Prevent, Detect, Respond

Dr. Eric Cole


<< SYSTEM FAILURE >>


CYBER
ATTACKS
AHEAD


CYBER
ATTACK
CRIME
INTERNATIONAL
CRIMINAL
THEFT
GROUPS
INFORMATION
COMPUTER
NETWORKS
INTERNET
WARFARE
COMMUNICATIONS
TERRORISM
PORNOGRAPHY
OFFENSIVE
TARGET
ACTIVITIES
UNAUTHORIZED
INDIVIDUALS
SERVICE
DATA
ILLEGAL
CHILD
ALTERING
SYSTEMS
CONTENT
SECURITY
HACKERS
CYBERSPACE
FRAUD
HACKING
DEVICES
CRIMES
MAIL
WEBSITES
NETWORK
ALLEGEDLY
DRUG

Prevention is Ideal

But

Detection is a Must

The METRIC to measure Security

The METRIC to measure Security

Attempted Attacks

The METRIC to measure Security

Attempted Attacks

via

Dropped Packets From the Firewalls

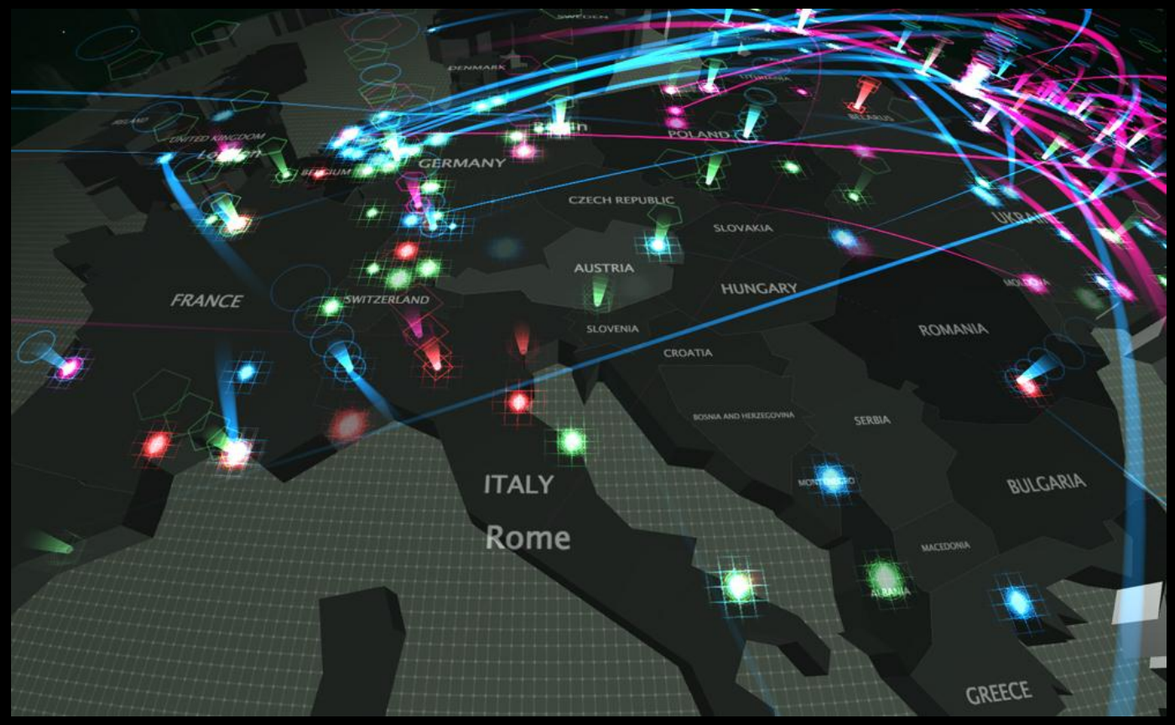
Paradigm Shift

- Deliberate/Malicious Insider
- Accidental Insider

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

Core Characteristics of Attacks

- Target an individual/system
- Deliver payload to system



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

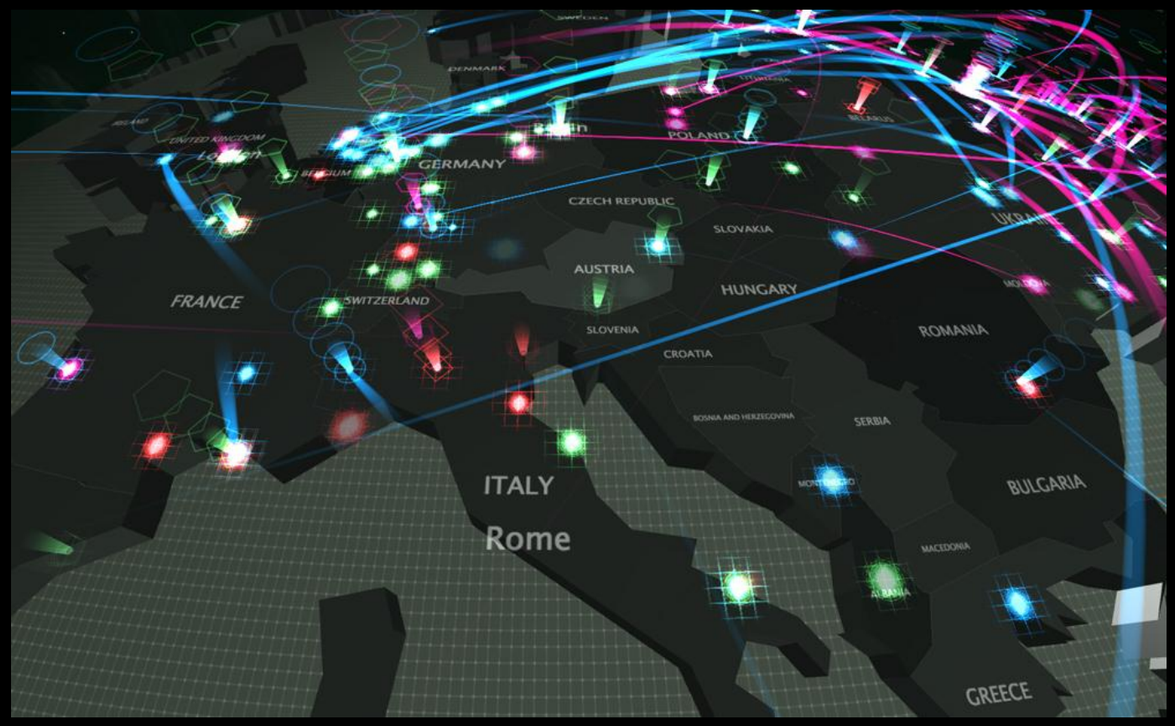
- Make outbound connections (beacons to C2)
- Perform internal reconnaissance
- Pivot into the network

Core Characteristics of Attacks

PREVENTION

- Target an individual/system
- Deliver payload to system

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

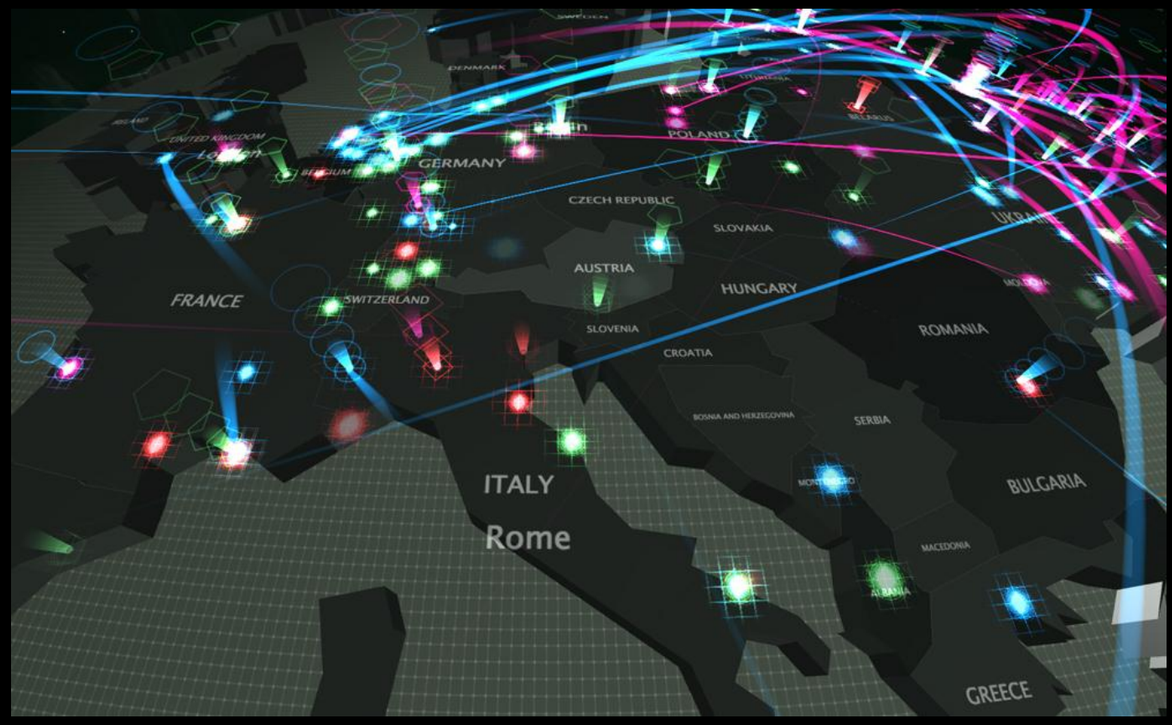


- Make outbound connections (beacons to C2)
- Perform internal reconnaissance
- Pivot into the network

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

PREVENTION

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

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

WHY?

PREVENT – DETECT – RESPONSE

Core to Success:

- Asset Inventory
- Configuration Management
- Change Control

5 Steps to a Secure Future

IDS That Catches Most APT’s

IDS That Catches Most APT’s

F B I

THANK YOU for your time

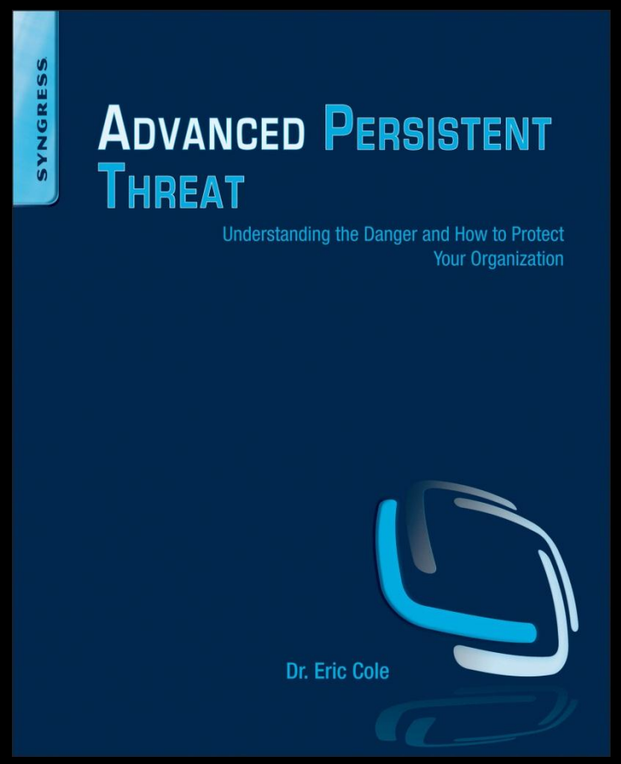
Dr. Eric Cole

Twitter: drericcole

ecole@secureanchor.com

eric@sans.org

www.securityhaven.com



SANS CYBER DEFENSE

SECURE ANCHOR