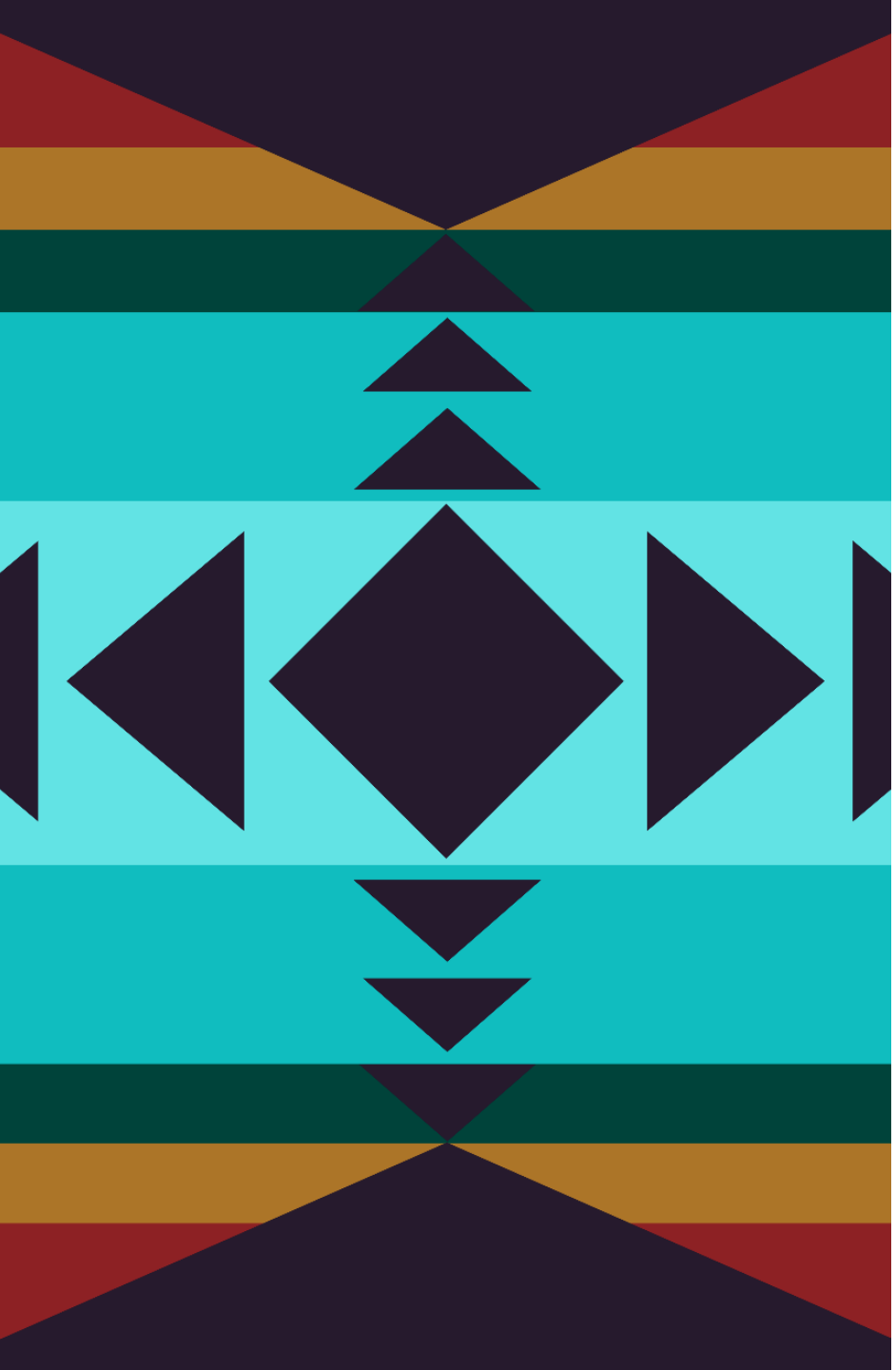
The Anatomy of a Ransomware Attack

Reese Weber, MBA, CISSP
Chief Information Security Officer
California Area Indian Health Service

What is Ransomware?

Ransomware is a type of malicious software (malware) that locks or encrypts your files, computer, or entire network and then demands money to unlock them.

Think of it like a digital kidnapping.
Instead of stealing a person, criminals “kidnap” your data — such as documents, photos, medical records, or business systems — and demand payment (usually in cryptocurrency) in exchange for giving it back.



Phase 1 - Infiltration: How does ransomware enter the network?

Initial Network Entry

It usually starts with something small. A single email. A harmless-looking attachment. A trusted-looking link. In most ransomware attacks, the first step is gaining a foothold — and it almost always involves a human unknowingly letting the attacker in.

- **Malicious attachments or links**
- **Exploiting software vulnerabilities**
- **Compromised credentials**

Phase 2 - Exploitation: The attackers look for ways to gain elevated access

Leveraging vulnerabilities

- Unsecured administrator accounts
- Unpatched Servers
- Websites with weak or no security

Depositing persistent mechanism on network

- Helps attackers maintain access even after remediation
- Separating the amount of time between access and attack lowers the chance of discovery by security teams

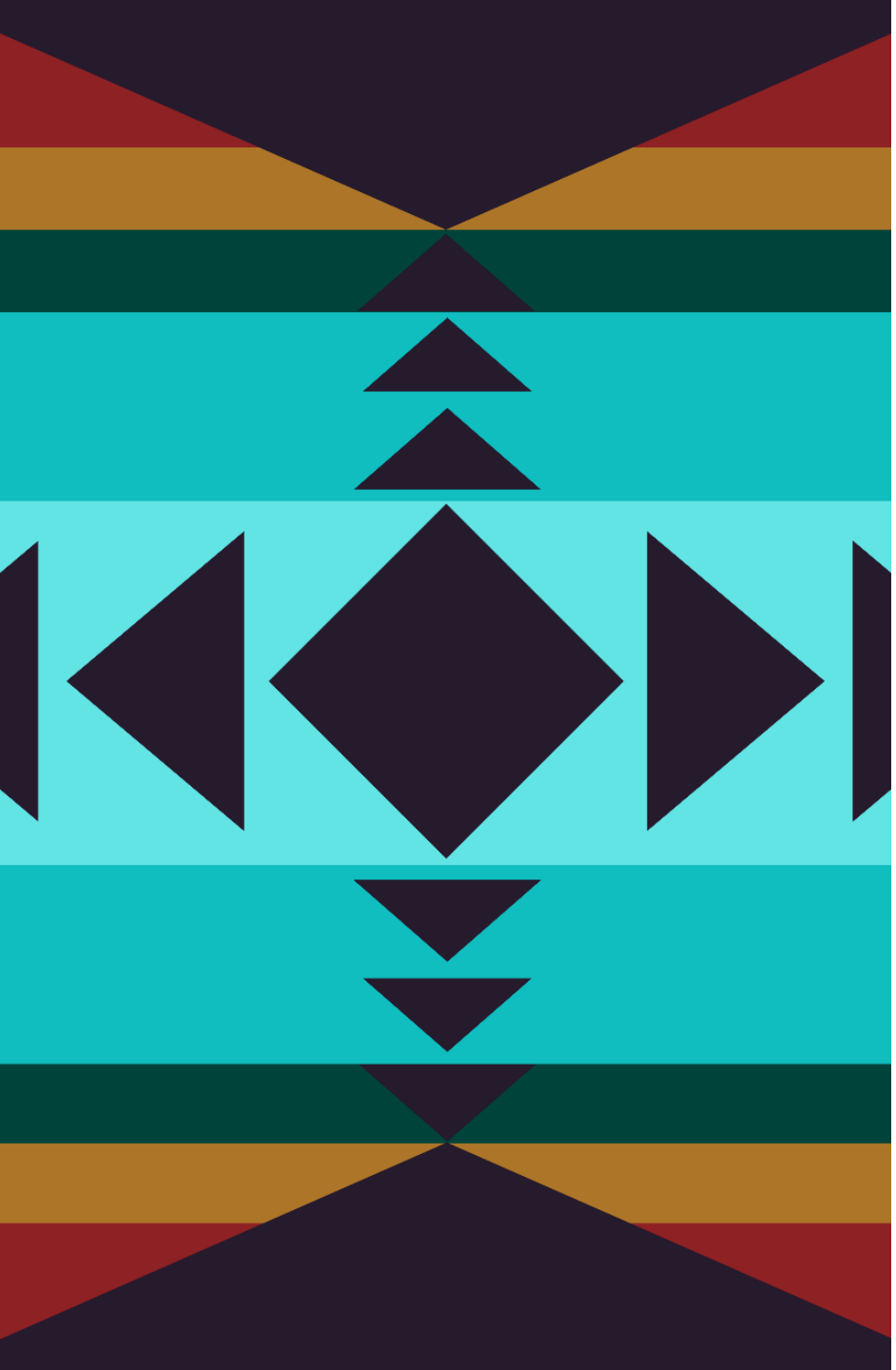
Phase 3 – Reconnaissance, lateral network movement

Gathering Network and Organization Information

- Identifying high value targets
- Searching for financial information and transactions

Moving Across the network

- Using obtained information, searching the network for other unsecured applications or opportunities for fraud or theft



Phase 4 - Exfiltration: The attackers steal the data

Data Exfiltration

is the unauthorized, intentional transfer of sensitive data from a computer, network, or device to an external location controlled by an attacker.

- **Files, folders and directories**
- **Sensitive Information**
  - PII, PHI, Financial Information, Trade Secrets

Phase 5 - Encryption

The attackers start encrypting

- Renders the data unusable to those without encryption key
- Renders the network unusable by encrypting applications servers that control the network, like DHCP, DNS and Domain Controllers

Phase 6 - Extortion

Time Remaining:

Days	Hours	Minutes	Seconds
01	23	59	56

View Locked Files

Payment has been made!

Your Files have been Encrypted and Locked!

Your documents, photos, videos etc have been encrypted and locked. But don't worry, I have not deleted them, they are safe, for now.

To get your files back safely, you'll need a decryption key. I have the only copy of this key.

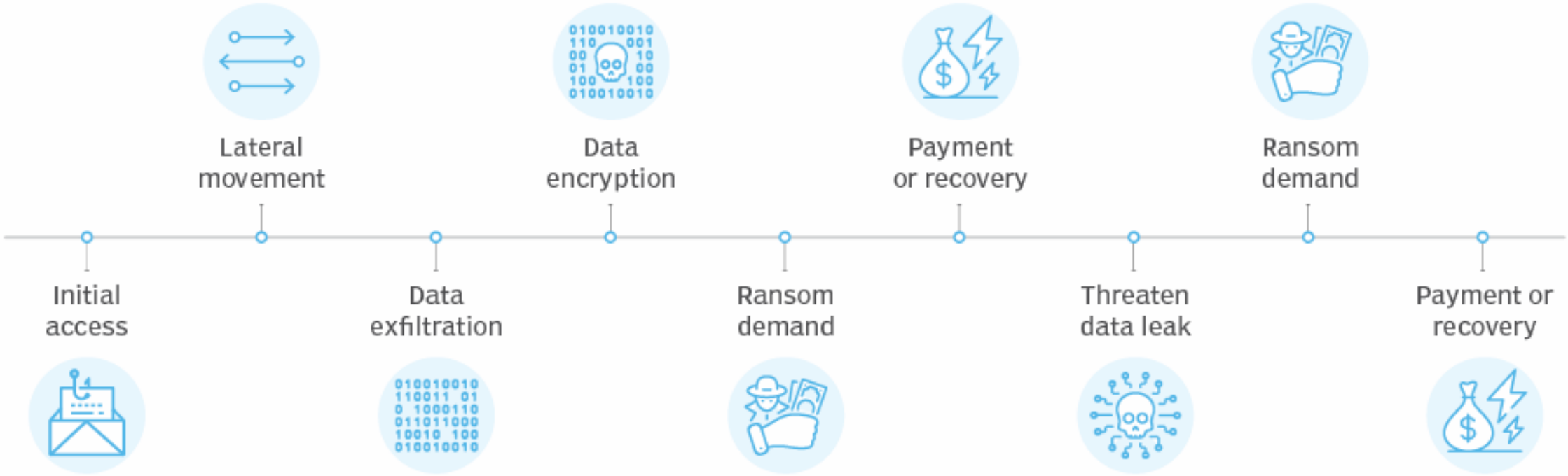
Simply pay me USD$200 in Bitcoins and I will give you the key.

The clock is ticking! Pay up before the timer runs out, otherwise all your files will be permanently deleted.

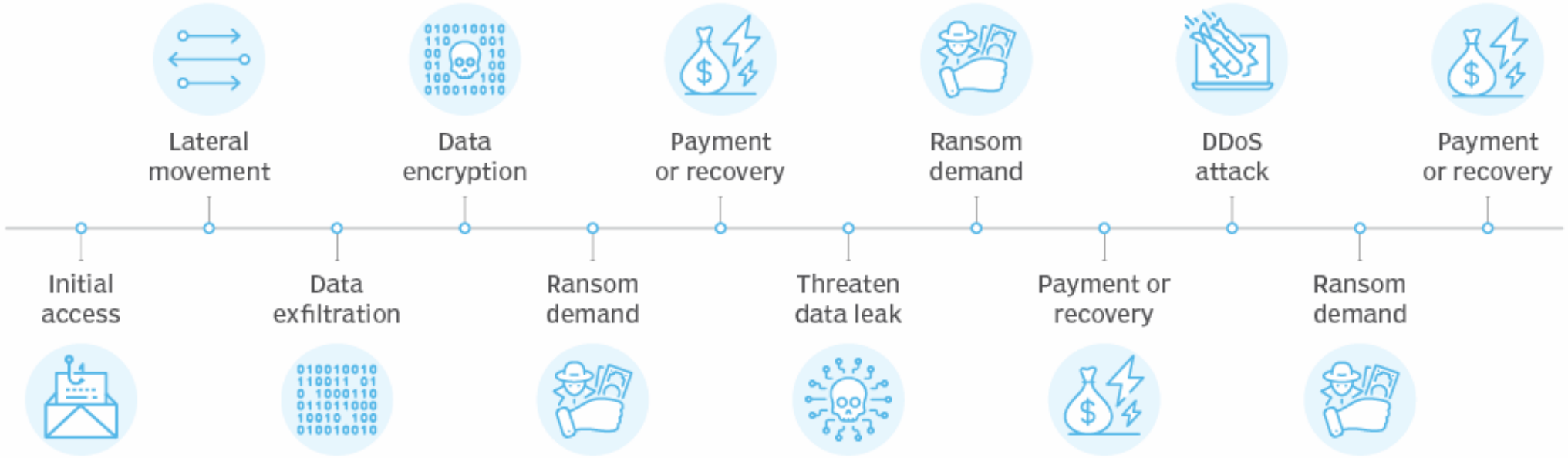
Payment Address:

8A6GdH4UnLK5C9eVNb1MxWzL7Pa Copy

Double extortion ransomware attack



Triple extortion ransomware attack



ICONS: BLANKSTOCK/GETTY IMAGES; ILYALIREN/GETTY IMAGES

Questions?

Reese Weber, MBA, CISSP
Indian Health Service
California Area Office
Theresa.weber@ihs.gov