RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SBX3-WIL7**

Tube – A Reverse SOCKS Proxy for Embedded Systems and Offensive Operations

Evan Anderson

Principal Technologist
Randori
@syndrowm

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Agenda

- Context
- Why Target Embedded Systems?
- Attack Scenario
- Tube Overview
- Defending Against Tube

Introduction

Evan Anderson

Founding Team & Principal Technologist, Randori

More than 15 years of experience in red teaming, vulnerability research, exploit development and is a founding member of the NCCDC Red Team. Prior to co-founding Randori, he worked at Kyrus Technologies supporting commercial and federal projects.

Randori

RSAConference2022

Let's Start With Some Context

Embedded System Attacks Are Not New

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

April 16, 2018 Wang Wei

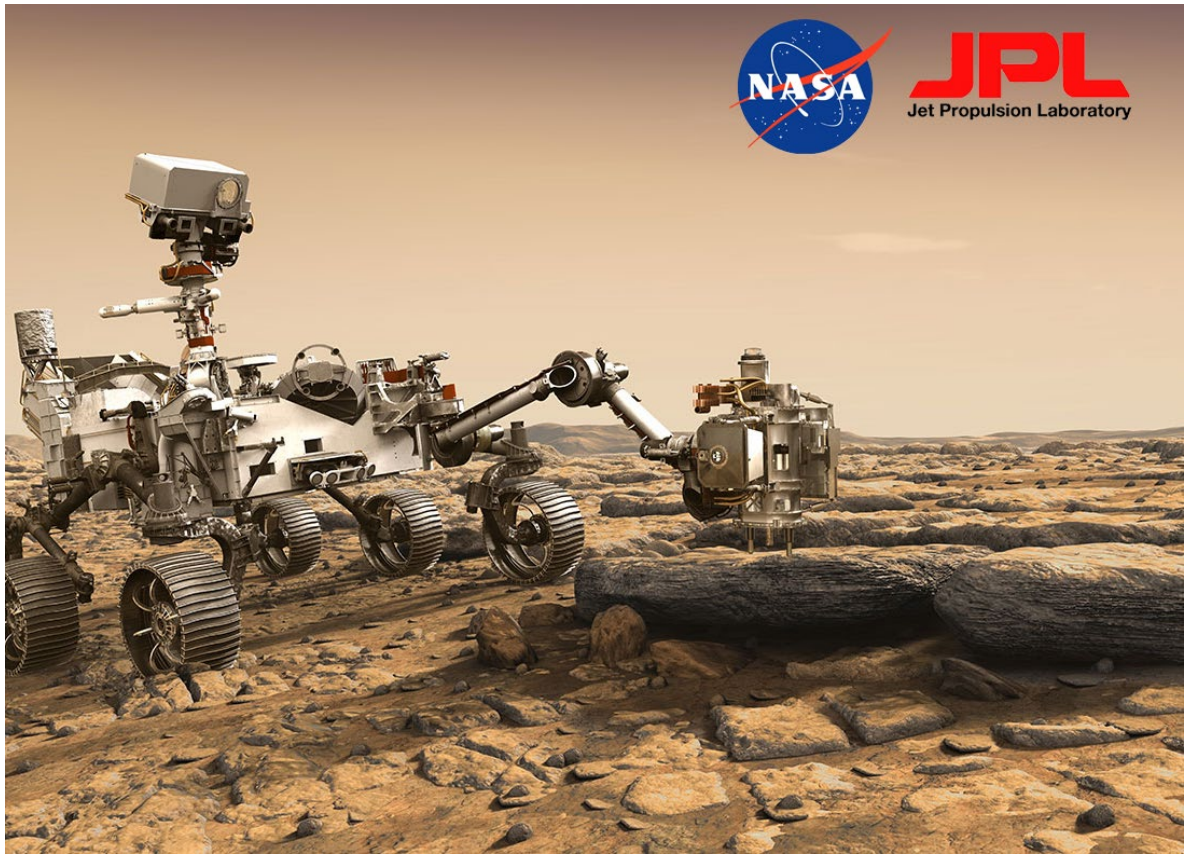
2017

"Somebody got into the fish tank and used it to move around into other areas of the network and sent out data… 10Gb were sent to a device in Finland"

- DarkTrace

Randori

JPL Breached by RasberryPi



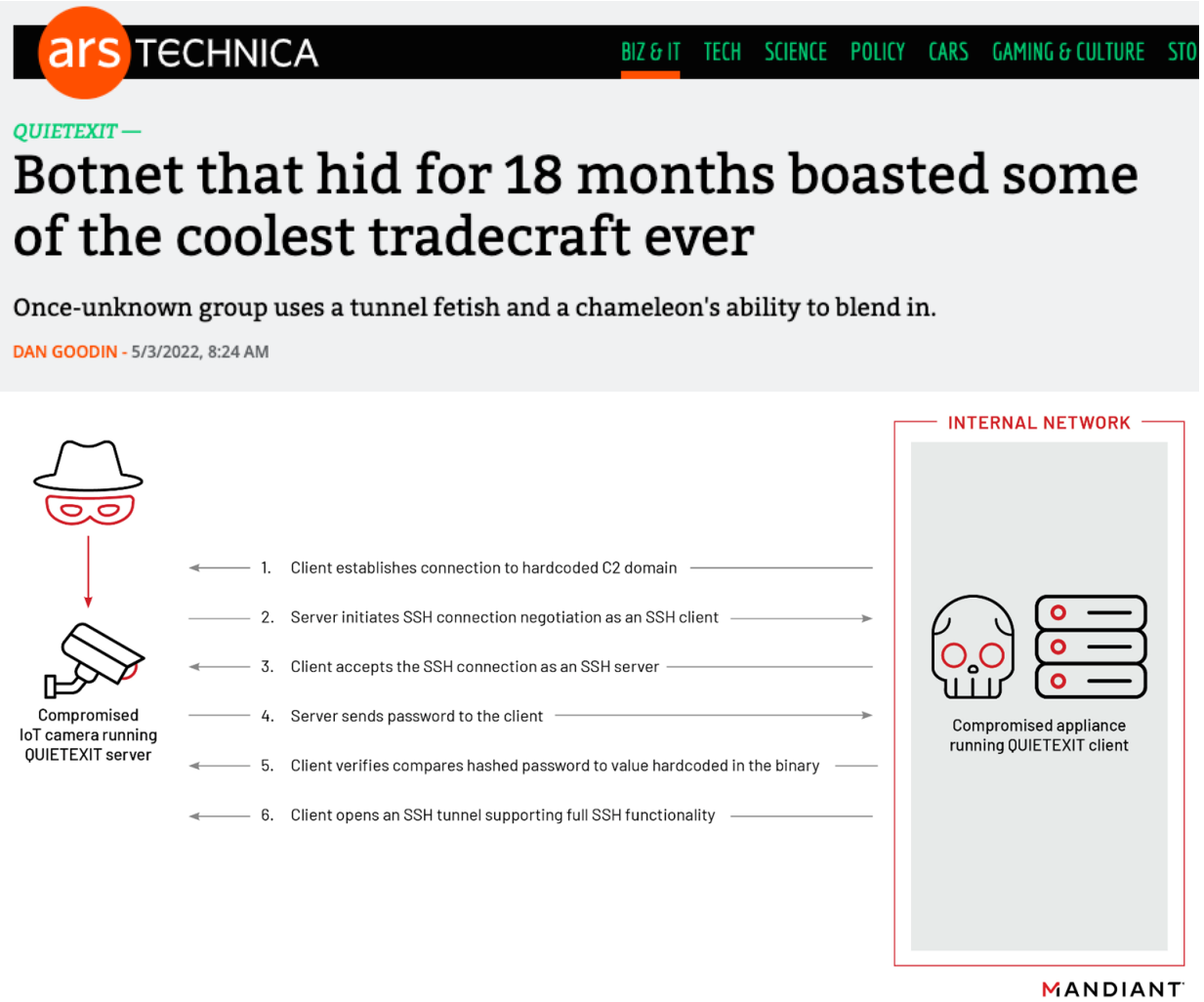
2019

"The attacker went undetected…for approximately 10 months…the attacker successfully accessed two of the three primary JPL networks. Accordingly, NASA…temporarily disconnected several space flight-related systems from the JPL network.

- NASA Inspector General Report

Randori

Mandiant UNC3524



2021

"Part of the group's success…can be credited to their choice to install backdoors on appliances within victim environments that do not support security tools…The high level of operational security, low malware footprint, adept evasive skills, and large IoT botnet set this group apart"

- Mandiant

Techniques

- Initial Access (?)
- Establish C2
- Persist
- Move Laterally
- Exfil

New Actors, Old Techniques

- tsocks/proxychains
- Metasploit
- SSH
- Cobalt Strike
- socat
- Tube

Researchers Have Been Pointing Out For Years

Attacking Networked Embedded Systems

Presented at DEF CON 10 (2002), Aug. 3, 2002, noon (50 minutes)

Servers, workstations and PCs are the common targets of an average attacker, but there is much more to find in todays networks. Every device that has a processor, some memory and a network interface can become a target. Using printers and other common devices as examples, we will show how to exploit design failures and vulnerabilities and use the target as an attack platform. We will also release some tools, methods and sample code to entertain the audience and aid further vulnerability research in this area.

black hat®

RSA® Conference

Randori

Link to Talk: https://www.youtube.com/watch?v=TpYRQOA3WLc

Folks Worth Following

https://twitter.com/michaelossmann
https://twitter.com/travisgoodspeed
https://twitter.com/devttys0
https://twitter.com/joegrand
https://twitter.com/_MG_
https://twitter.com/mubix
https://twitter.com/n00py1
https://twitter.com/sho_luv

RSAConference2022

Why Target Embedded Systems?

What Are Embedded Systems?

An **embedded system** is a computer system—a combination of a computer processor, computer memory, and input/output peripheral devices—that has a dedicated function within a larger mechanical or electronic system.

Randori

What Are Embedded Systems?

- Examples:
  - Security Cameras
  - VoIP Phones
  - Printers
  - Card Readers
  - HVAC Controllers…

Why Target Embedded Systems?

Embedded systems are just network-attached computers.

But you don’t treat them like that.

Why Target Embedded Systems?

- Attributes:
  - Unlikely to have EDR
  - Often setup and forgotten
    - Unpatched
    - No Updates
  - Typically use default passwords
  - Contain interesting data

Randori

Why Target Embedded Systems?

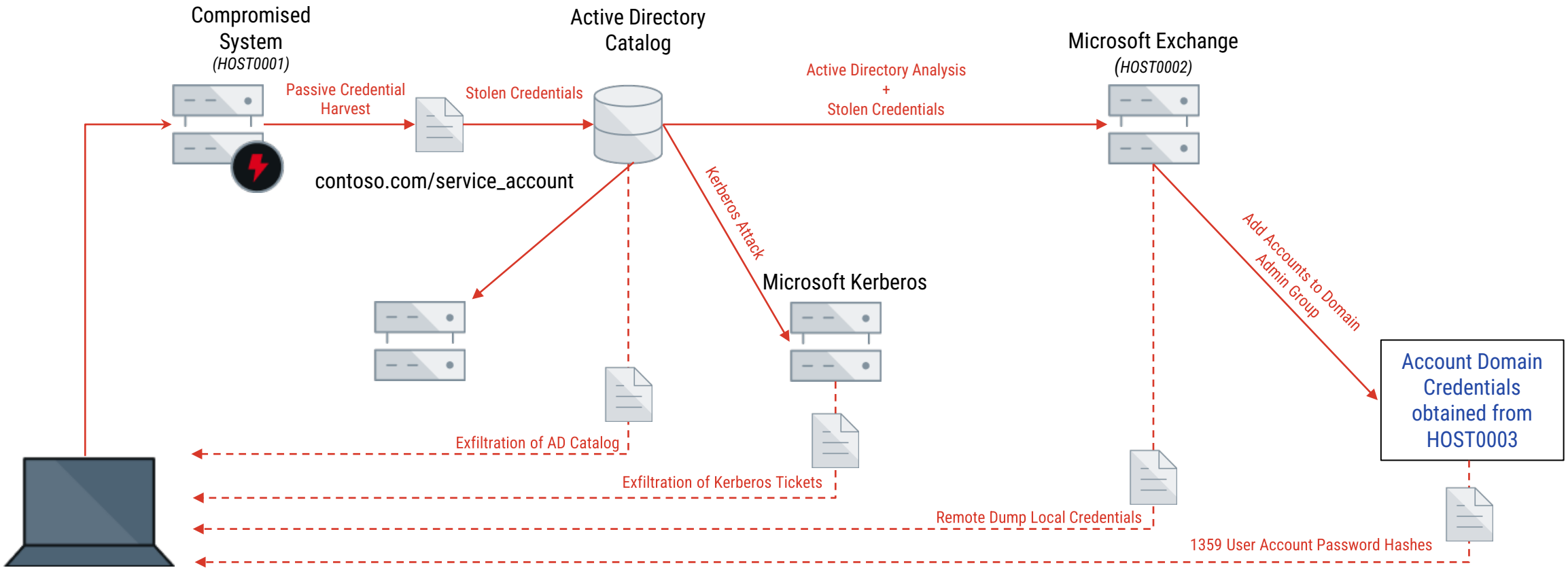
- An **embedded system** is a fantastic place to persist.
- Why:
  - Limited monitoring
  - Static environments
  - Access to other devices
  - Admin privileges

Randori

RSAConference2022

Attack Scenario

Example Kill Chain

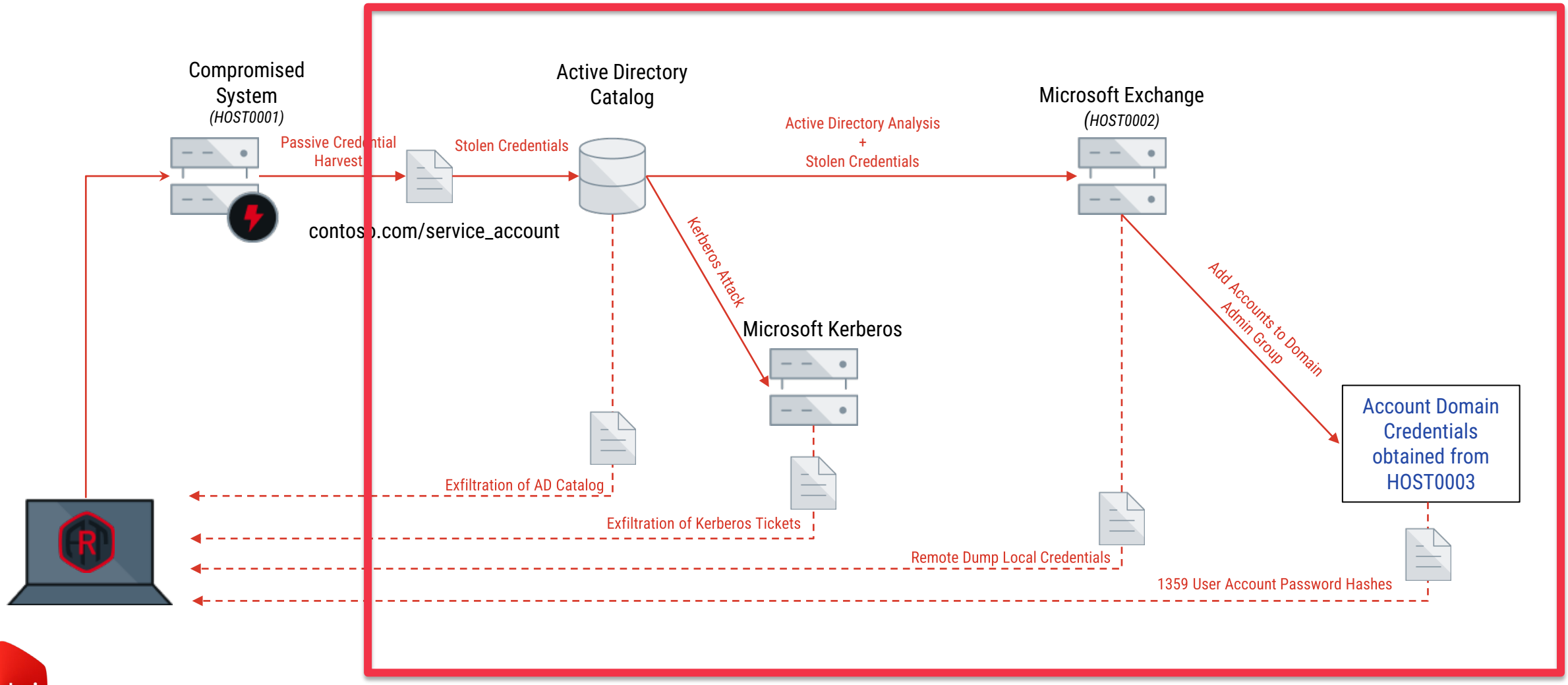


Randori

RSAConference2022

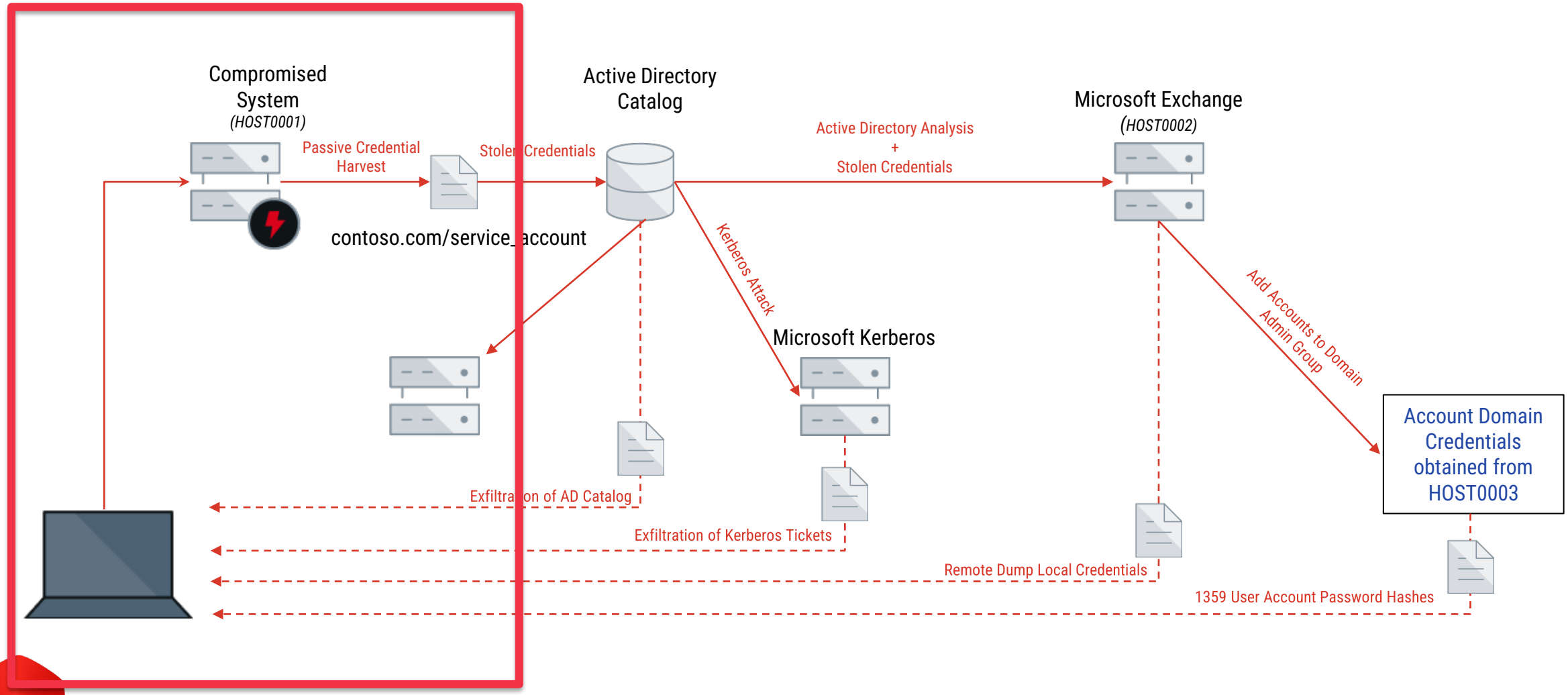
Tube Overview

Example Kill Chain



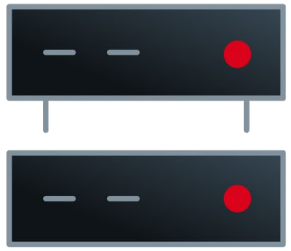
Randori

Example Kill Chain

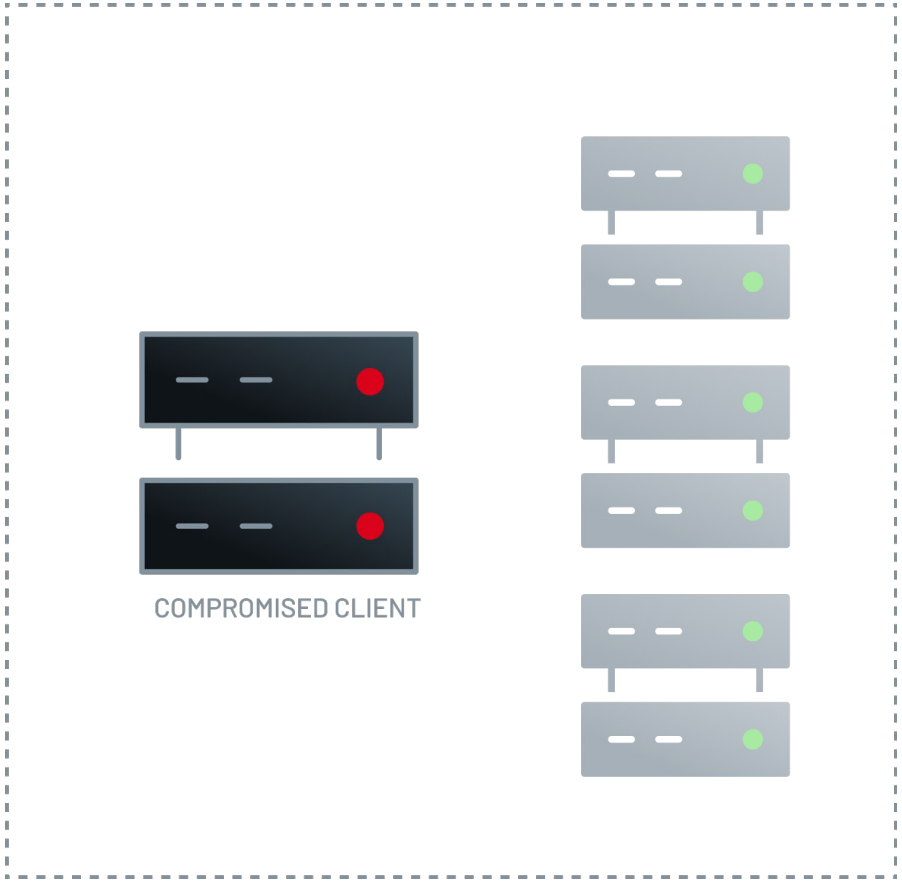


Tube – Reverse SOCKS4a Proxy

@SYNDROWM

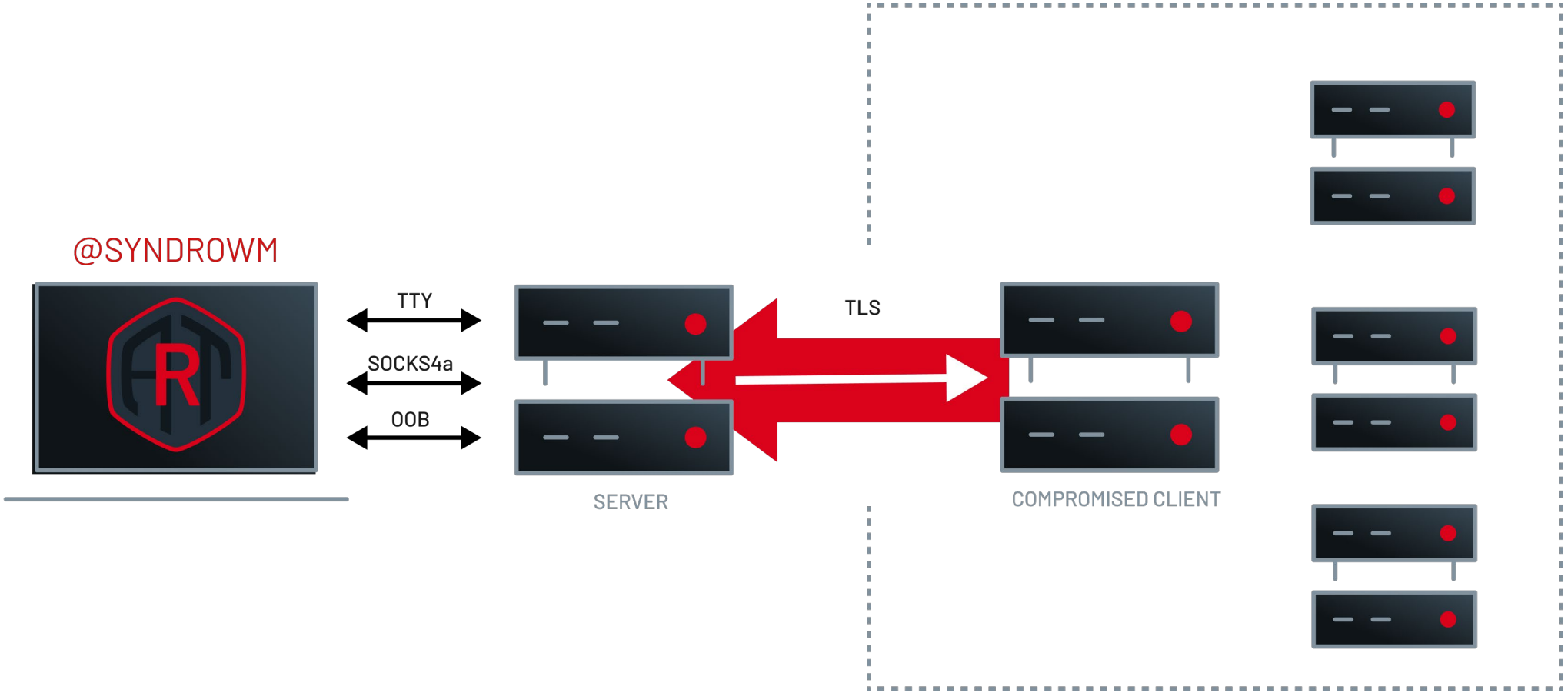


SERVER



Randori

Tube – Reverse SOCKS4a Proxy



Randori

Tube – Overview

- Reverse SOCKS proxy for use on embedded systems
- Component of Randori's CART platform
- Similar too existing toolsets

Tube – Problem We Were Solving

Operational Requirements

- Low memory footprint
- Cross-platform OS support
- Small binary
- Works without privileged access
- Stand alone
- Multi-protocol support

Randori

Tube – How We Use at Randori

- What We Can Do:
  - Exfiltrate data through embedded systems
  - Gain network access and establish C2
  - Bypass firewalls
  - Pivot across networks
  - Route traffic
  - Escalate privileges

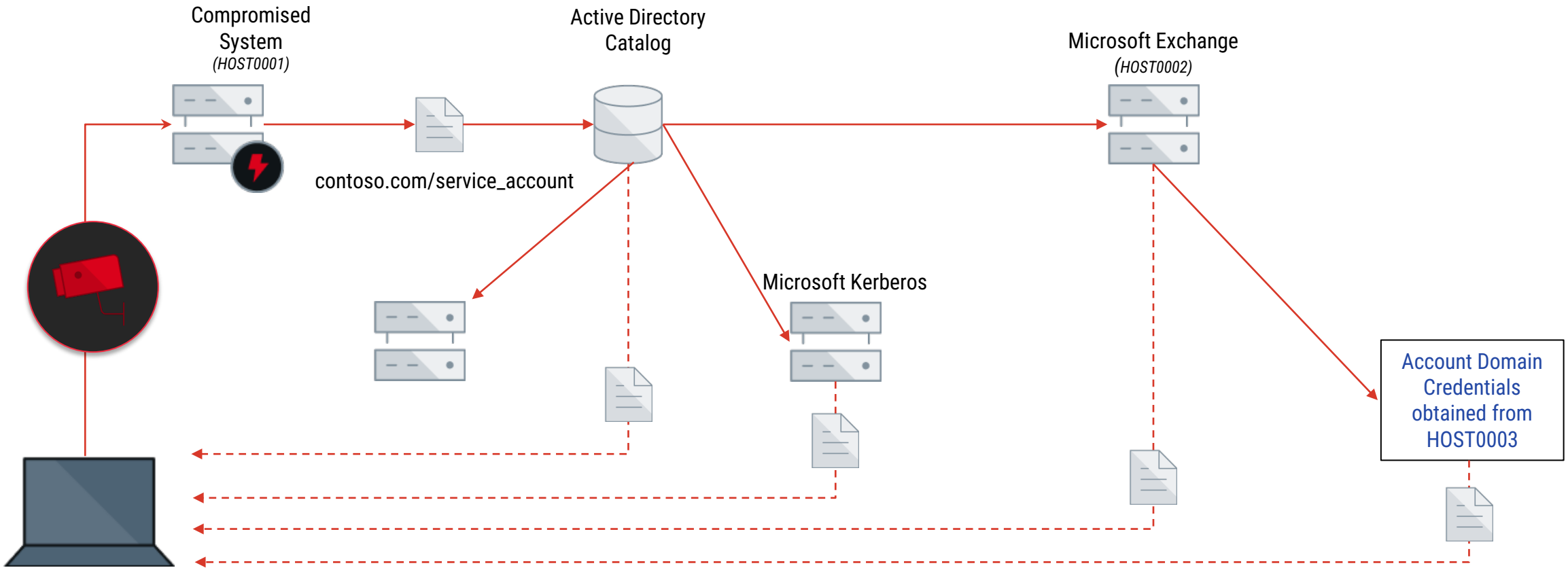
RSAConference2022

Defending Against Embedded System Attacks

Defending Against Embedded System Attacks

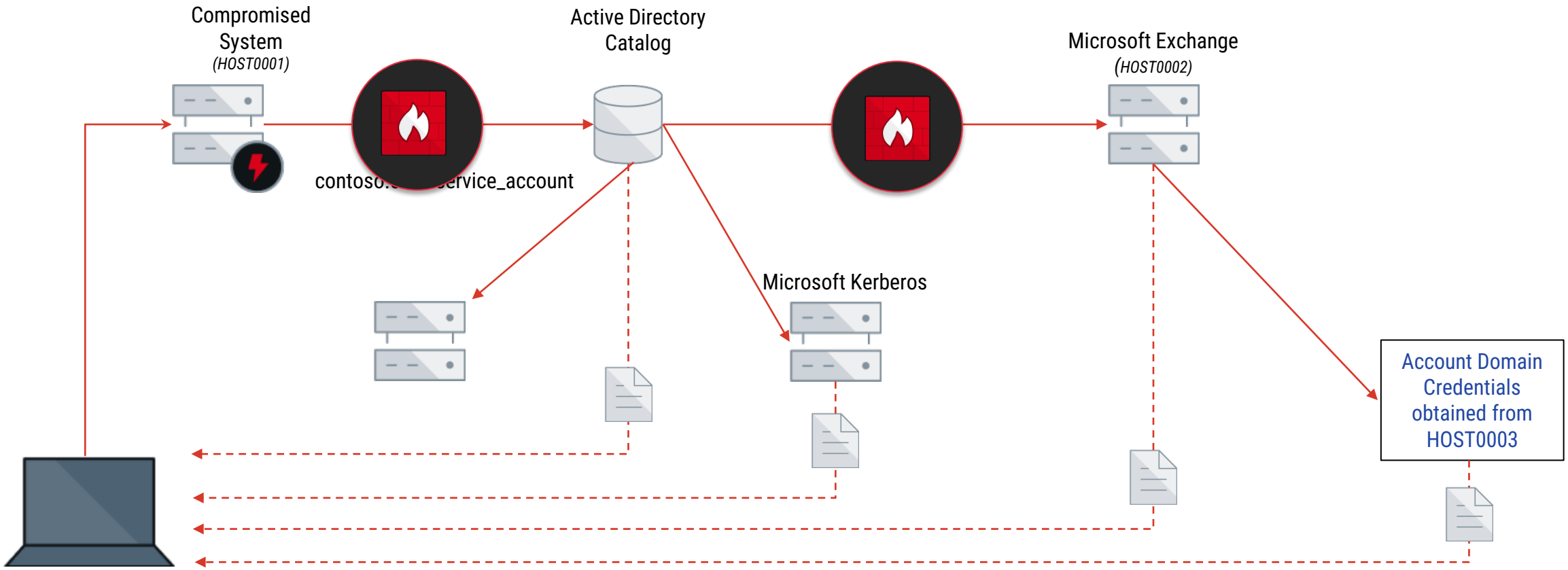
1. Monitor your attack surface
2. Segment your networks
3. Implement default-deny
4. Know what normal looks and alert on abnormal traffic
5. Check for default credentials
6. Manage and patch your embedded devices
7. Set Honey pots / tokens

Monitor Your Attack Surface



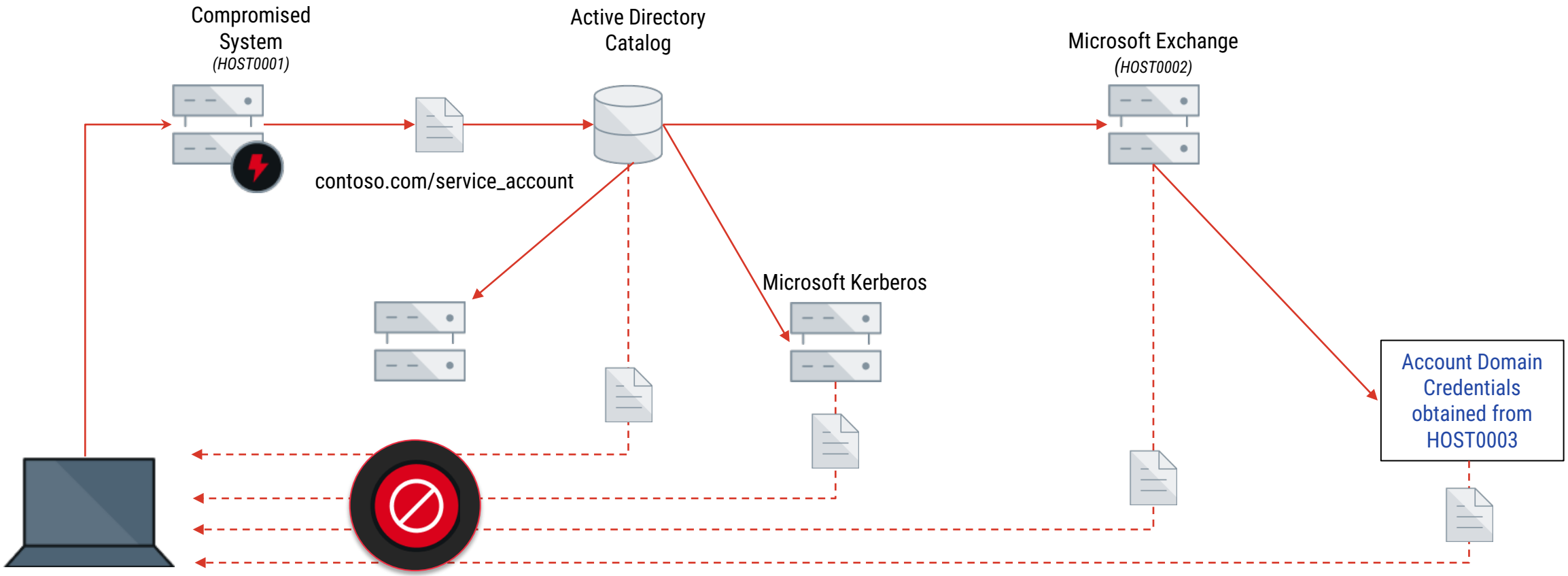
Randori

Segment Your Network



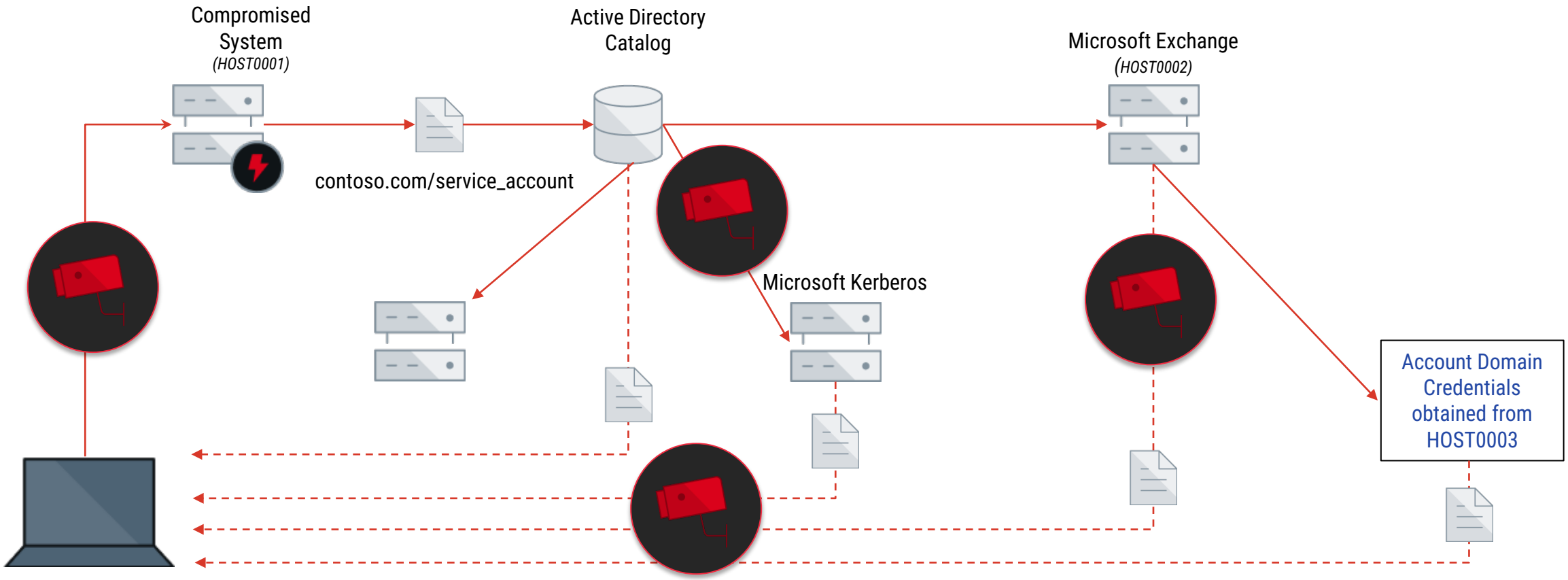
Randori

Implement Default Deny



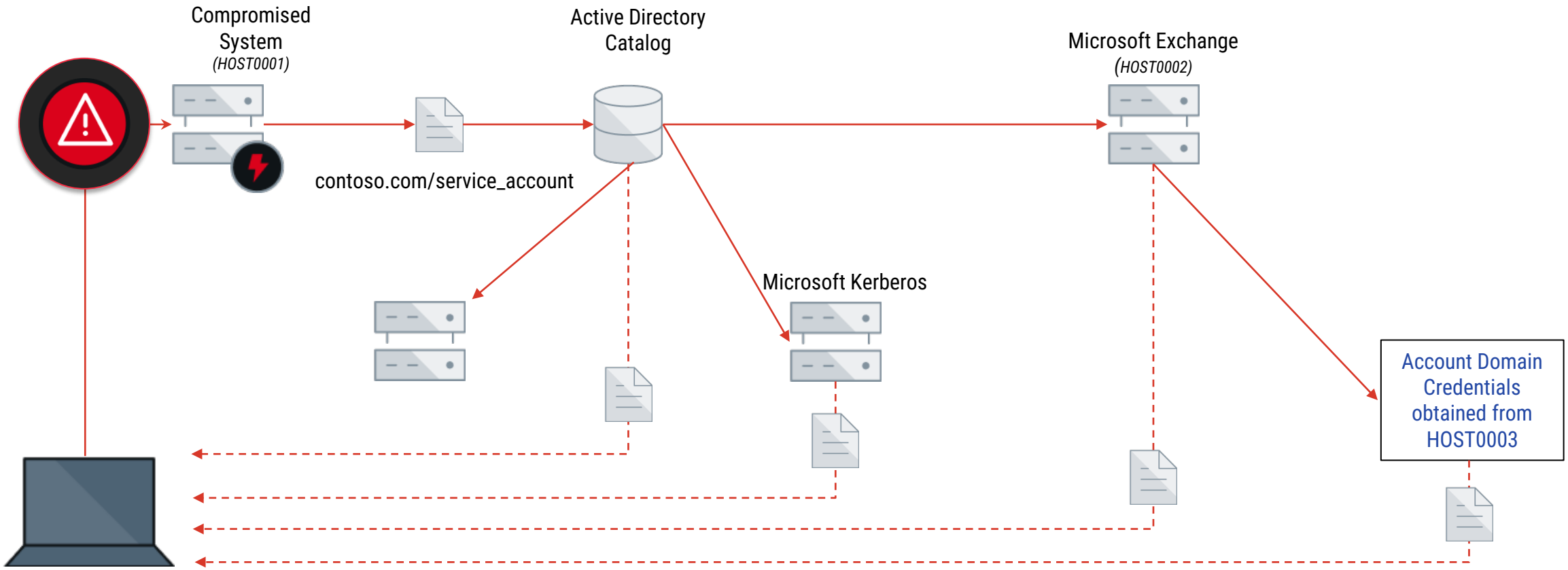
Randori

Know What Normal Looks Like



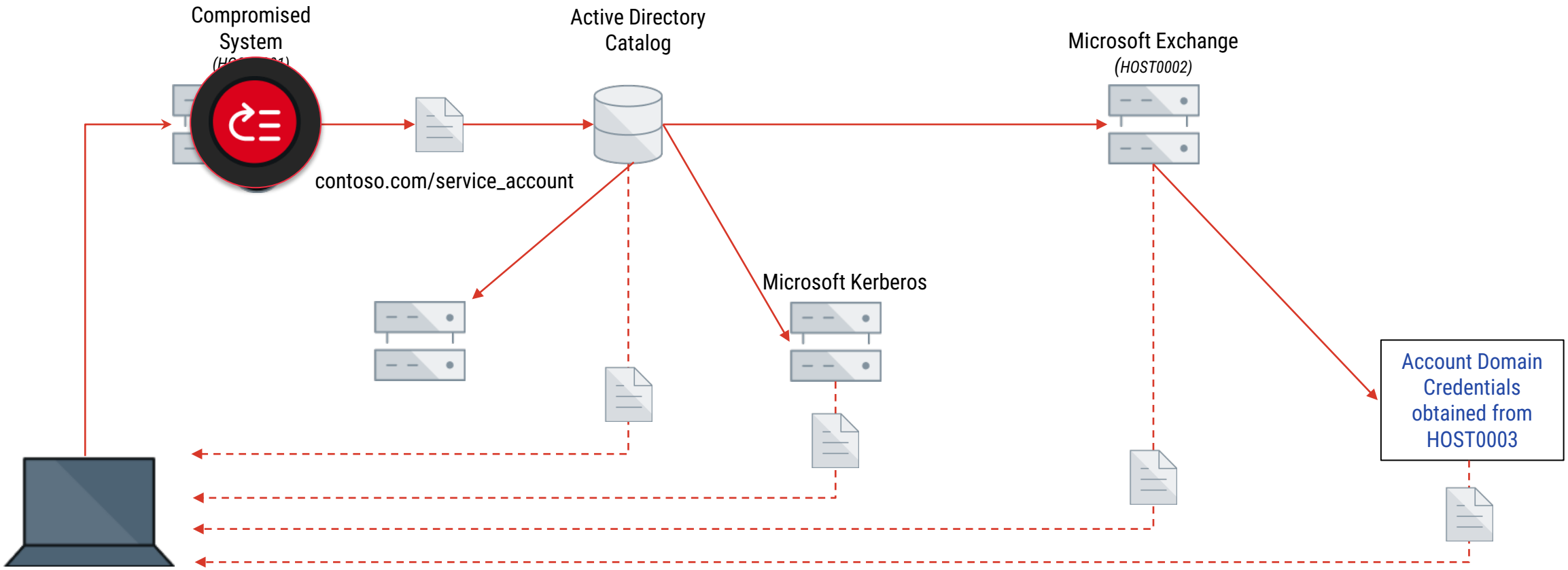
Randori

Check for Default Credentials



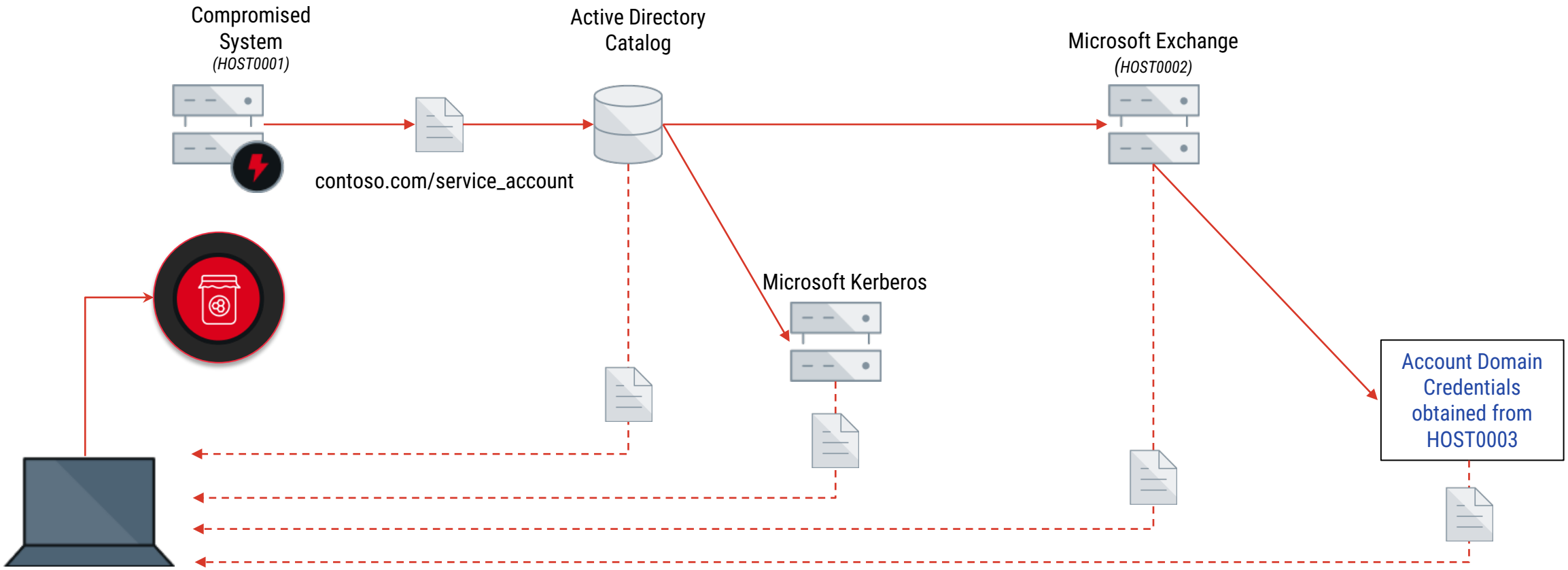
Randori

Manage & Patch Embedded Devices



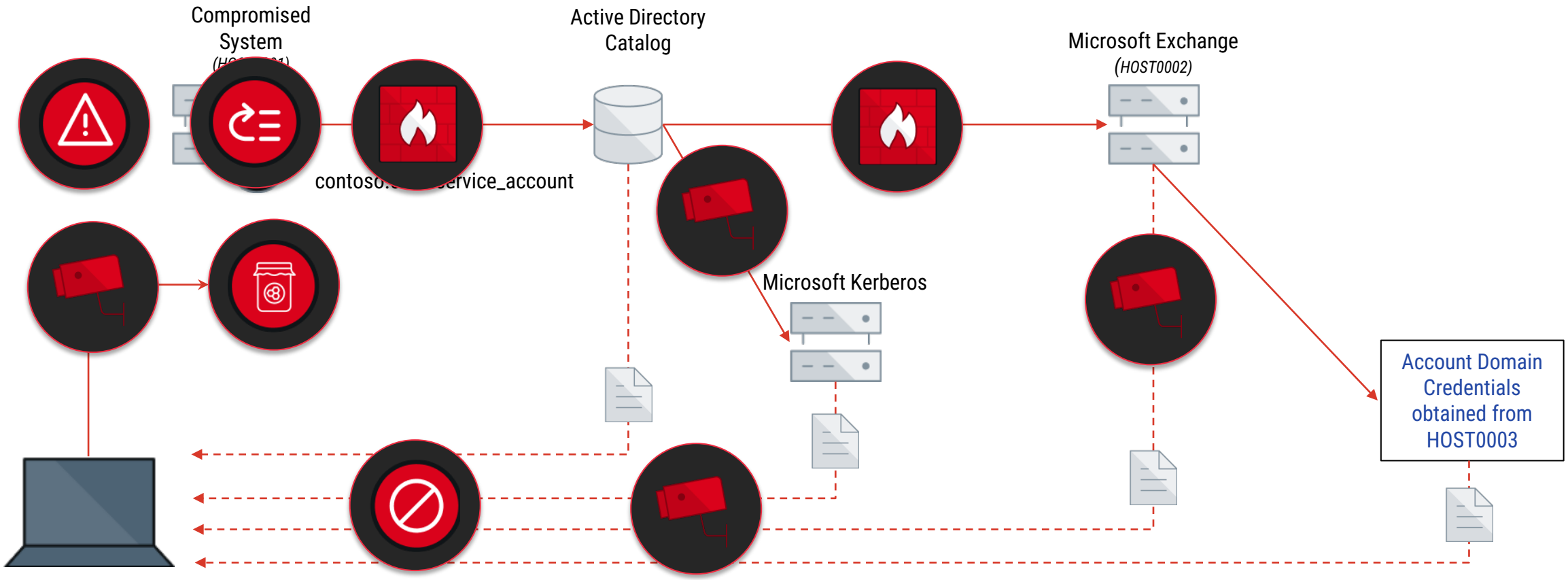
Randori

Set Honey Pots



Randori

Set A Minefield for Attackers



Randori

RSAConference2022

Get Your Tube [SOCKS] On!

Visit the Randori Booths to Get Your Pair

#5363 North Hall

#3202 South Hall