Deception for Detection and Automated Response

Greg Irvin | Security Engineer Lead | Dentons
Joseph Salazar | Technical Marketing Engineer | Attivo Networks
**YOUR PRESENTERS**

**Joseph R. Salazar**
- Information Technology since 1995
- Information Security since 1997
- Major (retired, USAR) with 22 years as a Counterintelligence Agent, Military Intelligence Officer, and Cyber-Security Officer
- CISSP, CEH, EnCE

**Greg Irvin**
- 15 years in Information Security
- Active member of the Chicago ECTF and Infragard
- Expertise in Intrusion Prevention and Digital Forensics
- B.A. degree from Indiana University and M.A. degree in Psychology from Governor's State University.
THE CHALLENGE: A LAW FIRM’S PERSPECTIVE
THE CHALLENGE: A LAW FIRM’S PERSPECTIVE

Most awesome Kitten riding a Fire Breathing Unicorn over a rainbow video ever
It is not enough to only think like an attacker, you must also know how to defend and respond.
ANATOMY OF A BREACH

1. Compromise
2. Reconnaissance
3. Lateral Movement
4. Complete Mission

Source: Infosecinstitute.org
ATTACK SEQUENCE AND METHODS

Attackers are Bypassing Prevention and Evading Detection

Advanced Attack Methods:
- HTTPS
- Zero-day
- Stolen employee credentials
- MiTM
- End-point/BYOD
- Phishing

1. Intelligence Gathering
2. Compromise User or Network
3. Compromise Credentials
4. Actions on the Objective
5. Complete Mission

The Target

C&C
A SHIFT TO DETECTION
Attackers Still Get In and Once Inside, Can Remain Undetected for Months

Why breaches are hard to investigate.

• Lack of Accurate Visibility to In-Network Threats
• Too Much Data to Correlate
• Alerts are Not Substantiated or Actionable
• Too Many False Positives/Investigation Complexity
• Limited Resources to Respond

Traditional security tools are not designed to detect threats that are already inside-the-network.
Detect Known Attacks
(Signature Based)

Detect Advanced Threats
(No Signatures)

Detect Known Attacks
(Signature Based)

Efficient: Not Resource Intensive
(Manpower, Money)

No False Positives

Slows Down the Attack

CHOICES IN CLOSING THE DETECTION BLIND SPOT

Deception: Detecting Attackers Better and Detecting Better Attackers

Deception

Hunt Teams

UEBA

SIEM

Network Anomaly Detection

Firewall/IDS/Proxy/AV
## DECEPTION IS NOT JUST A HONEYPOT

<table>
<thead>
<tr>
<th>ITEM</th>
<th>HONEYPOTS</th>
<th>NEXT-GEN DECEPTION PLATFORMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Standalone, AdHoc</td>
<td>Centralized configurations, updates, management, alerting, reporting</td>
</tr>
<tr>
<td>Honeypot OS’s</td>
<td>Emulated</td>
<td>Full Operating Systems, can use customer gold images</td>
</tr>
<tr>
<td>MAC Addresses</td>
<td>Single NIC emulation</td>
<td>Multiple customized MACs to match similar systems in VLAN</td>
</tr>
<tr>
<td>Engagement/Interaction Level</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Service Customization</td>
<td>Labor-Intensive</td>
<td>Easy GUI-enabled</td>
</tr>
<tr>
<td>Sandbox vs. Engagement VM</td>
<td>None</td>
<td>Configurable</td>
</tr>
<tr>
<td>Forensics</td>
<td>Simple artifacts</td>
<td>Full collection of disk, memory, and network activity</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Security Liabilities</td>
<td>Internal pivot point</td>
<td>None, with the proper architecture</td>
</tr>
<tr>
<td>Whitelisting</td>
<td>Complicated</td>
<td>Easy</td>
</tr>
<tr>
<td>Auto-Recovery</td>
<td>Manual rebuilds</td>
<td>Automatic restoration from snapshots</td>
</tr>
<tr>
<td>Scalability</td>
<td>Labor-intensive</td>
<td>Easy ~ 100s of decoys in minutes</td>
</tr>
<tr>
<td>Honey-Token Lures</td>
<td>None</td>
<td>Simple endpoint deployment, comprehensive deception</td>
</tr>
<tr>
<td>3rd Party API Integration</td>
<td>One-off</td>
<td>APIs for blocking, quarantining, analysis, threat hunting, and others</td>
</tr>
<tr>
<td>Detections</td>
<td>Brute Force</td>
<td>All threat vectors</td>
</tr>
<tr>
<td>Primary Deployment Function</td>
<td>Externally for research</td>
<td>Internally for detection</td>
</tr>
</tbody>
</table>
TYPICAL ATTACK PATH SEQUENCE

Once small security gap will present opportunity for attackers
DECEPTION
Obscures the Attack Surface and Disrupts Attackers

Deception to divert attention
- Decoy systems to misdirect attacker
- Disseminate deception credentials to key individuals and locations

Deception Forces the Attacker to Have to Be Right 100% of the Time

The entire network becomes a trap and a hall of mirrors.
Deception is not expected, so now defenders have the element of surprise in their favor.

Deception is advanced detection, designed for the attacker who is working around traditional countermeasures.

Effective deception can evade attacker detection, making it harder for the attacker to realize he is being deceived.

The attacker can’t tell that the decoy data they access is not real.
DECEPTION FOR EARLY DETECTION THROUGHOUT ATTACK PHASES

Confuse and Misdirect to Make the Attacker’s job harder

OBSCURING YOUR INFRASTRUCTURE

Before Deception

Production Servers

With Deception

Production Servers

Decoy Multiple Servers

What Attacker Sees With Deception

Production Servers
CHANGING THE GAME WITH DECEPTION AND DECOYS

Deception Obscures the Attack Surface and Disrupts Attacks

Deception to divert attention
Decoys to misdirect attacker
Authentic full VM’s running golden images
ENTERPRISE NETWORK

Adding in Deception

Data Center

User VLAN 3

User VLAN 4

SCADA Network VLAN 5

Network Deception Server

Deceptions
- Operating System
- Network Services
- Data and Document

Cloud Deception Server

Deception
- Makes Network a Trap
- Authentic Decoys
- End-Point lures
- Engagement-based
- No Signature Reliance
ENTERPRISE NETWORK

Adding in End-point Deception

- Network Deception Server
- Cloud Deception Server

Data Center

- User VLAN 3
- User VLAN 4
- SCADA Network VLAN 5

Deceptions
- Operating System
- Network Services
- Data and Document

Deception
- Makes Network a Trap
- Authentic Decoys
- End-Point lures
- Engagement-based
- No Signature Reliance
ENTERPRISE NETWORK

Deception for Real-Time Detection

- Operating System
- Network Services
- Data and Document

- Makes Network a Trap
- Authentic Decoys
- End-Point lures
- Engagement-based
- No Signature Reliance
PROVEN DECEPTION USE CASES
Early and Accurate Detection, Visibility, Accelerated Incident Response

1. Early and Accurate Detection
   - In-network Lateral Movement
   - Stolen Credential & Man-in-the-Middle Attacks
   - Insider, 3rd Party, Acquisition Integration
   - Ransomware
   - Specialized Environments Detection IOT (medical devices), POS, SCADA
   - Cloud and Data Center Security

2. Visibility and Streamlining Incident Response
   - Exposed Credential & Attack Path Assessment
   - Automation of Attack Analysis
   - Evidence-based alerts & Incident Response Automations
MYTHS AND REALITIES OF DECEPTION

- **It is Easy to Detect**
  - False: Real OS/Golden Images, dynamic deception, Active Directory integration match production assets; Pen Testers consistently deceived.

- **It is Resource Intensive**
  - False: Alerts are engagement based and automated attack analysis simplifies incident handling and response.

- **It is Hard to Operate and Not Scalable**
  - Depends: Non-inline designs are Friction-less to deploy and provide Cloud and Data Center Scalability; End-point deployment depends on approach.

- **It Creates a Dirty Network**
  - Depends: Understand how decoys are deployed; see what tools they provide to whitelist and not interfere with other tools.

- **No Incremental Value**
  - False: Achieves early detection at the end-point and in-network. DDP’s also provide the automations and integrations for simplified response.

- **There is Legal Risk**
  - False: Unless counter hacking, deception is viewed in line with typical security defense controls, and does not conflict with EU privacy laws.
DECEPTION TECHNOLOGY

Evaluation Criteria

- Types of Deception Technology
- Environments
- Authenticity
- Ease of Deployment and Operations
- Attack Analysis
- Forensic Reporting
- Threat Vulnerability Assessment
- Response Automation

Early In-Network Threat Detection (All Attack Vectors)

Accelerate Incident Handling

Visibility and Incident Response
FIRSTHAND EXPERIENCES WITH DECEPTION

- Wild Wild West Law Firms
- Curious insider
- Malicious Insider
- Combination & Acquisitions
- Usability vs. Security
- Intra-network visibility
FIRSTHAND EXPERIENCES WITH DECEPTION

- Deployment across multiple network segments
  - User VLANS
    - Wired computers
    - Wireless computers
    - Virtual computers
  - Server VLANS
    - Windows servers
    - Linux servers

- Interesting files as bait
  - Administrator_passwords.xlsx
  - Missing Clinton emails.pst
  - 2017 Financials.xlsx
  - Network_diagram20170501.vsd
  - Incriminating photos folder - 1.jpg, 2.jpg, 3.jpg
QUESTIONS?
THANK YOU