



**REAL EYES. REALIZE.  
REAL LIES**

**Beating Deception Technologies**

**Matan Hart**

@machosec  
[matan@cymptom.com](mailto:matan@cymptom.com)





**REAL EYES. REALIZE.  
REAL LIES**

**Beating Deception Technologies**

**Matan Hart**

@machosec  
[matan@cymptom.com](mailto:matan@cymptom.com)



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

*Leonardo da Vinci*

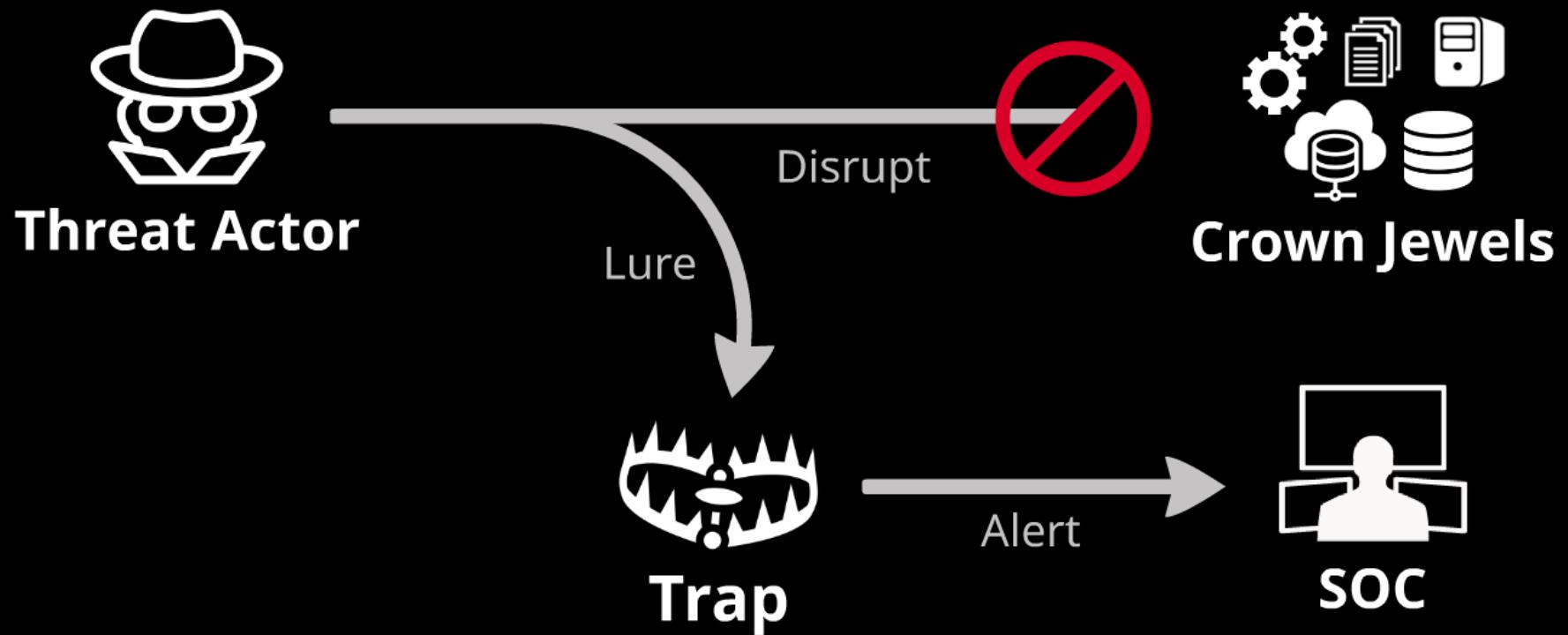


# WHO AM II

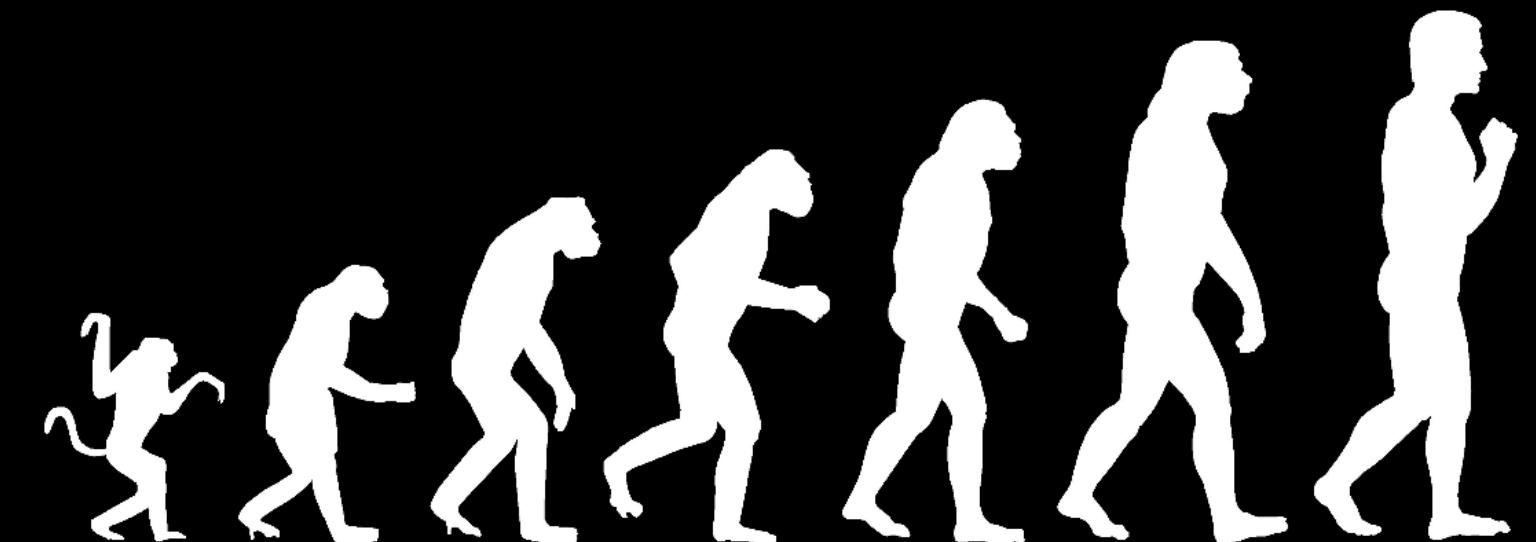
- Co-Founder and CEO @ Cymptom
  - Still at stealth :)
- Speaker
  - Black Hat, BSides
- Addictions
  - Poker, TV shows



# DECEPTION



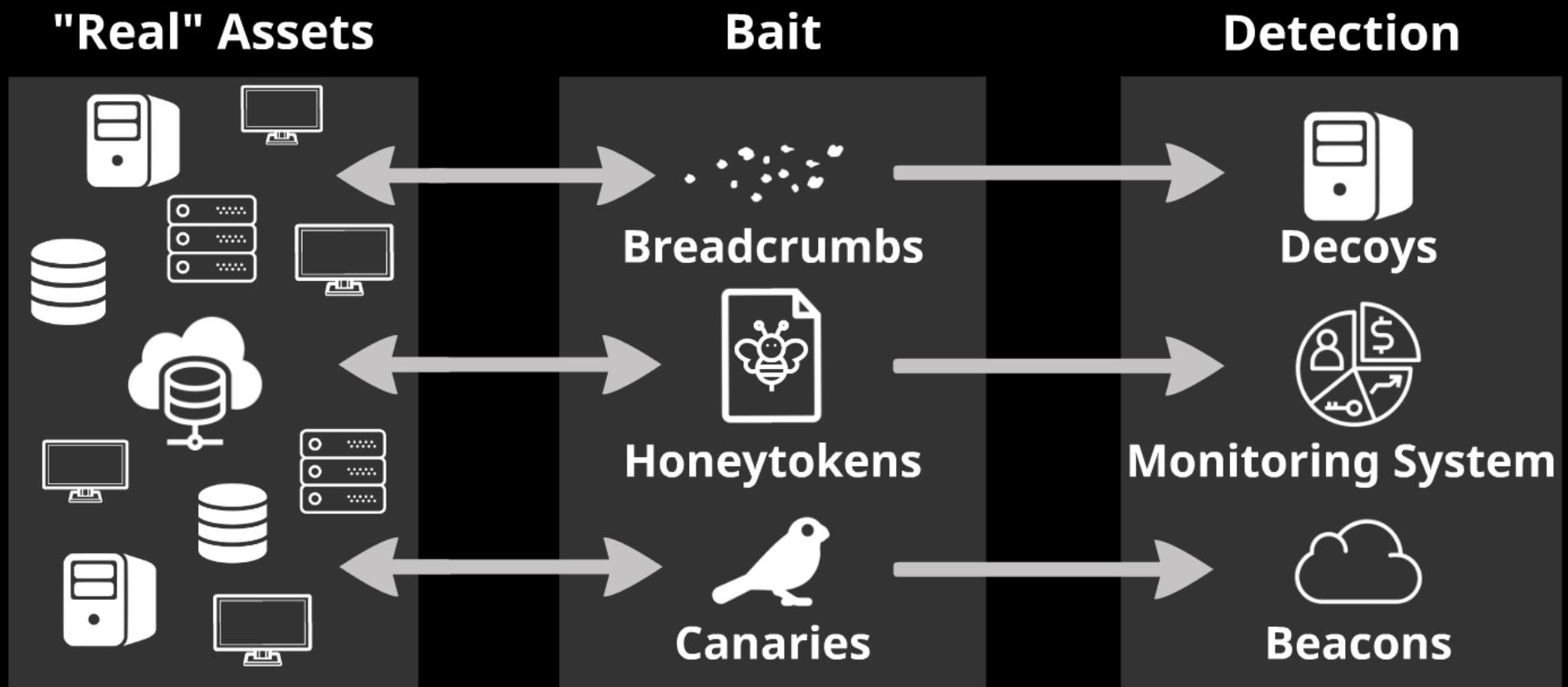
# EVOLUTION



1993

2018

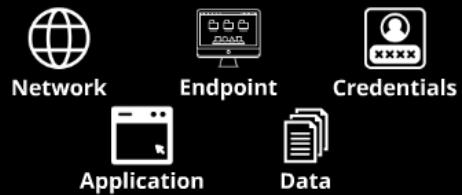
# ARCHITECTURE



# EFFECTIVENESS



## Confrontation



## 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.welbusherp.com/page/0/264#slide0>

# Confrontation



Network



Endpoint



Credentials



Application

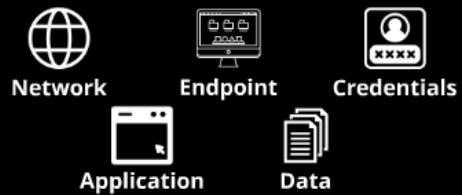


Data

# EFFECTIVENESS



## Confrontation



## Believability

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

TURNING DECEPTION OUTSIDE-IN: TRICKING ATTACKERS WITH OSINT  
<https://www.welbusherp.com/page/0/264#slide0>



## Success Rate

# Believability

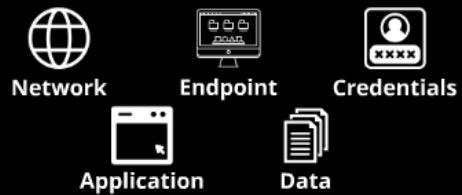
- ≡ ARP, DNS and DHCP records
- ≡ Active Directory entries
- 👉 High interaction services
- 🌐 OSINT information

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

# EFFECTIVENESS



## Confrontation



## 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.welbusherp.com/page/0/264#slide0>

# 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

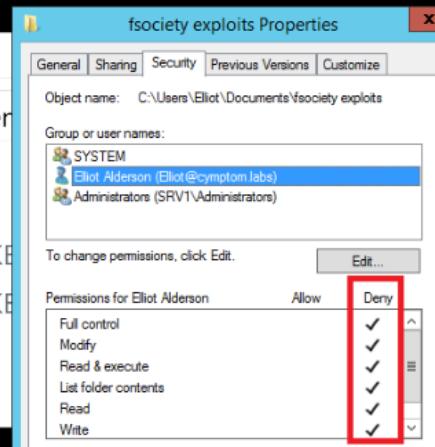
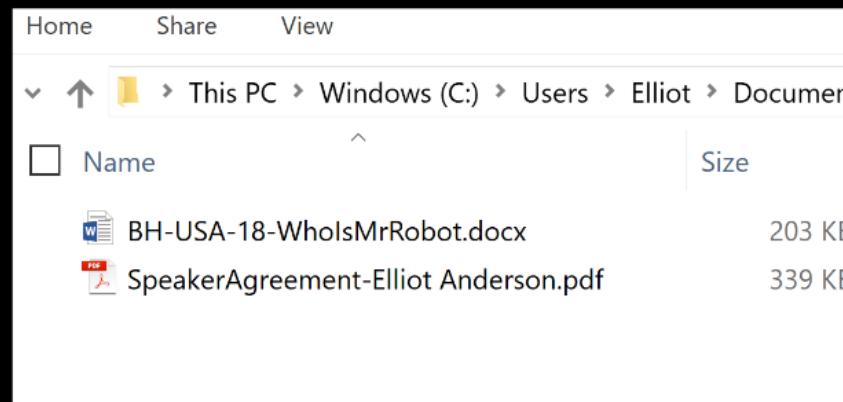


Disruption Risk



# AVOIDING DISRUPTION

## User's view



## Attacker's view

A screenshot of an 'Administrator: Command Prompt' window. It shows a directory listing for 'C:\Users\Elliot\Documents'. The output includes:

```
\Elliot\Documents>dir
In drive C is Windows
Serial Number is 5E01-FD9B

      of c:\Users\Elliot\Documents

3 17:59    <DIR>          .
3 17:59    <DIR>          ..
3 13:01    207,209  BH-USA-18-WhoIsMrRobot.docx
3 17:53    <DIR>          fsociety exploits
3 11:27    346,841  SpeakerAgreement-Elliott Anderson.pdf
      2 File(s)      554,050 bytes
      3 Dir(s)   197,683,675,136 bytes free

\Elliot\Documents>
```

A screenshot of an 'Administrator: Command Prompt' window. The command 'attrib "fsociety exploits" +SH' is run, changing the attributes of the 'fsociety exploits' folder. The output shows the folder path 'c:\Users\Elliot\Documents>'.

```
c:\Users\Elliott\Documents>attrib "fsociety exploits"
SH
C:\Users\Elliott\Documents\fsociety exploits

c:\Users\Elliott\Documents>
```

# Which one is fake?

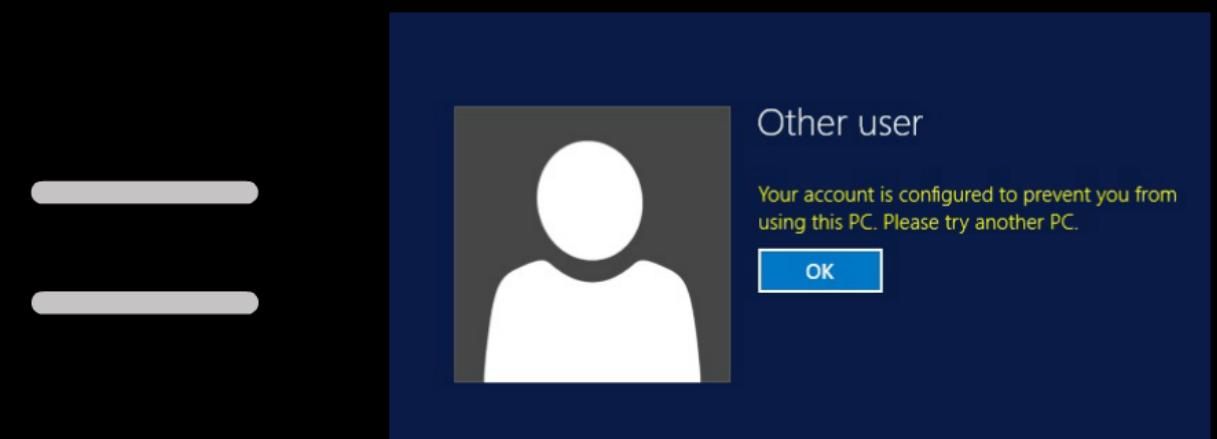
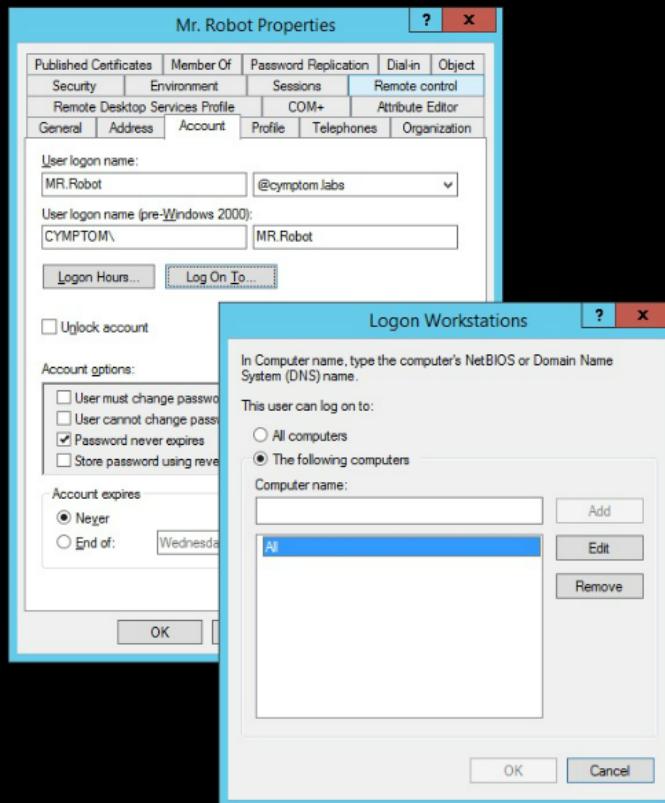
The image displays three windows side-by-side:

- Left Window (CMD):** Shows the output of the command `c:\>net user MR.Robot /domain`. The output includes fields like User name, Full Name, Comment, etc., for the user MR.Robot. The "Workstations allowed" field is set to "All". A red circle highlights this value.
- Middle Window (CMD):** Shows the output of the command `c:\>net user Elliot /domain`. The output includes fields like User name, Full Name, Comment, etc., for the user Elliot. The "Workstations allowed" field is also set to "All".
- Bottom Window (PowerShell):** Shows PowerShell commands to compare the LogonWorkstations properties of the two users. The commands are:

```
PS C:\> $MRRobot = Get-ADUser MR.Robot -Properties LogonWorkstations
PS C:\> $Elliot = Get-ADUser Elliot -Properties LogonWorkstations
PS C:\> $MRRobot.LogonWorkstations -eq $Elliot.LogonWorkstations
```

The output of the final command is `False`, which is highlighted with a red box.

# MINIMIZING RISK



An Administrator: Windows PowerShell window is open, displaying the following command and its output:

```
PS AD:\> (Get-AdC "DC=cymptom,DC=labs").Access | ? {$_.IdentityReference -eq 'CYMPTOM\MR.Robot'} | Select-Object ActiveDirectoryRights, AccessControlType | Format-List
```

The output shows two entries:

- ActiveDirectoryRights : GenericAll  
AccessControlType : Deny
- ActiveDirectoryRights : ReadProperty, GenericExecute  
AccessControlType : Allow

# THE TOOL

Reveal effective rights



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

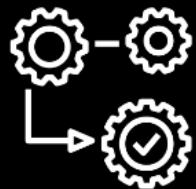


***“True success requires sacrifice”***

*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