How MSPs Can Survive a Coordinated Ransomware Attack

Presented by ninja RMM HUNTRESS

Hello,

Kyle Hanslovan

Co-founder & CEO, Huntress Labs

In a former life
Worked in the intelligence community

Big fan of
Long walks on the beach contemplating security

Favorite security advice
Make sure all of your best practices are truly in order before adding another product to your security stack

HUNTRESS

Kyle Hanslovan is CEO and Co-Founder of Huntress Labs. He comes from the U.S. Intelligence Community, where he supported **defensive and offensive cyber operations** for the past decade.

He actively participates in the ethical hacking community as a Black Hat conference trainer, STEM mentor, and DEF CON CTF champion. Additionally, he serves in the Maryland Air National Guard as a Cyber Warfare Operator. At this stage in life, Kyle is focused on **making hackers earn every inch of their access** within the networks he protects.

Agenda

What We'll Cover

- Timeline of Coordinated Ransomware Attacks on MSP Clients
- Example Attack Diagram
- Live Demo of Attack Tactics
- Attack Network Effect
- Rapid Response Checklist
- Triage System
- Incident Response Prep
- Q&A

Got Questions?

Ask a question here at any time,
or join the discussion

@HuntressLabs

#responseready

“Since Fall 2018 there has been a 400-500% increase in activity specifically targeting MSPs and their end users.”

— Ryan Weeks, CISO at Datto

“We’re seeing roughly 3 MSPs getting hit a week.”

— Kyle Hanslovan, CEO at Huntress Labs

ninja RMM HUNTRESS

Timeline

Coordinated Ransomware Attacks on MSPs

Precursor

FEBRUARY 4

Tool hijacked: Kaseya VSA (via ConnectWise ManagedITSync plugin vulnerability)

GandCrab ransomware deployed

Summer of Sodinokibi

Incidents where attackers compromised MSPs and abused tools / credentials to deploy ransomware.

JUNE 19

Tools hijacked: Webroot, Kaseya VSA, ConnectWise Control

JULY 3

Tools hijacked: Go2Assist, Passcape

JULY 22

Tool hijacked: NinjaRMM

AUGUST 2

Tool hijacked: Continuum

* ransomware variant unconfirmed

AUGUST 16

Tool hijacked: ConnectWise Control

22 Texas municipalities

AUGUST 25

Datto backups compromised, GlobeImposter 2.0 deployed

AUGUST 26

Backup software DDS Safe compromised, Sodinokibi deployed

Note: Dates are when incidents became public

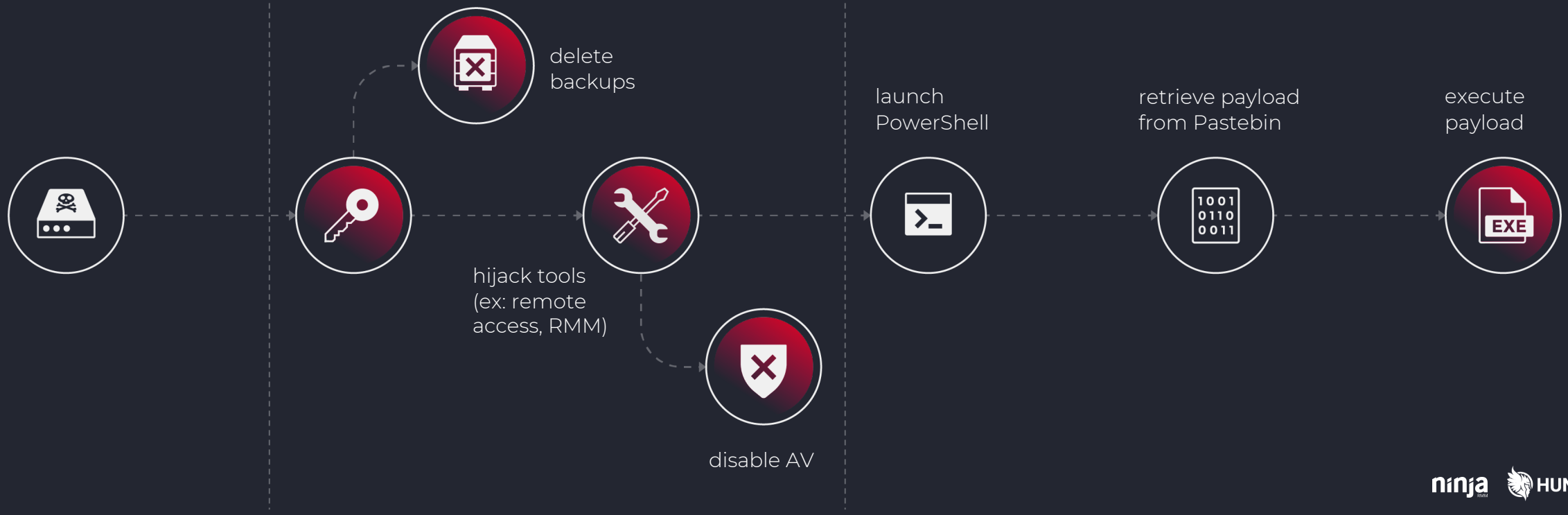
Attack Diagram

Example MSP Compromise

Step 1
Attackers gain initial access

Step 2
Attackers use compromised credentials to...

Step 3
Hijacked tools used to manually deploy ransomware payload



ninja RMM HUNTRESS

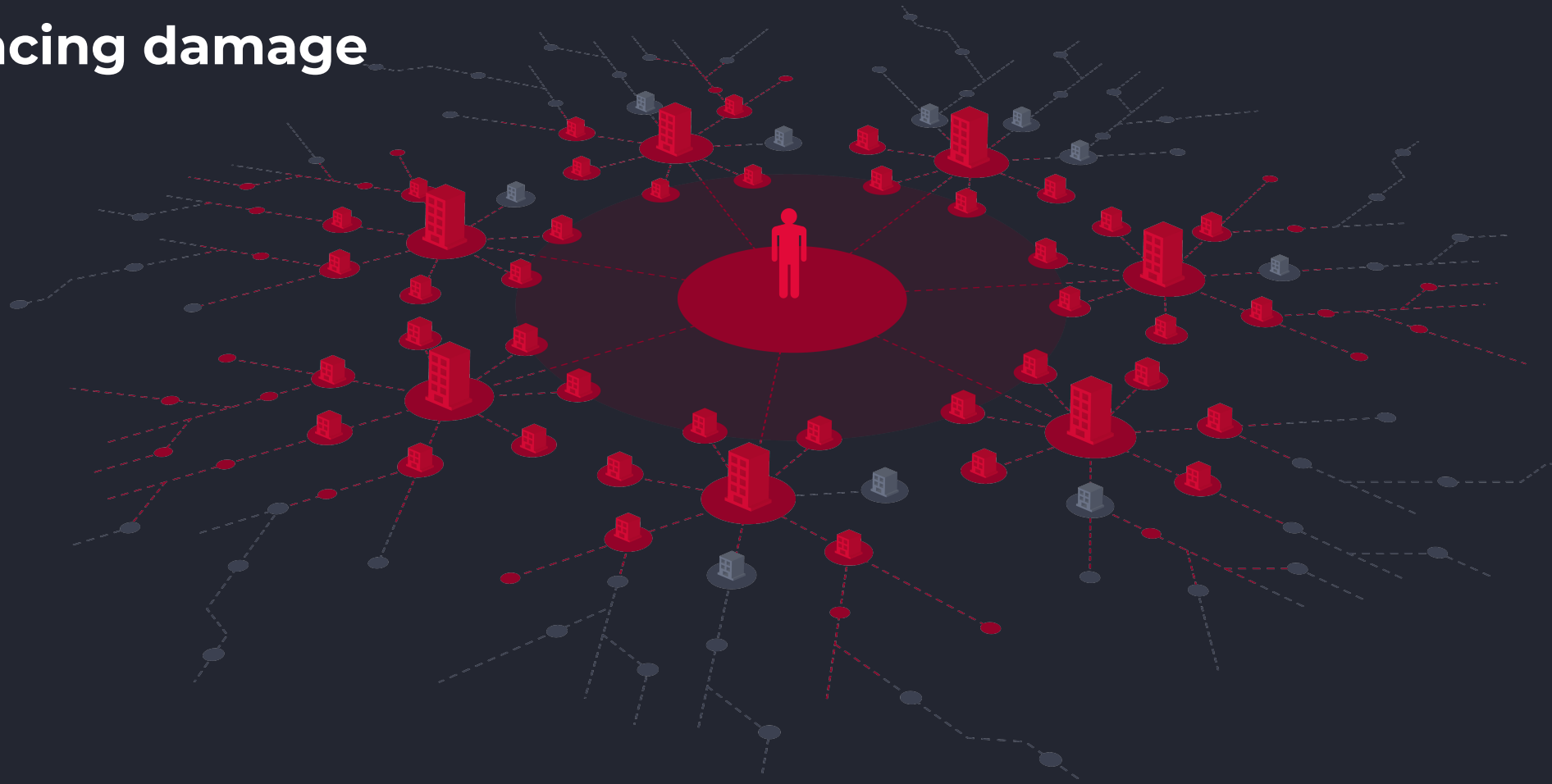
Live Demo

Attack Tactics

Attack Network Effect

Parties experiencing damage and disruption:

- MSP
- MSP's clients
- Clients' customers



From the Trenches

In the July 22 email announcing its closure, PM said it had been "inundated with calls" on the morning of the ransomware attack, "and we immediately started investigating and trying to restore data. Throughout the next several days and into the weekend, we worked around the clock on recovery efforts. ... However, it was soon apparent the number of PC's that needed restoration was too large for our small team to complete in any reasonable time frame."

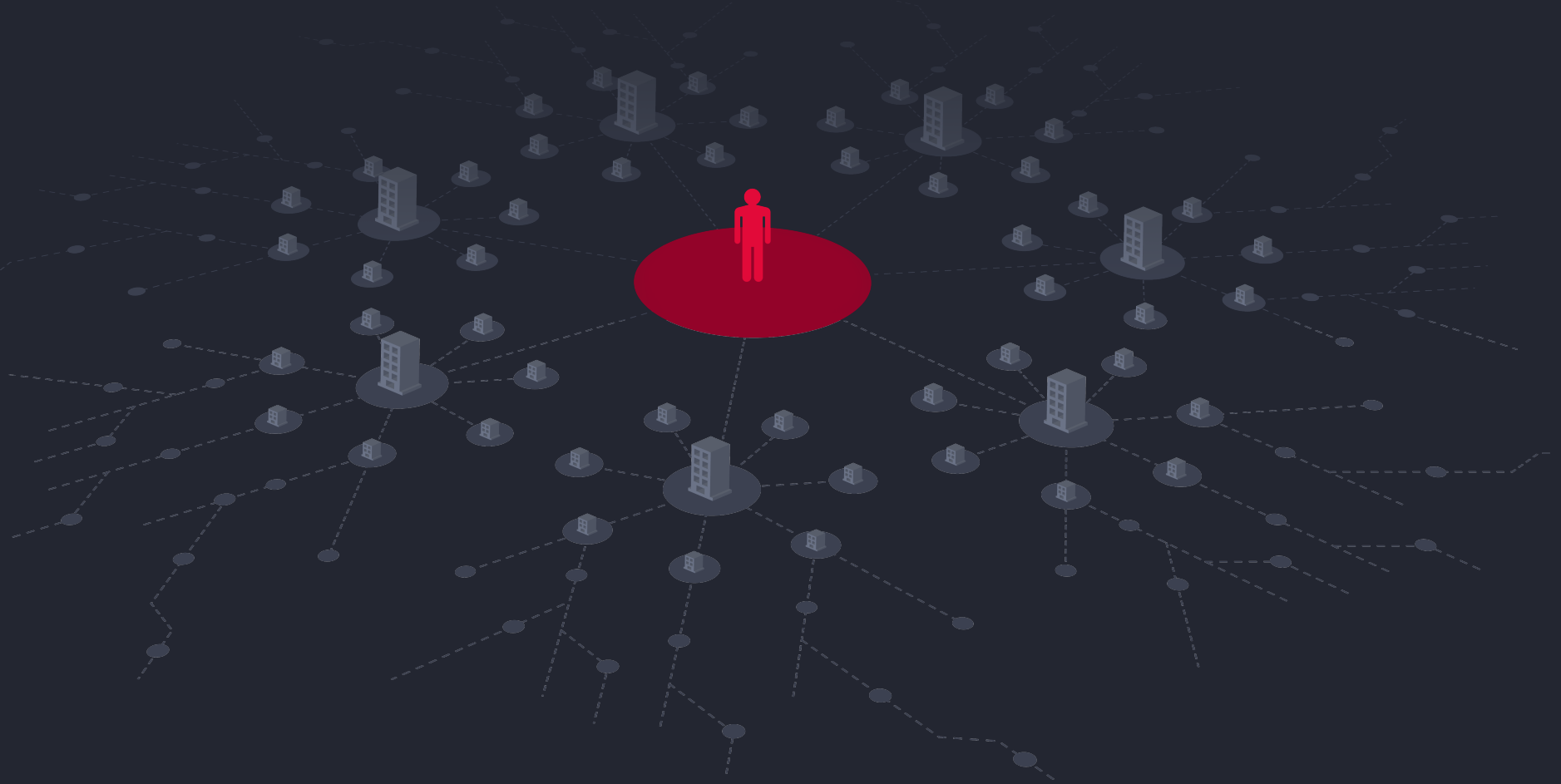
The company was also "receiving hundreds of calls, emails and texts to which we were unable to respond."

It advised customers, "At this time we must recommend you seek outside technical assistance with the recovery of your data."

from ProPublica article describing ransomware incident affecting customers of Portland-based PM Consultants, Inc.

“No one trusts me anymore. You go from IT advisor to being questioned on everything.”

from CRN.com interview with anonymous MSP whose customers were infected with ransomware in a separate incident



ninja RMM HUNTRESS

Hey, Still With Us?

Thinking it will never happen to you

Preparing for the worst so you can recover quickly and avoid paying ransom

Response Planning

Roles & Responsibilities

Goal: Divide and conquer

CEO / COO

Responsible for
Critical decision making

- Discussing liability w / insurance, lawyer
- Key account damage control
- Prioritizing
- Delegating
- Outsourcing
  (IR provider, additional surge capacity)

Sales / Marketing

Responsible for
Communications

- Outbound to clients
- Inbound from clients
- External
  (press, 3rd parties)

All comms approved by CEO & lawyer

Technicians

Responsible for
Containment & restoration

- Locking down affected systems
  (your own + clients')
- Investigation / forensics gathering
- Recovery
- Vendor coordination
- Regular services

ninja RMM HUNTRESS

CEO Checklist

Rapid Ransomware Response

Goal: Delegate & run interference

Assess damage

- [ ] How widespread is attack? Is it ongoing?
- [ ] Do you need to pull the plug on your tools; temporarily halt support?
- [ ] Delegate triaged outreach to affected customers
- [ ] Be aware of regulations & requirements (HIPAA, GDPR, etc.)

Get on the phone (just not with your clients yet)

- [ ] Contact cybersecurity insurance provider
- [ ] Contact lawyer
- [ ] Coordinate with (insurance-approved) IR provider
- [ ] Secure additional outside help / surge capacity
- [ ] Contact law enforcement (discretionary)

Get your story straight

- [ ] Determine how much to share, with who
- [ ] Coordinate with team re: communication scripts/templates for:
  - [ ] Notifying and updating clients
  - [ ] Responding to public / press inquiries
- [ ] Review comms with lawyer

Utilize everyone to the full extent

- [ ] Run damage control with key affected clients
- [ ] Use your best / most technical staff to stop the bleeding
- [ ] Delegate keeping the lights on to other techs
- [ ] Have non-technical staff answering phones, responding to email

* Disclaimer: Any actions taken obviously need to be tailored to your unique situation & environment. We don't take responsibility for results or outcomes.

ninja RMM HUNTRESS

Technician Checklist

Rapid Ransomware Response

Goal: Isolate and contain

Lock down your accounts and tools

- ☐ Disable access to your RMM and remote access tool(s)
- ☐ Audit for unusual tasks, scripts, policy changes, etc.
- ☐ Disable user accounts associated with abnormal/malicious behavior; terminate active sessions
- ☐ Isolate any endpoints & other accounts associated with those users
- ☐ Minimize logging into affected systems using privileged credentials
- ☐ DO NOT shut down affected systems
- ☐ Change all passwords
- ☐ Ensure MFA is enabled on all accounts
- ☐ Confirm AV is enabled and updated, run deep scan
- ☐ Backup log files

Lock down affected clients

- ☐ Isolate affected client endpoints by taking them off the network
- ☐ Ensure backups are isolated/protected
- ☐ Minimize logging into affected systems using privileged credentials
- ☐ DO NOT shut down affected systems

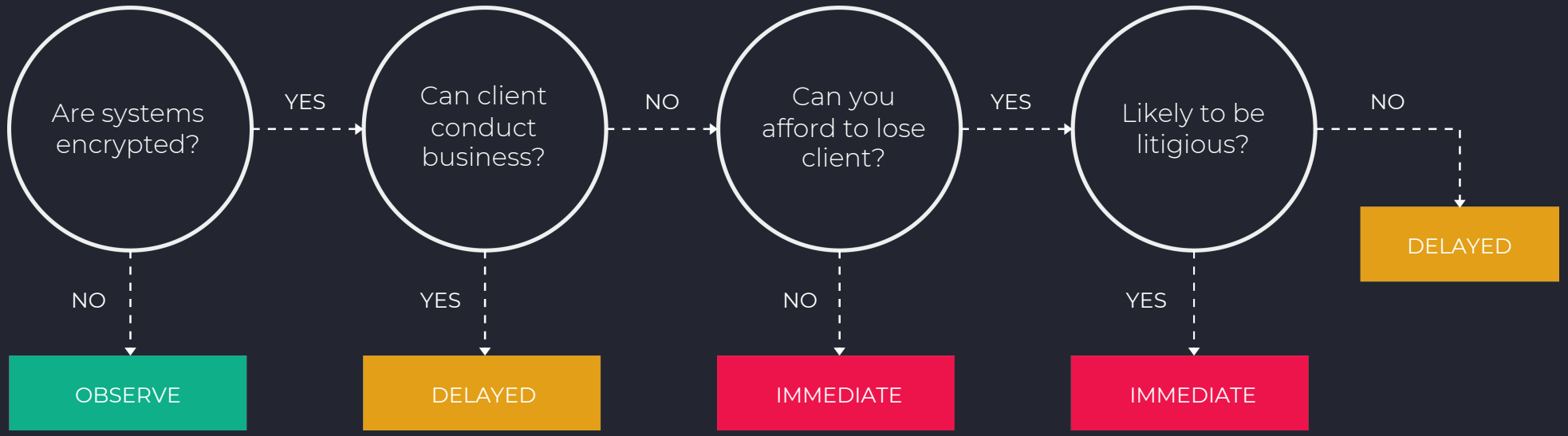
Next steps after isolation

- ☐ Triage to determine further remediation priorities
- ☐ Strongly consider bringing in incident response specialist

* Disclaimer: Any actions taken obviously need to be tailored to your unique situation & environment. We don't take responsibility for results or outcomes.

ninja RMM HUNTRESS

Mass Ransomware Incident Triage



Triage Categories

Priority #1

IMMEDIATE

- Business-critical operations disrupted
- Requires urgent recovery efforts beyond initial isolation

Priority #2

DELAYED

- Systems encrypted, but initial remediation can focus on isolation with additional efforts to follow

Priority #3

OBSERVE

- Actively monitor

* Disclaimer: Any actions taken obviously need to be tailored to your unique situation & environment. We don't take responsibility for results or outcomes.

ninja RMM HUNTRESS

The Good News

You’re Not Here Yet

Checklist

Incident Response Prep

Goal: Have everything ready before you need it

- ☐ Develop (and drill) your own incident response plan
- ☐ Document and practice lockdown procedures (your clients AND your own systems)
- ☐ Run through mock triage
- ☐ Audit backups
- ☐ Practice backup restoration
- ☐ Know how to retrieve/request access to relevant event and activity logs
- ☐ Have cybersecurity insurance
- ☐ Have a go-to (insurance-approved) incident response specialist
- ☐ Have other emergency options in place for increasing surge capacity
- ☐ Have a communication strategy and lawyer-approved scripts/templates prepared
- ☐ Know regulations affecting your clients

Q&A

Questions?

Keep up-to-date

Subscribe to our blog

https://www.ninjarmm.com/blog/

Register for Tradecraft Tuesday

https://tradecrafttuesday.com