

# High fidelity detection with honeypots

Don't search for your adversary, let them come to you

Andrew Muller, Ionize

TLNOG2 21st November 2025

# Introduction

- We are constantly trying to detect malicious activity. Living off the land techniques make this very difficult.
- So why look for adversaries when they can come to you?
- Honeypots are not new. Now called "deception technology" because honeypots didn't sound cool enough.
- This talk will explore cheap and easy ways to get started.

# Cyber adversaries

Adversary type	Motivation	Target
Cybercriminals (Organised Crime)	Financial Gain	Anyone
Nation-State Actors (APT Groups)	Espionage, Political Advantage, Sabotage, Military/Strategic Advantage	Government, government contractors, critical infrastructure, high-tech research
Hacktivists	Protest	Government, controversial organisations
Malicious Insider	Revenge, Financial Gain, or Intellectual Property	Current employer
Competitors	Intellectual Property	Competitors

# Honeypots

## Not new

- First mentioned in 1980's
- The HoneyNet Project (1999)
- Evolution in broader deception technologies
- Lots of options
  - Server, network honeypots
  - Low interaction, high interaction
  - Honeytokens



# Honeypot Strategies

What are you worried about?

- Focus on your most valuable assets
- Focus on who wants them and most likely to get them
- Build honeypot to attract them





# Cybercriminals

## What are you worried about?

- Will briefly look around network then cryptolocker it
- Honeypots unlikely to help



# Nation-State Actors

## What are you worried about?

- Will look have detailed look at network
- Common honeypots will be identified
- Honeytokens best and easy option
- Create a SECRET or CONFIDENTIAL folder and alert when its accessed



# Hacktivists

## What are you worried about?

- Will have detailed look at network
- Common honeypots won't be identified
- Honeytokens best and easy option
- Create a SECRET or CONFIDENTIAL folder and alert when its accessed

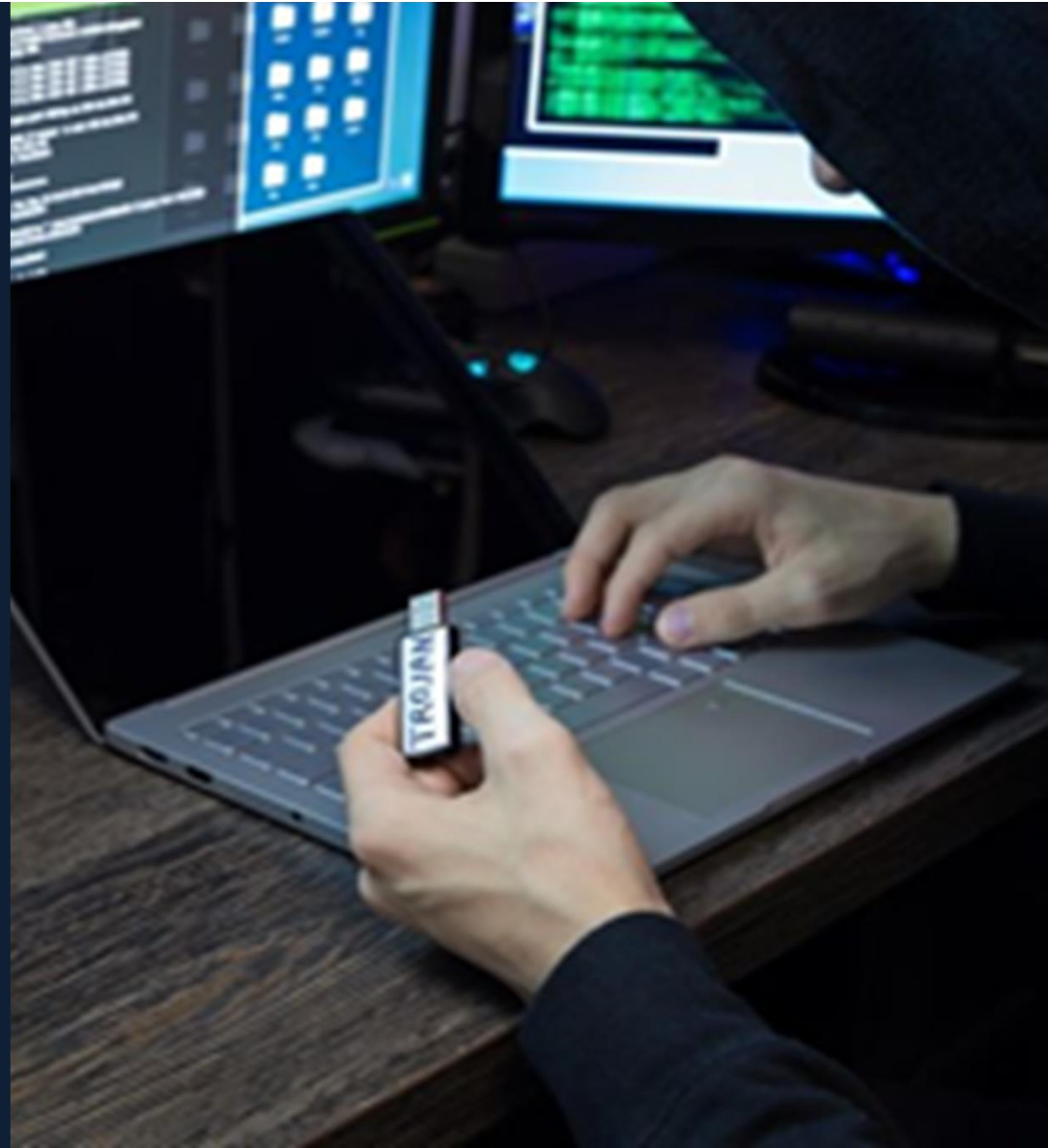




# Malicious Insider

## What are you worried about?

- Will have detailed look at network
- Common honeypots won't be identified
- Honeytokens best and easy option
- Create a SECRET or CONFIDENTIAL folder and alert when its accessed



# Competitors

## What are you worried about?

- Will have detailed look at network
- Common honeypots won't be identified
- Honeytokens best and easy option
- Create a SECRET or CONFIDENTIAL folder and alert when its accessed



# How?

## Keep it simple

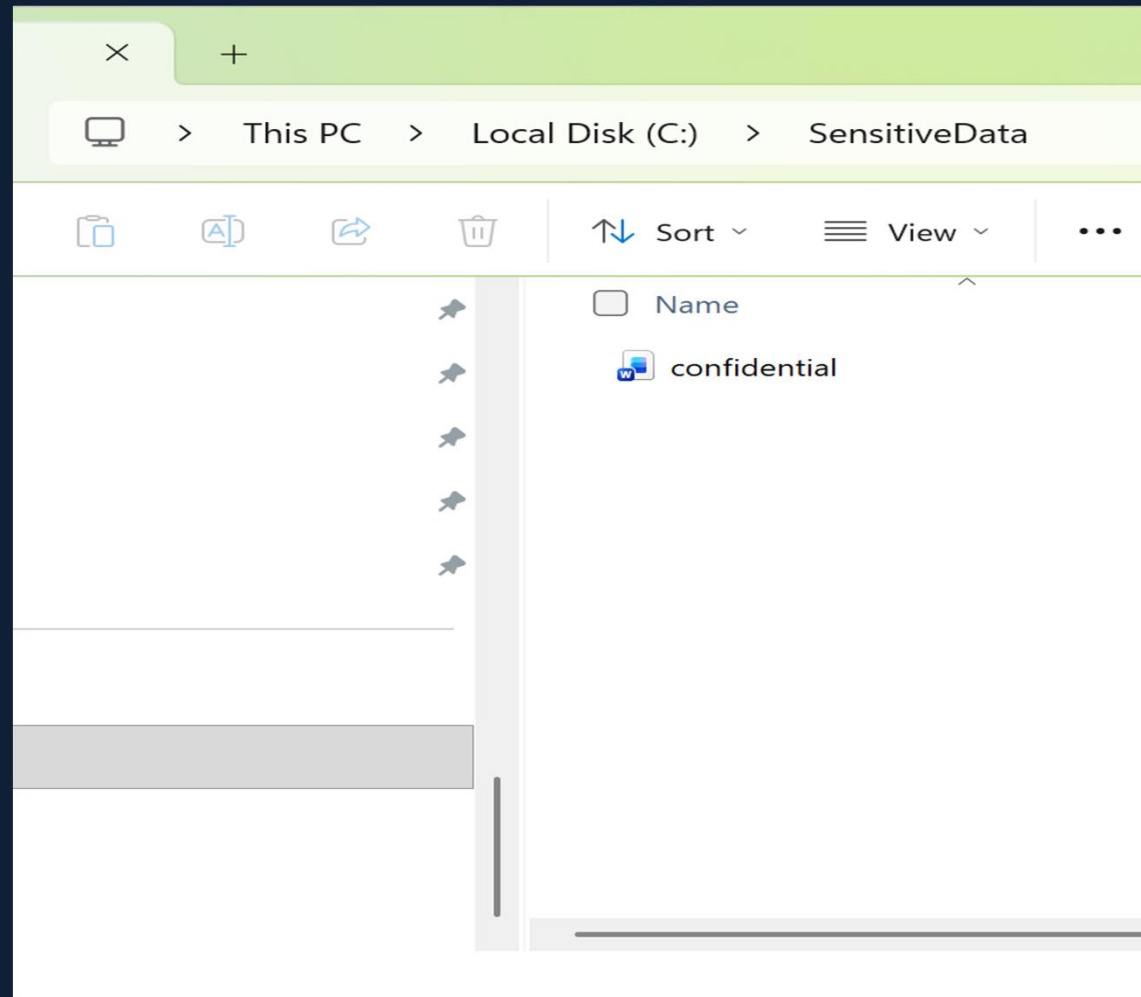
- Set a trap with something desirable
- Use a honeypot
- Create a folder or file labeled SECRET or CONFIDENTIAL and fire an alert when its accessed



# Example

## Create a honeypot

- Create a SECRET or CONFIDENTIAL folder





# Example

## Create an alert

- Create an alert when its accessed

```
• let targetFile = @"C:\SensitiveData\confidential.docx";  
• DeviceFileEvents  
• | where Timestamp > ago(7d) // Search last 7 days  
• | where ActionType == "FileAccessed" // Only file access events  
• | where FileName == "confidential.docx"  
•     or FolderPath =~ targetFile  
• | project Timestamp, DeviceName, InitiatingProcessAccountName,  
  FolderPath, FileName, InitiatingProcessFileName, ReportId  
• | order by Timestamp desc  
•
```



Copilot

New query\* X | New query\* X | New query

< Run query Last 30 days Save

Query

```
1 EmailEvents  
2 | take 1000
```

Getting started Results Query history

Export 142 items Search

Filters: Add filter

<input type="checkbox"/>	TimeGenerated	Timestamp
<input type="checkbox"/>	> Apr 9, 2024 5:37:5...	Apr 9, 2024 5:37:54 AM
<input type="checkbox"/>	> Apr 11, 2024 2:13:...	Apr 11, 2024 2:13:21 P
<input type="checkbox"/>	> Apr 9, 2024 5:37:5...	Apr 9, 2024 5:37:57 AM
<input type="checkbox"/>	> Apr 11, 2024 2:13:...	Apr 11, 2024 2:13:17 P
<input type="checkbox"/>	> Apr 11, 2024 2:13:...	Apr 11, 2024 2:13:18 P
<input type="checkbox"/>	> Apr 11, 2024 2:13:...	Apr 11, 2024 2:13:24 P
<input type="checkbox"/>	> Apr 11, 2024 2:13:...	Apr 11, 2024 2:13:23 P

# Example

## Setup alert

- Setup up a KQL alert to trigger when its accessed.

The screenshot displays the 'Detection Rules' management interface. At the top, there is a search bar with the text 'Ara'. Below the search bar, a table lists various detection rules. The 'demo' rule is selected, indicated by a blue checkmark in the first column. To the right of the table, a sidebar provides details for the selected 'demo' rule, including its alert title, category, and applied actions.

<input type="checkbox"/>	Detection rule name	Alert title	Severity	Created on
<input checked="" type="checkbox"/>	demo	demo	High	7 Kas 2022 15:0
<input type="checkbox"/>	Fairu test	Fairu test	Medium	20 Oca 2023 12
<input type="checkbox"/>	CW: Persistence: Scheduled task cre...	CW: Persistence: Scheduled task cre...	Informational	26 Oca 2023 11
<input type="checkbox"/>	CW:DE.AE.1 Suspicious Activiy: New...	CW:DE.AE.1 Suspicious Activiy: N...	Informational	28 Mar 2023 12
<input type="checkbox"/>	CW:DE.CM.1: Malware: Redline Stea...	CW:DE.CM.1: Malware: Redline S...	Low	28 Mar 2023 00
<input type="checkbox"/>	CW:DE.CM.7: Suspicious Activity: To...	CW:DE.CM.7: Suspicious Activity:...	Informational	31 Mar 2023 11
<input type="checkbox"/>	CW:DE.CM.1: Vidar Stealer Detected	CW:DE.CM.1: Vidar Stealer Detec...	High	27 Mar 2023 05
<input type="checkbox"/>	TEST1: Başarısız Giriş Denemesi (Ne...	TEST1: Başarısız Giriş Denemesi (...)	Medium	14 Nis 2023 14

**demo**

Open detection

**Detection details**

Alert title  
demo

**Category**  
Collection

**Applied Actions**  
Isolate device  
Run antivirus scan  
Initiate investigation  
Quarantine file

**Execution details**

Last run  
4 Şub 2024 14:37:

**Thank  
you.**

