January 22, 2020

Ransomware:
Strategies of Prevention & Mitigation

Michael Hale

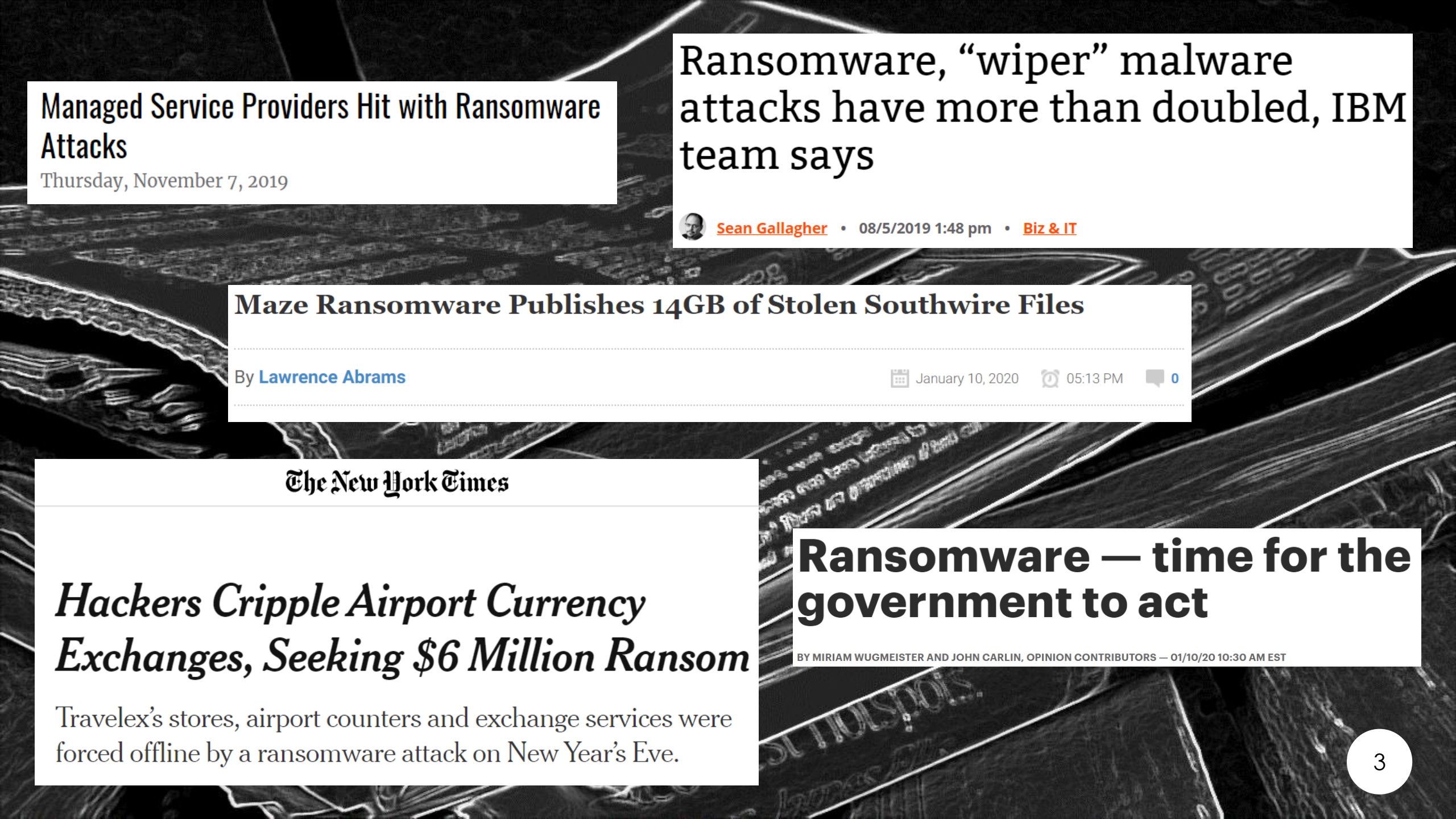
mhale@primetsr.com

Consultant, Cloud Computing

https://primetsr.com

What this covers

- Background
- Best-practices
- Training Points
- Post-infection



Managed Service Providers Hit with Ransomware Attacks

Thursday, November 7, 2019

Ransomware, “wiper” malware attacks have more than doubled, IBM team says

Sean Gallagher • 08/5/2019 1:48 pm • Biz & IT

Maze Ransomware Publishes 14GB of Stolen Southwire Files

By Lawrence Abrams

January 10, 2020 05:13 PM 0

The New York Times

Hackers Cripple Airport Currency Exchanges, Seeking $6 Million Ransom

Travelex’s stores, airport counters and exchange services were forced offline by a ransomware attack on New Year’s Eve.

Ransomware — time for the government to act

BY MIRIAM WUGMEISTER AND JOHN CARLIN, OPINION CONTRIBUTORS — 01/10/20 10:30 AM EST

Every Organization At Risk

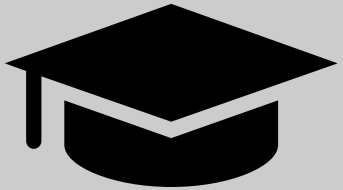
In 2019 alone – "…attacks that impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost in excess of $7.5 billion."

-- Emisoft Report

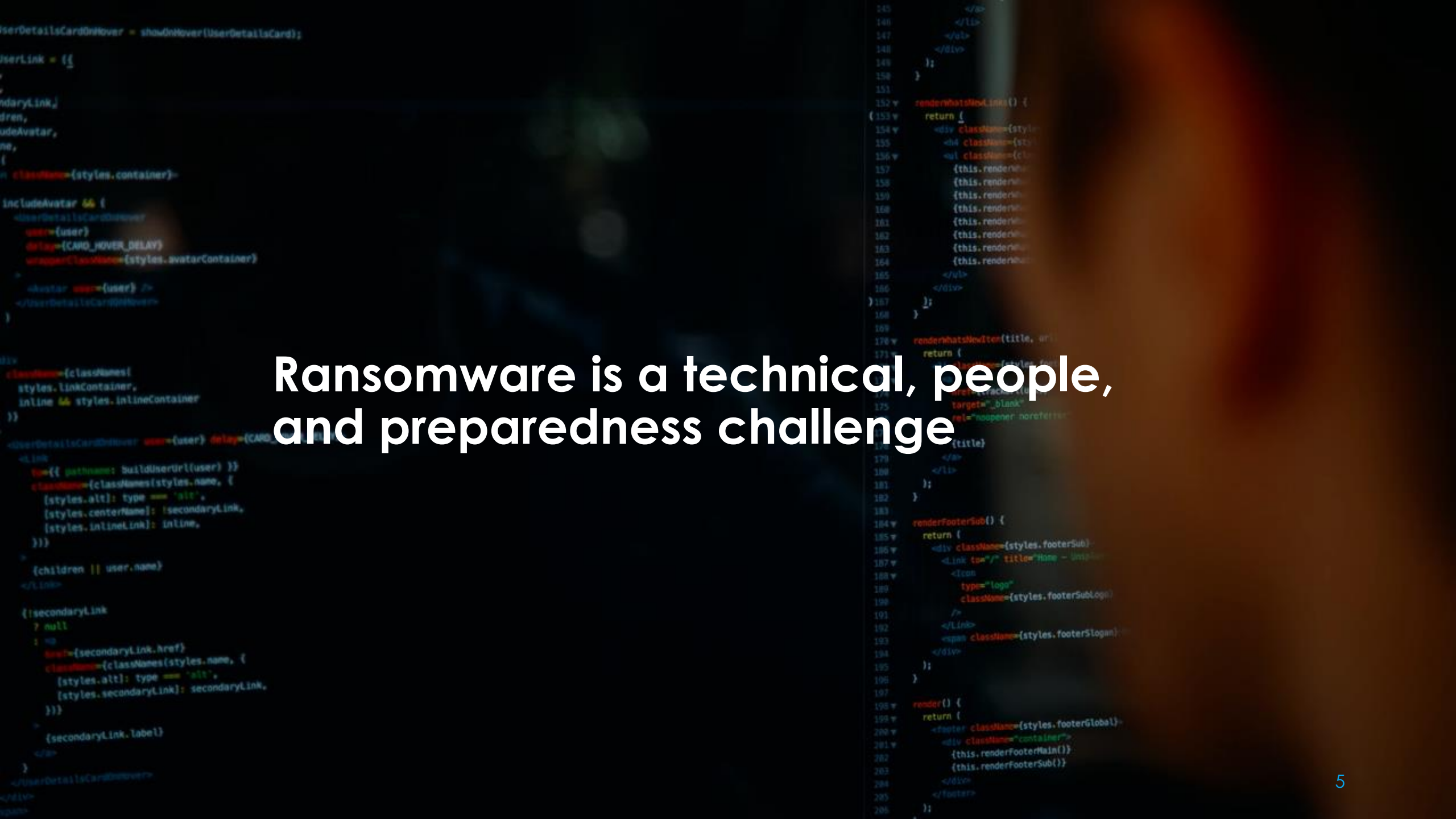
764

primetsr

113



89
(1,233)



Ransomware is a technical, people, and preparedness challenge

The Road To Preparedness

Prevention

The best and most often only defense is being proactive - so if you don't already have a playbook, start one tomorrow.

A playbook is an action plan that documents an actionable set of steps an organization can follow to successfully recover from a cyber event.

Detection

How will you know?

Millions of event logs in a day are easily capable; you only need to know the one that that could indicate a security compromise.

Develop situational awareness about what is normal, then alert on abnormal activity.

Remediation

The recovery process is just that – a process. At a given time, the status of your organization would be better expressed along a spectrum of recovery.

How quickly can you stand up the basic operations, and/or operate in a reduced capacity?

Avoid thinking black or white.

Everyday Best Practices

- Backup: 3-2-1 rule
- Windows Defender
- Email lockdown
- Segment the network
- Least privilege
- Two-factor authentication
- Application Whitelist

Watch Your Bits

- Logging / Alerting
- Canary

- USN Journal Deletion
- Deleting Shadow Copies
- Spike in File Writes
- Common Ransomware Extensions
- Common Ransomware Notes
- Detect SMB Traffic Allowed
- Detect Spike in SMB Traffic
- Monitor TOR traffic

The Cloud Way

Object Storage

- w/ versioning

Databases

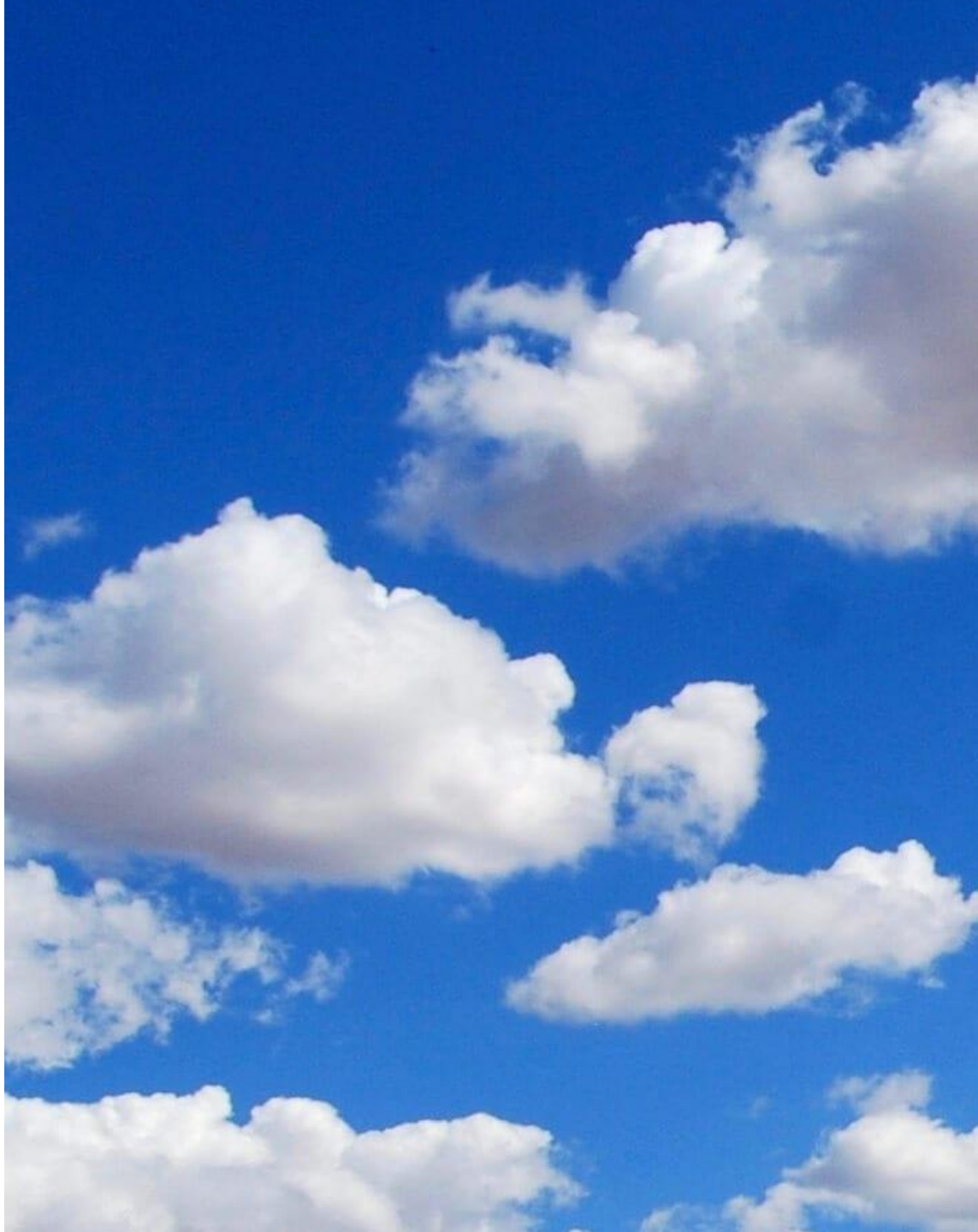
- Redundancy, failover

Logging

- Offsite, scalable

GovCloud

- Templated compliance



Training

Training Fundamentals

Start with balanced hiring

Comprehensive onboarding

Formal in-house training program

Continuing education & certifications

Social engineering

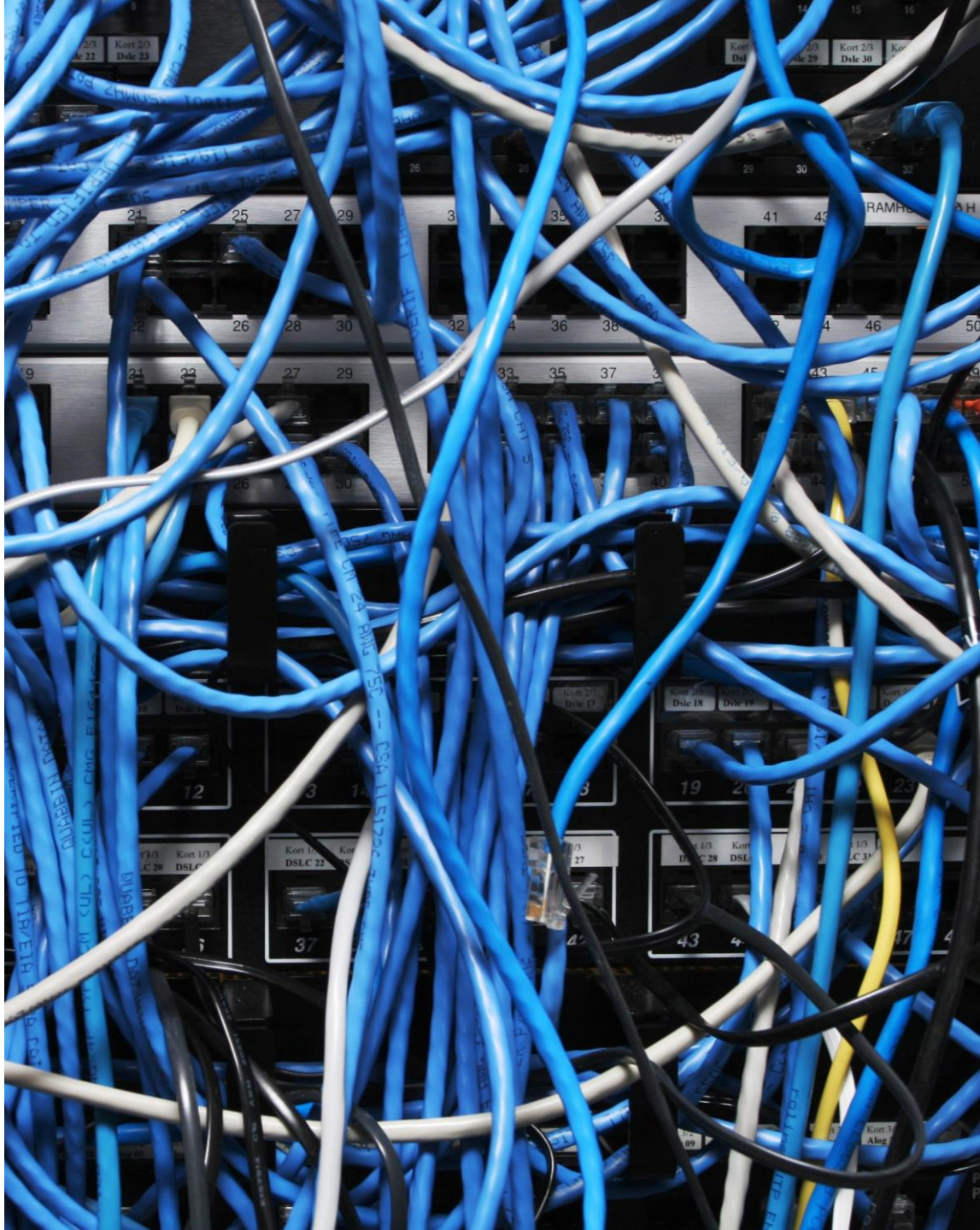
Chaos Engineering

"Drill, baby, drill!"

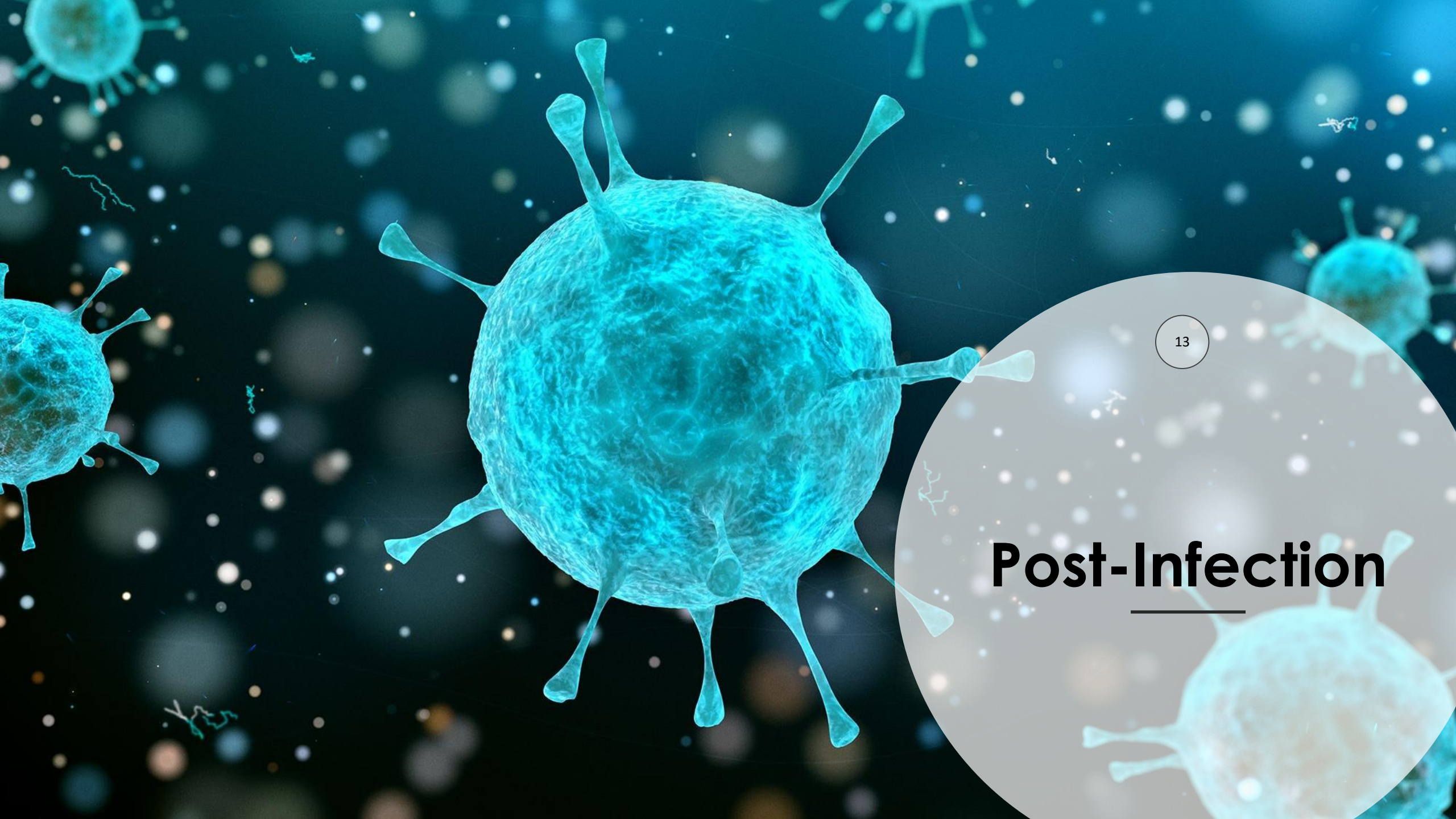
What does your operation look like with pen and paper…

Or stone tablets and abacuses?

- Build the muscle-memory
- Discover the questions

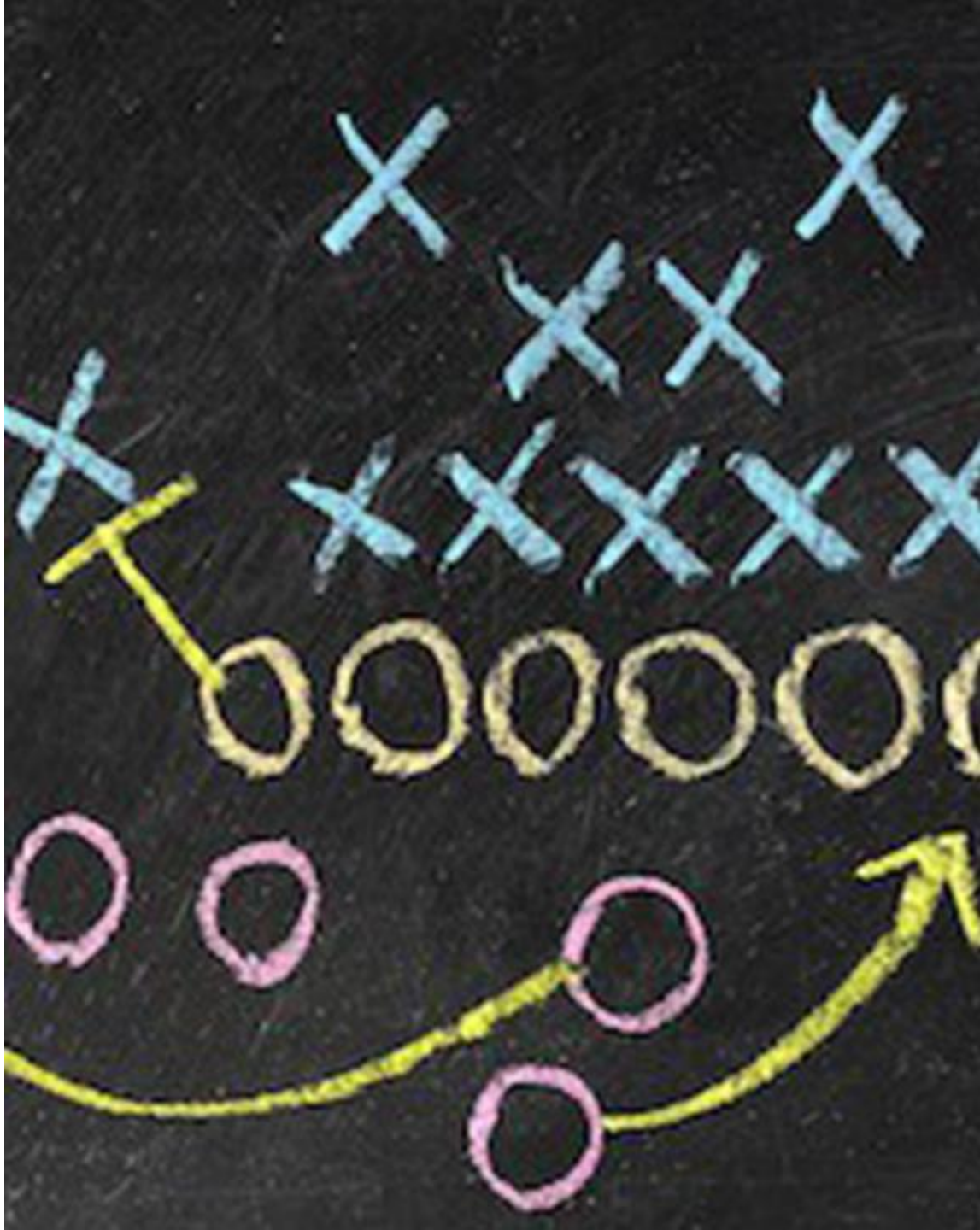


Post-Infection



The Clock Is Ticking

- Act quickly to shut down further encroachment
- Establish communication



Checks

- Does a key exist?
- Get help if needed
  - Vendor
  - US-CERT
- Can you determine “patient zero”?
- Does the attacker still have access?

Thank You

Michael Hale

mhale@primetsr.com

Consultant, Cloud Computing

1 N. Dearborn St

Chicago, IL 60602


Further Reading

Referenced Articles

(Corresponding slide in brackets)

[3] Maze Ransomware Publishes 14GB of Stolen Southwire Files

https://www.bleepingcomputer.com/news/security/maze-ransomware-publishes-14gb-of-stolen-southwire-files/

[3] Ransomware: Cybercriminals are adding a new twist to their demands

https://www.zdnet.com/article/ransomware-cybercriminals-are-adding-a-new-twist-to-their-demands/

Referenced Articles

[4] FBI flash alert warns of LockerGoga and MegaCortex Ransomware attacks

https://securityaffairs.co/wordpress/95573/breaking-news/lockergoga-megacortex-ransomware-attacks.html

[4] Ransomware Attack Count 2019

https://www.msspalert.com/cybersecurity-research/ransomware-attack-count-2019/

[4] Bitcoin Ransomware Hackers Lose Control of Their Decryption Tool

https://www.cryptoglobe.com/latest/2019/12/bitcoin-ransomware-hackers-lose-control-of-their-decryption/

[4] Only Half of Those Who Paid a Ransomware Were Able to Recover Their Data

https://www.bleepingcomputer.com/news/security/only-half-of-those-who-paid-a-ransomware-were-able-to-recover-their-data/

Referenced Articles

[3C > 12] US mayors group adopts resolution not to pay any more ransoms to hackers

https://www.zdnet.com/article/us-mayors-group-adopts-resolution-not-to-pay-any-more-ransoms-to-hackers/

[11] USB Drop Attacks: The Danger Of "Lost And Found" Thumb Drives

https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives/

[15] The ransomware superhero of downstate Normal

https://chicago.suntimes.com/crime/2019/10/28/20934591/ransomware-superhero-normal-illinois-fbi-cybercrime

[15] No More Ransom

https://www.nomoreransom.org

Referenced Articles

[15] New Orleans Ransomware Attack Update: City to Raise Cyber Insurance to $10M

https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/new-orleans-cyber-insurance-plan/

[15] United States Computer Emergency Readiness Team (US-CERT)

https://www.us-cert.gov/

[15] Sting Catches Another Ransomware Firm — Red Mosquito — Negotiating With "Hackers"

https://www.propublica.org/article/sting-catches-another-ransomware-firm-red-mosquito-negotiating-with-hackers

[15] The Trade Secret

https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/

Additional Resources

Shodan (an IoT vulnerability search engine)

https://www.shodan.io/

National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *Guide for Cybersecurity Event Recovery*. Gaithersburg, MD, 2016.

https://doi.org/10.6028/NIST.SP.800-184