CROWDSTRIKE

Detecting and Responding PANDAS AND BEARS

Chris Scott, Director of Remediation, CrowdStrike Services
Wendi Whitmore, Global Partner, IBM Security Services

TODAY'S SPEAKERS

IBM **Security**

Intelligence. Integration. Expertise.

14+ YEARS

Incident response and security breach investigations experience

PRIOR TO IBM

Vice President, CrowdStrike Services
Managing Director, Mandiant
Special Agent, Air Force Office of Special Investigations

CONNECT

LINKEDIN: Wendi Whitmore

TWITTER: @WendiLou2

wwhitmor@us.ibm.com

WENDI WHITMORE
PARTNER, IBM SECURITY SERVICES

TODAY'S SPEAKERS

18+ YEARS

Conducting security assessment, incident response, insider threat analysis, and security architecture.

PRIOR TO CROWDSTRIKE

Defended networks for the Defense Industrial Base

CONNECT

LINKEDIN: Christopher Scott

TWITTER: @NetOpsGuru

chris@crowdstrike.com

CHRIS SCOTT
DIRECTOR OF REMEDIATION

UNCOVER THE ADVERSARY

CHINA

Comment Panda: Commercial, Government, Non-profit

Deep Panda: Financial, Technology, Non-profit

Foxy Panda: Technology & Communications

Anchor Panda: Government organizations, Defense & Aerospace, Industrial Engineering, NGOs

Impersonating Panda: Financial Sector

Karma Panda: Dissident groups

Keyhole Panda: Electronics & Communications

Poisonous Panda: Energy Technology, G20, NGOs, Dissident Groups

Putter Panda: Governmental & Military

Toxic Panda: Dissident Groups

Union Panda: Industrial companies

Vixen Panda: Government

CRIMINAL

Singing Spider: Commercial, Financial

Union Spider: Manufacturing

Andromeda Spider: Numerous

IRAN

Magic Kitten: Dissidents

Cutting Kitten: Energy Companies

INDIA

Viceroy Tiger: Government, Legal, Financial, Media, Telecom

RUSSIA

Energetic Bear: Oil and Gas Companies

NORTH KOREA

Silent Chollima: Government, Military, Financial

HACTIVIST/TERRORIST

Deadeye Jackal: Commercial, Financial, Media, Social Networking

Ghost Jackal: Commercial, Energy, Financial

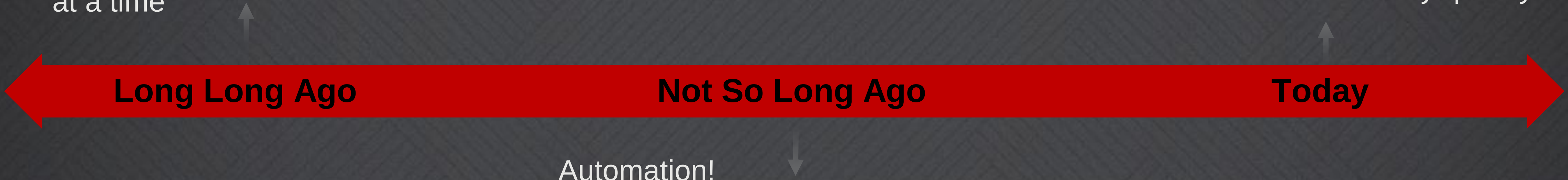
Corsair Jackal: Commercial, Technology, Financial, Energy

Extreme Jackal: Military, Government

IR & HUNTING

EVOLUTION & BEST PRACTICES

EVOLUTION OF INCIDENT RESPONSE



Long Long Ago

Remove affected machine from network immediately

Collect data from one machine at a time

Not So Long Ago

Automation!

Search for indicators of compromise

Clean entire network before beginning to remediate

Conduct forensics for months before containment of the adversary

Today

Track attackers and actively hunt for them in real-time

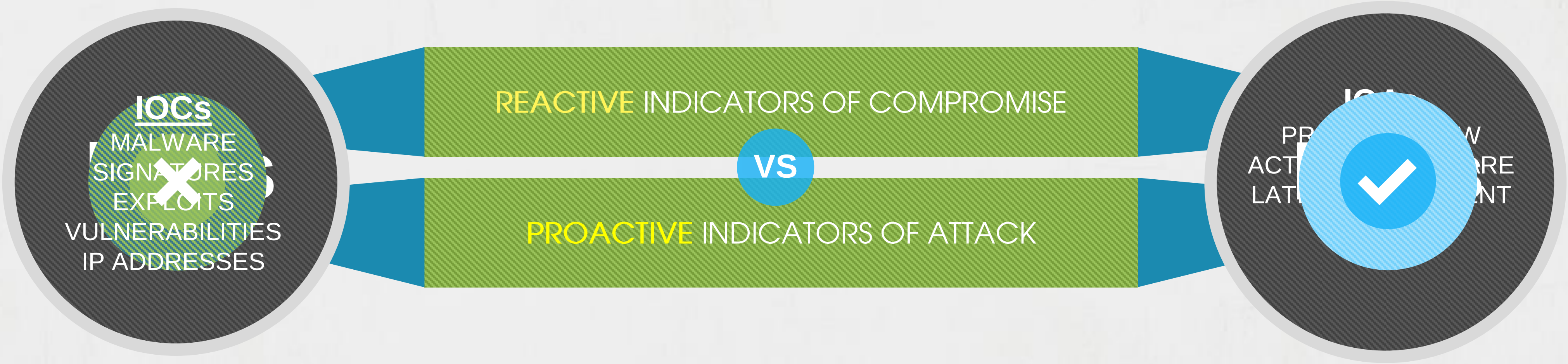
Search for indicators of attack

Begin posturing for remediation on Day 1 of IR

Contain the adversary quickly

INDICATORS OF COMPROMISE ARE JUST THE BEGINNING. WE NEED TO TRACK HUMAN BEHAVIORS AND ATTACK METHODOLOGY AS WELL. **WE NEED TO COMBINE IOC AND IOA METHODOLOGIES TO BE SUCCESSFUL.**

INDICATORS OF ATTACK



TRACKING HUMAN ADVERSARIES REQUIRES NEW WAYS OF DETECTION

We need a shift in detection capabilities from indicators of compromise to **Indicators of Attack**

DEEP PANDA

CASE STUDY

GET TO KNOW THE ADVERSARY

Forces attackers to change behaviors

Not all behaviors change - good intel and pattern analysis can identify the new TTPs

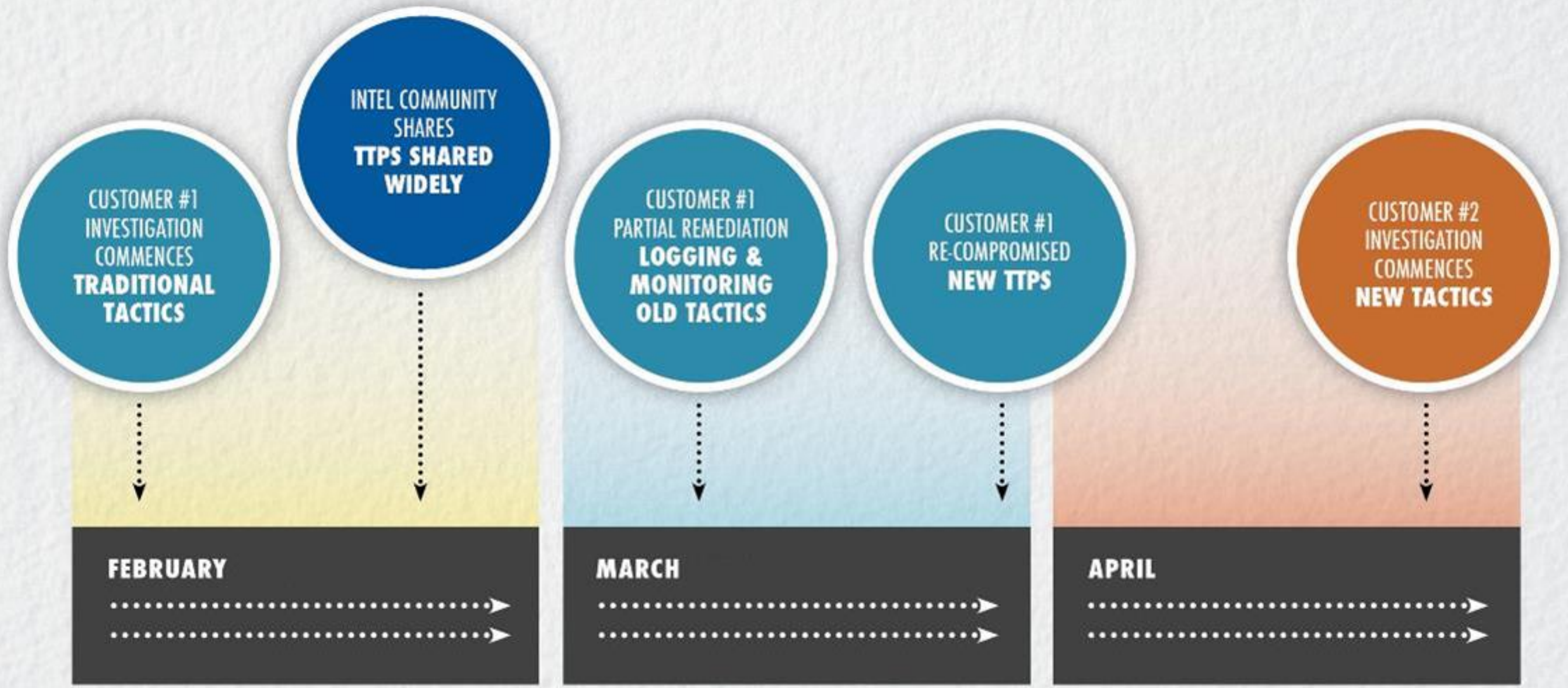
Analysts need the ability to tailor intel and extract relevance via tools and skillsets

Understanding your adversaries helps you gain focus and understand what intel is relevant

CASE STUDY: DEEP PANDA

Attacker TTP	Historic Trends	New Trends
Initial Attack Vector	Spearphish and Vulnerable External Facing Applications (Most Common)	No Significant Changes - Why change if it still works?
Malware - Persistence Mechanism	Installed as Service, Run Key, ect.	No Persistance
Malware - Command & Control	Beacon to malicious IP or Doman	No Standard Beacon Activity
Malware - Functionality	Simple functionality (provide shell or basic upload/download functional-	Memory resident - robust Functionality
Lateral Movement	Net Use, RDP or utilities (PSExec)	WMI, Service Accounts - Evade Logging and blend in
Obfuscation	Time Stamp Standard Times (Windows API)	Time Stamp both Standard and File times (Windows API and MFT)
Data Extraction	Compress data and send to compromized host provider	No Significant Changes

CASE STUDY: DEEP PANDA



CUSTOMER #1 INVESTIGATION COMMENCES **TRADITIONAL TACTICS**

INTEL COMMUNITY SHARES **TTPS SHARED WIDELY**

CUSTOMER #1 PARTIAL REMEDIATION **LOGGING & MONITORING OLD TACTICS**

CUSTOMER #1 RE-COMPROMISED **NEW TTPS**

CUSTOMER #2 INVESTIGATION COMMENCES **NEW TACTICS**

FEBRUARY

MARCH

APRIL

GET TO KNOW THE ADVERSARY

TTPs are now rapidly changing

- Some things must still remain

What are adversaries adjusting to?

- Better intelligence
- Hiding from forensics
- Better analysts
- Better technology

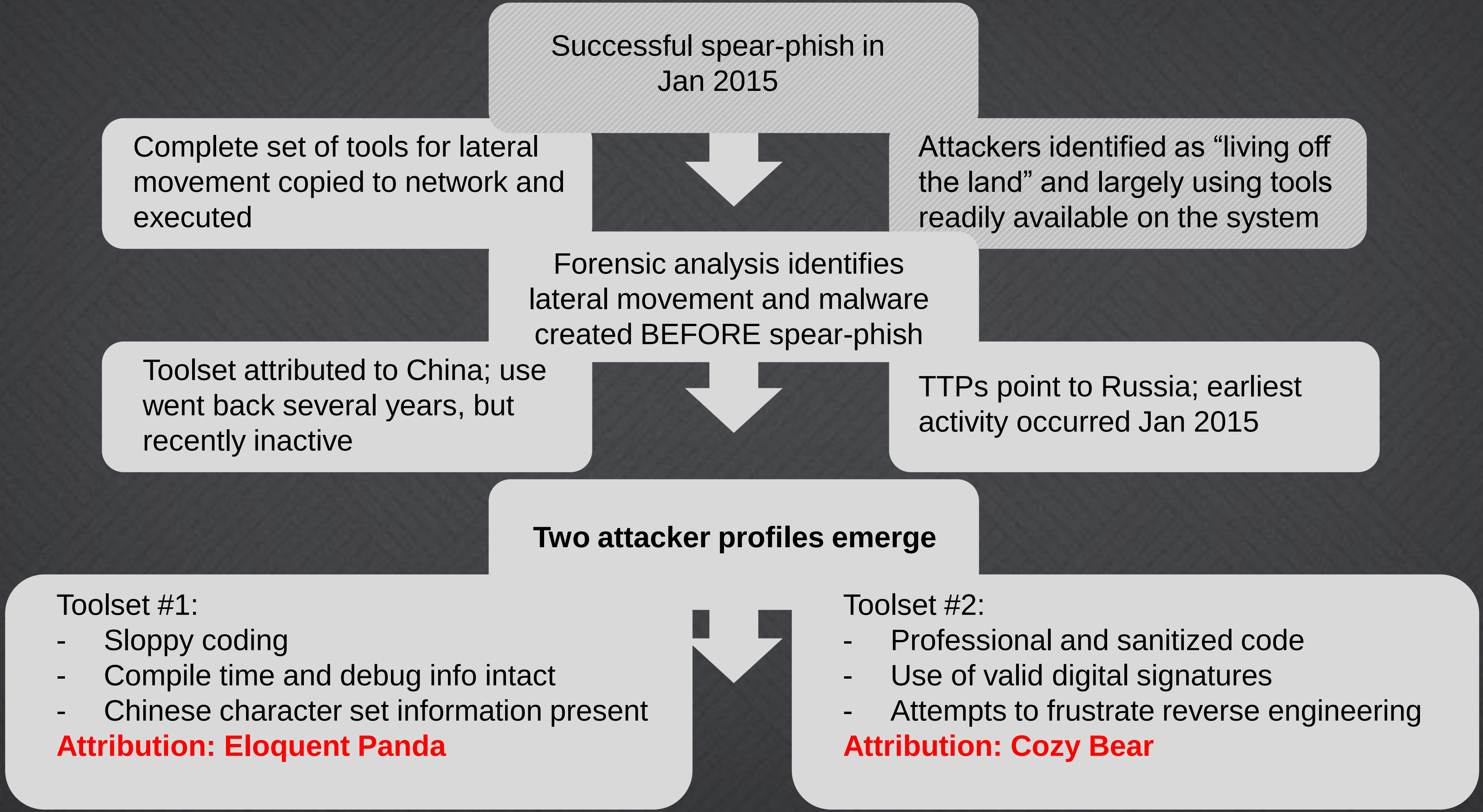
How many adversaries are attacking you?

BEAR VS PANDA

WHY ATTRIBUTION MATTERS

TIMELINE OF EVENTS

CrowdStrike OverWatch Alert at Think Tank



Successful spear-phish in Jan 2015

Complete set of tools for lateral movement copied to network and executed

Attackers identified as “living off the land” and largely using tools readily available on the system

Forensic analysis identifies lateral movement and malware created BEFORE spear-phish

Toolset attributed to China; use went back several years, but recently inactive

TTPs point to Russia; earliest activity occurred Jan 2015

Two attacker profiles emerge

Toolset #1:
- Sloppy coding
- Compile time and debug info intact
- Chinese character set information present

Attribution: Eloquent Panda

Toolset #2:
- Professional and sanitized code
- Use of valid digital signatures
- Attempts to frustrate reverse engineering

Attribution: Cozy Bear

TIMELINE OF EVENTS

Complete set of tools for lateral movement copied to network and executed

Toolset attributed to China; use went back several years, but recently inactive

Toolset #1:
- Sloppy coding
- Compile time and debug info intact
- Chinese character set information present

Attribution: Eloquent Panda

Attackers identified as “living off the land” largely using tools readily available on the system

TTPs point to Russia; earliest activity occurred Jan 2015

Toolset #2:
- Professional and sanitized code
- Use of valid digital signatures
- Attempts to frustrate reverse engineering

Attribution: Cozy Bear

POS Malware “Big Picture“

GET TO KNOW THE ADVERSARY

Multiple Adversaries?

Multiple Locations – Franchise Expansion

Different POS Software and Vendors

Different Support Vendors

Different Concerns on Security

Hunting and Responding

Understand the Environment

Do You Have Access to the Endpoint?

This is not a technical question ;-)

Do You Have Tools to Respond?

This is a technical question

Mergers & Acquisitions

GET TO KNOW THE ADVERSARY

Multiple Adversaries?

- Plans to purchase
- What adversaries would be interested?
- Understand the negotiation plans

Hunting and Responding

- Do you have access in multiple environments?
  - Law firm?
  - Other company?
- Targeted hunting on people key to the M & A
  - …and their assistants

DETERMINING MULTIPLE ADVERSARIES

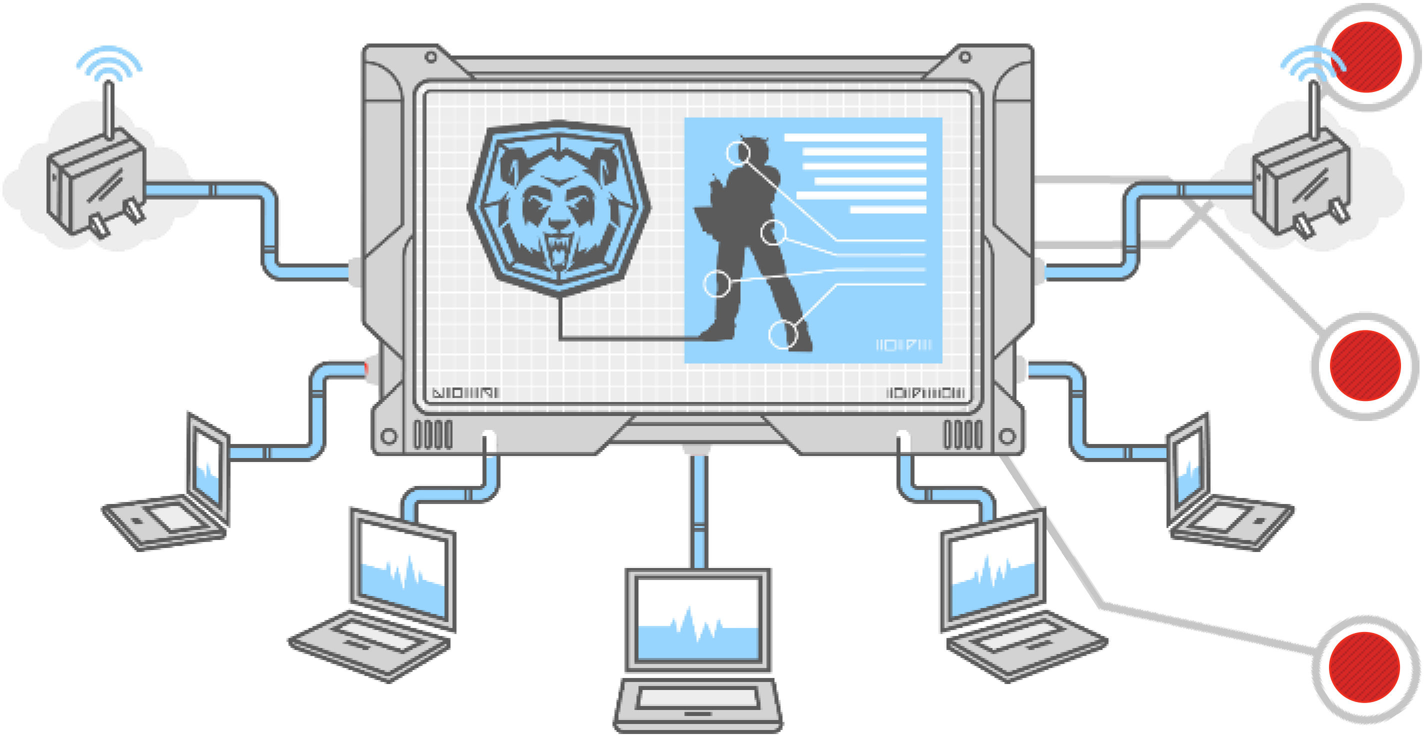
- Why would you care?
  - Understand who is targeting your intellectual property
  - Plan to spend your security budget better
  - Employ more effective containment and mitigation strategies
    - What areas of the kill chain is the adversary targeting?
    - Where is the weakness?
- What would better help you identify?
  - Context of the incident
    - M & A, Franchises, Development Plans
  - Malware tools used
  - Sequencing of commands
  - Known C2 channels

THE SPEED OF CONTAINMENT

- Why?
  - – Intellectual property leaving the building during the attack
  - – What makes you unique is quickly being taken
  - – Containment is not “Remediation”
- How?
  - – Visibility, Visibility, Visibility
  - – Isolate in real time
  - – New technologies allow for this
  - – Look at the IOAs
    - Where in the attack cycle?
- When?
  - – As soon as possible
  - – Before forensics is complete? YES. Are you crazy? No.

THE TAKEAWAYS

Intel-Driven Response



Not every adversary group is created equal. Groups have differing skills, resources, and capabilities.

Do not fit data into your expectations – **Look for anomalies in your findings** focusing on timing, behavior, and tradecraft

The likelihood of being targeted by multiple adversaries is high. In this example, remediation had to include both actors simultaneously!

REMEDIATION PLANNING SHOULD COINCIDE WITH INITIAL INCIDENT RESPONSE

REMEDIATION ACTIONS

- All Adversaries
  - Privileged Account Control
    - Think outside of the box on ways to do this
  - Blacklisting known IOCs?
    - What is the effort vs the reward?
  - Service Accounts
    - Can you reset them?
    - Who has the source code?
    - How long to fix it?

REMEDIATION ACTIONS

- Where is the adversary in the kill chain?
- The earlier in the kill chain, the more options at your disposal.
  - Visibility, Visibility, Visibilty
  - If you can find them at: exploitation, installation, command and control
    - You can stop them quickly
  - If you understand the pattern of the attack you have additional options
    - Anticipate the next move
    - Use the intel you collected

CONTAINMENT ASAP

ACHIEVE VISIBILITY AND ISOLATE THE ADVERSARIES

Q&A