Artifice:
Leveraging MDE's deception capabilities

whoami

Dylan Tenebruso

- Dad & Husband
- @dylaninfosec - blogger @ attackthesoc.com
- 10 years in IT - 5 in IT Security - Senior IT Security Spc.
- Identity & Access Management | Detection Engineering and Threat Hunting
- AzSecOps repo - https://github.com/AttacktheSOC/Azure-SecOps
- Collector of hobbies - Death Metal enthusiast

What is deception in the context of IT Security?

Deception in IT security refers to the strategic deployment of techniques within an environment to detect, mislead, and ultimately manipulate malicious actors. It aims to elicit specific responses from attackers by wasting their time with red herrings, deterring them from proceeding with attacks, or exposing their presence through interactions with carefully placed decoy assets designed to mimic legitimate environment objects.

A (very)brief history of deception in IT

HoneyPots

Conceptualized in 1989 by Clifford Stoll and first documented use was in 1991 by Bill Cheswick (Bell Labs)

1989/91

2003

HoneyToke n

Term first coined in 2003 by Augusto Paes de Barros

Categorize d

Gartner identifies “Deception” as an emerging category

2015

Present

GA

Deception tech is readily available to all and anyone can deploy it

Prerequisites

Subscription

- Office 365 E5
- Microsoft Security E5
- Defender for Endpoint P2

System Reqs

- Windows 10 1809 and up
- PowerShell is enabled
- Automated investigation and response enabled
- MDE as primary EDR

Permissions

- Global Admin
- Security Admin
- Manage portal system settings (XDR RBAC)

Enable Deception

XDR Portal > Settings > Endpoints > Advanced Features > Deception capabilities

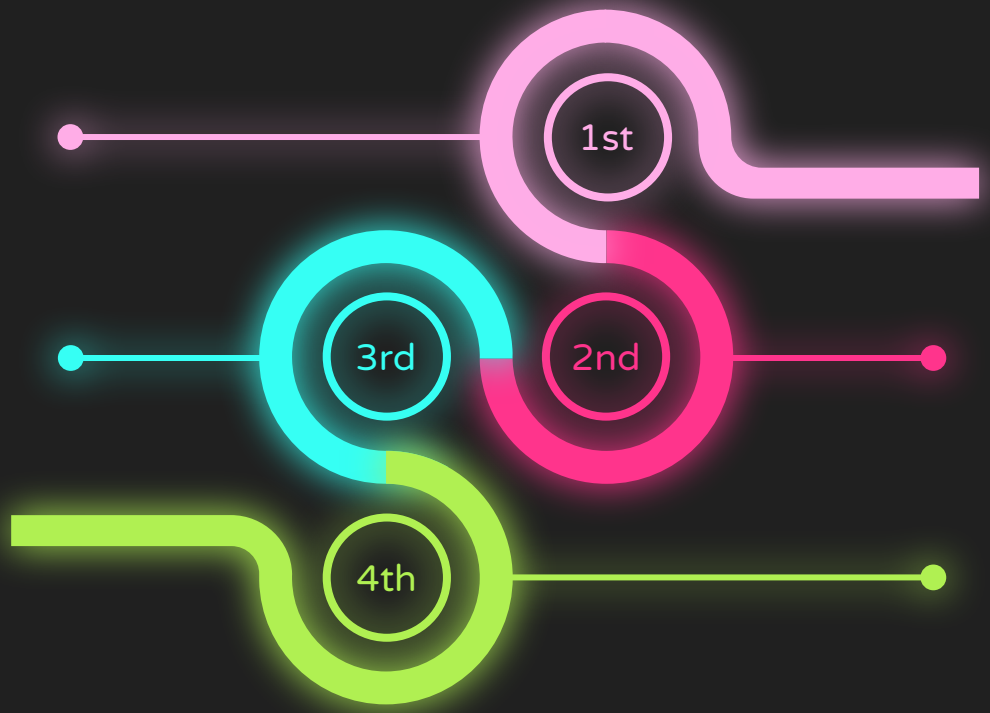
Crafting the trap

Review past breaches

What was the TAs path? What systems did they touch? What was their goal?

Decoy & Lure Strategy

If they stand out too much, you risk raising suspicion. However, a recent study showed that the knowledge of their presence may be enough to deter TAs.



Diversify your rules

Target different Device Tags with different rules

Stack your deception

Leverage CanaryTokens to create highly specific and customized rules

Provide a name and choose lure types

Rule name *

Finance-Dept

Description *

Deception rules targeting finance

Lure types

- [x] Basic
  Plant documents, link files, and other files containing decoy information that attackers might utilize.
- [ ] Advanced
  Plant cached user credentials and inject responses to Active Directory queries with decoy information that attackers might utilize.

Next

Manage decoy acco

Decoys are nonexistent accoun
attacker activity will generate al

Add new | Edit

Alias or Host name

ats-7hd8jw3746fh.attackthes
ats-bdyQXv7eUvtt.attackthes
ats-dc.attackthesoc.com

Edit decoy host ats-dc.attackthesoc.com

Host name *

ats-dc.attackthesoc.com

Plant lures to *

- ( ) Default IP address
- (•) Custom IP address
  Provide a static IP address to lead attackers to an existin
  connections to this IP address will trigger an alert.

IP address *

192.168.12.45

Define rule scope

Choose the devices where you'd like to plant lures.

Deception is currently applied only to Windows client devices.

Plant lures to *

- ( ) All Windows client devices
- (•) Devices with specific tags

Choose device tags

Select up to 100 tags

Lures

- ( ) Use autogenerated lures
  Generated by the system
- (•) Use custom lures only
  Use lures created by you

Add new lure | Edit

Lure name

Back | Next

Add new lure

Add and edit custom lures such as documents, config files and link files. These lures will automatically be planted on devices in your organization.

Upload file Maximum file size is 10 MB

Lure name *

Select a file to populate this field

Planting path *

{HOME}\Documents\Employee Reporting\

You can use {HOME} as the active user's home folder, which must be at the beginning if used, or a regular Window path. Network paths are not supported.

- [x] Plant on all devices in scope
- [x] Plant as hidden

Save | Cancel

Rules for the rules

10 Deception rules

Decoys and Lures deploy to Win10/11

Advanced rules include LSASS and LDAP decoys

Use auto-generated lures <u>or</u> custom

Custom lures <= 10MB and no .exe or .dll

Export of deployed rules

Rule Name	Device Id	Device Name	Decoy Type	Decoy	Lure Type	Decoy Entity Path	Deployment Status	Comments
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Fake Host	ats-6te7lksi833g.attackthesoc.com	Basic	<redacted>	Deployed	
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Fake Credentials	htsugumo	Advanced	LSASS	Deployed	
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Fake Credentials	htsugumo	Advanced	LDAP	Deployed	
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Fake Credentials	rzaadmin	Advanced	LDAP	Deployed	
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Fake Credentials	dylanbackup	Advanced	LDAP	Deployed	
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Fake Credentials	jsupport	Advanced	LDAP	Deployed	
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Fake Credentials	atsadmin	Advanced	LDAP	Deployed	
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Custom lure		Basic	<redacted>	Failed	Device communication error
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Fake Host	atsdc03.attackthesoc.com	Basic	<redacted>	Failed	Device communication error
[TEST] Custom Lure	33009	AtS-2309283hdk1f	Fake Credentials	mchijiwa	Basic	<redacted>	Deployed	

Laws of MDE Deception Detection

MDE Onboarded

Detections come from decoys used on any MDE onboarded device

User Decoy, no pwd required

User decoys will alert via any use of the username, correct password not required

Generated Lures don’t alert

Auto-generated lures don’t trigger alerts, custom lures can*

Connection attempt to a deceptive host on one endpoint

Manage incident ···

High | Active | Unassigned | Lateral Movement | Deception | dylan-testing

Attack story | Alerts (2) | Assets (2) | Investigations (0) | Evidence and Response (4) | Summary

Alerts

View story item details

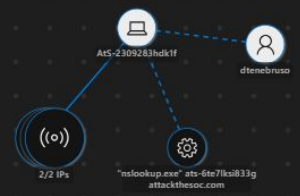
Play attack story | Unpin all | Show all

Jan 09, 2025 1:08 PM · New
Connection attempt to a deceptive host
AtS-2309283hdk1f · dtenebruso

Jan 09, 2025 1:02 PM · New
Connection attempt to a deceptive host
AtS-2309283hdk1f · dtenebruso

Incident graph

Layout | Group similar nodes



— Communication ····· Association

Connection attempt to a deceptive host

M

DNS query using a deceptive hostname Deception

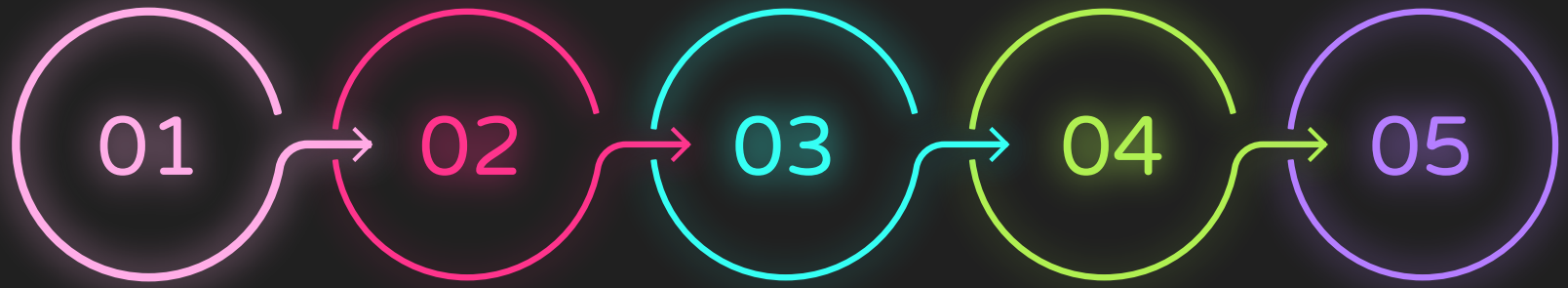
Connection attempt to a deceptive host ···

Network Conn

What other devices have they touched? What was their path to here?

Persistence

Do they have persistence?



Host/Acct

Who hit the decoy and from which host?
How did they login to the device?

Processes

What other processes ran or file events took place around the time of triggering?

Exfil

Have they staged anything for exfil?

Hey everyone!
here are some links to some of the resources, social media posts and other references mentioned in the talk.

Microsoft ----------
Microsoft Defender Deception rules Overview: https://learn.microsoft.com/en-us/defender-xdr/deception-overview
Configuration Guide: https://learn.microsoft.com/en-us/defender-xdr/configure-deception
Nov '23 MDE What's New announcing Deception (Preview):
https://learn.microsoft.com/en-us/defender-xdr/whats-new#november-2023
MS Virtual Ninja training with Heike Ritter & Dean Pickering on Deception:
https://learn.microsoft.com/en-us/shows/microsoft-sentinel-defender-xdr-virtual-ninja-training/microsoft-defender-for-endpoint-deception

Personal ----------
AttacktheSOC blog: https://attackthesoc.com/
Stack your Deception article: https://attackthesoc.com/posts/stacking-your-deception/

Social Media ----------
Twitter post by Spencer Alessi (@techspence) asking the community for their definition of Deception in Cybersecurity:
https://twitter.com/techspence/status/1877410511681118272

YouTube video - DEF CON 32 - Counter Deception: Defending Yourself in a World Full of Lies - Tom Cross, Greg Conti:
https://www.youtube.com/watch?v=gHqDEMrqTjE&pp=ygUSZGVmY29uMzIgZGVjZXB0aW9u

Twitter post from Haroon Meer (@haroonmeer) showcasing a study performed to identify the cognitive and psychological effects deception tools can have on threat actors: https://twitter.com/haroonmeer/status/1878452009143075318
The study: https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/6c188375-03f6-4d66-afee-296308c9f2c0/content