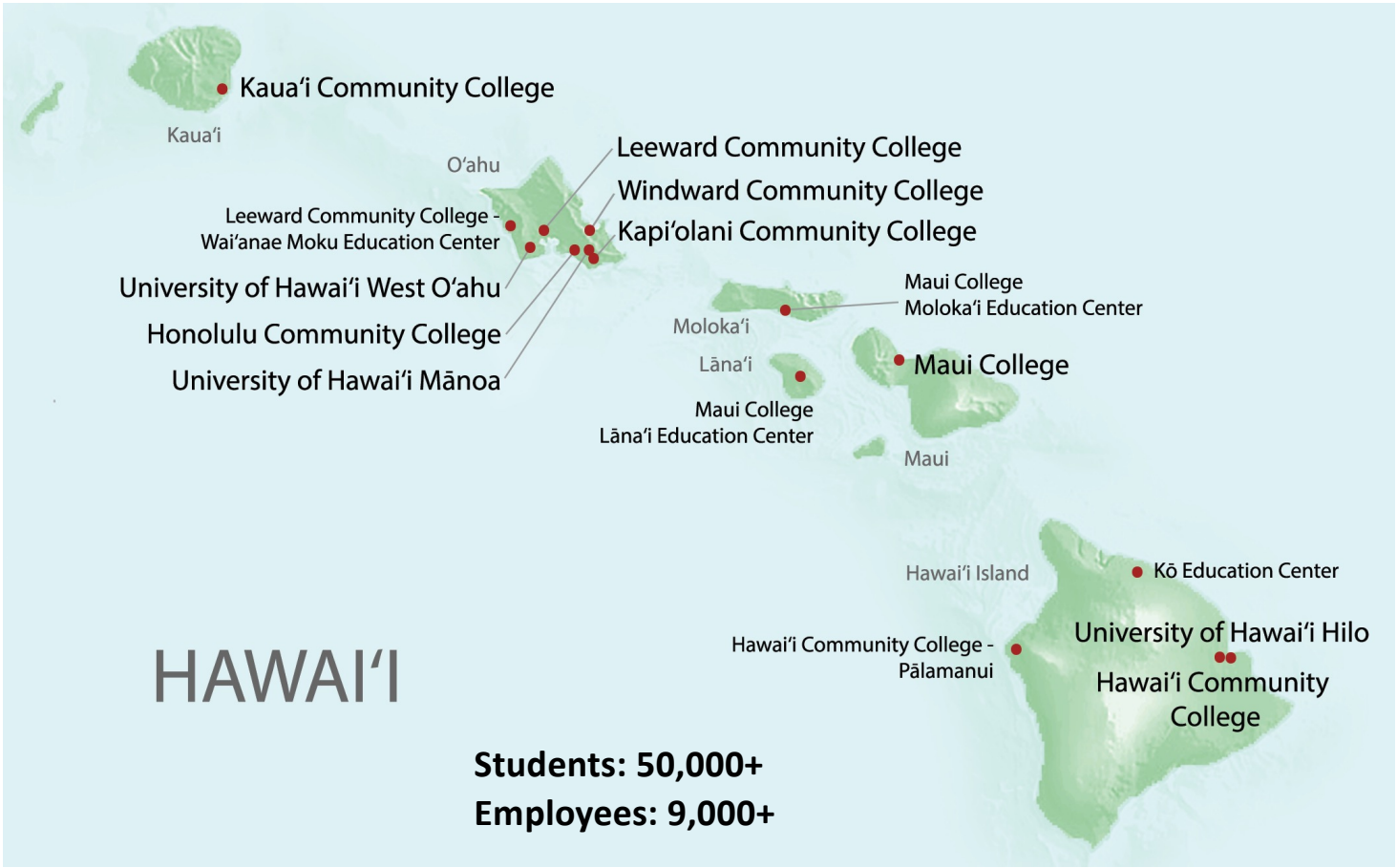
Network Reclamation: Taming Chaos After a Ransomware Incident

PacNOG 35 – June 23, 2025

Melvin Quemado
Information Security Specialist
University of Hawaii System

University of Hawai‘i (UH) System



3 Universities

- UH Hilo
- UH Mānoa
- UH West O‘ahu

7 Community colleges and community based learning centers

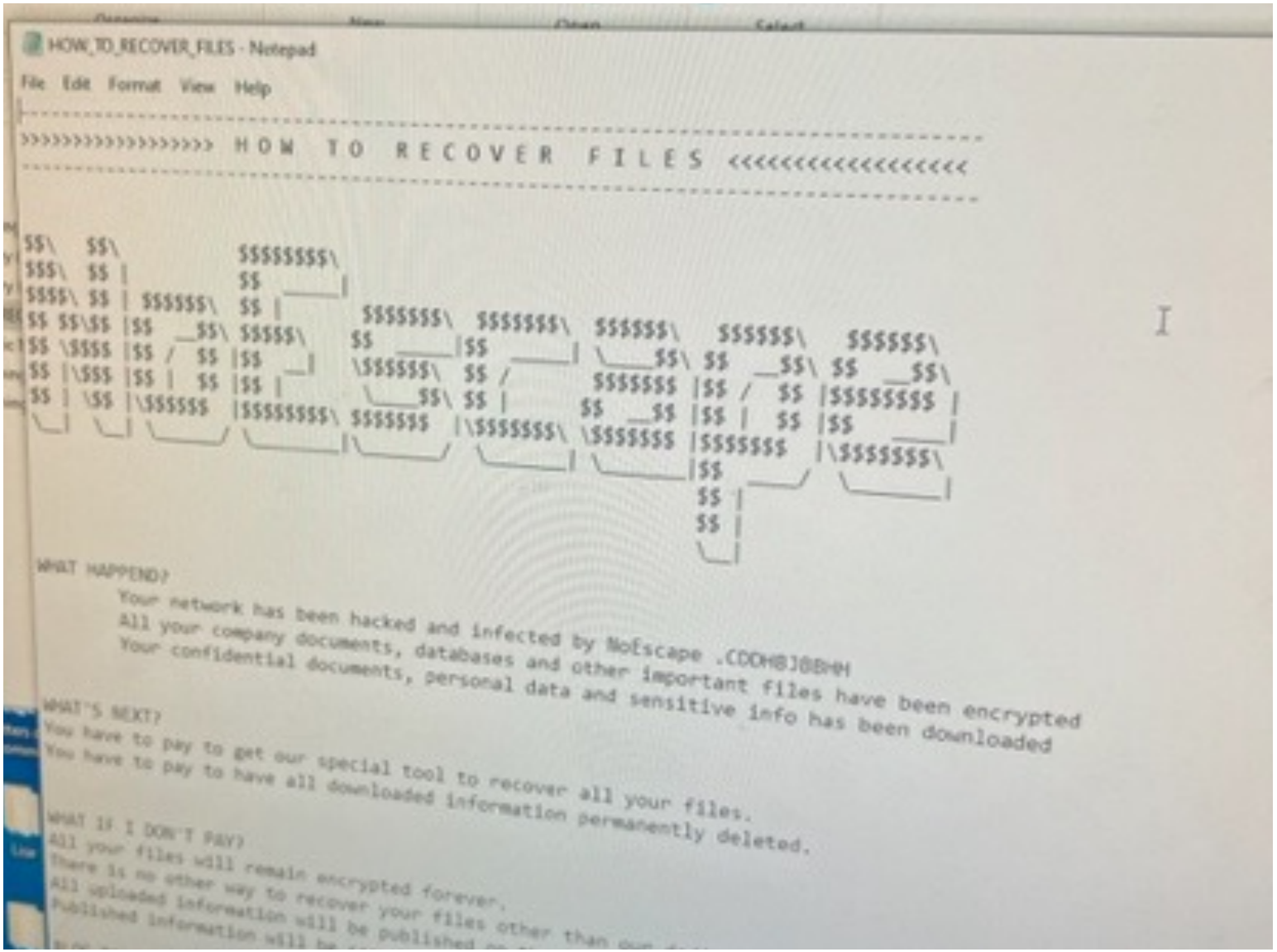
- Hawai‘i Community College
- Honolulu Community College
- Kapi‘olani Community College
- Kaua‘i Community College
- Leeward Community College
- UH Maui College (Maui)
- Windward Community College

Information Technology Services

- Vice President for IT & CIO
- Manage and maintain all system-wide information systems & services
  - Institutional Information Systems
  - Network & Technology Infrastructure
  - High Performance Research Computing
  - Information Security
- 160+ full time staff, 120+ student employees
- CISO direct report to VP IT & CIO
  - InfoSec Staff = CISO + 5 Information Security Specialists

Distributed IT

- Many of our campuses and colleges within the University have their own IT staff
- Follow recommendations from Central IT
- Some centralized tooling but need Distributed IT to implement
- Lots of public IPv4 usage so… BIG ATTACK SURFACE!


HOW_TO_RECOVER_FILES - Notepad
File Edit Format View Help
>>>>>>>>>>>>>>>>>>> HOW TO RECOVER FILES <<<<<<<<<<<<<<<<<<<
WHAT HAPPEND?
Your network has been hacked and infected by MoEscape .CDCHBJBBHH
All your company documents, databases and other important files have been encrypted
Your confidential documents, personal data and sensitive info has been downloaded
WHAT'S NEXT?
You have to pay to get our special tool to recover all your files.
You have to pay to have all downloaded information permanently deleted.
WHAT IF I DON'T PAY?
All your files will remain encrypted forever.
There is no other way to recover your files other than
All uploaded information will be published
Published information will

NoEscaping…

- Received multiple reports from users that a note was on their machine
- Users reported
  - Files were not accessible
  - Could not connect to servers on their network

NoEscape

HAWAII.EDU

19 Jun 2023 3

University of Hawaii

2444 Dole St, Honolulu, Hawaii, 96822, United States

www.hawaii.edu

[redacted]

[redacted]

Total data to be published: **65 GB**

Next update: **1 week left**

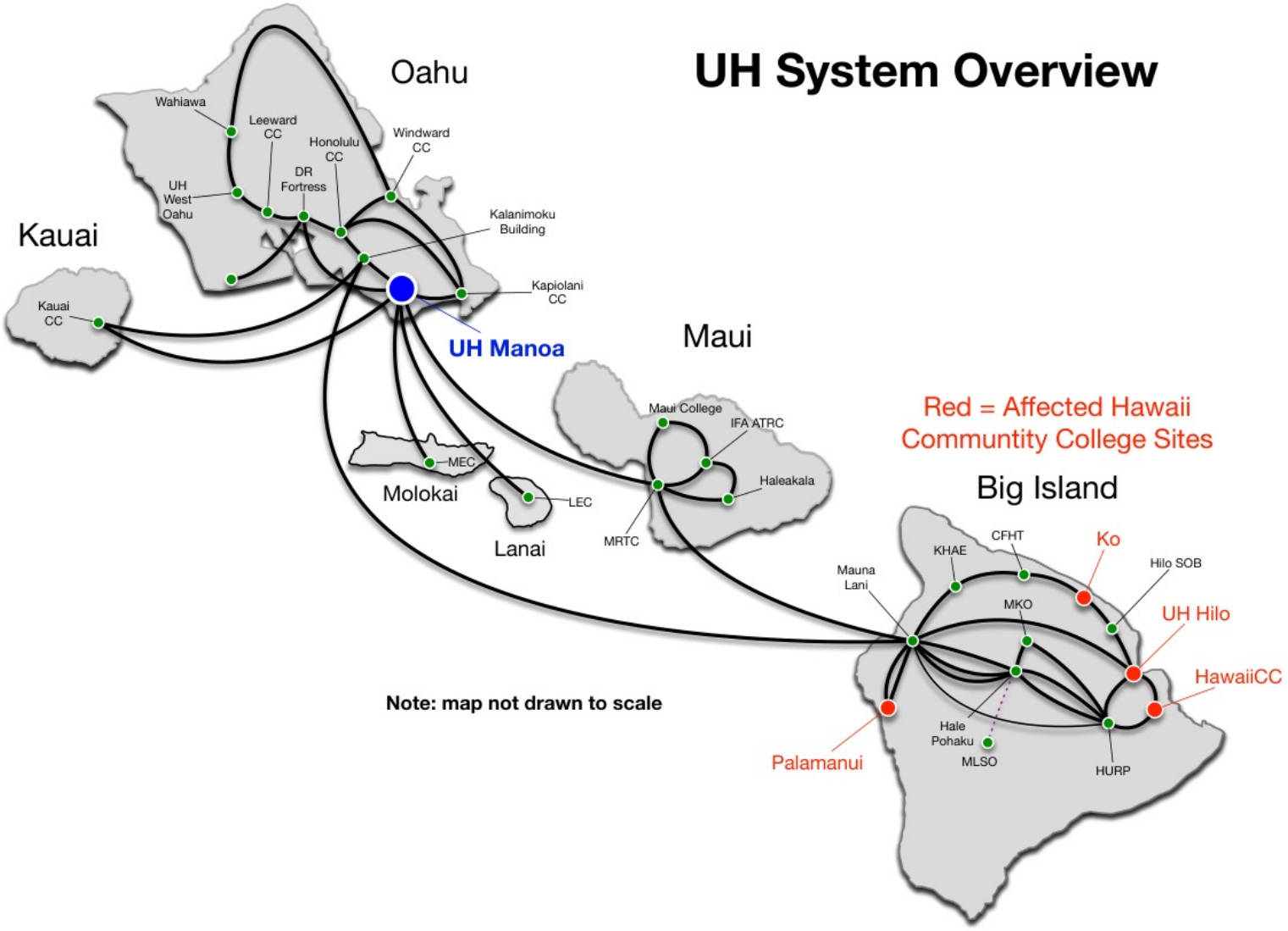
[redacted]

University of Hawaii, founded in 1907 and headquartered in Honolulu, Hawaii, offers degrees in both undergraduate and graduate-level curriculum. The University programs include undergraduate and graduate degree programs in Arts and Community and Engineering.

Hawai‘i Community College

- Small community college located on Hawai‘i Island
- Four different sites across the island
- No central Hawai‘i CC network
  - Each site connected to the UH backbone to get to the internet
- No campus firewalls

UH System Overview



What we knew so far…

- Multiple computers across the Hawai‘i CC network have a ransom note
- Computers that weren’t impacted can’t access important servers on their network
- The ransom note links to a leak site claiming to have stolen data

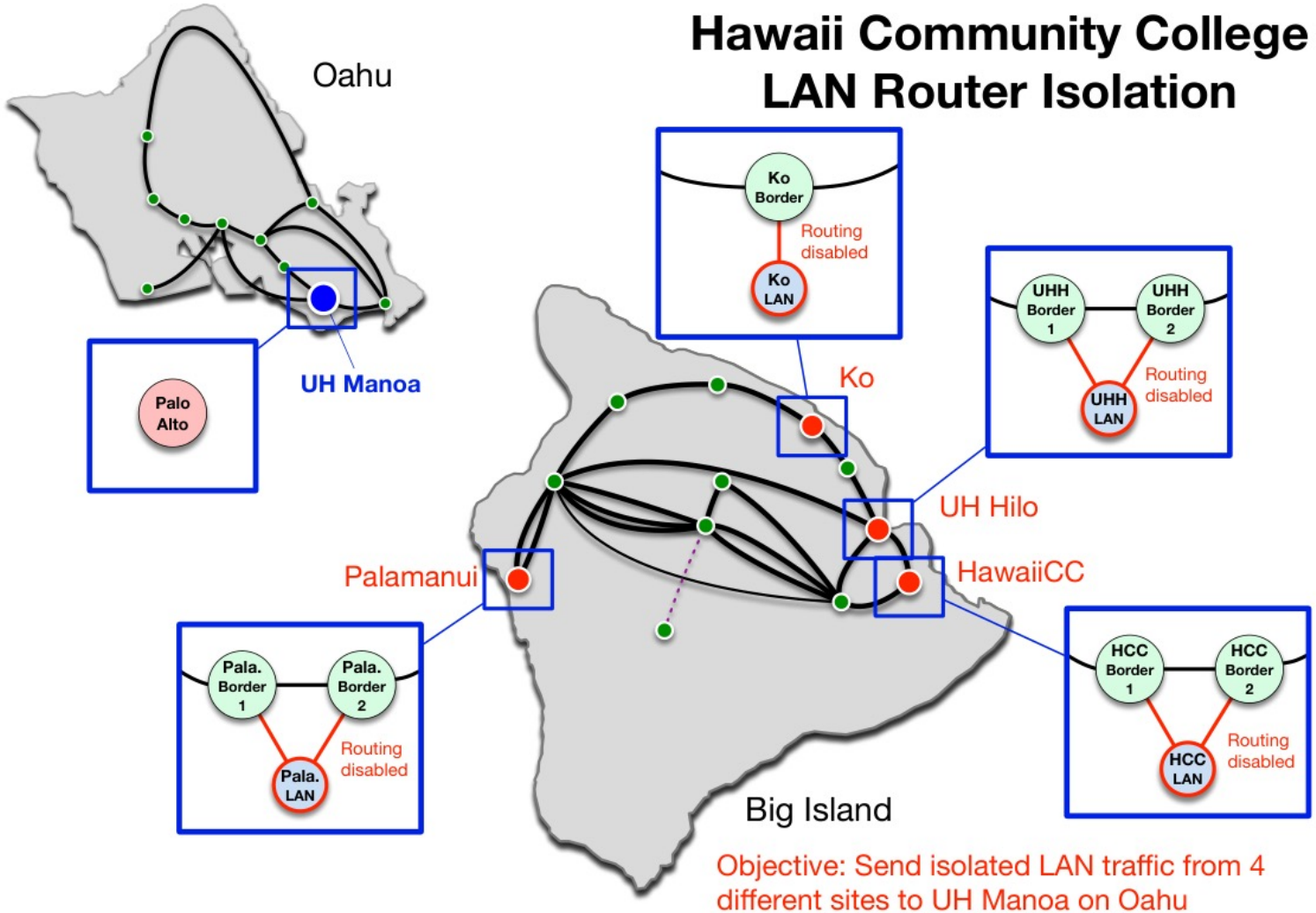
Taming the Chaos

- Stop the spread
- Is there any impact to other campuses?
- Determine what data was stolen and from where?
- Are they still in the network? What else did they compromise?
- Get “business” up and running again

Escaping NoEscape

- Shut down all WAN connections at each of the four sites' gateways
- Temporarily reengineer the network from the four remote sites to come under our spare firewall on O'ahu
- Implement firewall rules to take campus offline (block all network traffic)
- Stand up new clean network on our firewall
- Bring campus systems back online

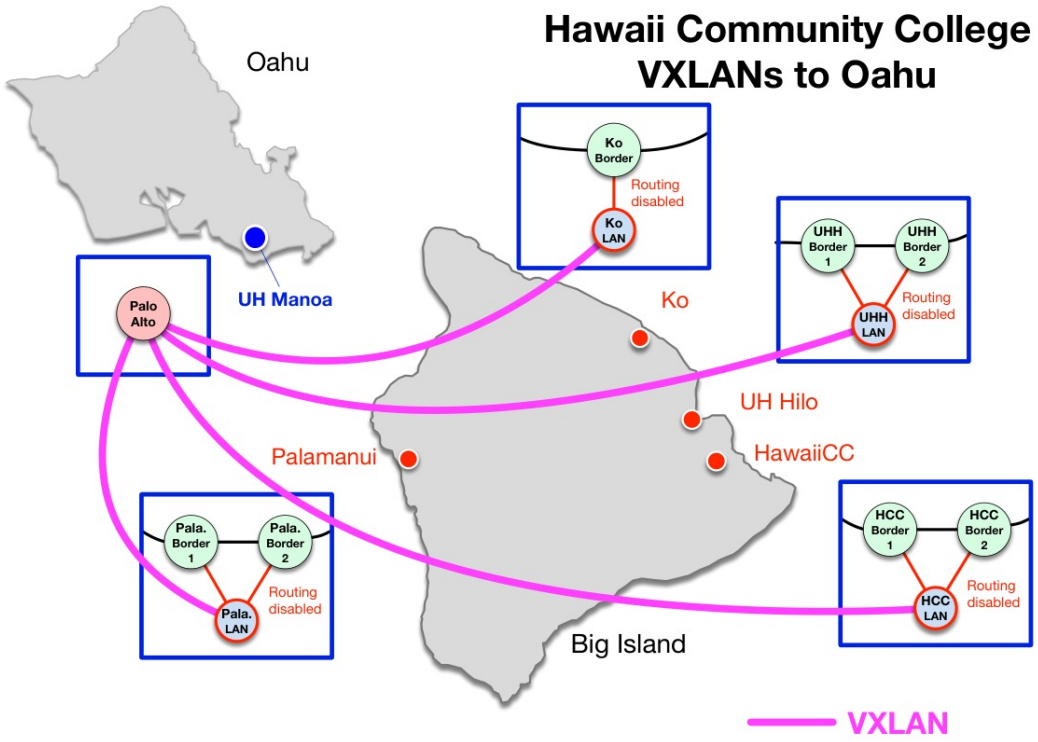
Hawaii Community College
LAN Router Isolation



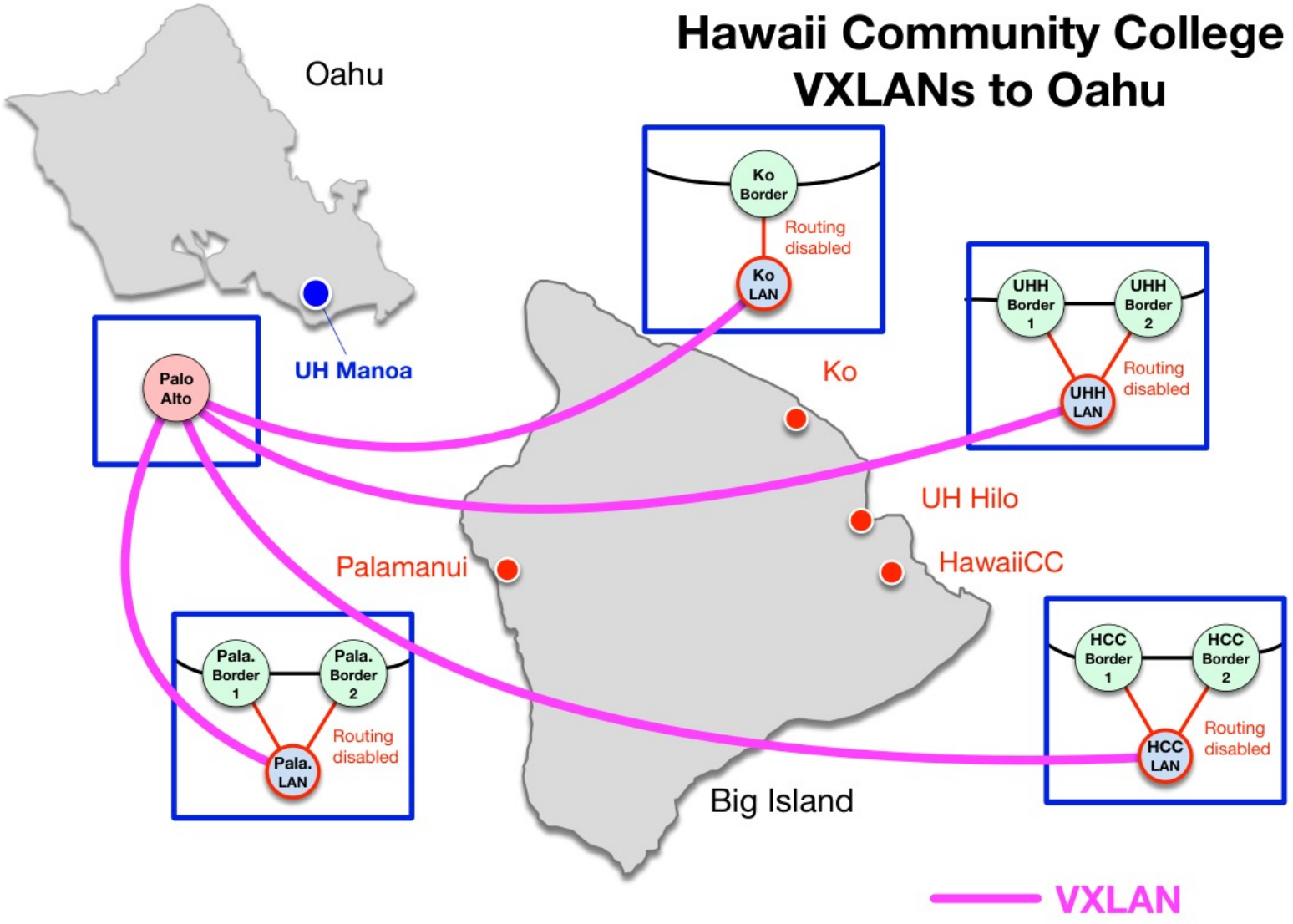
Objective: Send isolated LAN traffic from 4 different sites to UH Manoa on Oahu
without affecting border router traffic

Temporary Hawaii CC Network

- Remote sites have multiple VLANs that are VXLAN'ed (tunneled) across UH network to UH Manoa
- Temporary firewall to control access
- Moved to private RFC1918 addressing + NAT



Hawaii Community College VXLANs to Oahu



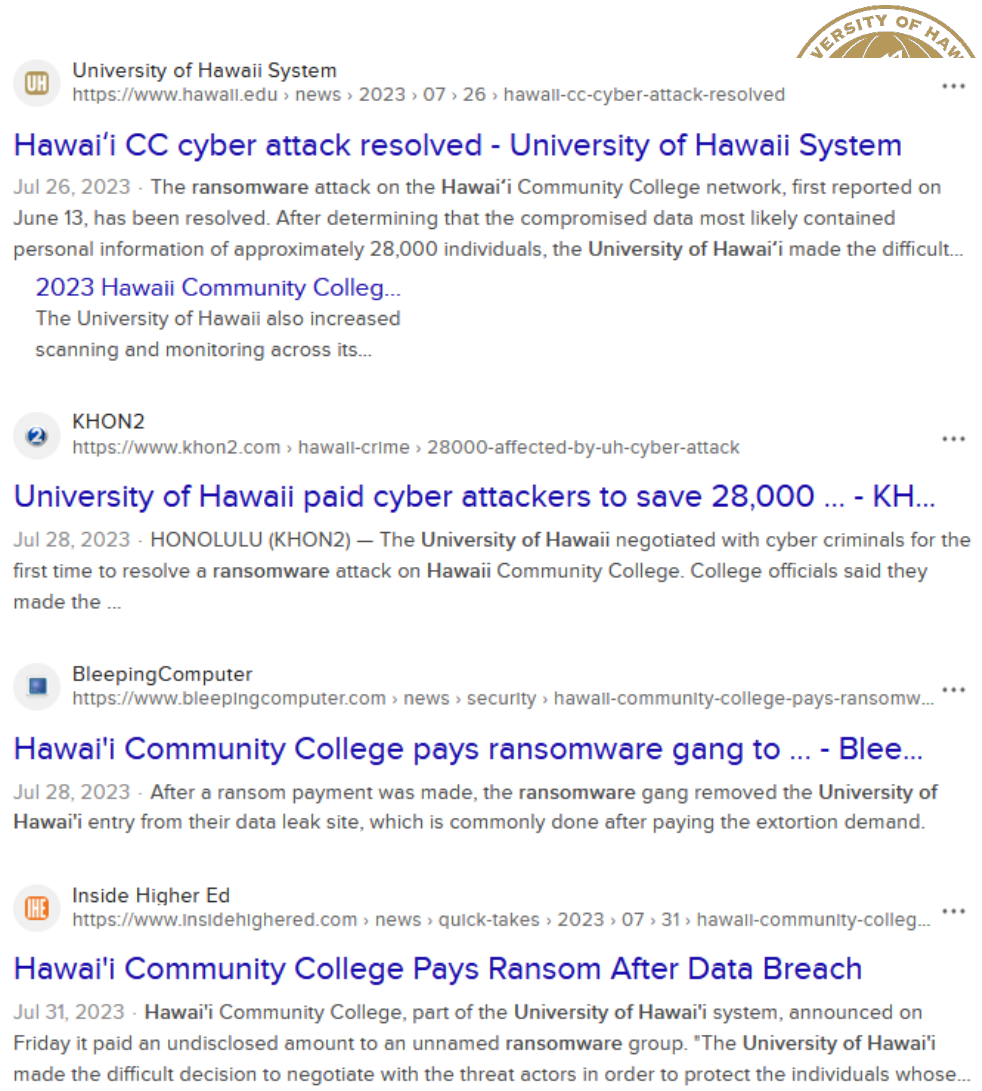
Reclaiming the network

- Prioritize business functions to bring back online
- Wipe and bring machines back online into clean network with secure configuration
- Rebuilt critical servers with hardened configurations
- Continue investigation into impacted data and source of intrusion

After the escape…

Impacts of Ransomware

- Reputational damage
- Lots of time and money spent on:
  - Recovery
  - Loss of productivity
  - Investigation
- Stolen data, damage to data
- Staff burnout
- Will you pay the ransom?



University of Hawaii System
https://www.hawaii.edu › news › 2023 › 07 › 26 › hawaii-cc-cyber-attack-resolved

Hawai'i CC cyber attack resolved - University of Hawaii System

Jul 26, 2023 · The **ransomware** attack on the **Hawai'i** Community College network, first reported on June 13, has been resolved. After determining that the compromised data most likely contained personal information of approximately 28,000 individuals, the **University of Hawai'i** made the difficult...

2023 Hawaii Community Colleg...
The University of Hawaii also increased scanning and monitoring across its...

KHON2
https://www.khon2.com › hawaii-crime › 28000-affected-by-uh-cyber-attack

University of Hawaii paid cyber attackers to save 28,000 ... - KH...

Jul 28, 2023 · HONOLULU (KHON2) — The **University of Hawaii** negotiated with cyber criminals for the first time to resolve a **ransomware** attack on **Hawaii** Community College. College officials said they made the ...

BleepingComputer
https://www.bleepingcomputer.com › news › security › hawaii-community-college-pays-ransomw...

Hawai'i Community College pays ransomware gang to ... - Blee...

Jul 28, 2023 · After a ransom payment was made, the **ransomware** gang removed the **University of Hawai'i** entry from their data leak site, which is commonly done after paying the extortion demand.

Inside Higher Ed
https://www.insidehighered.com › news › quick-takes › 2023 › 07 › 31 › hawaii-community-colleg...

Hawai'i Community College Pays Ransom After Data Breach

Jul 31, 2023 · **Hawai'i** Community College, part of the **University of Hawai'i** system, announced on Friday it paid an undisclosed amount to an unnamed **ransomware** group. "The **University of Hawai'i** made the difficult decision to negotiate with the threat actors in order to protect the individuals whose...

New Hawai‘i Community College Network

- Remote sites have multiple VLANs that are VXLAN’ed (tunneled) across UH network to main Hawai‘i CC campus
- New centralized campus firewall that connects all of the four Hawai‘i CC sites
- On the same private RFC1918 addressing + NAT as the temporary network

“Copy cats”

From: **No Escape** <noescape@contractor.net>
Date: Fri, Aug 18, 2023 at 4:47 PM
Subject: Payment rquired within 5 buisness days.
To: <[name]@[institution].edu>

We have infilrated your servers.
We have exfiltrated gigabytes of your colleges most sensitive data.
We now have your college in a perilous position.
We have used undocumented zero day exploits to accomplish this.

Unless your college pays 30 bitcoin to BTC address 1FnmGBp4L1JLYTvgR6U7uLCFmzGEuVhLqV
in a timely manner; specifically within 5 buisness days from the moment your college recieved this
your colleges information and exfiltrated data will be added to our data leak site. Which has gained much media attention as of late.

We have decided to offer your affected school a chance to mitigate the damage done
before any knowledge of the exflitrated data reaches the public and media.

This matter can stay private.

This is a gentlemens offer to prevent any damage before any data leaks
or public knowledge of this situation happens. Secure deletion of all exfiltrated
data to US DoD standards will happen if timely payment is recieved.

A wave of ransomware attacks will also be unleashed on your college
network-wide if this is gentlemens agreement is not honored in a timely manner.

Our reputation is unblemished this is public knowledge.
We honor our agreements.
This is NoEscape...
There is No Escape...

No negotiations. We have offered you a fair offer.

Lessons Learned

Active Directory

- Attackers leverage insecure configurations/usage to compromise network
  - Most common active directory security issues and how to fix them: https://adsecurity.org/?p=1684
- Harden Active Directory using Tiered Model
  - https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/protecting-tier-0-the-modern-way/4052851
- Audit Active Directory health using Ping Castle
  - https://www.pingcastle.com/

Know your data

- What data are you keeping?
- Is there any reason to keep it?
- If it’s important, is it protected?
- It’s okay to delete!

Security Tooling

- Endpoint Detection and Response (EDR)
- Security Information and Event Management (SIEM)
  - Wazuh (https://wazuh.com/)
- Review and respond to your alerts
  - Baseline normal so abnormal is obvious

Other Takeaways

- Develop a positive security culture
- Are you able to “lock down” your network quickly?
- Know your attack surface / device inventory
- Patch, stay up to date
- Regularly check your defenses
  - Firewall rule review
  - Vulnerability scanning
    - Inside/Outside of your network

Thank You!

Melvin Quemado

mquemado@hawaii.edu