Botnet Tracker

Gathering IOCs straight from source

Masterfox

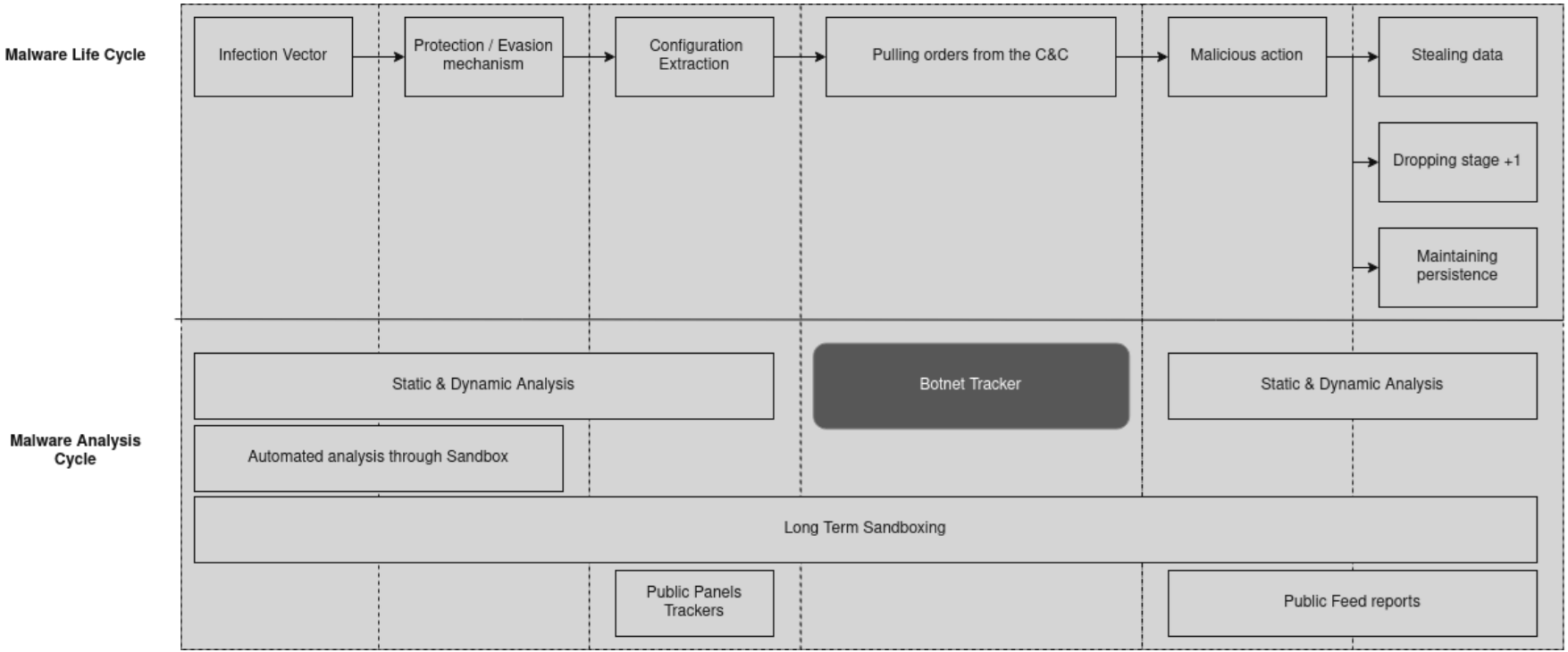
Masterfox

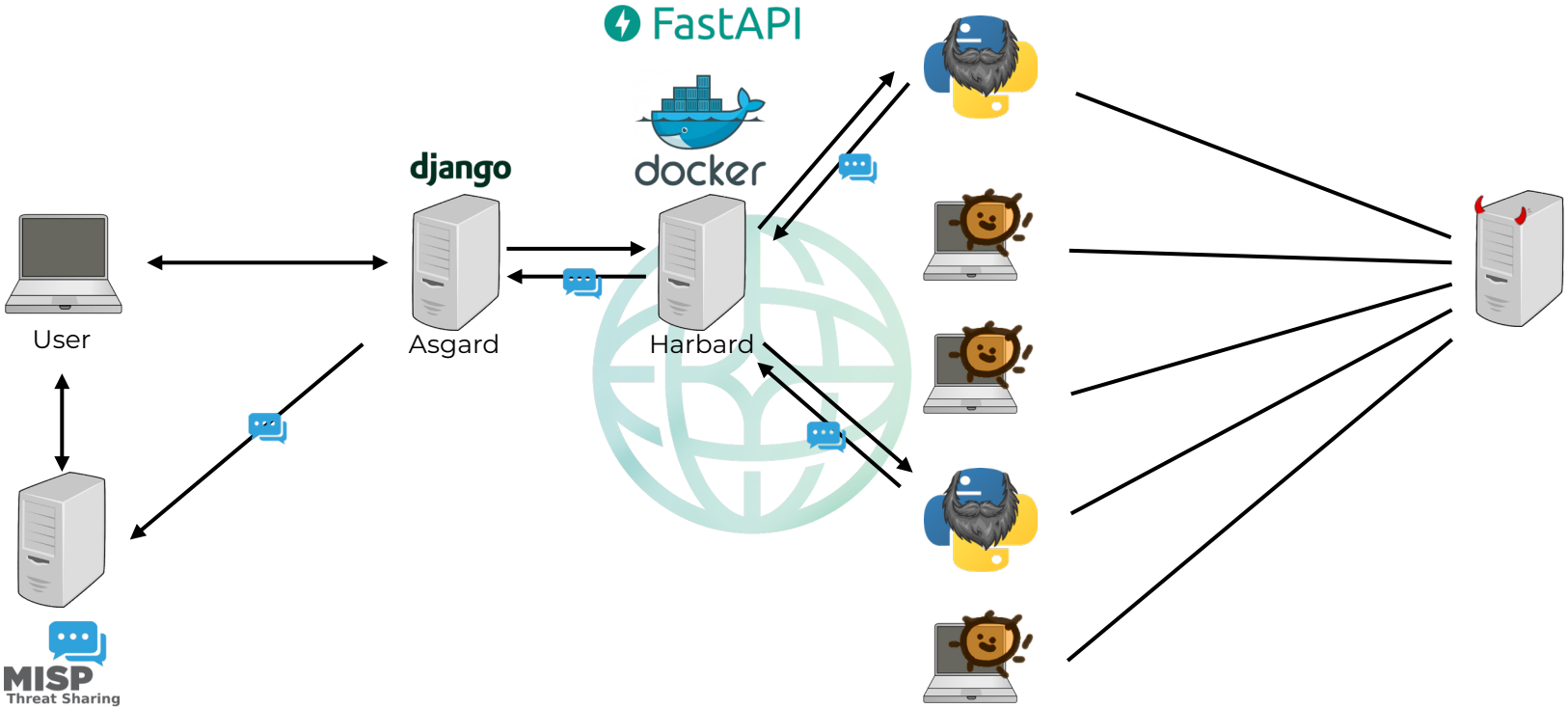
Tom Mounet

entropy.land/cv

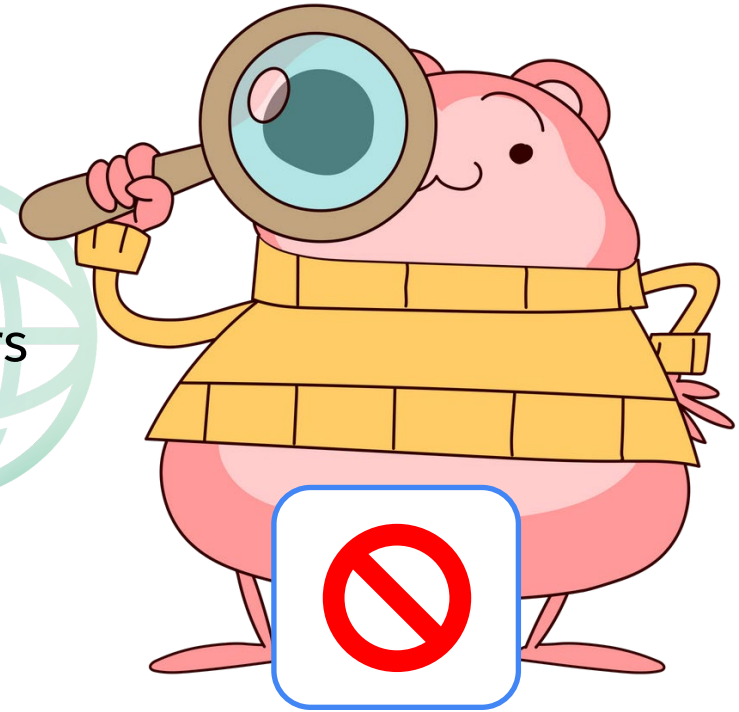
fakenews.sh

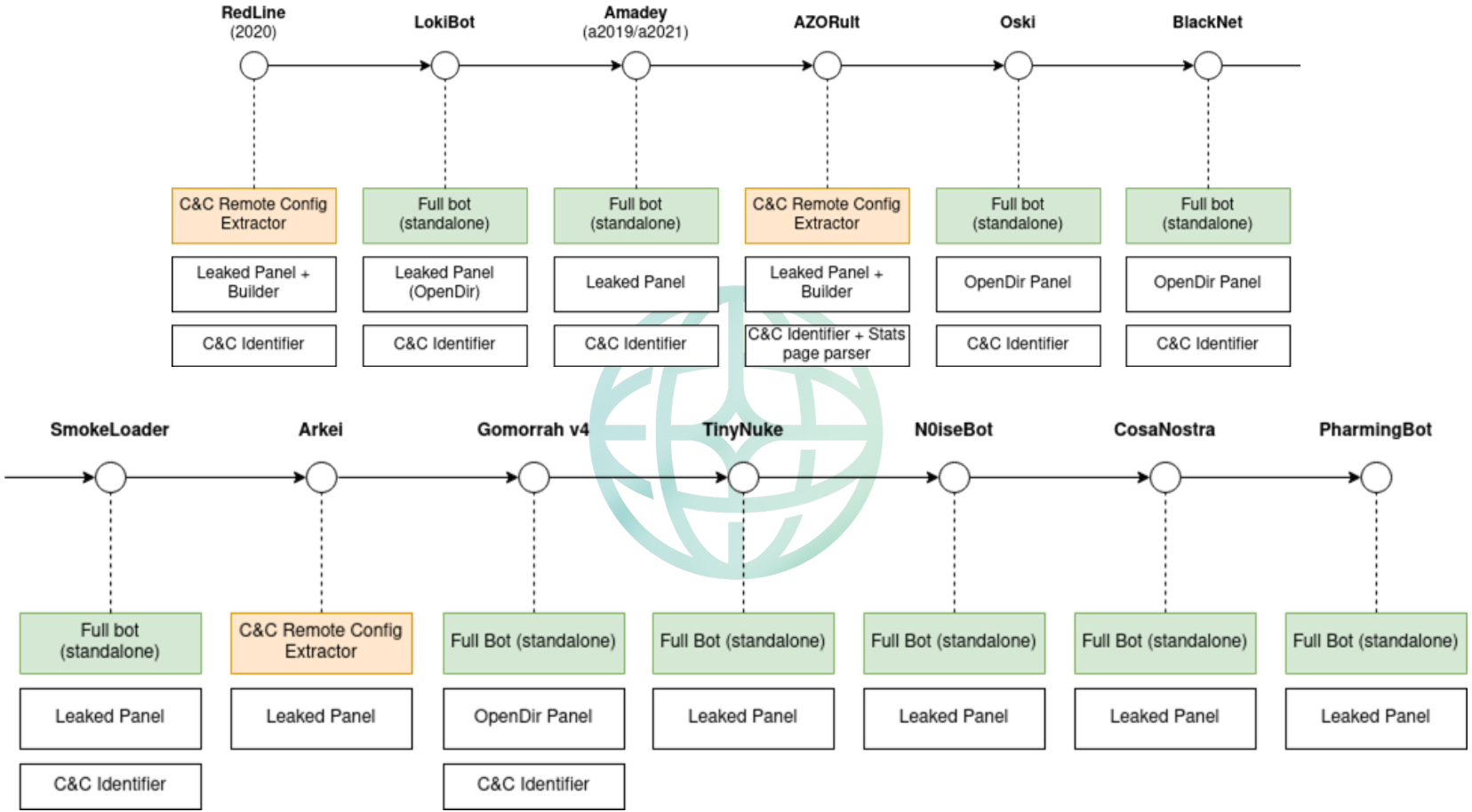

AIR


Malware Life Cycle
Infection Vector
Protection / Evasion mechanism
Configuration Extraction
Pulling orders from the C&C
Malicious action
Stealing data
Dropping stage +1
Maintaining persistence
Malware Analysis Cycle
Static & Dynamic Analysis
Botnet Tracker
Static & Dynamic Analysis
Automated analysis through Sandbox
Long Term Sandboxing
Public Panels Trackers
Public Feed reports


FastAPI
django
docker
User
Asgard
Harbard
MISP
Threat Sharing

- ➔ 10 Fully implemented bots
- ➔ 2 Silent Bots
- ➔ 3 Remote configuration extractors
- ➔ 1 Utility library (👋 🦢)
- ➔ 13 Panels Sources




RedLine
(2020)
LokiBot
Amadey
(a2019/a2021)
AZORult
Oski
BlackNet
C&C Remote Config Extractor
Full bot (standalone)
Full bot (standalone)
C&C Remote Config Extractor
Full bot (standalone)
Full bot (standalone)
Leaked Panel + Builder
Leaked Panel (OpenDir)
Leaked Panel
Leaked Panel + Builder
OpenDir Panel
OpenDir Panel
C&C Identifier
C&C Identifier
C&C Identifier
C&C Identifier + Stats page parser
C&C Identifier
C&C Identifier
SmokeLoader
Arkei
Gomorrah v4
TinyNuke
N0iseBot
CosaNostra
PharmingBot
Full bot (standalone)
C&C Remote Config Extractor
Full Bot (standalone)
Full Bot (standalone)
Full Bot (standalone)
Full Bot (standalone)
Full Bot (standalone)
Leaked Panel
Leaked Panel
OpenDir Panel
Leaked Panel
Leaked Panel
Leaked Panel
Leaked Panel
C&C Identifier
C&C Identifier

➔ **Finding a consistent dataset of live malware panels**

☑ Implementation of our own modular panel tracker

➔ **Some tedious bots that have a lot of features to implement**

☑ Cry and go back to work

➔ **Malware with complex decentralized infrastructure**

❌ We can’t connect our solution with this type of malwares

➔ **Malware with embedded configurations**

❌ These malwares are de facto out of our scope

➔ Open our tracker to wider malware families and protocols

➔ Automated VPN / proxy system to hide our harbard instances

➔ Integrate (with?) the usual malware analysis pipeline

➔ Work with other public trackers (eg. automatic submission)

➔ Open source !!!

FakeCTF

Our bank 🐖 is under attack !

*Pentest + Forensic ... **Malware analysis***

Come join us

June 17th

Vannes, France

Thanks


ctf.fakenews.sh


ctf.team.fakenews@gmail.com


@MaestroZorro_


@HomardBoy