident

Attacker gets a foothold via a compromised router

- A compromised router is the source of extensive interaction with decoys on multiple ports including SSH

Adversary spends over 6 hours executing hundreds of commands in 3 SSH decoys

- Login with root/root
- Situational awareness commands
- Attempted to compile custom network scanner binary
- Steal passwords from /etc/passwd + /etc/shadow
- Attempt to use decoy as a pivot (blocked)
- Attempt to sniff network using TCPDump

Deception Strategy

- High-interaction network decoys that not just detect adversaries but also engage them long enough to reveal their strategy and intention

Outcome

- Prevented impact as attacker was busy in the decoy while customer attempted to locate and access the router

Takeway

Human-driven attacks consider their target's defense strategy and avoid traditional detection controls altogether. In this case, they targeted a router — a device that typically doesn't have EDR installed. Security teams should deploy decoys of such devices to detect sophisticated adversaries

CASE STUDY 4

Credential Stuffing Attack On A Law Firm With High-Profile Clients

The Incident

Alert raised for credential stuffing on internet-facing Citrix decoy

- 200+ compromised domain credentials submitted to decoy
- Attack originated from the infrastructure of a Russian cloud service provider

Response and containment actions

- Dynamic block list at the Firewall using the orchestration capability
- Attempt to use decoy as a pivot (blocked)
- Attempt to sniff network using TCPDump

Deception Strategy

- Internet-facing decoy applications commonly attacked by adversaries for credential validation
- Managed Threat Hunting service

Outcome

- Zscaler Deception deflected an attack away from production assets right at the beginning of the kill chain

Takeway

Internet-facing decoys that mimic remote access services and applications with zero-days and known vulnerabilities deflect pre-breach attacks

CASE STUDY 5

MikroTik Router Exploitation Activity

The Incident

Alarm raised on a custom MikroTik SSH decoy

- Scanned decoys on known MikroTik RouterOS ports like 8291/tcp, 8728/tcp, and 22/tcp (SSH)
- Interacted with custom MikroTik decoy's SSH service using a GO-based tool (SSH-2.0-Go)
- Credential brute force recorded
- Multiple situational awareness commands captured
- Scheduled task was created to fetch and execute from the Internet

Deception Strategy

- Customised decoys to mimic specific components actively used in the environment

Outcome

- Source isolated
- Upfront access to useful telemetry like credentials and commands without having to pour through logs

Takeway

Deception is only as good as how believable it is. Decoys must appear and be functional enough to facilitate attacker engagement. In this case, the SSH decoys were successfully able to confuse the adversary into revealing the tooling C2 server

CASE STUDY 6

Brute Force Attacks On A Large Financial Institution

The Incident

Perimeter decoys detect multiple brute-force attempts

- Attacks originated from numerous sources
- Attempts made against decoys with publicly known default credential combinations
- Comprehensive manual web application exploitation identified based on timestamps using BurpSuite and Nuclei Scanner

Response and containment actions

- Dynamic block list at the Firewall for all sources submitting credentials via orchestrate function
- Attack sources were not identified in any threat intel sources until three days later

Deception Strategy

- Internet-facing decoys mimicking remote access applications and other services with known vulnerabilities or zero days
- Managed Threat Hunting service

Outcome

- Ability to block multiple sources based on a tactic was leveraged to limit impact

Takeway

Zscaler's Internet-facing decoys generate valuable private threat intelligence not captured by traditional threat intel feeds and is a reliable source of early warning of an imminent attack

CASE STUDY 7

Human-operated Targeted Attack On a Hospital

The Incident

PsExec-like behaviour usually associated with APT group observed against decoys

- Source was an X-ray machine controller
- Accessed service control manager via DCE/RPC on decoys to start services (PsExec behaviour)
- Port scan for common lateral movement ports on multiple decoys (135,445,3389)
- Common remote access software detected (RemCom RemoteAdmin)
- Investigation reveals presence of tools like Mimikatz

Deception Strategy

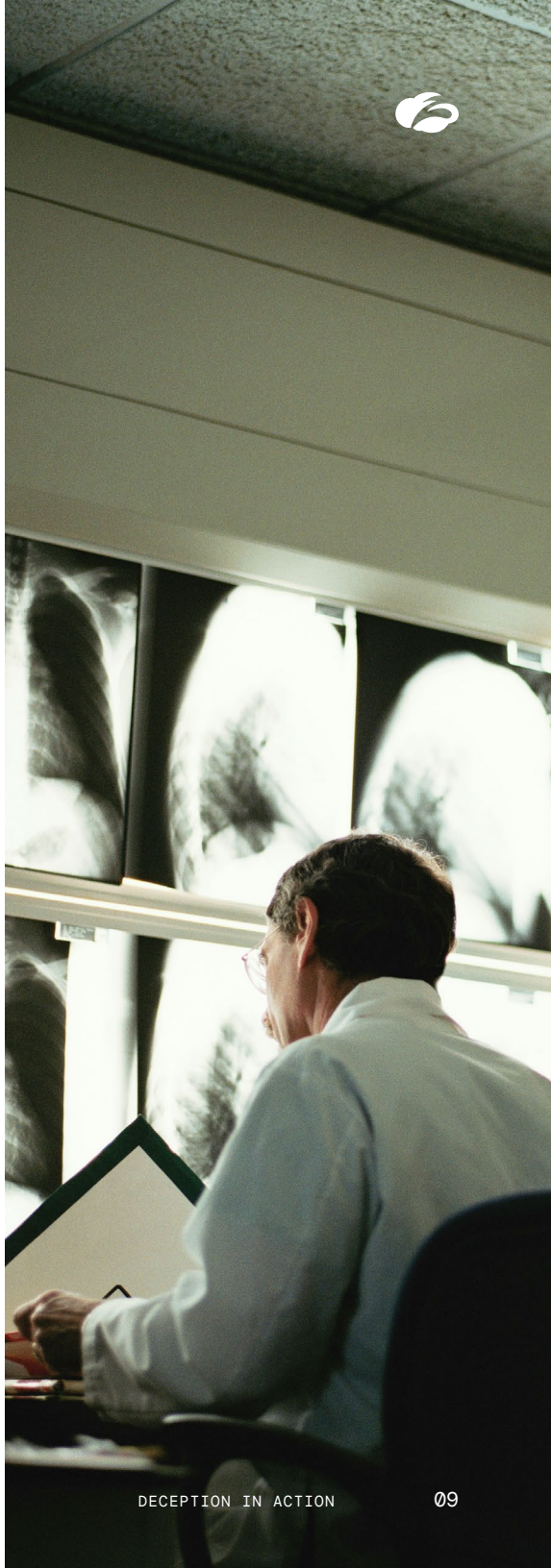
- Strategic placement of decoys in segments hosting critical hospital equipment
- Endpoint lures pointing to decoys

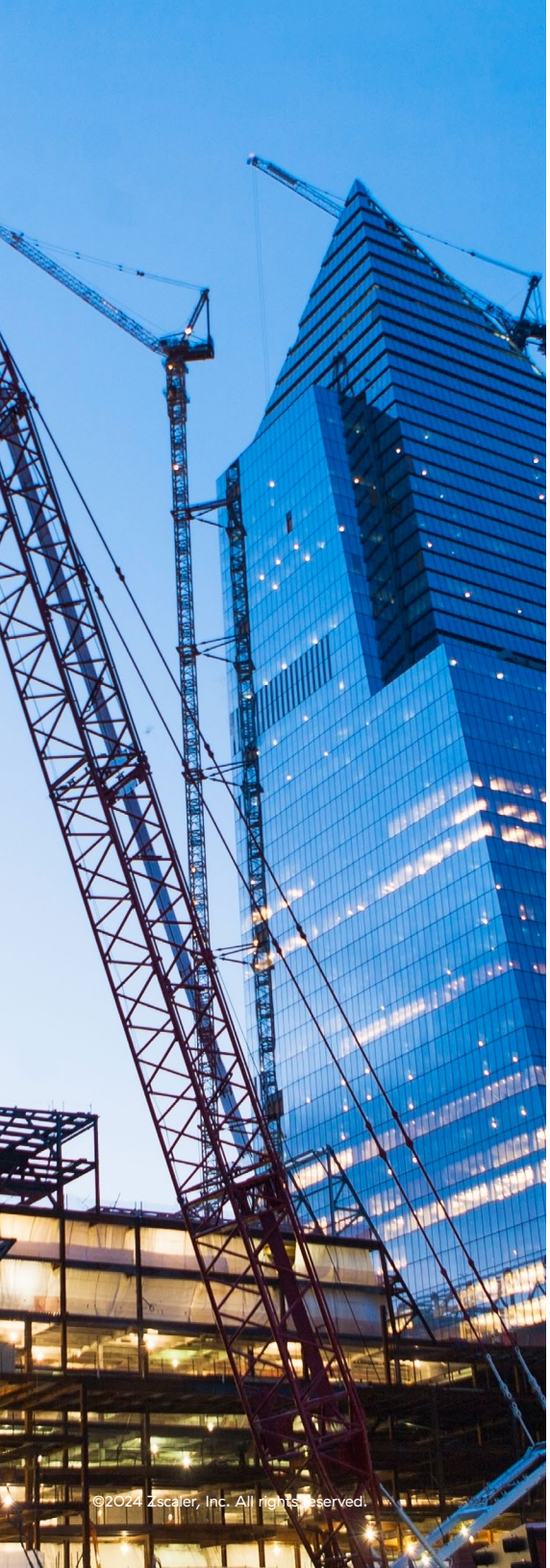
Outcome

- Timely detection and containment of a targeted attack

Takeway

Deception is effective for assets like hospital equipment, IoT devices, PoS systems, etc. where traditional threat detection controls cannot be deployed





CASE STUDY 8

MedusaLocker Ransomware Spread At a Conglomerate

The Incident

Alarm raised on encryption of decoy file shares

- More than 50 sources accessed decoy SMB shares
- Decoy files were renamed with the extension ".ReadInstructions"
- Username captured was a privileged credential

Deception Strategy

- Strategic deployment of SMB Share decoys in key segments specifically for Ransomware use-cases

Outcome

- Rapid isolation of server segments limited the spread of ransomware

Takeway

One decoy is better than no decoy at all. Even if you're not ready for a full scale deployment, a limited and strategic deployment will punch above its weight when it matters

CASE STUDY 9

Early Warning Of An Impending Compromise

The Incident

Privileged credential usage on a decoy triggered an alarm at a global manufacturing organization

- Source accessed multiple decoy shares
- NTLM username captured triggers ThreatParse rule to identify potentially privileged accounts based on keywords like *adm*, *svc*, *bkp*
- Account confirmed to be compromised domain administrator

Deception Strategy

- Deception deployment with many constraints. Relied on Active Directory and endpoint lures to channel adversary towards decoys
- Customised rules and phone alerts for interactions with particular decoys

Outcome

- Detected the threat one week before the FBI alerted the client about an impending ransomware attack based on intel they gathered from the dark web

Takeway

Sometimes, organizations have to work around certain environmental constraints. Unlike traditional detection controls that need to be pervasive to be effective, you can go really narrow with deception and still accomplish the goal

CASE STUDY 10

Shadow RDP Detection At FMCG company

The Incident

Decoy user logon failures observed

- Multiple logon failures for decoy accounts
- Captured Windows logs did not reveal source
- Worked extensively with customer on RCA which involved tracing authentication flow
- Discovered Azure system with RDP open to the Internet

Deception Strategy

- One of the AD Decoy users was created with a name available in a common dictionary

Outcome

- Revealed a first-of-its-kind detection use case
- Identified a misconfiguration that could have serious business impact
- Leveraged the learning to extend the use case to other managed service clients and proactively identify 3 similar occurrences

Takeway

Since deception detects attacks based on the intention of the adversary instead of signatures and heuristics, it results in effective detection of unknown-unknowns from time to time

When it comes to hunting, decoys aren't new. But in today's digital world, decoys take a different shape. Dynamic, strategic, and clandestine, trapping attacks is not only a way to mitigate threats, but also a means of gaining intelligence—which is immediately added to the Zscaler security cloud.

Interested in learning more about decoys as a security tactic? Explore some of our resources here: zscaler.com/products/deception-technology

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. To learn more, visit www.zscaler.com.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com