#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART3-W09**

What Will it Take to Stop Ransomware?

Mark Bowling

VP of Security Response Services
ExtraHop

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Mark Bowling

VP Security Response Services

ExtraHop

Ransomware in Context of Current Events

Attackers Have Weaponized Your Network

EXTORTION

$1.85M

Average cost per ransomware incident

4 ransomware attacks per org. over 5 years

EXPLOITATION

$4.87M

Average cost per supply chain attack

3x increase in supply chain attacks in 2021

EXTINCTION

$300M

cost of Maersk's near-extinction

Price of Zero Day Exploits is now $2M

RANSOMWARE

It’s not if.

It’s when.

85%

experience ransomware in the past 5 years

$

72%

paid the ransom

60%

hit more than once

Cyber Confidence Survey 2022

Modern Ransomware is Advanced

	2016 The "quick buck"	2018 The "fire-and-forget"	2021 The "more-pain-more-gain"
Attack Strategy	Spray & Pray, automated malware	Spear Phish, automated malware, self propagating	Land-n-Pivot, sophisticated lateral tooling
Initial Access	Phish Stolen credentials Drive-by downloads Vulnerability exploit	BYoD Trusted relationships Misconfiguration	RDP Initial Access Broker(IAB) Supply chain
Target	Consumers	Employees	Enterprise IT
Avg. Ransom Paid	**$1,077**	**$6,700**	**$170,404**
Traditional Mitigation Strategies	EDR, Backup	EDR, MFA, Phish training, Backup	EDR, Zero-trust, Phish training, Backup

What will it take to stop ransomware?

What does it take to stop a criminal?

Who’s responsible for the crime?

What is their MO (modus operandi)?

What is their motivation?

What are their tools?

What advantages do they have over us?

What tactics have we already tried?

- Why didn’t they work? What did we learn?
- What emerging tactics have we not yet tried?

Knowing who's behind the attack is critical

Affiliation	Ransomware Gang	Nation State
MO	More pain, more gain	Penetrate as deeply and quietly as possible
Target	Targeted at victims of financial consequence	Directed at specific targets based on strategic calculus
Motivation	Financial gain	Gather intelligence or achieving military objectives
Tools	Phishing, RaaS	Zero Days, Supply Chain

Motivation: Ransomware Gangs

Money

Why do bank robbers rob banks?

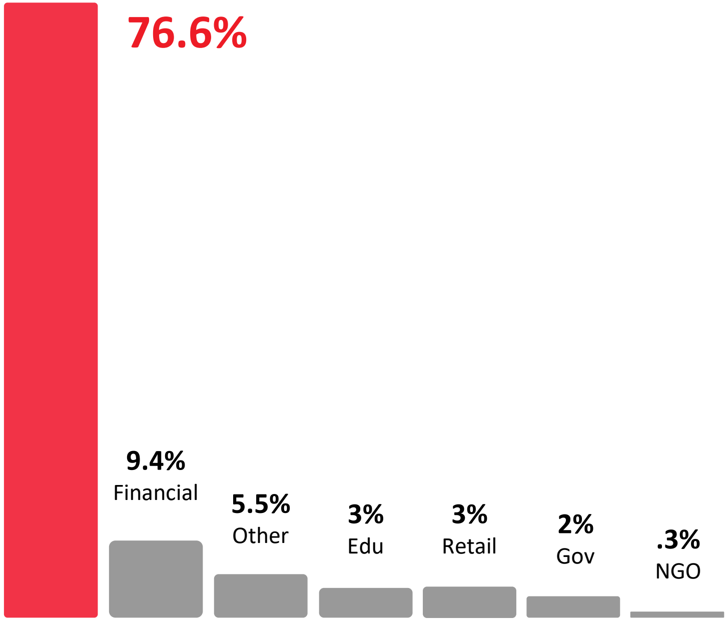
Because that’s where the money is.

(And because they pay!)

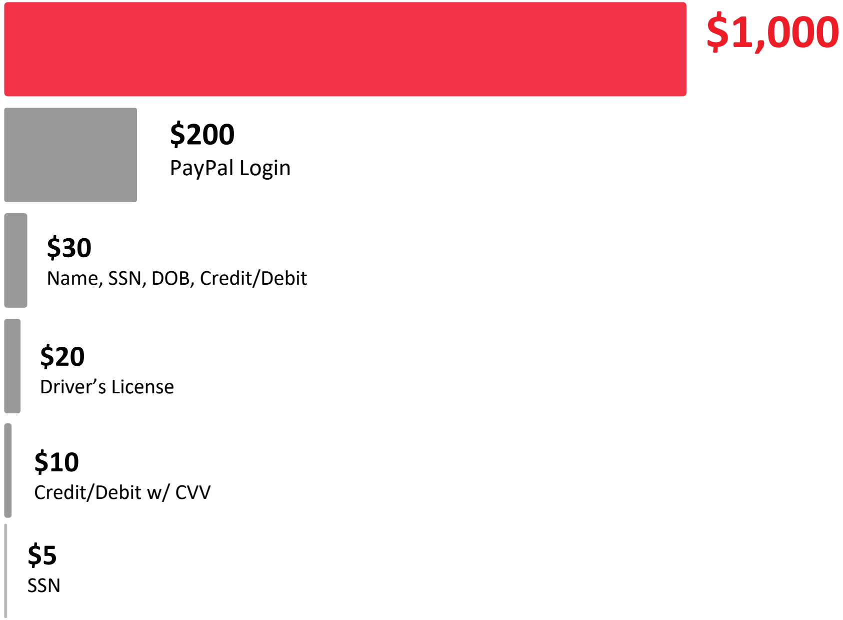
Willie Sutton

Example: Ransomware in Healthcare

Percentage of breaches
2015-2019



Personal data value on the dark web according to Experian



Healthcare Data Breaches: Insights and Implications, MDPI, May 13, 2020
Here's How Much Your Personal Information Is Selling For on the Dark Web, Experian, December 6, 2017

Motivation: Nation States

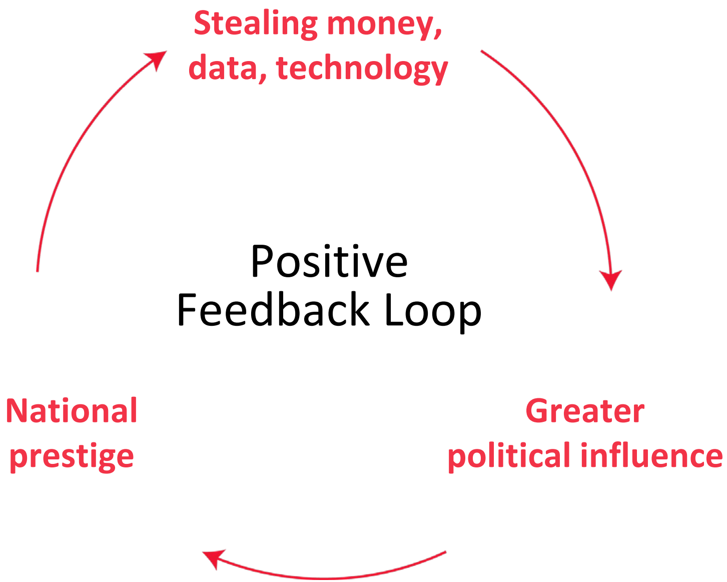
Cyber Warfare - Achieving Political and Military Objectives

Power, Intimidation, & Influence

Ideology

Retaliation

Intelligence



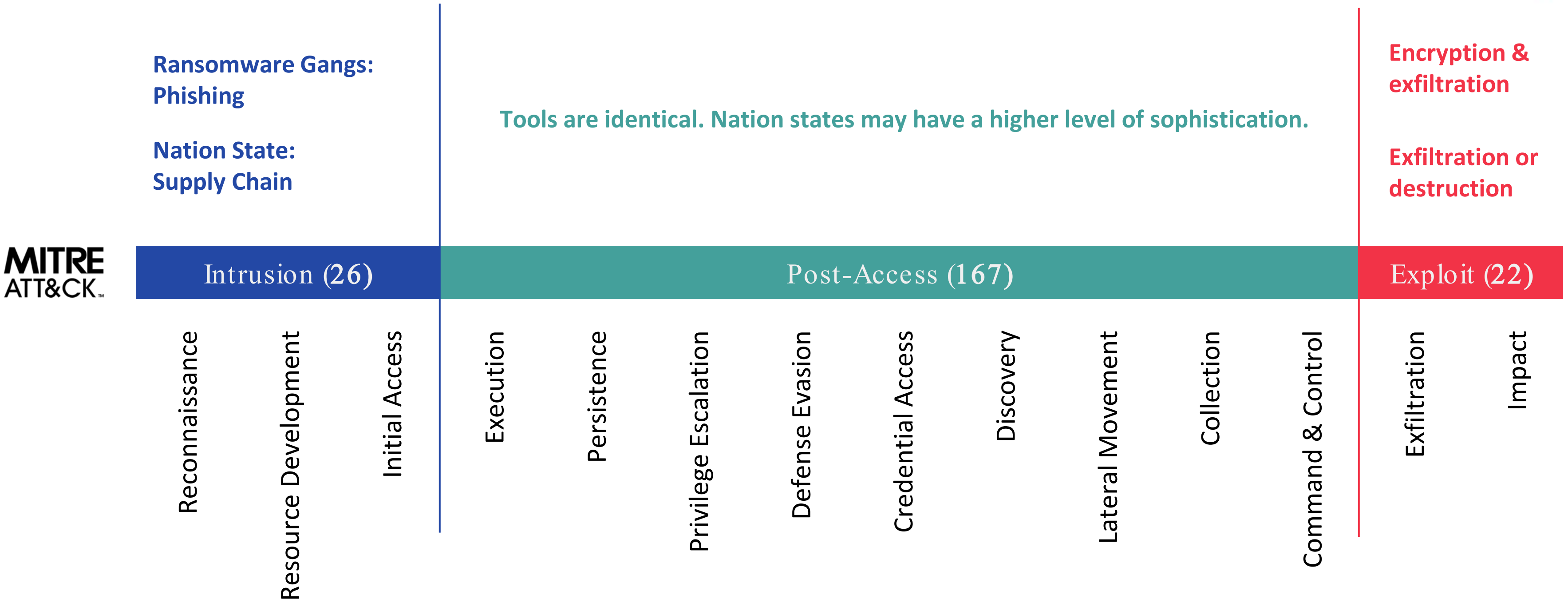
Stealing money, data, technology

Positive Feedback Loop

Greater political influence

National prestige

The Tools



Ransomware Gangs: Phishing

Nation State: Supply Chain

Tools are identical. Nation states may have a higher level of sophistication.

Encryption & exfiltration

Exfiltration or destruction

MITRE ATT&CK™

Intrusion (26)

Post-Access (167)

Exploit (22)

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

Attackers have the advantage

Resources

Teams

Funding

Safe harbor

Time

Focus

Misdirected attention

So, what can we do?

Existing Tactics

Conventional Wisdom Hasn't Slowed Ransomware

MYTH #1

The only way to stop ransomware is to prevent them from getting in.

4.8%

of phishing links still clicked after one year of phishing training

KnowBe4 Annual Phishing Benchmark Report

93%

of Pentests land inside—without using social engineering tactics

Positive Technologies Annual Report

Existing Tactics

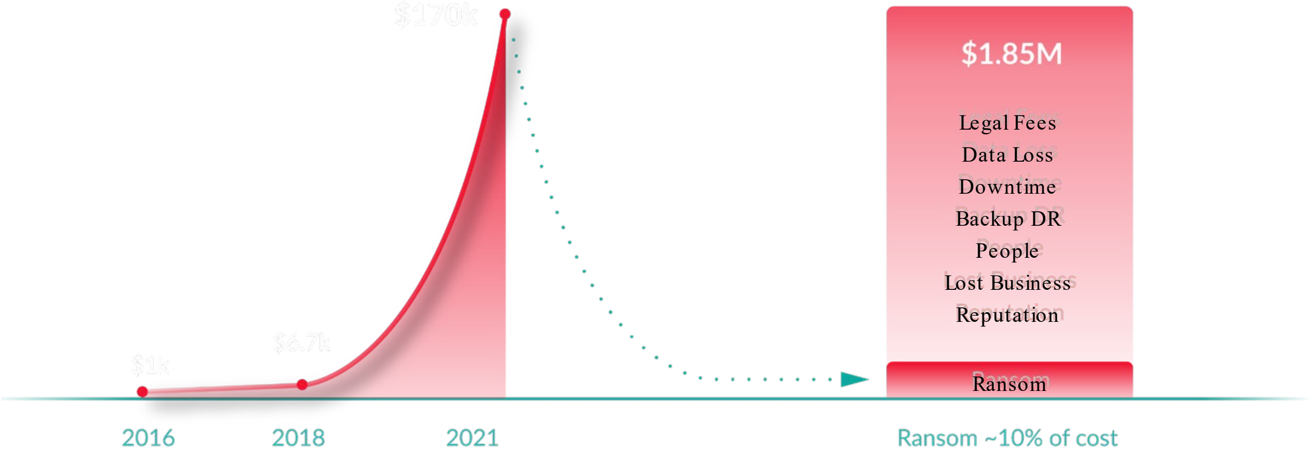
Conventional Wisdom Hasn’t Slowed Ransomware

MYTH #2

We have backup (risk mitigation) and cyber insurance (risk transfer), we are resilient to ransomware

The more sophisticated the attack tactics, the more ransom attackers can command.

Recovery is expensive and imperfect



Ransom ~10% of cost

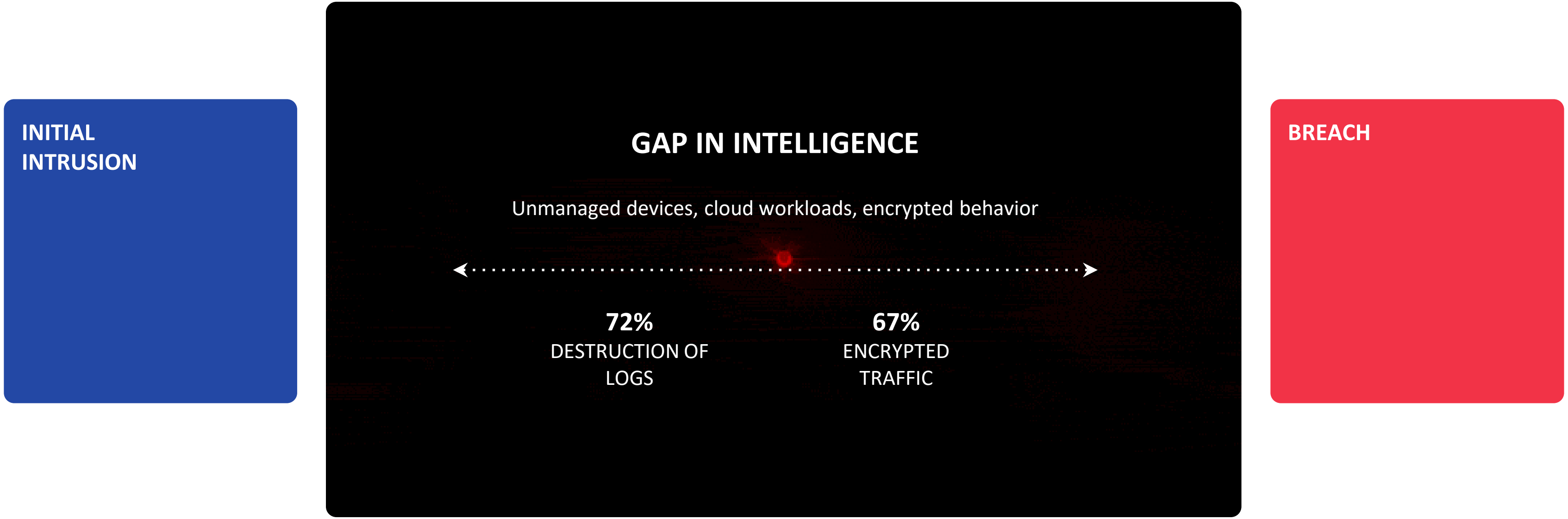
AVERAGE RANSOM PAYOUT

RANSOM & RECOVERY

Sophos State of Ransomware

Emerging Tactics

Attack Innovation is Happening Inside



INITIAL INTRUSION

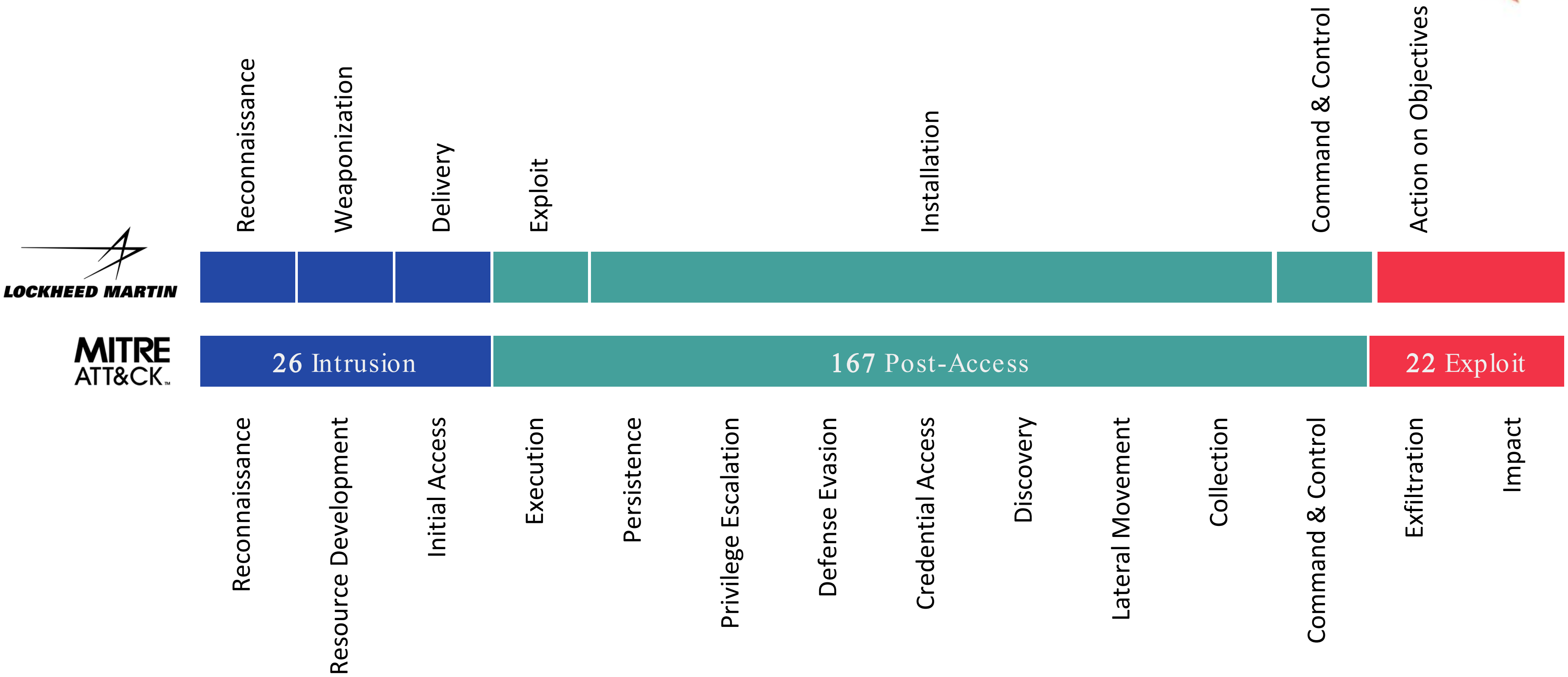
GAP IN INTELLIGENCE

Unmanaged devices, cloud workloads, encrypted behavior

72%
DESTRUCTION OF LOGS

67%
ENCRYPTED TRAFFIC

BREACH



LOCKHEED MARTIN

Reconnaissance

Weaponization

Delivery

Exploit

Installation

Command & Control

Action on Objectives

MITRE ATT&CK

26 Intrusion

167 Post-Access

22 Exploit

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

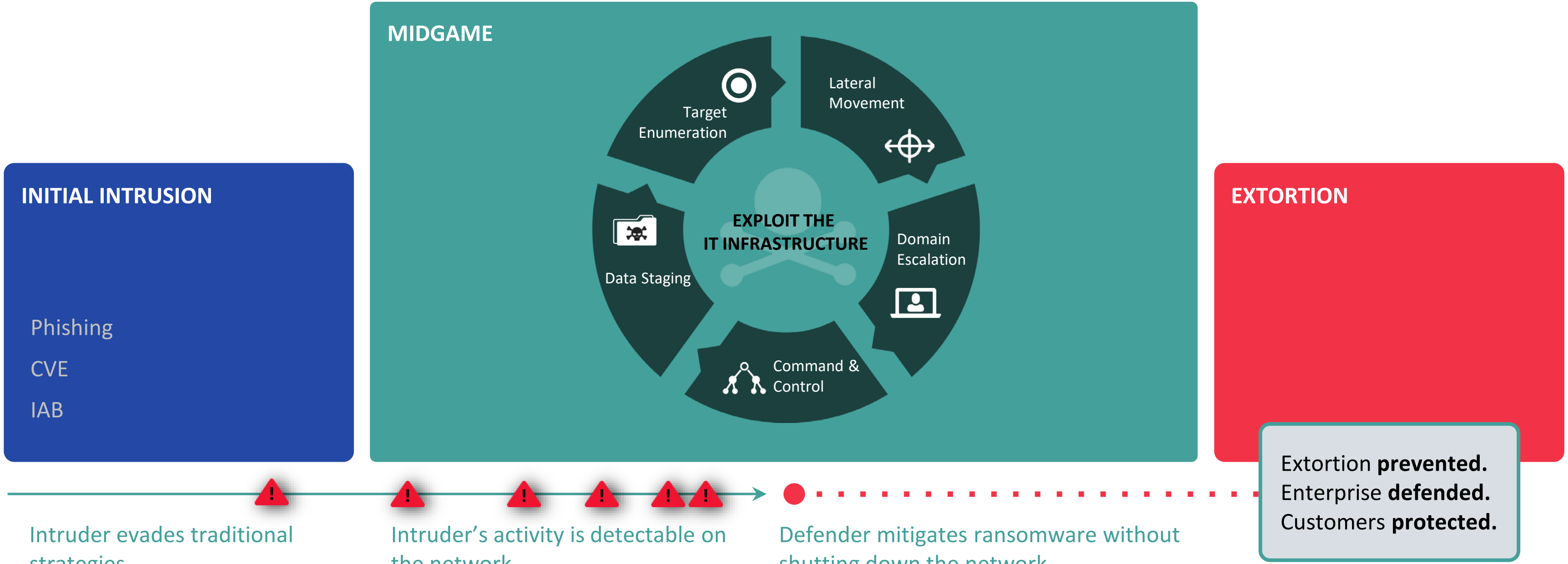
Command & Control

Exfiltration

Impact

Emerging Tactics

A new layer of defense is required in the Midgame



INITIAL INTRUSION

- Phishing
- CVE
- IAB

MIDGAME

EXPLOIT THE IT INFRASTRUCTURE

EXTORTION

Intruder evades traditional strategies

Intruder's activity is detectable on the network

Defender mitigates ransomware without shutting down the network

Extortion **prevented.**
Enterprise **defended.**
Customers **protected.**

Additional Tactics

Zero Trust architecture → Builds resilience

Mandatory payment disclosure → Increases deterrence

Make crypto traceable → Removes anonymity

Apply

What is their crime?	Extortion
What is their motivation?	Money Cyber warfare
What advantages do they have over us?	Resources Teams Funding Safe harbor Time Focus Misdirected attention
What tactics have we already tried? Why didn’t they work?	Keep intruders out – Attack surface is too great Backup & cyber insurance make us resilient to ransomware – Helpful solutions in case of emergency, but not a defensive strategy
What emerging tactics have we not yet tried?	Stopping intruders in the midgame Legislative deterrence

Prepare for Cyber Warfare

Every organization needs to take action to reduce threat likelihood and impact

- Reduce the likelihood of a damaging cyber intrusion
- Take steps to quickly detect a potential intrusion
- Ensure that the organization is prepared to respond if an intrusion occurs
- Maximize the organization's resilience to a destructive cyber incident

Takeaways

- The more damage ransomware causes, the higher the payout they ensure
- You need to fully understand the opponent to stop them
  - Affiliation, MO, Target, Motivation, Tools
- Ransomware relies on midgame attack techniques
  - A new layer of defense is required in the midgame

RSAConference2022

Thank you

Mark Bowling

markb@extrahop.com