



# Leveraging the ATT&CK Framework for

## Deception-based Active Cyber Defense



# Raj Gopalakrishna

- **Co-founder, Acalvio Technologies Inc**
- **Most of my 30+ years experience in Cybersecurity and R&D**
- **Previously**
  - **SVP & Distinguished Engineer @ CA Technologies (Broadcom)**
  - **Chief Architect, Head of R&D @ Arcot Systems Inc**
  - **Lived and worked in USA for 2 decades**
- **20+ Patents**



# Touch Points

## ➤ Introduction

➤ **Deception Technology**, Active Cyber Defense (ACD)

## ➤ Strategy for leveraging Deception Technology

➤ For precise and early Detections

## ➤ Combining Deception Tech and ATT&CK Framework

## ➤ Examples:

- Identity Threat detection
- Ransomware Detection
- Tactic & Technique detection



# Active Cyber Defense

## Traditional Security

- What the attacker did?
- Observations /Telemetry based



***Log, Anomaly & behavior analytics  
require visibility for detection***

## Deception Technology based

- What the attacker can do?
- Change reality / perception
- Provide opportunity to attacker seeks
- Observe deception artifacts only
- High fidelity detections enables automation and rapid responses
- Gartner calls [Preemptive Cybersecurity](#)

# Strategy for precise and early Detection using Deception Technology

- **Design for Efficacy:**

- **Design deception artifacts** for specific **use case**
- Carefully **place** deceptions for impact
- Ensure **attractiveness** to attacker/malware
- Ensure **visibility in attacker tools**

- **Avoid Detection (Fingerprinting):**

- **Personalize** per endpoint, domain, ...
- **Blend** into the environment
- Create a "***lived-in***" appearance for authenticity

- **Security Measures:**

- Design **containment** strategy
- Design continuous **observations**

**Threat-Informed Detection**

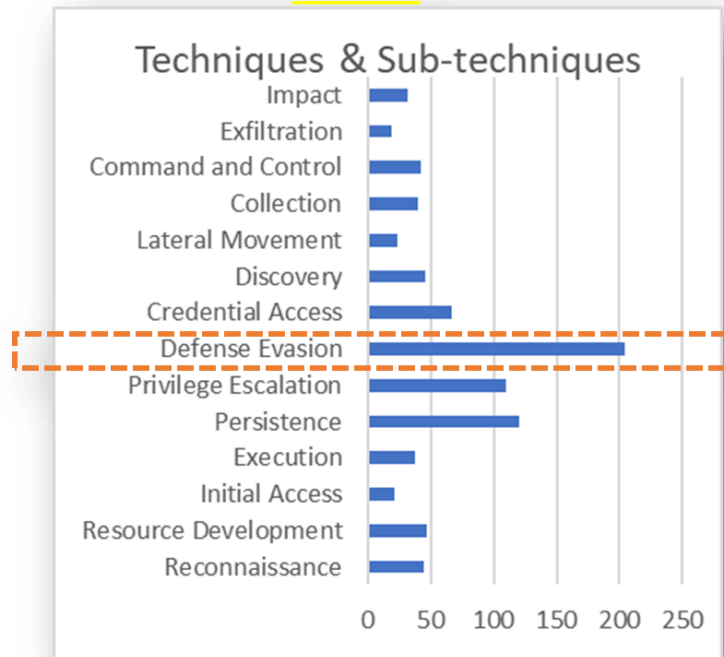
# Leveraging MITRE ATT&CK framework

## Deception-based Detections at different granularities

### Threats



### Tactics



### Techniques

#### Top 10 MITRE ATT&CK Techniques

The most prevalent ATT&CK techniques identified in 2024, ordered by the percentage of malware samples which exhibited the behavior.




# Identity ecosystem - plenty of targets



The diagram illustrates a Denial of Service (DoS) attack using a botnet. It shows a sequence of five steps:

1. Connect to \\TYPO-server01
2. \\TYPO-server01 Not Found
3. Anyone know \\TYPO-server01?  
(Attacker will be needed)
4. Yes! That is me!
5. Okay, here are my credentials!

The visual elements include a desktop computer and monitor on the left, a server tower on the right, a laptop at the bottom labeled 'Attacker', and a cloud labeled 'Botnet' in the center. Arrows indicate the flow of communication between these entities.



**Attackers prefer to sign-in instead of breaking-in**



# Identity Protection

## Active Directory

### Add Honey Accounts

- User Accounts, Service Accounts, Groups, ...



## Endpoints

### Add Honeytokens

- Credentials, Keys, Tickets, Tokens, ...
- OS caches, App profiles, Logs, Registry, ...



## Network

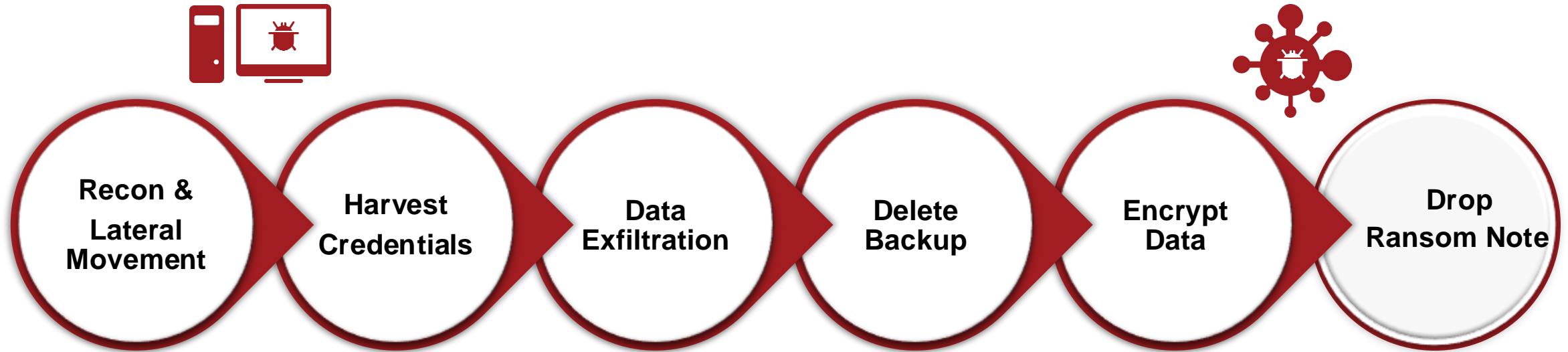
### Generate fake requests

- Detect malware Responder.py, Inveigh.ps1, ...





# Strategy for Ransomware Detection



- **Identify the key TTPs/stages of ransomware threat**
- **Design and deploy deceptions to provide opportunity to ransoms**
- **Quickly Detect and stop ransomware threat**

# Detecting a specific Tactic, (Sub-)Technique

PICUS | RED REPORT™ 2025

## Top 10 MITRE ATT&CK Techniques

The most prevalent ATT&CK techniques identified in 2024, ordered by the percentage of malware samples which exhibited the behavior.

### T1055 Process Injection

Hiding in Plain Sight

#1 2024:1 31%

Defense Evasion Privilege Escalation

### T1059 Command and Scripting Interpreter

The Puppet Master

#2 2024:2 29%

Execution

### T1555 Credentials from Password Stores

The Master Keys to Treasure

#3 \* NEW 25%

Credential Access

### T1071 Application Layer Protocol

The Whispering Channels

#4 2024:7 24%

Command and Control

### T1562 Impair Defenses

Blinding the Watchdogs

#5 2024:3 23%

Defense Evasion

### T1486 Data Encrypted for Impact

Holding Secrets Hostage

#6 2024:5 21%

Impact

### T1082 System Information Discovery

Mapping the Treasure Trove

#7 2024:4 19%

Discovery

### T1056 Input Capture

Stealing in Real Time

#8 \* NEW 15%

Collection Credential Access

### T1547 Boot or Logon Autostart Execution

The Persistent Thief

#9 2024:8 15%

Persistence Privilege Escalation

### T1005 Data from Local System

Harvesting the Crown Jewels

#10 \* NEW 12%

Collection

- Leverage Deceptions
- Give **attractive opportunity** that the attacker/malware seek
- **Early and Precise Detection**



A Great Gray Owl is perched on a tree trunk, its mottled gray and white feathers blending perfectly with the rough bark. The owl's large, dark eyes are fixed forward, and its long, light-colored beak is visible. The background is a dense forest with green foliage and thin tree branches.

# Thank you

Raj Gopalakrishna

[www.linkedin.com/in/rajgopalakrishna](http://www.linkedin.com/in/rajgopalakrishna)

[www.acalvio.com](http://www.acalvio.com)