RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: **TECH-T07R**

Network Security and Operations When the Network is Already Compromised

Dr. Eric Cole

Secure Anchor Consulting – Chief Scientist
SANS – Fellow
Twitter: drericcole

If you have not detected an attack/compromise in the last 6 months, it is not because it is not happening – it is because you are not looking in the right areas…

Introduction

- In implementing security the following assumptions must be made:
  - The network is compromised
  - Client systems are compromised
  - 100% security does not exist
- The goals of implementing security are:
  - Control damage
  - Minimize impact
- Which requires timely detection and response

Control the amount of damage

Inbound prevention and outbound detection

Verify all assets with 802.1x

Control applications - application whitelisting

Limit visibility with highly segmented VLANs

Control and monitor configurations with NAC

Prevention is Ideal

But

Detection is a Must

Even though all attacks cannot be prevented you should still try….

Paradigm Shift

- Deliberate/Malicious Insider
- Accidental Insider

- Source of the damage
  - External
- Cause of the damage
  - Internal

Reflection Point

- What percent of your budget are you spending on external threats?
- What percent of your budget are you spending on internal threats?
- What is the exposure of your organization to external threats?
- What is the exposure of your organization to internal threats?

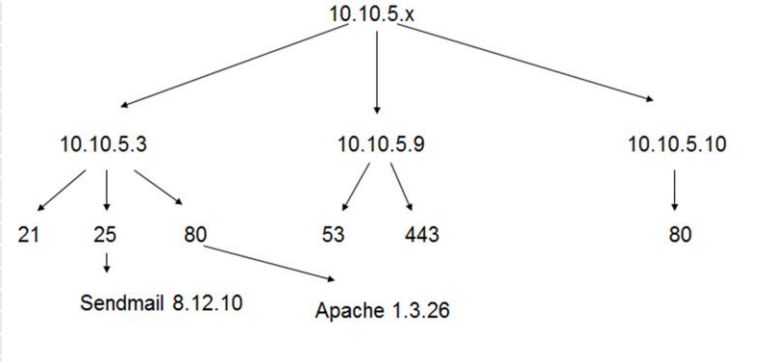
ARE THE NUMBERS ALIGNED?????

You Will Not Win Without a Solid Foundation

- Asset Inventory
- Configuration Management
- Change Control
- Data Discovery

Asset Inventory – You Cannot Protect What You Do Not Know

- Identify your most critical assets
- Trace back what systems they reside on
- Understand all threats and vulnerabilities
- Heavily segment with isolated VLANS
- Determine inbound and outbound data flows
- Setup strict filtering and monitor for anomalies



Assets	Threats	Vulnerabilities

To defend against an adversary you must understand how the adversary operates, so proper defense can be built….

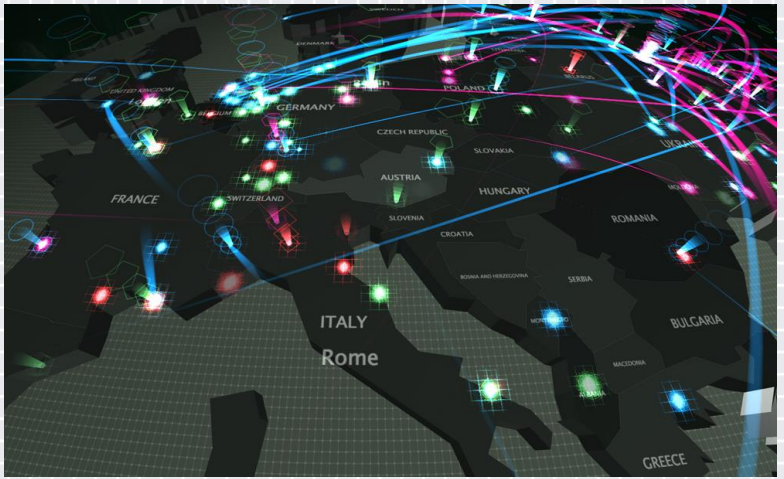
If the offense knows more than the defense you will loose…..

Core Characteristics of Attacks

- Target an individual/system
- Deliver payload to system

- Upload files to the system
- Run processes
- Survive a reboot

- Make outbound connections (beacons to C2)
- Perform internal reconnaissance
- Pivot into the network

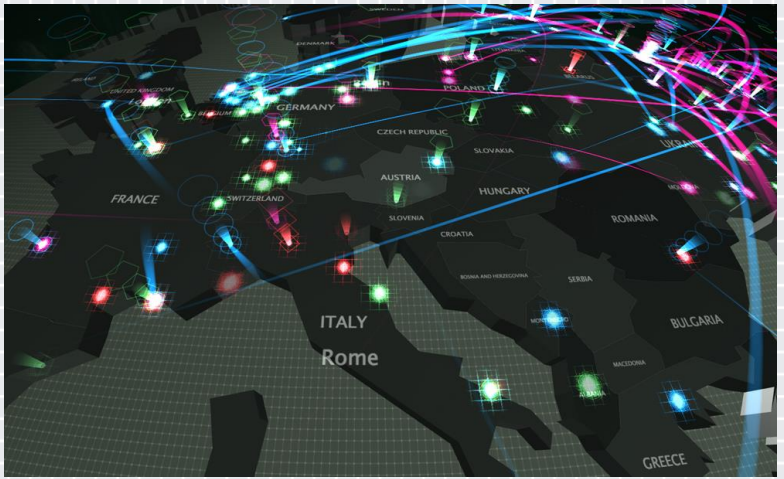


Core Characteristics of Attacks - PREVENTION

- Target an individual/system
- Deliver payload to system

- Upload files to the system
- Run processes
- Survive a reboot

- Make outbound connections (beacons to C2)
- Perform internal reconnaissance
- Pivot into the network

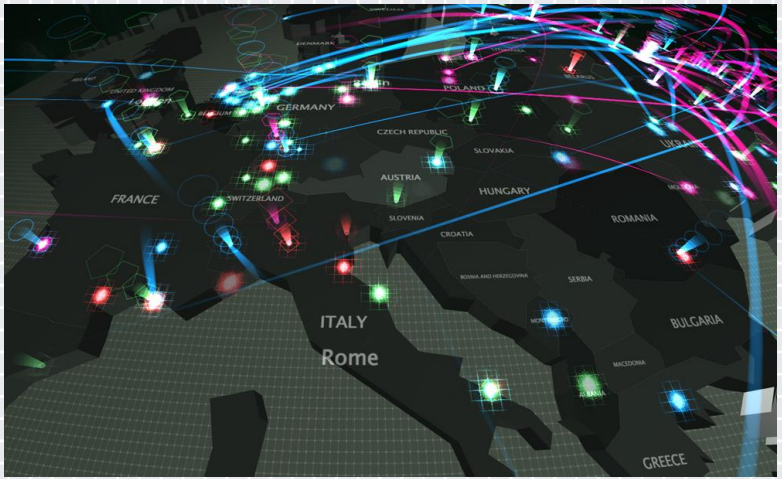


Core Characteristics of Attacks - DETECTION

- Target an individual/system
- Deliver payload to system

- Upload files to the system
- Run processes
- Survive a reboot

- Make outbound connections (beacons to C2)
- Perform internal reconnaissance
- Pivot into the network



Prevent and Control the Damage

- Limit visibility
- Implement principles from 2000 with targeted systems being:
  - Isolated
  - Contain no sensitive data
  - Heavily segmented and firewalled
- Think out of the box
  - Contain dangerous applications
  - Dynamic NAC
  - Crypto free zone
- Block incoming executable content

Timely Detection

Internal activity patterns focused on data:

- Amount of data accessed
- Failed access attempts
- Data copied or sent to external sources

Focus on outbound traffic – The Dr. Cole Challenge

- **Number of connections**
- **Length of the connections**
- **Amount of data**
- Percent that is encrypted
- Destination IP address

Case Study Utilizing NAC for Continuous Monitoring

- Perform high level data classification to segment systems
- Validate which devices can connect to each network utilizing 802.1x
  - Tie to purchasing/acquisitions database to central manage all assets
- Create internal zones within each segment
- Monitor for anomalies with NAC and use to determine level of access

Continuous Monitoring with NAC

OUTBOUND Detection is Key:

1) Length of the connection
2) Number of connection
3) Amount of data

Network Access Levels

Level 5 – Full internal and full external access

Level 4 – Full internal and limited external access

Level 3 – Limited internal and limited external access

Level 2 – Limited internal and no external access

Level 1 – No access

Apply Slide

- If you network is compromised you must control damage and perform timely detection:
  - Network segmentation is key to controlling damage
  - Anomaly detection of outbound traffic will catch compromise
  - Asset identification will allow monitoring of approved devices
  - Data discovery will focus in on key areas
  - Outbound proxies will monitor and control traffic

Apply What You Have Learned Today

- Next week you should:
  - Verify your budget against risk
- In the first three months following this presentation you should:
  - Implement asset management
  - Perform data discovery
- Within six months you should:
  - Re-design your network
  - Take advantage of network segmentation, 802.1x and NAC
  - Control the damage of an adversary