

Monitoring Processes Download Behavior with Python



Sean Wilkins

Network Engineer & Author

swilkins@infodispersion.com

www.infodispersion.com



Module Introduction

**Monitoring LOLbin process
behavior**

**Watching for abnormal
process spawning and
transfers**



Overview



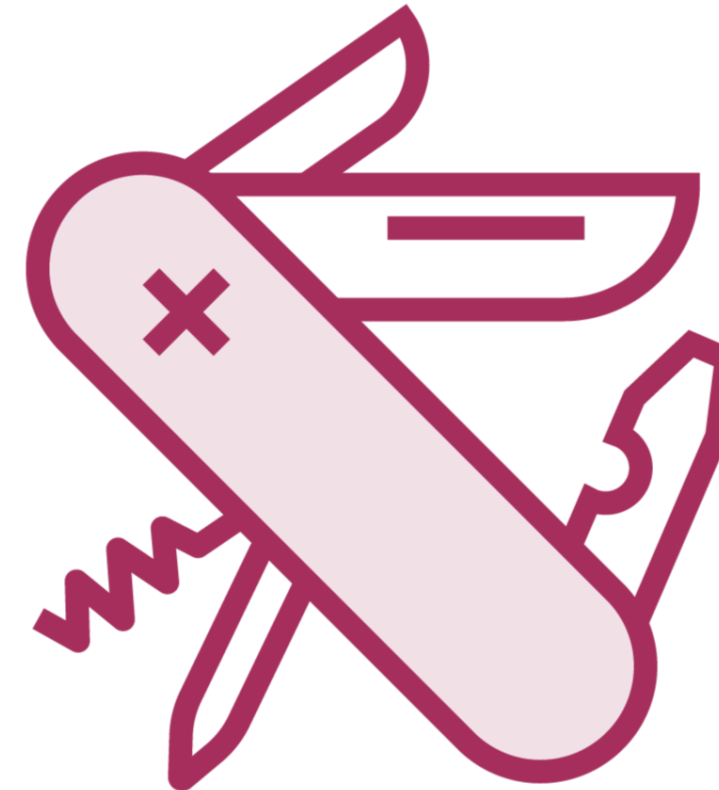
- **Watching LOLbin processes**
- **Concepts Demonstration - Monitoring LOLbins**



LOLbin Processes



Module focuses on LOLbin processes

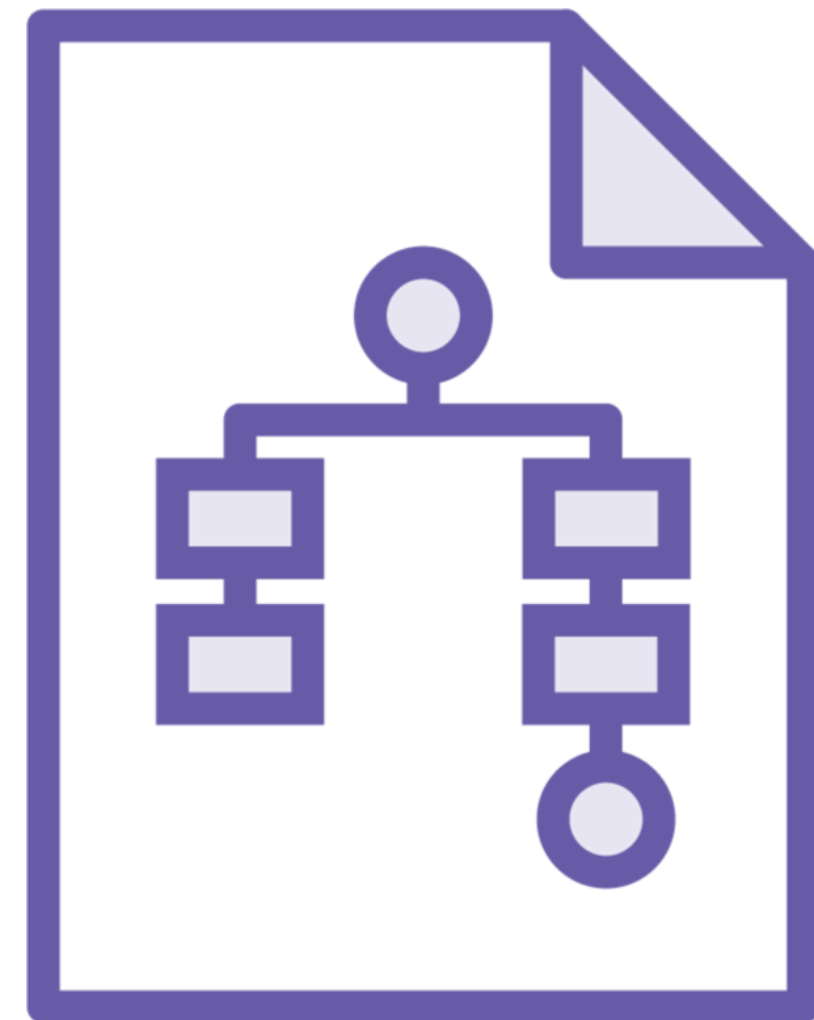


Same techniques can be used for all processes

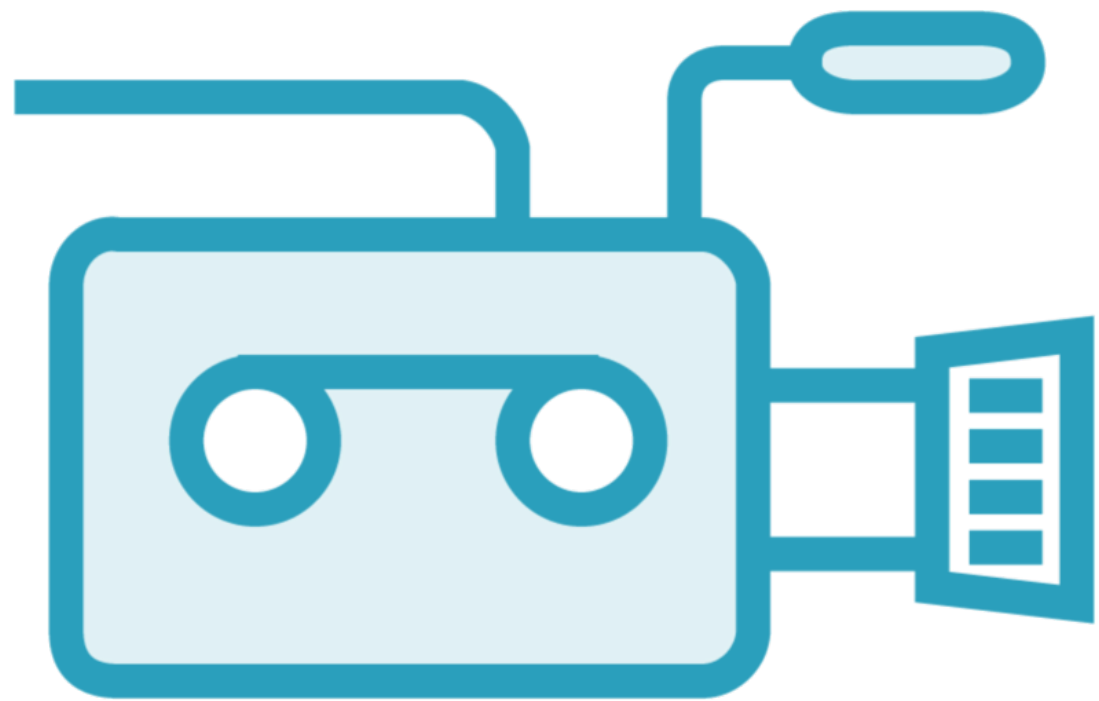
LOLbin Processes

**Utilize the dictionary variable
shown in previous module**

Focus will be on specific process trees



LOLbin Processes



Targeted process will have their traffic tracked
Monitoring is limited by Scapy



LOLbin Processes

New modules used include:

Collections

Threading

Used to build LOLbin monitor



Demo



How to monitoring LOLbin process trees

Building a process traffic monitoring



Summary



- **Watching LOLbin processes**
- **Concepts Demonstration - Monitoring LOLbins**

