Feasible (Solution) for the Web Threat Jigsaw

The Honeynet Project

Annual Workshop 2012

Lukas Rist

My Mom

My Mom

Seriously!

Virtual Machines

Browser Emulator

Virtual Machines

Browser Emulator

Domain Reputation

Anti-Virus engines

Observe the infection process

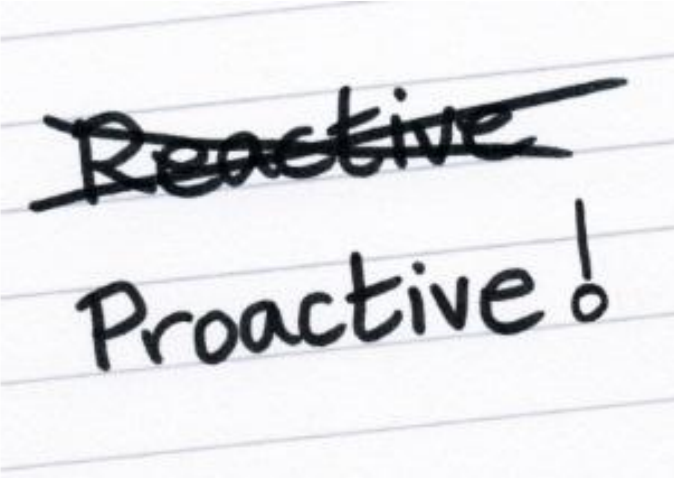
Get malware distribution domain

Observe the infection process

Get malware distribution domain

Reduce spreading

make them **Suffer!**



~~Reactive~~

Proactive!

Automation

Bang for the buck

Efficiency

~~Piles of data~~

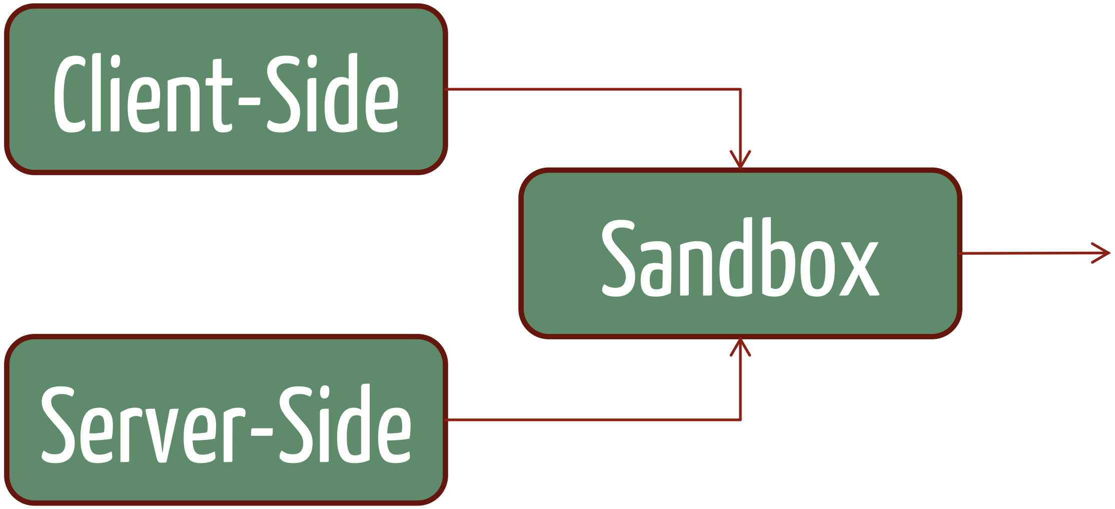
~~Manual workflow~~

Actionable items

~~Static system~~

Share data

Proposal

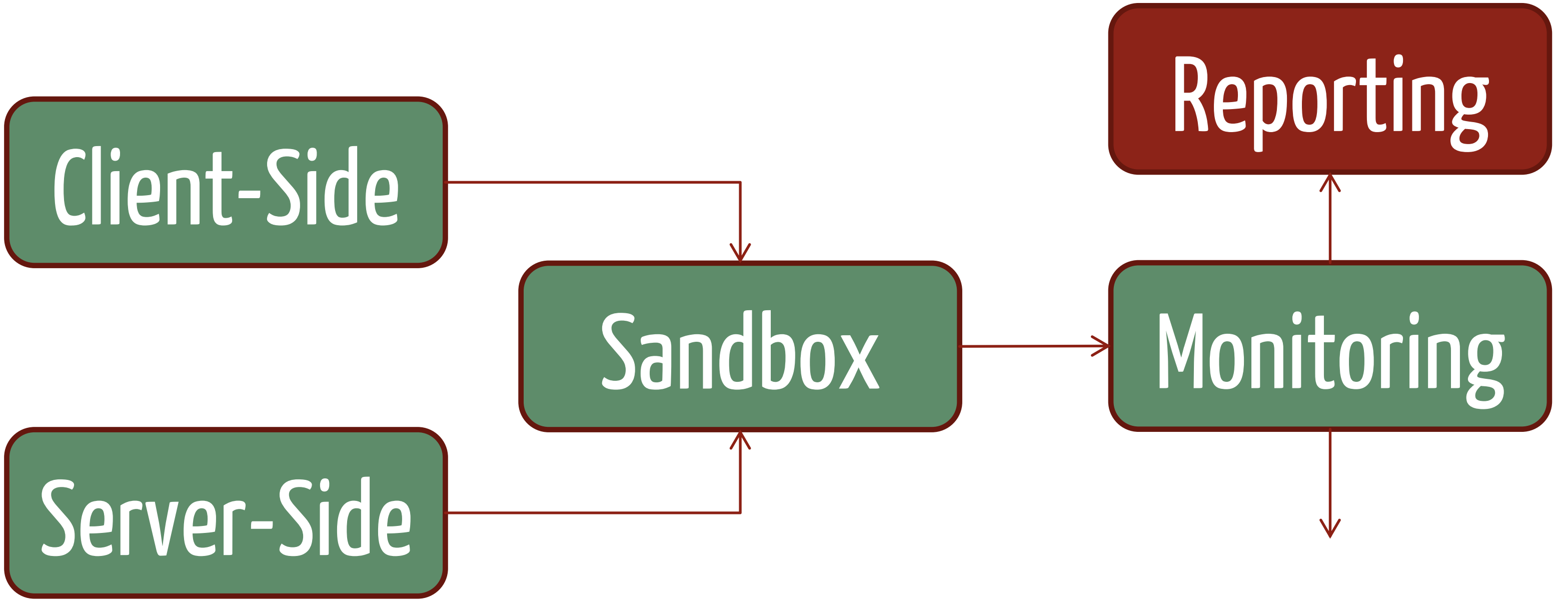


Client-Side

Sandbox

Server-Side

Proposal



Client-Side

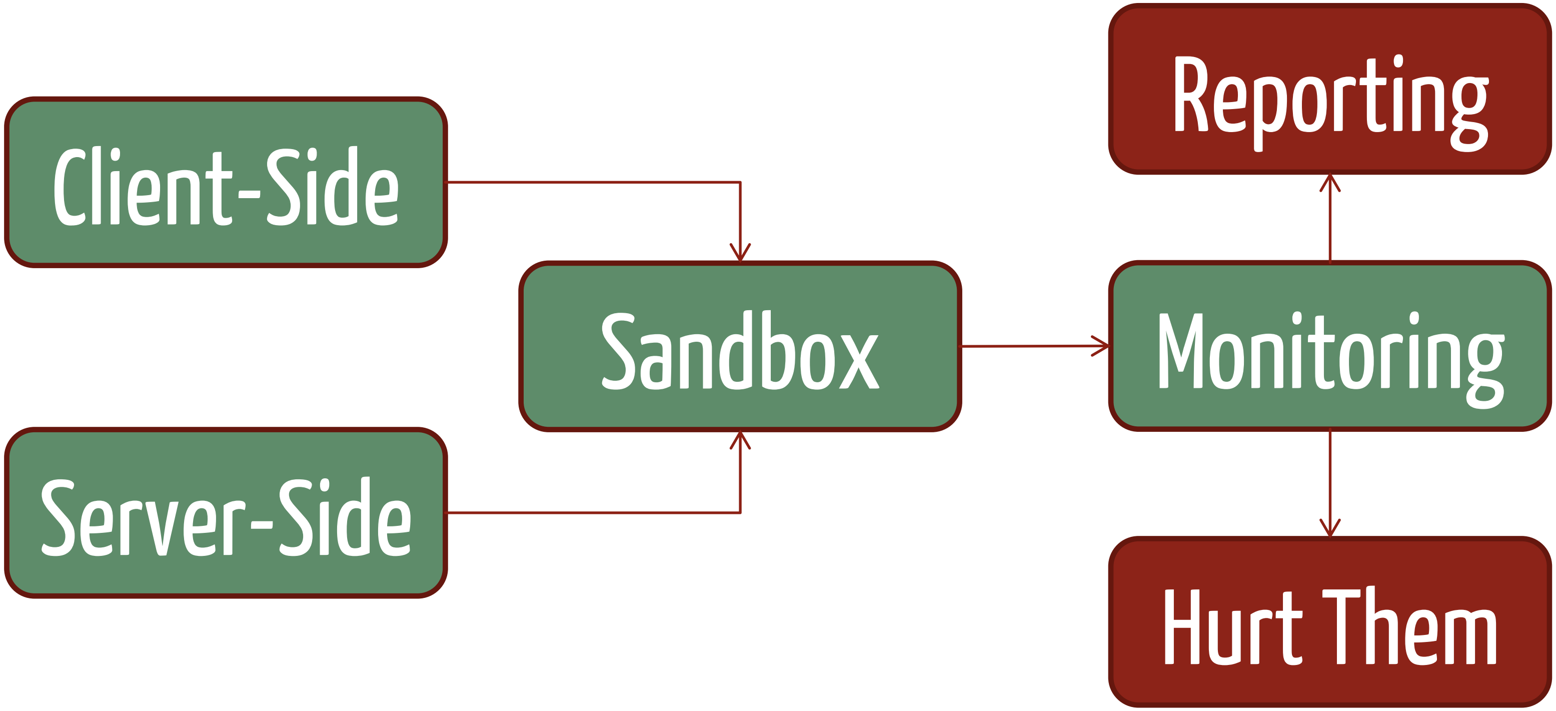
Server-Side

Sandbox

Monitoring

Reporting

Proposal



Client-Side

Server-Side

Sandbox

Monitoring

Reporting

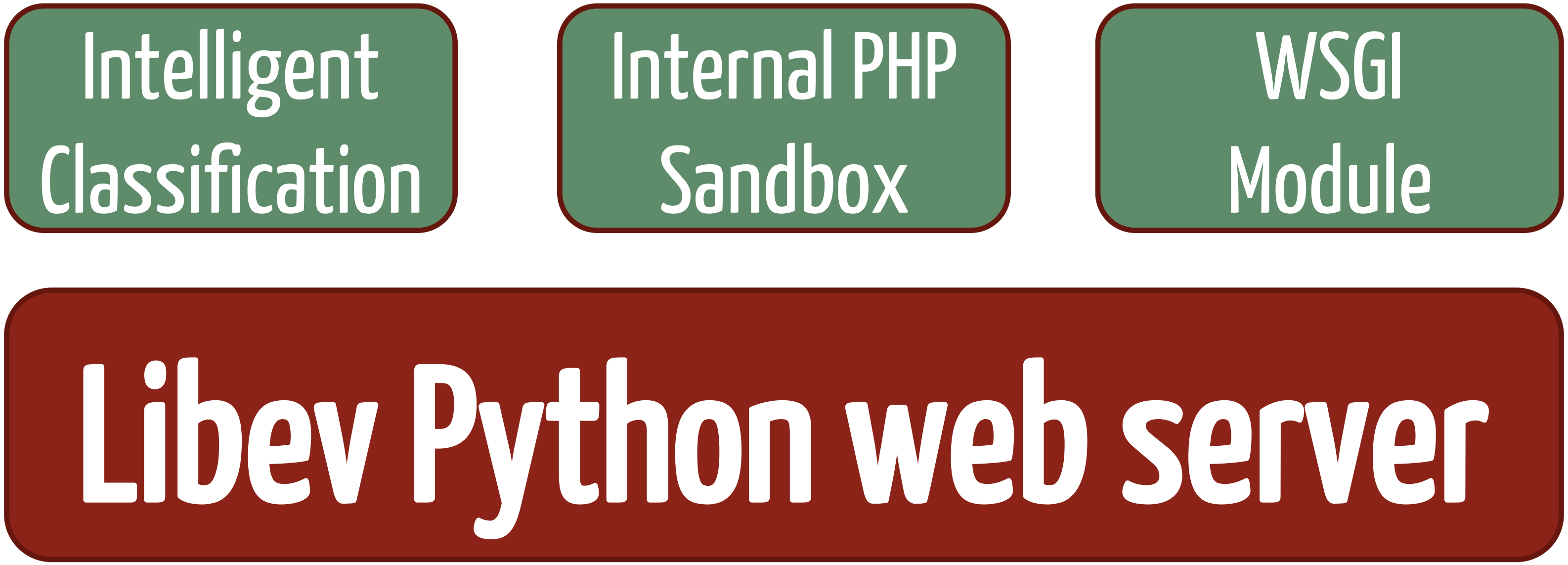
Hurt Them

Honeynet Project Feeds

Generic, Live, Authenticated

Announcing:

Glastopf$_{v3}$

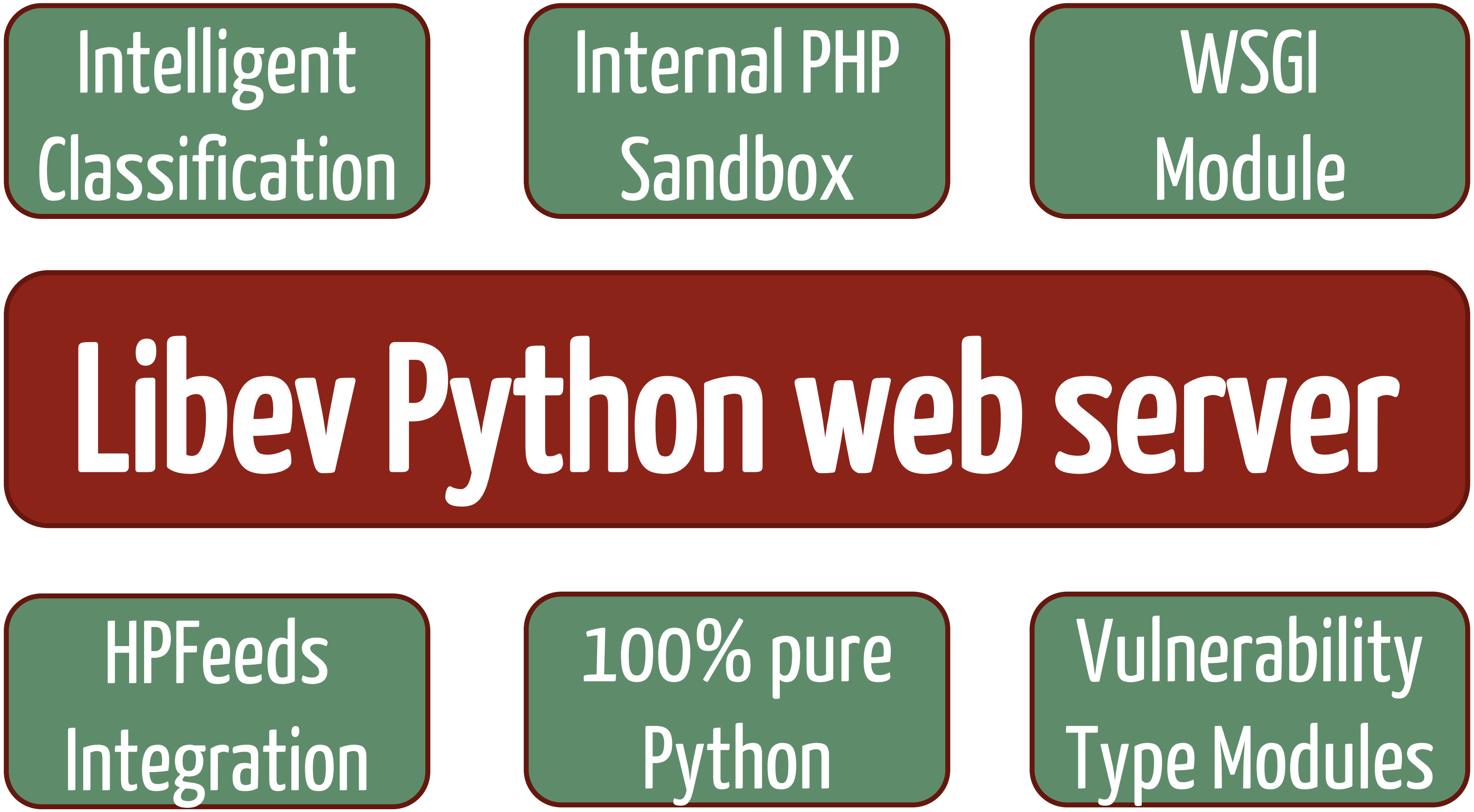


Intelligent Classification

Internal PHP Sandbox

WSGI Module

Libev Python web server



Intelligent Classification

Internal PHP Sandbox

WSGI Module

Libev Python web server

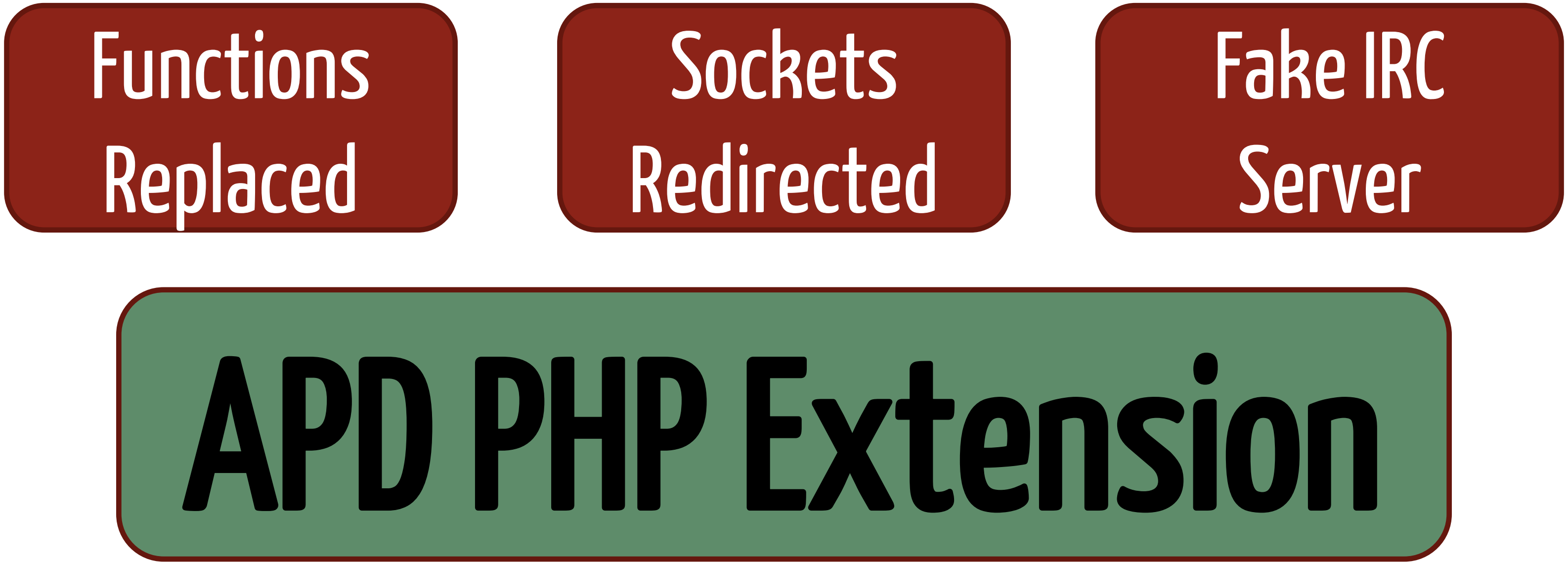
HPFeeds Integration

100% pure Python

Vulnerability Type Modules

PHP

Sandbox

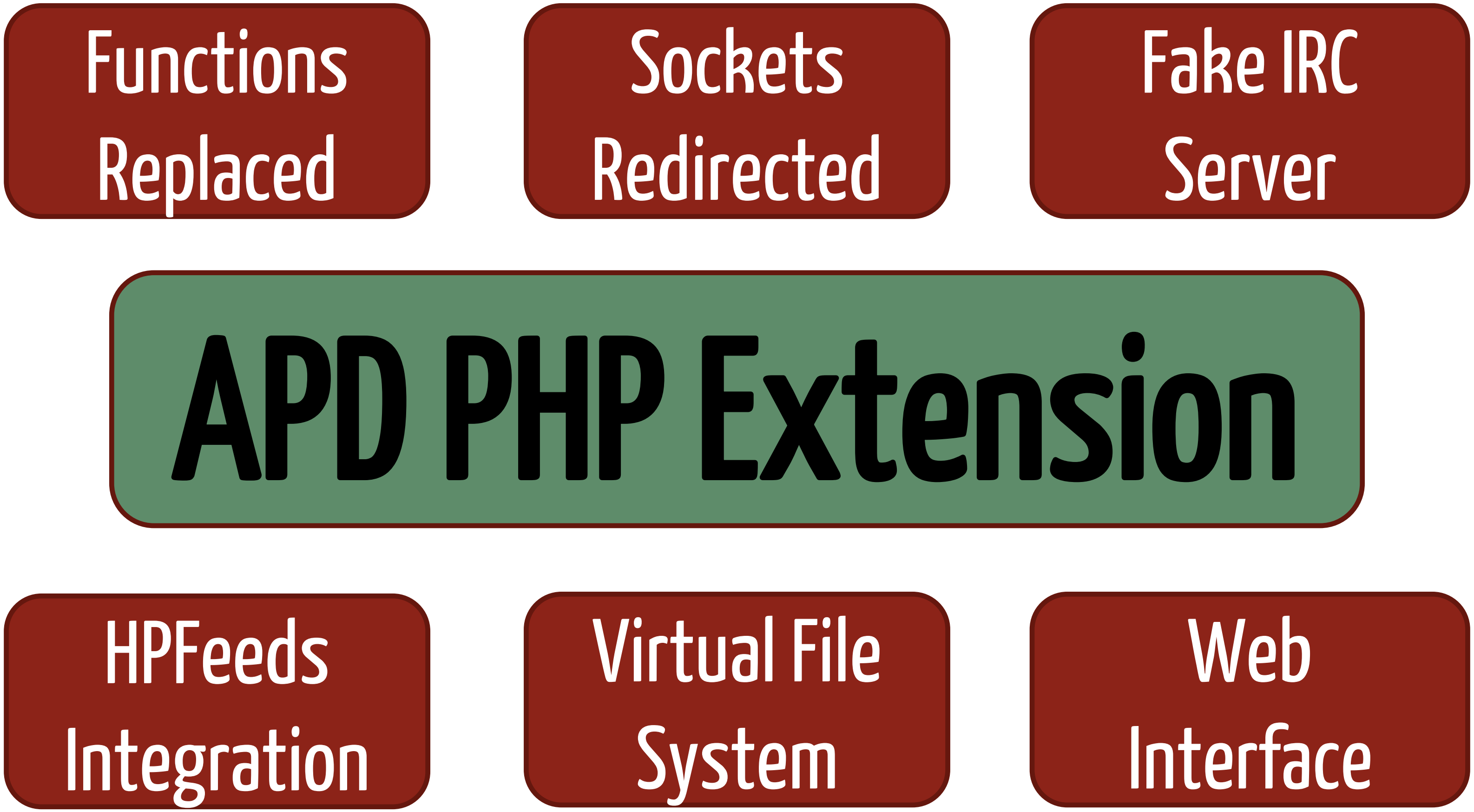


Functions Replaced

Sockets Redirected

Fake IRC Server

APD PHP Extension



Functions Replaced

Sockets Redirected

Fake IRC Server

APD PHP Extension

HPFeeds Integration

Virtual File System

Web Interface

Botnet

Spy

Fully Automated

Pretends to be a Bot

IRC Client

HPFeeds Integration

100% Python

Client-Side

Honeypots

Virtual Machine

Sandbox

Brute-Forcing Botnet Passwords

Automated Botnet **Evaluation**

Botnet **Overtake**

Brute-Forcing Botnet Passwords

Automated Botnet **Evaluation**

Botnet **Overtake**

Relocate the Botnet

Get **Intelligence**

Shut-Down the Botnet

Q&A

```
while len(questions) > 0:
    if time <= 0:
        break
    print answers[questions.pop()]
```

ddddddddddddddemo