black hat USA 2018

REAL EYES, REALIZE, REAL LIES

Beating Deception Technologies

Matan Hart

@machosec
matan@cymptom.com

black hat USA 2018

REAL EYES, REALIZE, REAL LIES

Beating Deception Technologies

Matan Hart

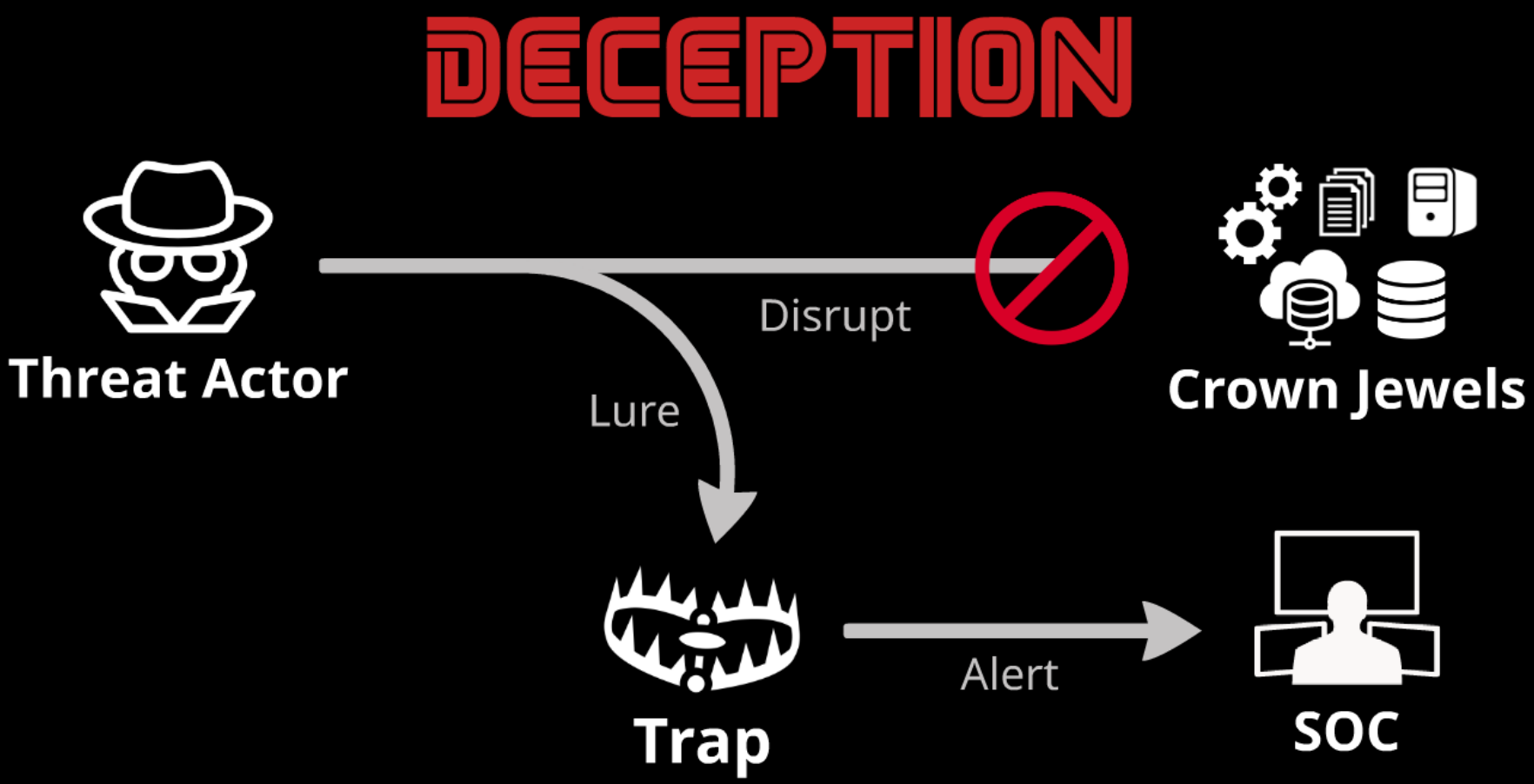
@machosec
matan@cymptom.com

“The greatest deception men suffer is from their own opinions”

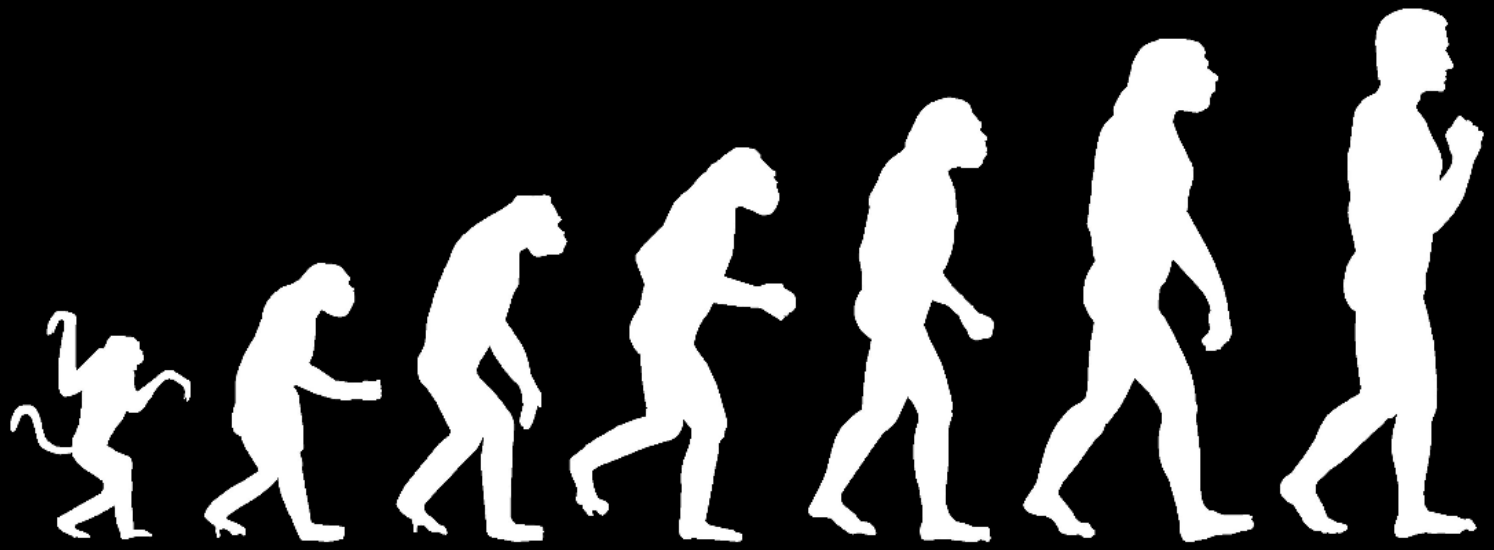
Leonardo da Vinci

WHO AM I

- Co-Founder and CEO @ Cymptom
  - Still at stealth :)
- Speaker
  - Black Hat, BSides
- Addictions
  - Poker, TV shows

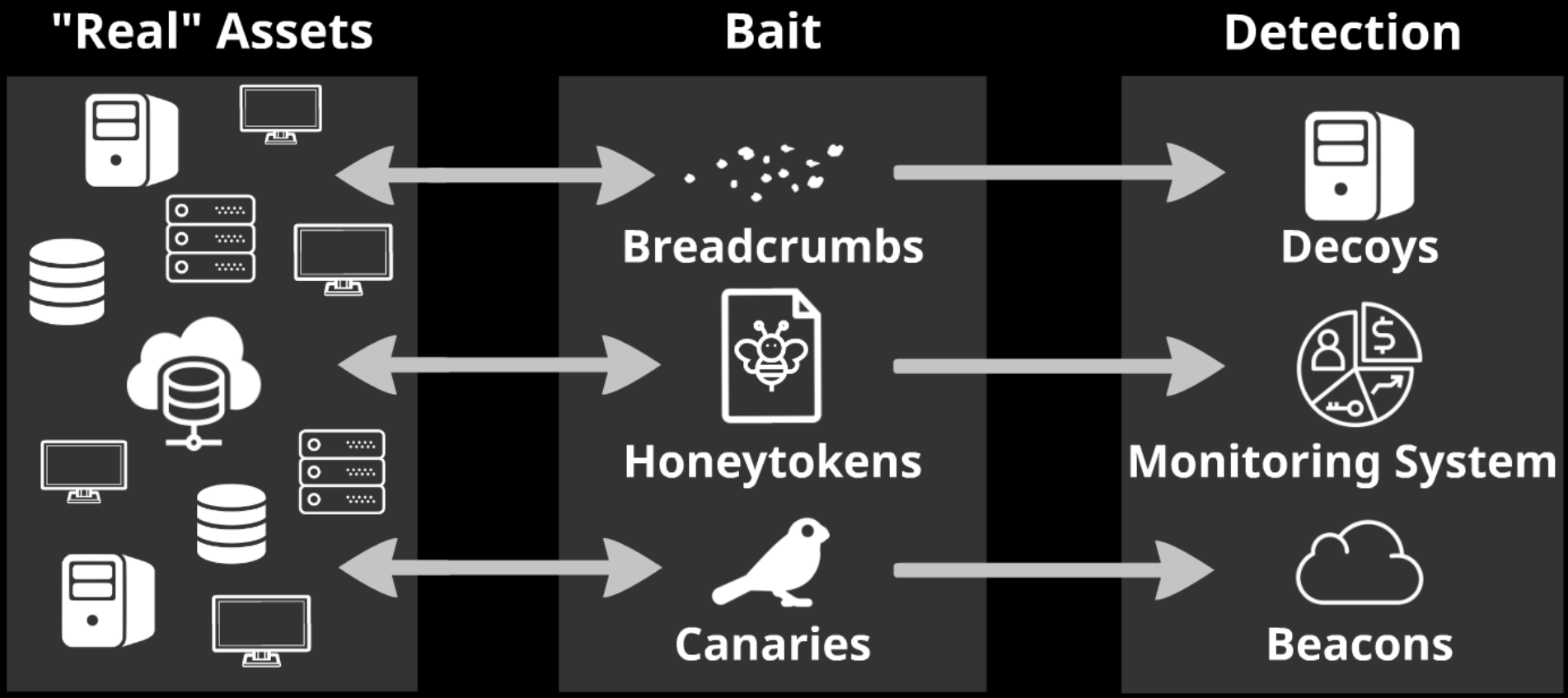

DECEPTION
Threat Actor
Disrupt
Crown Jewels
Lure
Trap
Alert
SOC

EVOLUTION



1993 2018

ARCHITECTURE



EFFECTIVENESS

Confrontation

- Network
- Endpoint
- Credentials
- Application
- Data

Believability

- ARP, DNS and DHCP records
- Active Directory entries
- High interaction services
- OSINT information

Success Rate

TURNING DECEPTION OUTSIDE-IN: TRICKING ATTACKERS WITH OSINT
https://www.willofsheep.com/pages/dc2f4fhyudovich

Confrontation

Network

Endpoint

Credentials

Application

Data

EFFECTIVENESS

Confrontation

- Network
- Endpoint
- Credentials
- Application
- Data

Believability

- ARP, DNS and DHCP records
- Active Directory entries
- High interaction services
- OSINT information

Success Rate

TURNING DECEPTION OUTSIDE-IN: TRICKING ATTACKERS WITH OSINT
https://www.willofsheep.com/pages/dc2f4fhyudovich

Believability

- ARP, DNS and DHCP records
- Active Directory entries
- High interaction services
- OSINT information

TURNING DECEPTION OUTSIDE-IN: TRICKING ATTACKERS WITH OSINT
https://www.wallofsheep.com/pages/dc26#hyudovich

EFFECTIVENESS

Confrontation

- Network
- Endpoint
- Credentials
- Application
- Data

Believability

- ARP, DNS and DHCP records
- Active Directory entries
- High interaction services
- OSINT information

Success Rate

TURNING DECEPTION OUTSIDE-IN: TRICKING ATTACKERS WITH OSINT
https://www.willofsheep.com/pages/dc2f4fhyudovich

COUNTER-DECEPTION

DO NOT COUNT ON:

- Your gut feeling
- Storyline plot holes
- Predictable patterns
- Endpoint isolation

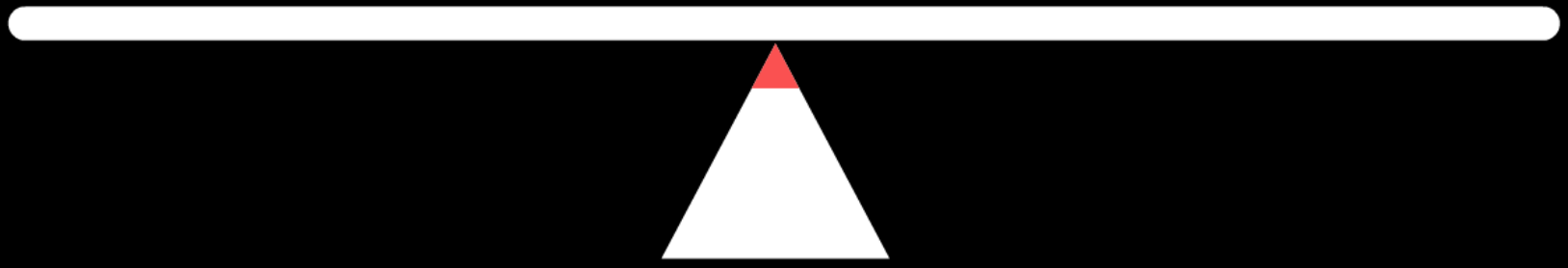
"DON'T PLAY THE ODDS PLAY THE MAN"

Harvey Specter, Suits

ACHILLES' HEEL

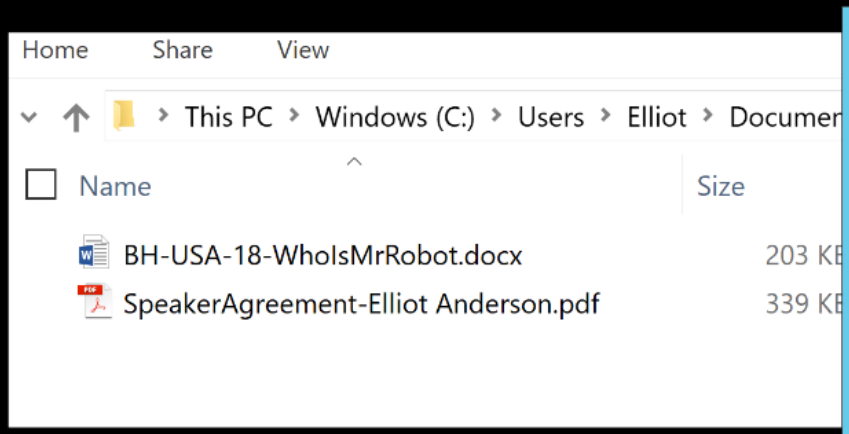
Authenticity

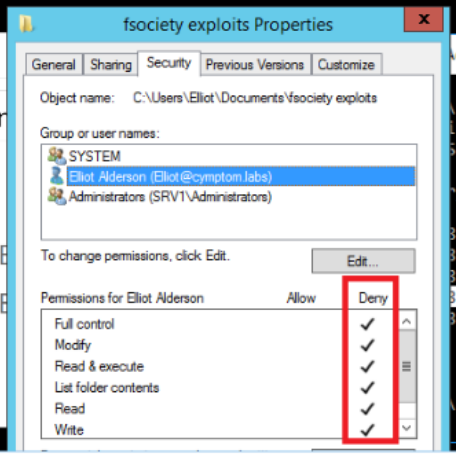
Disruption Risk



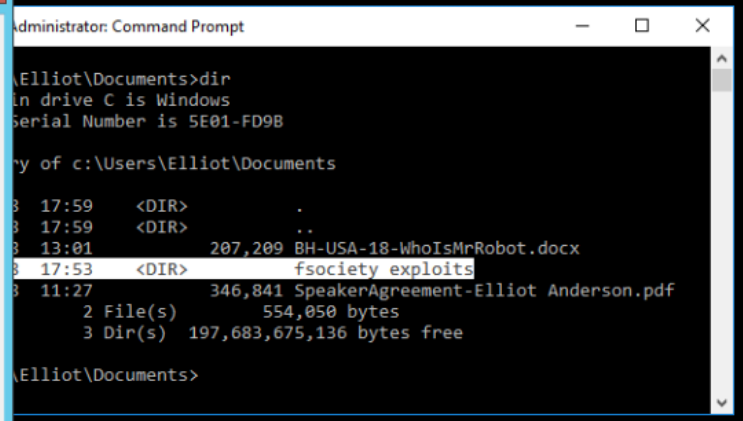
AVOIDING DISRUPTION

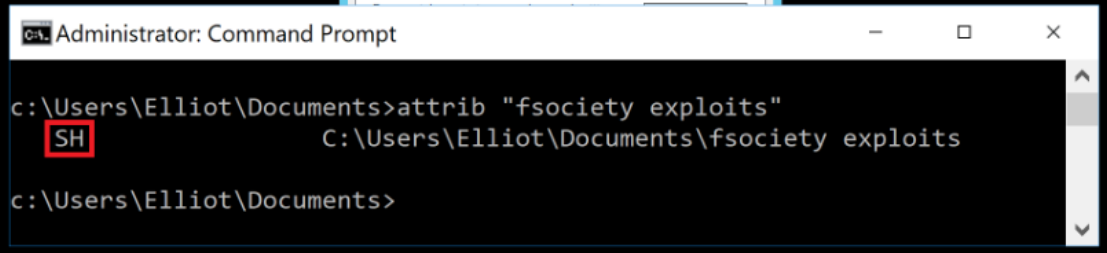
User's view



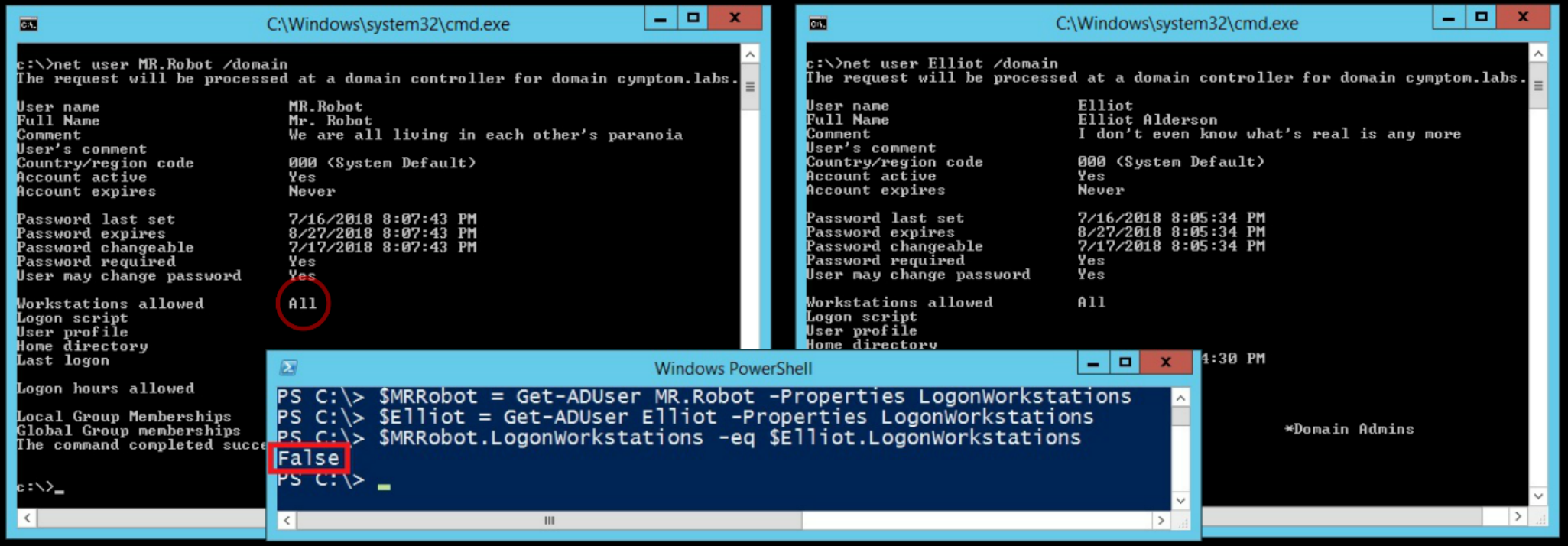


Attacker's view

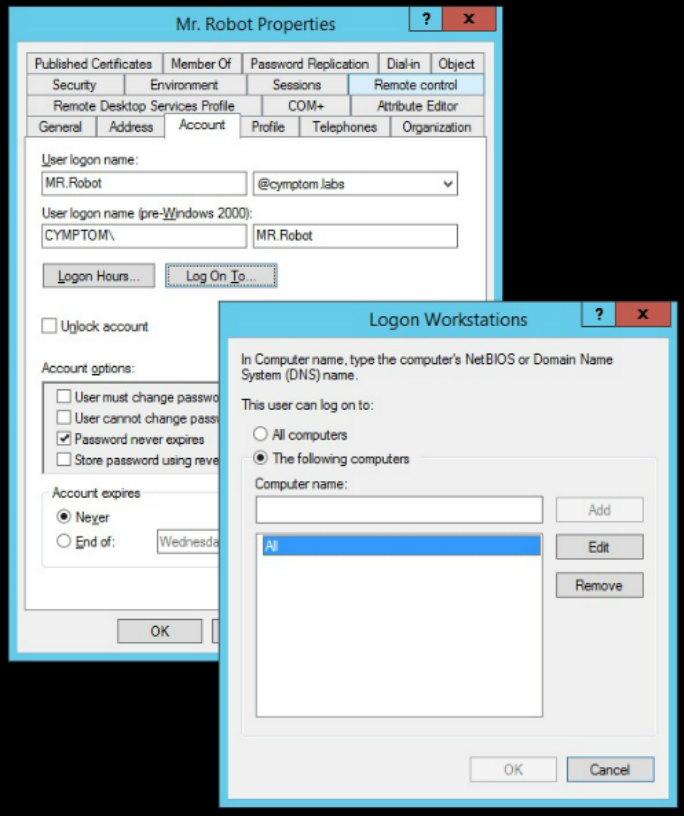


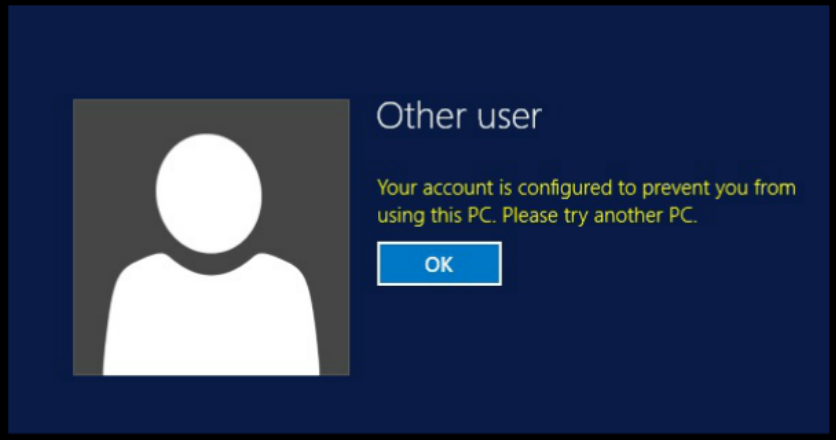


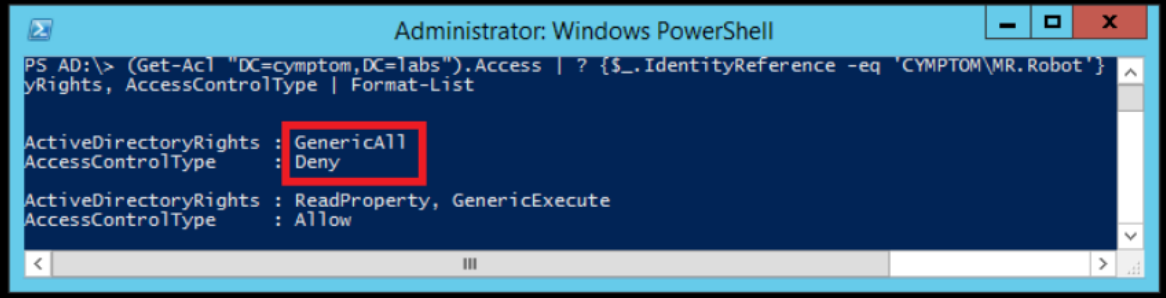
Which one is fake?



MINIMIZING RISK







THE TOOL

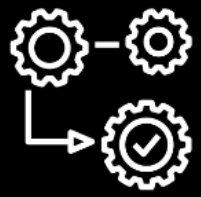
Reveal effective rights

- Users (local/domain)
- Files/Folders
- Emails
- Registry
- Processes
- Active Directory objects
- Shares/Printers

“True success requires sacrifice”

Rick Riordan

SOUND BYTES



Effective deception requires Believability and Diversity

Deception's achilles' heel lies in practical business trade-offs

Beat deception by exploiting disruption and risk precautions

THANKS!

Assume Nothing. Question Everything.

@machosec

matan@cymptom.com

CYMPTOM