Implementer's Guide to Deception Technologies

Today's Speaker

- Kyle Dickinson – SANS Analyst, Author, Instructor

Today's Agenda

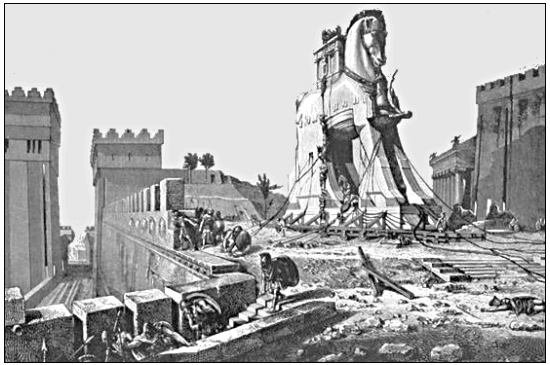
- A history of deception
- Benefits of deception technology
- Attack prevention
- Implementing deception technology
- Open source vs. commercial solutions

Deception in History

- First United States Army Group
  - Created to deceive enemy about location of allied invasion in France
  - Created decoy tanks, airplanes and ships, documents, radio traffic
  - Forced enemy to focus on wider-spread areas

Deception in Greek Mythology

- The Trojan horse
  - The Greeks constructed a giant wooden horse and hid a force of men inside.
  - The Trojans pulled the horse into the gated city.
  - At night, the Greeks crept out and opened the gates for other Greek forces.



How Can Deception Technology Help?

- Reduces false positives—alerts on interaction vs. pattern matching
- Creates more “fruitful” targets to increase likelihood of attacker interaction
- Decoys won’t contain critical data—affords more ability to observe attack

Deception Technologies 101

- Token-based deception
  - Using “bait files,” keys, certificates
- Appliance-based deception
  - Small appliances to emulate various systems
- Enterprise-level deception
  - Heavily integrated into environment
  - Emulates full infrastructure with enhanced visibility

Detection and Response

Detection

- Placing sufficient quantity of decoys increases attacker interaction
- Creation of target-rich decoys
- Higher fidelity alerts

Response

- Increased efficiency with higher fidelity alerts
- Observability for threat collection

Attack Prevention

- Decoy: Production ratio increases attack surface—as a benefit
- Density of decoys
- Emulation of “crown jewels” increases likelihood of attacks against faux environment

Know Thy Enemy

- Collect information about:
  - Attacker's behavior
  - Techniques
  - Tools
- Provides security teams opportunity to disrupt future attacks by creating new controls and alerting

Network Assets

- Attackers attempt to learn the landscape:
  - Ping sweeps
  - Port scans
  - Vulnerability scans
- Target identification

Active Directory

- Leveraged by most organizations
- Contains users, computers and groups for organization
- Attacks include:
  - LDAP reconnaissance
  - Local admin mapping
  - NTDS.dit extraction
  - Stealing passwords from memory

Account and Credential Hijacking

Analyst Program

- When attacker has credentials, detections may not be as efficient
- Discovery of username/ password
- Cloud service provider access keys
- Passwords stored in plain text

Phishing

- Effective attack vector for attackers:
  - Targeting phishing campaigns (spearphishing)
  - Credential harvesters
    - Spoofing O365, popular in 2019
  - Social media spoofs
- Attackers are transforming phishing attacks to circumvent spam filters.

Deception Technology Implementation

Analyst Program

- When implementing deception technologies, organizations should consider:
  - Effectiveness of current security controls and processes
  - Desired outcomes
  - What solution(s) will work best?
  - How many decoys will be deployed?
  - Build/buy?

“Bait Files”

- Leveraging “bait files” can be an early detection for ransomware, as well as insider threat.
- When ransomware is executed and begins to encrypt files. Should the ransomware begin encrypting bait files, trigger an alert for the incident response team to react.
- Using bait files for insider threat detection can also be a practice: “Employee Salaries.xlsx”

Honeypots

Low interaction	A small VM or appliance with a port listener, and typically nothing else
Medium interaction	Emulated service such as a database or web server
High interaction	Fully operational production infrastructure and emulated enterprise network

Active Directory Decoy

- Mimics a production Active Directory environment
- Faux users/groups
- Faux servers/domain
- Generate additional decoys to have attack possibly follow the rabbit hole further

Account/Credential Decoys

- Creating resources that are (1) easily discoverable, and (2) easier to crack
- Allow security teams to monitor the usage of these specific accounts/credentials
- Common use cases for account/credential decoys can include:
  - Cloud service provider access keys
  - Usernames
  - Passwords
  - passwd files

Phishing Decoys

- Increase visibility on phishing attempts
- Placing e-mail addresses in location common to open source intelligence
- Decoy mailboxes should have limited interaction—which can create higher fidelity alerting

Open Source Tools

Advantages

- Lower start-up costs
- Ability to deploy extremely small, focused, targeted solutions
- Flexibility and customization
- Ability to leverage operational budget

Disadvantages

- Hidden initial and ongoing operational costs associated with learning, deploying and managing the solution
- Lack of dedicated customer support systems
- No service level agreements (SLAs)
- Risk of open source project being discontinued
- Difficulty in migrating to a commercial solution

Commercial Tools

Advantages

- Comprehensive solution for all networked environments
- Well-developed documentation and customer service
- Defined SLAs
- Ease of configuration and deployment
- Automation through built-in third-party integrations

Disadvantages

- Higher start-up costs
- Some lack of flexibility

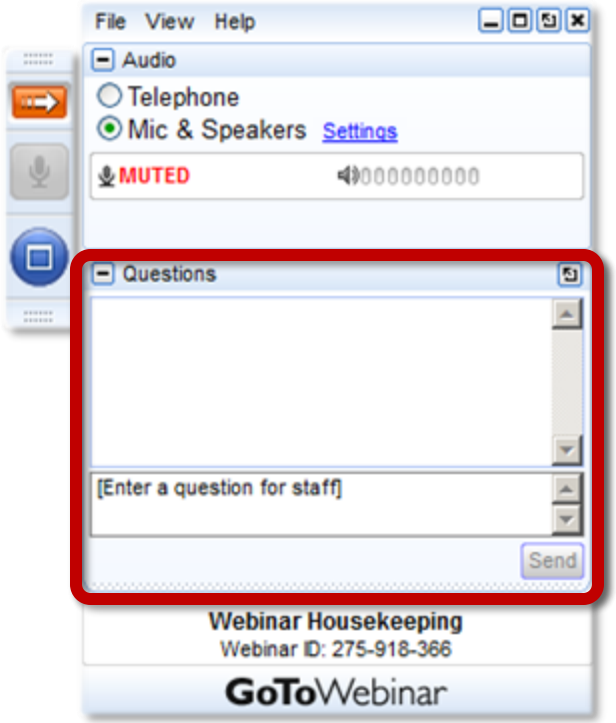
Key Points

- Deception technologies having measurable success
- Various “decoys” for several use cases
- Decoy: Production system ratio

Q&A

Please use **GoTo**Webinar's Questions tool to submit questions to our panel.

Send to "Organizers" and tell us if it's for a specific panelist.



Acknowledgments

Thanks to our sponsors:

And to our attendees, thank you for joining us today!