ACALVIO

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

www.linkedin.com/in/rajgopalakrishna

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**

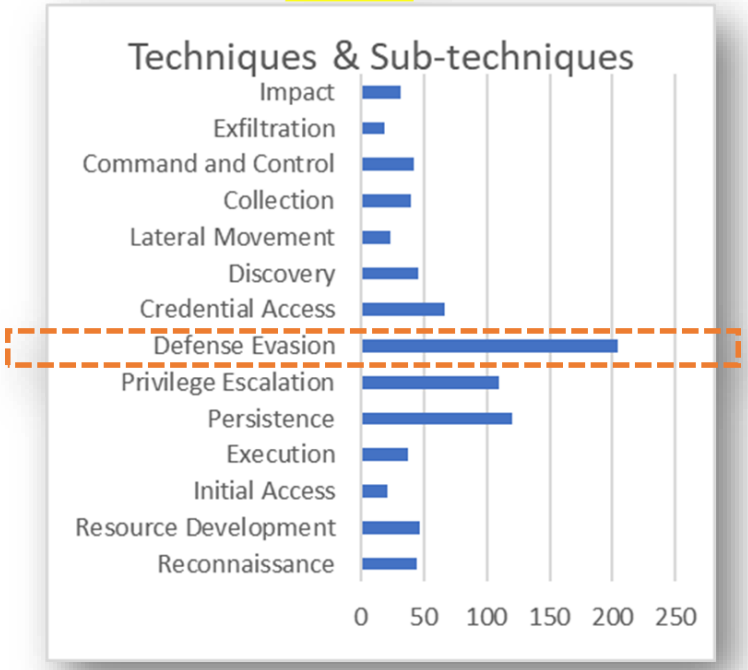
Threat-Informed Detection

Leveraging MITRE ATT&CK framework

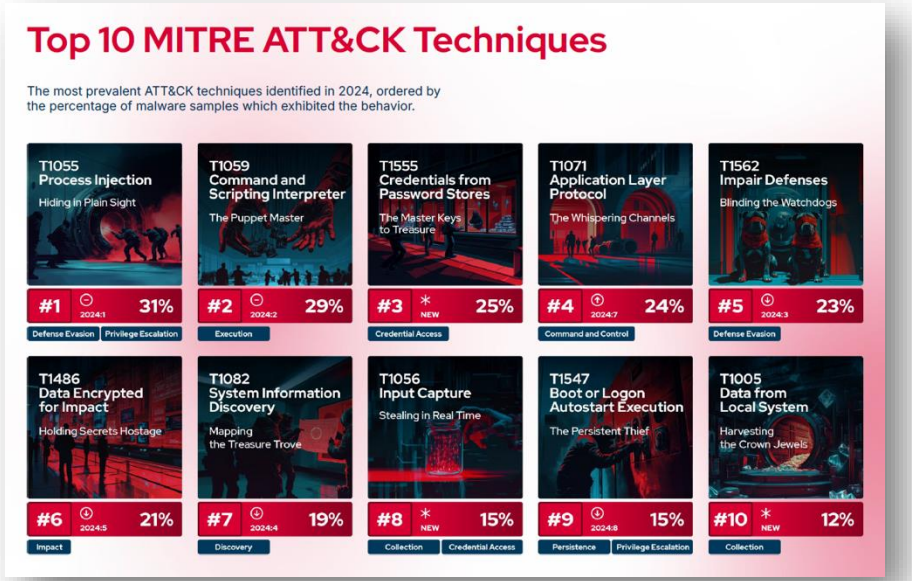
Deception-based Detections at different granularities

Threats

Tactics



Techniques

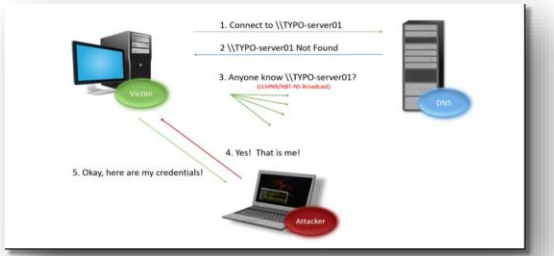


Identity ecosystem - plenty of targets

Identity Store

Endpoints

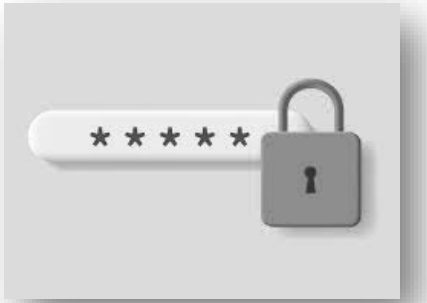
Network



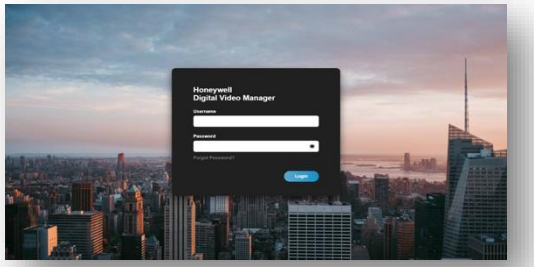
Domain Controller

Accounts

Password Managers



Applications



Browsers

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

Identity Protection

Active Directory

Add Honey Accounts

- User Accounts, Service Accounts, Groups, …

Endpoints

Add Honeytokens

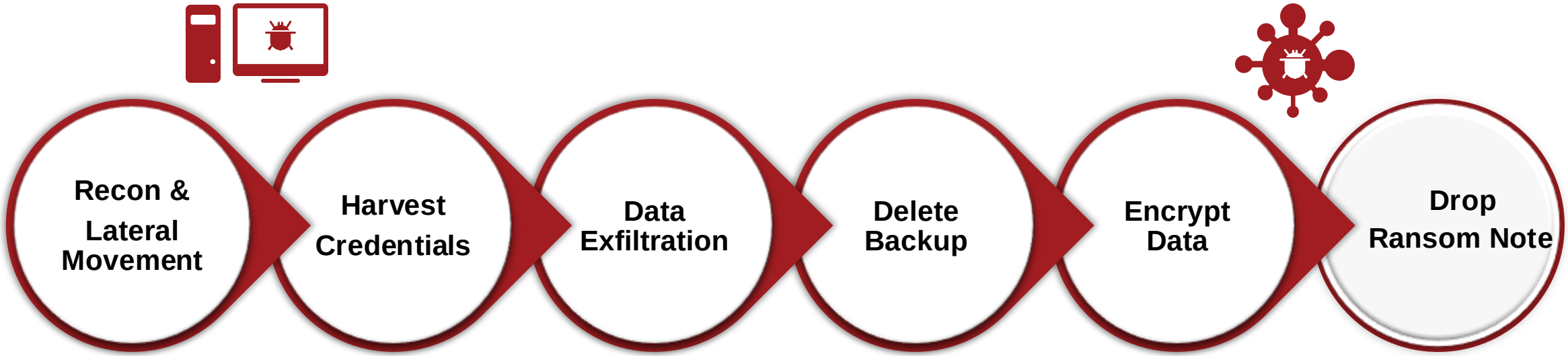
- Credentials, Keys, Tickets, Tokens, …
- OS caches, App profiles, Logs, Registry, …

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 <u>deceptions</u>**
  to **provide opportunity** to **ransomwares**
- **Quickly Detect and stop ransomware threat**

Detecting a specific Tactic, (Sub-)Technique

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


Thank you
Raj Gopalakrishna
www.linkedin.com/in/rajgopalakrishna
www.acalvio.com