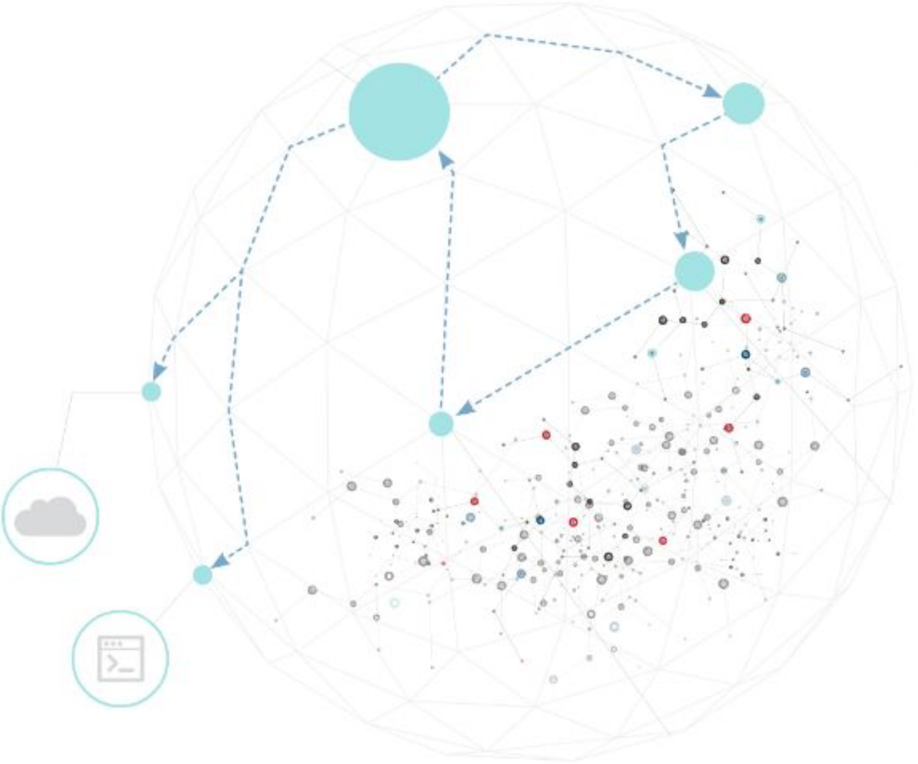
Detecting Hidden Command & Control

Aprendizagem Aplicada a Segurança
Camila Fonseca - 97880
Rodrigo Lima - 98475
2022/2023

The Problem

It is possible for Command & Control (C2) servers to issue commands to Remote Access Trojans (RAT) in a variety of obscure ways that easily blend in with legitimate traffic which can make them nearly impossible to detect.

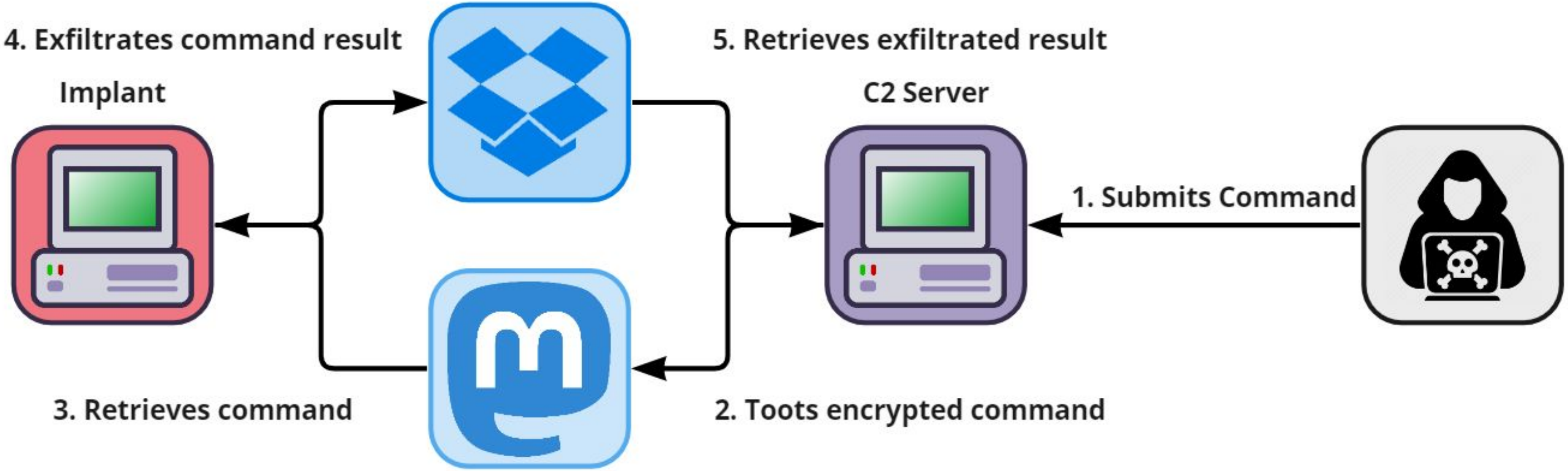
For example, posts on social media and files uploaded to file sharing services were used as C2 in the Hammertross malware, as a real-world scenario.



The Problem

The existence of RATs in a network means it has already been compromised, but the real damage (data exfiltration, execution of payloads) is caused by further commands.

Successfully detecting C2 communications is vital to mitigate a malware's impact after the initial breach has occurred and identifying infected devices.


4. Exfiltrates command result
5. Retrieves exfiltrated result
Implant
C2 Server
1. Submits Command
3. Retrieves command
2. Toots encrypted command

The Solution

Machine Learning Models can be used to solve the complex task of detecting malware that communicates through everyday communication channels used on the user's computers where the malicious agent also resides in order to detect its presence.

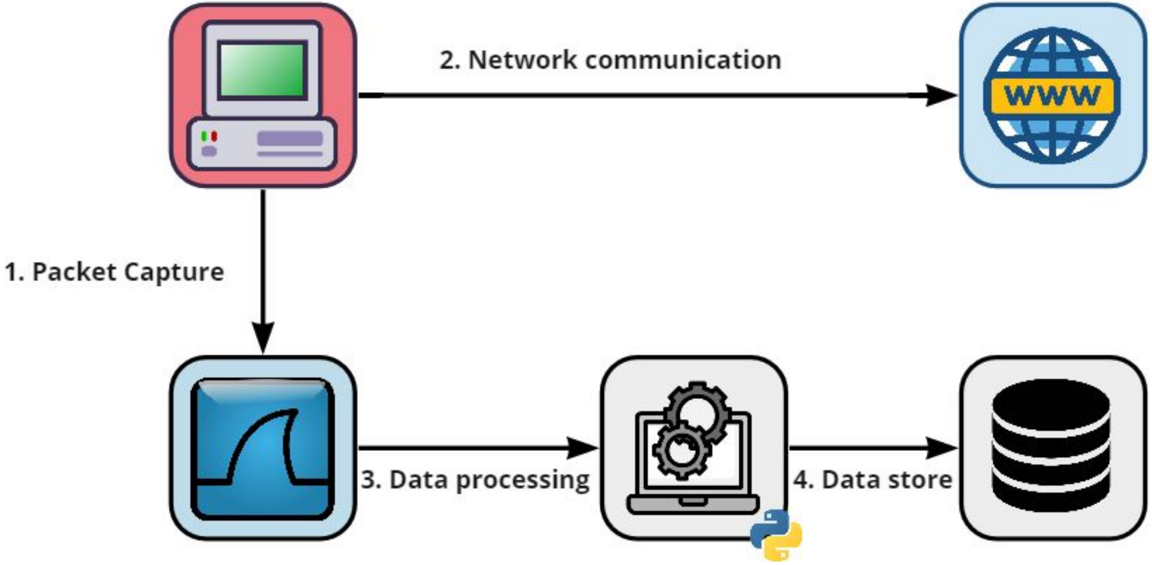
Although the agent mimics regular users' behavior the ML model is a viable method to detect this agent in the network.

Our dataset can simulate a real-world situation by simulating a threat actor's exfiltration technique and by capturing raw data packets to be later filtered.

Data Source - Packet Capture

Test scenario - Capturing packets on individual hosts.
https://github.com/ZeroDollarSecurity/LarryChatter/blob/master/rpt-apt29-hammertoss.pdf

Real world scenario - Capturing network-wide traffic via a cable tap or a switch mirror port.



Features

Goal: Find patterns in request timings & destinations

- Metrics:
  - Source/Destination Address
  - Timestamps
  - Type of L4/L5 Protocol
  - Ports used
- Features:
  - Periodicity of requests
    - Average time between requests to same host
  - Repeated destination sequences

Goal: Detect payloads being downloaded and data being exfiltrated

- Metrics:
  - Packet size
  - Size of the first packet
- Features:
  - Ratio between data/time over time
  - Periodicity in similarly sized packets
  - Measure various Download/Upload metrics (Ratio, averages...)

Features

Type of L4/L5 Protocol	Measuring metrics on the protocols used: - Ratios for each protocol (ex. 70% HTTPS, 1% HTTP, 29% ICMP)
Ports used	Detecting rarely used ports (headless browsers etc), by the victim machine
Periodicity of requests	Periodicity of requests between requests to twitter and the requests to dropbox.