SkyHelm TECHNOLOGY

Ransomware: Modern Day Pirates

Jeremy Dreyer | SkyHelm | Chief Architect/CTO

Rickey Bowen | Choctaw EC | IT Director

Choctaw Electric Cooperative CEC

SkyHelm TECHNOLOGY

Presentation Overview

Ransomware

- What is ransomware
- History of ransomware
- Actors and their motivations
- Anatomy of a ransomware attack
- Cost of a ransomware attack
- Effective ransomware defenses

Choctaw EC

- Method of Attack
- Detection
- Mitigation and Triage
- Interim Actions and Operational Impact
- Getting back to normal
- Forensic Findings

SkyHelm TECHNOLOGY

What is Ransomware?

- Dictionary “A type of malicious software designed to block access to a computer system until a sum of money is paid”
- A trojan or virus that takes control of a system
- Demands a ransom for access
- Spreads quickly across systems and companies
- Close Cousin: Info releasing trojans

SkyHelm TECHNOLOGY

History of Ransomware

Pre 2013

Initial

- Unsophisticated and badly programmed
- Marginally effective “Wide Net” indiscriminate target hunting
- Small Ransoms
- Limited cross-system contamination
- Reversible Encryption

2013 - 2016

Enhanced Sophistication

- Automated replication
- Effective “wide net” target hunting
- Ransom amount based on victim
- Strong Encryption
- ”CryptoLocker” first major highly sophisticated malware
- SkyHelm team discovered one of the first CryptoLocker installations in September 2013

2016 - Present

RaaS

- Highly sophisticated criminal enterprises
- Build and sell ransomware kits
- Full support to criminal groups
- Highly effective
- Increased ransoms based on target

Ransomware Actors

Reference: US Directory of National Intelligence. 2017. The Future of Ransomware and Social Engineering.

Attack in Action | Phase 1

Reconnaissance

- Harvesting Email Information
- Harvesting Conference Information
- Automated Process

Weaponization

- Exploit paired with delivery mechanism

Delivery

- Delivery of weaponized bundle
- Victim opens infected email or website

Delivered via

- Email
- Web
- USB
- Infected Devices
- Remote Access Systems (RDP/VPN/etc)

Triggering by victim

Reference: Lockheed Martin. 2019. The Cyber Kill Chain

SkyHelm TECHNOLOGY

Attack in Action | Phase 2

Exploitation/Installation

- Exploit of victim's system
- Installation of payload

Installation and Control

- Persistent Installation on Victim's System
- Connection to Command and Control Server
- Control of victim's system obtained

Scan and Spread

- Scan network for shares and machines
- Send emails to contacts
- Leverage privileged access to spread
- Delete online backups

Reference: Lockheed Martin. 2019. The Cyber Kill Chain

Attack in Action | Phase 3

Action on Objectives

- File encryption on victim's machine
- File encryption of connected systems
- Communication to C&C servers
- Continued spread of ransomware

Ransom

- Ransomware posts Ransom messages
- Victim receives notice
- Victim is contacted by cyber criminals
- Victim determines whether to pay ransom or perform self recovery

Reference: Lockheed Martin. 2019. The Cyber Kill Chain

Ransomware Statistics

Average Ransom Amounts are increasing due to Ryuk and Sodinokibi appearing in 2019

- 2013 - $<$500
- 2014 - $<$500
- 2015 - $<$500
- 2016 - $500-$1000
- 2017 - $500-$1000
- 2018 - $500-$1000
- Q1 2019 - $12,762
- Q2 2019 - $36,295

Attack Vectors are changing

- RDP most common attack vector
- Email attack vector decreasing

Many attacks are coming through MSPs

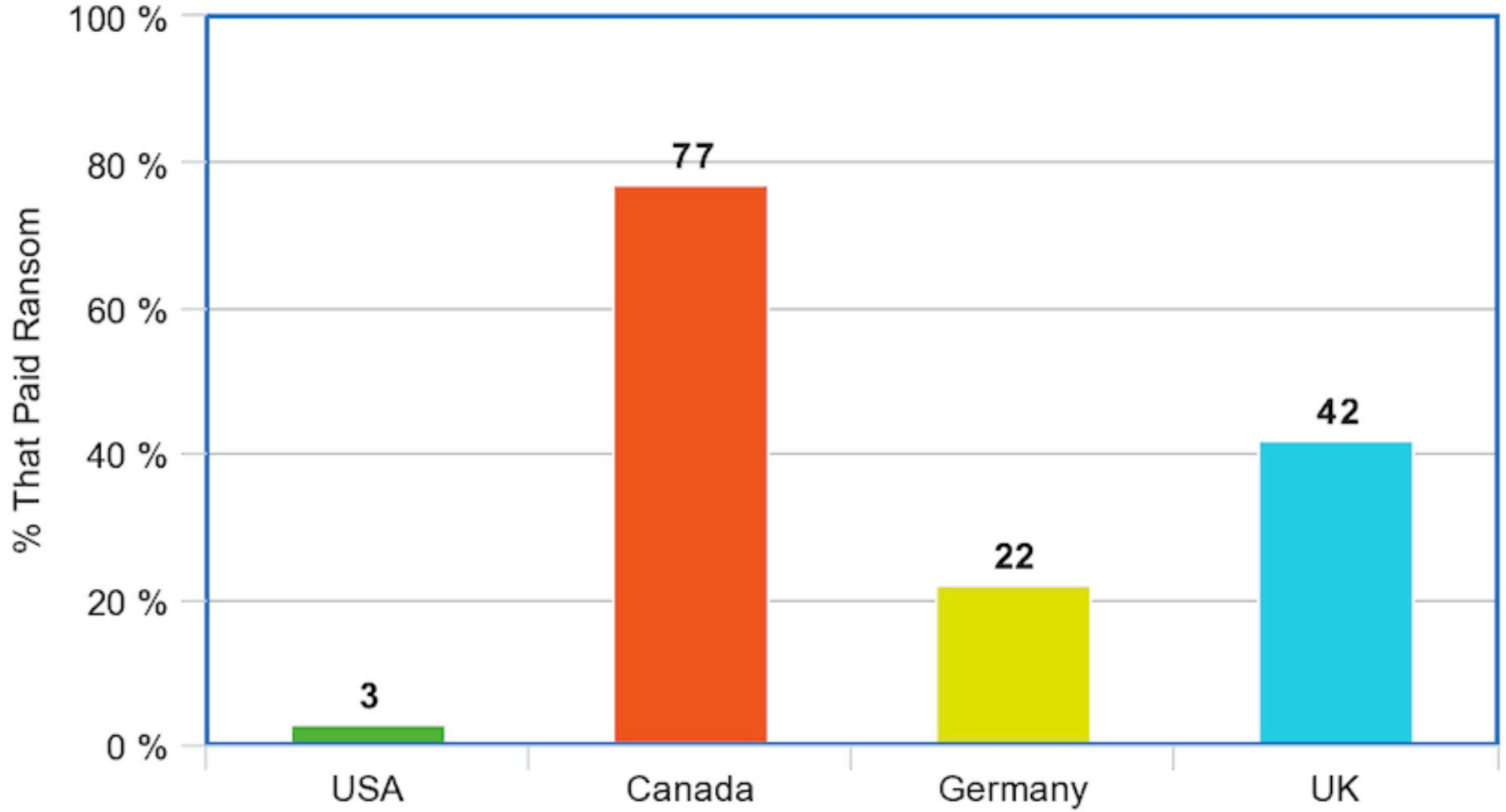
Combination of major operations and RaaS affiliates are operating ransomware schemes

Payment of ransom is increasing criminal opportunity and more players are entering the market

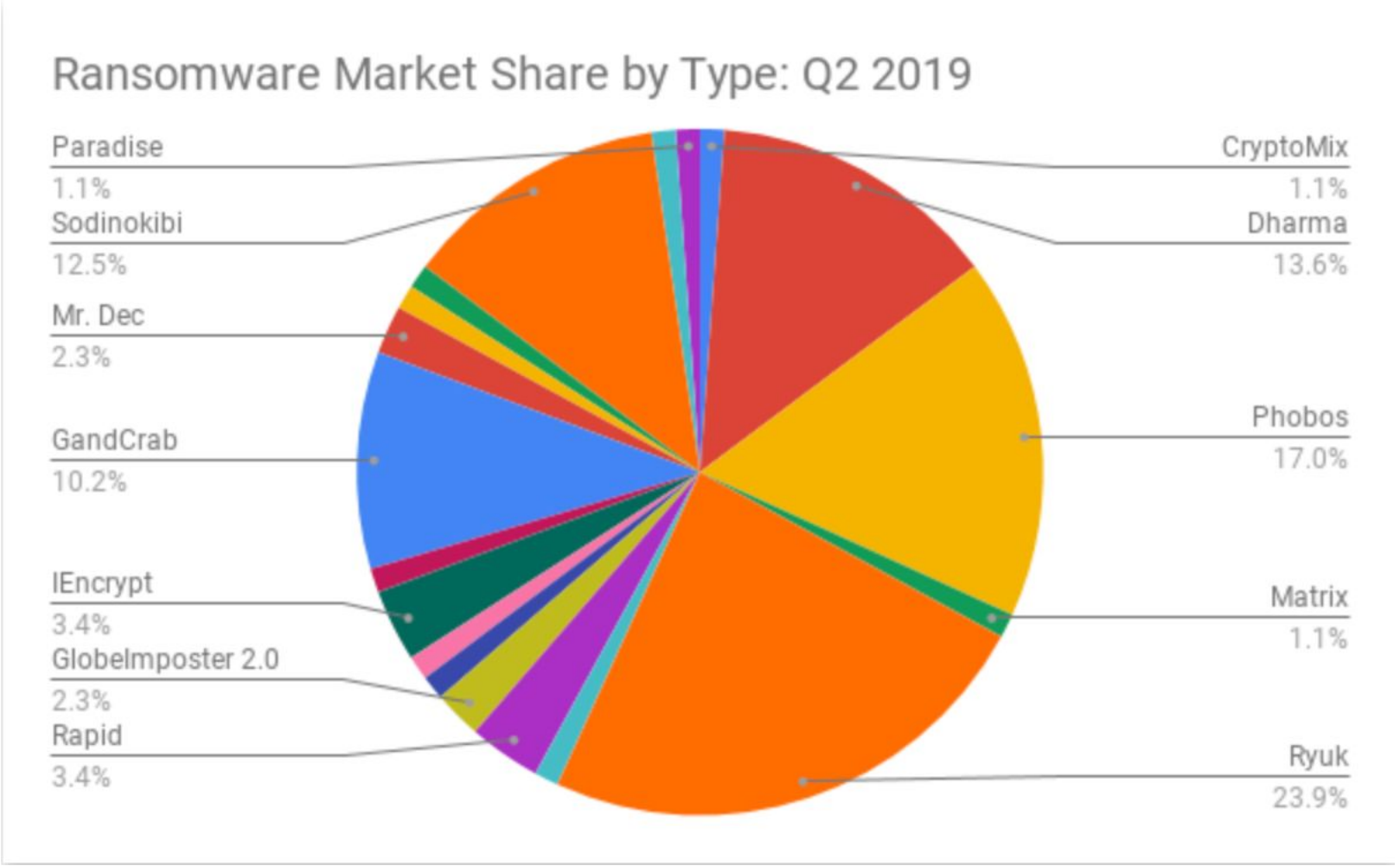
Reference: Coveware. 2019. Ransomware amounts rise 3x in Q2 as Ryuk and Sodinokibi spread.
Reference: Health IT Security. 2019. Ransomware Costs on the Rise

SkyHelm TECHNOLOGY

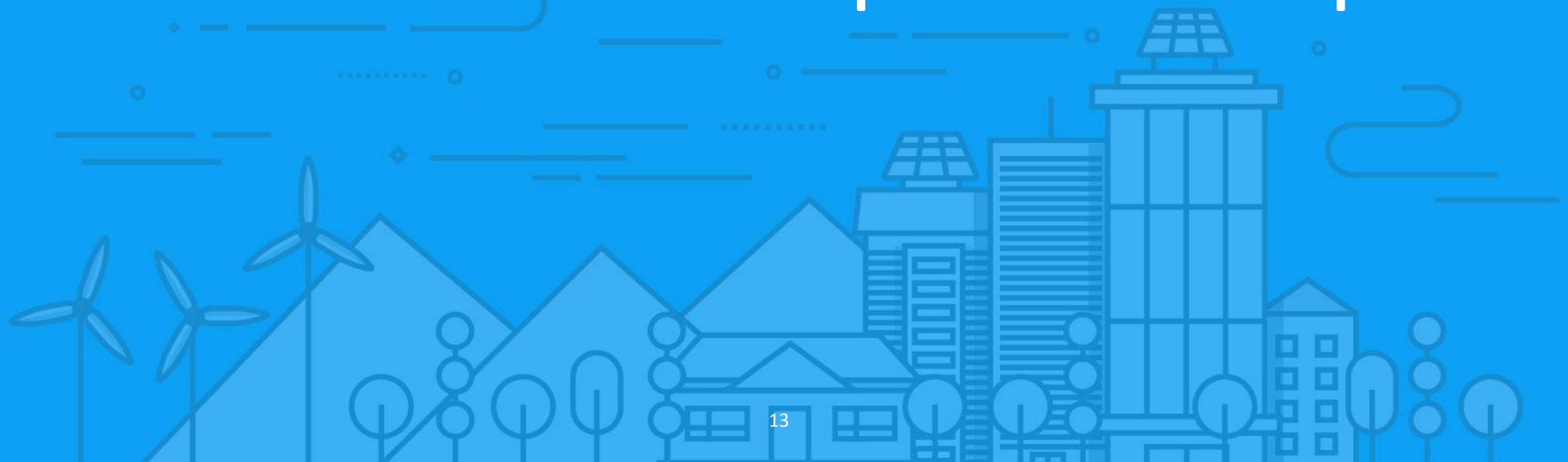
Was The Ransom Paid, Comparison By Nation



SkyHelm TECHNOLOGY



Ransomware Impact to Coop



Impact to Coop | Part 1

Impact to operations

- Customer Service
- Engineering/SCADA Operations
- Metering and Billing
- Safety Systems (Two-way radio, etc)

Loss of data

- Customer Data
- Engineering Data
- Contracts and Deeds

Exposure of data

- Customer Billing and Personal Information
- Exposure of critical grid confidential data that may be used in another attack

Impact to Coop | Part 2

Possible spread to Grid partners

- Infection can be spread using privileged credentials and access found at the Coop.

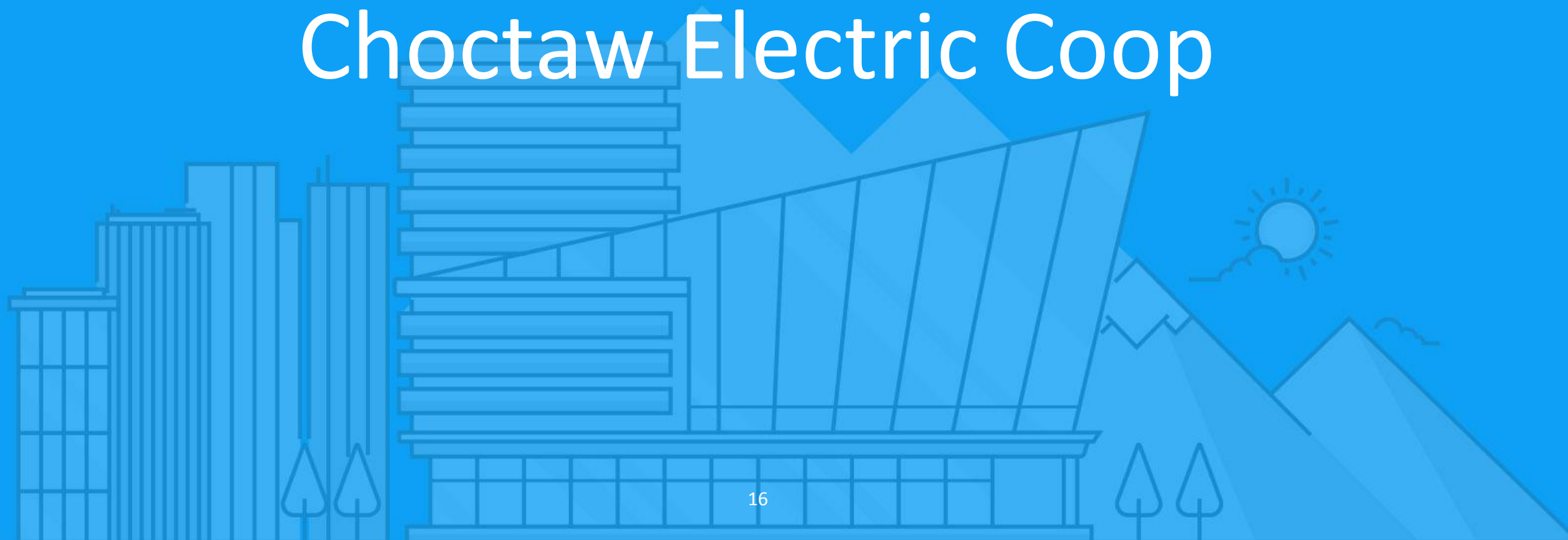
Recovery Costs

- New Hardware Infrastructure
- Rebuilding servers and infrastructure

Damage to reputation

- Community PR issues if customer data was exposed
- Possible compliance violations.

Choctaw Electric Coop



Choctaw EC | Timeline of Events | Part 1

- Thursday Feb 14th 2019 - Ryuk Ransomware began infection on Choctaw Electric Coop network
- Friday Feb 15th 2019 10am - Rickey identified the malware spreading across Choctaw EC's network
- Friday Feb 15th 2019 4pm - Rickey contacted IT partner to begin analysis and troubleshooting
- Friday Feb 15th 2019 10pm - Initial Containment and Recovery plan determined
- Saturday Feb 16th 2019 10am - Containment and Recovery plan refinement
- Saturday - Sunday Feb 16th - 17th - Identification and Isolation of all ransomware infected machines

Choctaw EC | Timeline of Events | Part 2

- Monday Feb 18th 2019
  - Coop running on paper operations
  - Implement temporary network infrastructure at Hugo (Fortinet firewall and LTE)
  - Engaged NISC to inspect NISC servers behind firewall
  - Brought temporary computers online on interim Hugo network
  - Began scans of offline (external hard drive) backups prior to infection and confirmed Ryuk had not infected the backups
  - Gathered and physically isolated infected laptops and workstation hard drives.

Choctaw EC | Timeline of Events | Part 3

- Tuesday Feb 19th 2019
  - Coop running on paper operations
  - Implement NGFW at ANTLERS and IDABEL branch offices
  - Implement secure routing between HUGO and branch office sites
  - NISC Server replacement discussion
  - Begin bringing workstations onto the new network at HUGO

Choctaw EC | Timeline of Events | Part 4

- Wednesday Feb 20th 2019
  - Coop moved to partial computer based operations
  - Turn up new NISC servers at HUGO
  - Bring new workstations onto the network at ANTLERS and IDABEL
  - Build IPSEC Tunnel to SkyHelm's Datacenter
  - Turn up new core services servers in SkyCloud (AD, Files, etc)
  - Begin scan and restore of backups to SkyCloud hosted servers.

Choctaw EC | Timeline of Events | Part 5

- Thursday Feb 21th 2019
  - Turn up Coop operations on new workstations and servers
  - Resolve issues and ensure smooth operations
  - Engage FBI Field Office

Choctaw EC | Timeline of Events | Part 6

- Friday Feb 22nd 2019 and beyond
  - Completing turn up of Coop resources
  - SkyHelm monitoring of logs and systems for re-infection
  - Engage FBI Field Office

SkyHelm TECHNOLOGY

Choctaw EC | Summary

- 1 Week from infection to partially back in operation
- Choctaw had planned to implement new CyberSecurity systems prior to attack
- Ransomware - TrickBot/Ryuk
- Ransomware Amount - 25btc ~$110,000
- Direct Recovery Costs ~ $150,000
- This would have been much worse if the hackers were successful in getting into NISC

SkyHelm TECHNOLOGY

Choctaw EC | Ransom Instructions

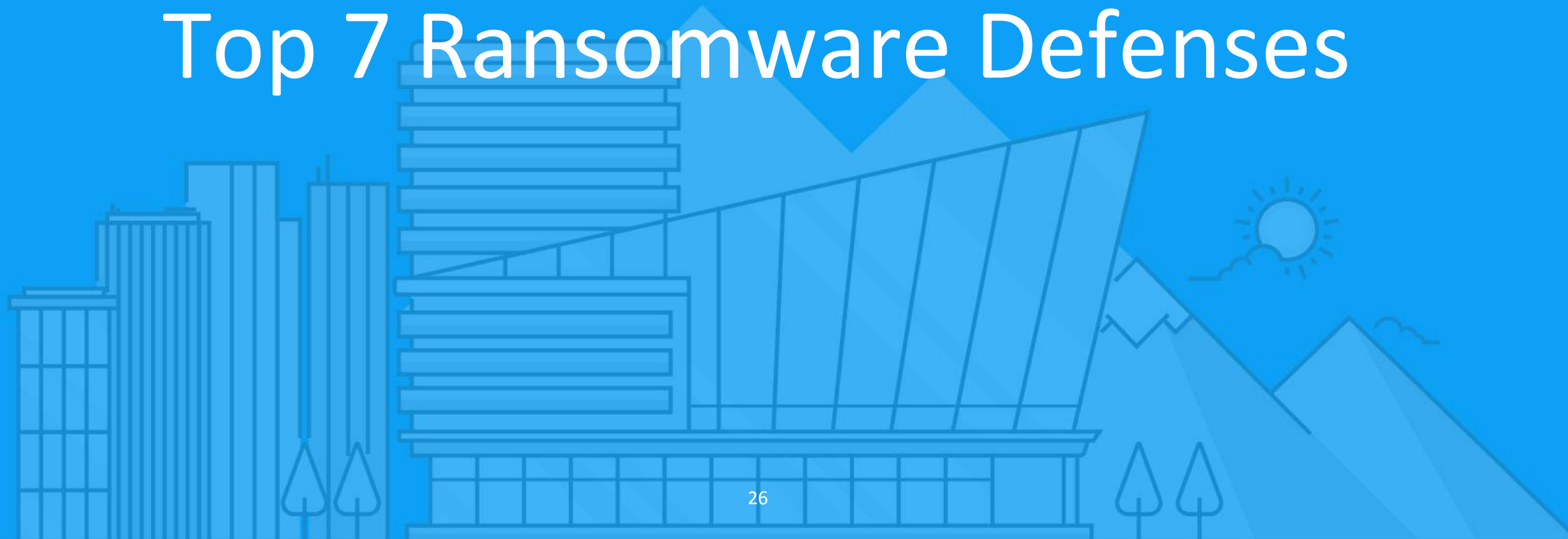
---------- Forwarded message ----------
From: LaneRusse <LaneRusse@protonmail.com>
To: Rickey Bowen <rbowen@choctawelectric.coop>
Cc:
Bcc:
Date: Sat, 16 Feb 2019 12:56:49 +0000
Subject: Re: Decryption
to unlock files, needs to pay 25 btc
wallet 1QBw6YwAHy2PGddRQJvKGQPvVJMR9BnYpg

1) turn off any AV running
2) turn off internet (for your safety while decryption is in progress)
3) start that exe on each workstation or server and wait for it's prompt that "operation complete" (it takes time depending on amount of data on current system)
4) check that all fine and get back to normal work.

Choctaw EC | Lessons Learned

- NGFW Firewall Implementation
  - Network Segregation
  - IDS/IPS/UTM
- User Security Awareness Training
- TESTED Backup and Recovery Plan
- Lock down of email system
- Unified Endpoint Protection
- Do not delay Cyber Security systems implementations

Top 7 Ransomware Defenses



Top 7 Ransomware Defenses

1. User Security Awareness Training Program
2. Lock down Email System
3. Secure Remote Access
4. Segregate Network, allow only Trusted/Secured devices
5. Effective Endpoint Protection
6. 3-2-1 Backup System with Air Gapped Offline Backups
7. Create and Test Disaster Recovery/Backup Plan regularly

SkyHelm TECHNOLOGY

Questions

Jeremy Dreyer | SkyHelm
Chief Architect/CTO

E: Jeremy@skyhelm.com
O: 281.972.0051

Rickey Bowen | Choctaw EC
IT Director

E: rbowen@choctaw