

**MICHIGAN STATE**  
**U N I V E R S I T Y**

# Alpha Presentation

## Defeating Malware Payload Obfuscation

The Capstone Experience

Team Proofpoint

Adam Johanknecht

Nick Lojewski

Vivian Qian

Derek Renusch

Dan Somary



*From Students...*  
*...to Professionals*

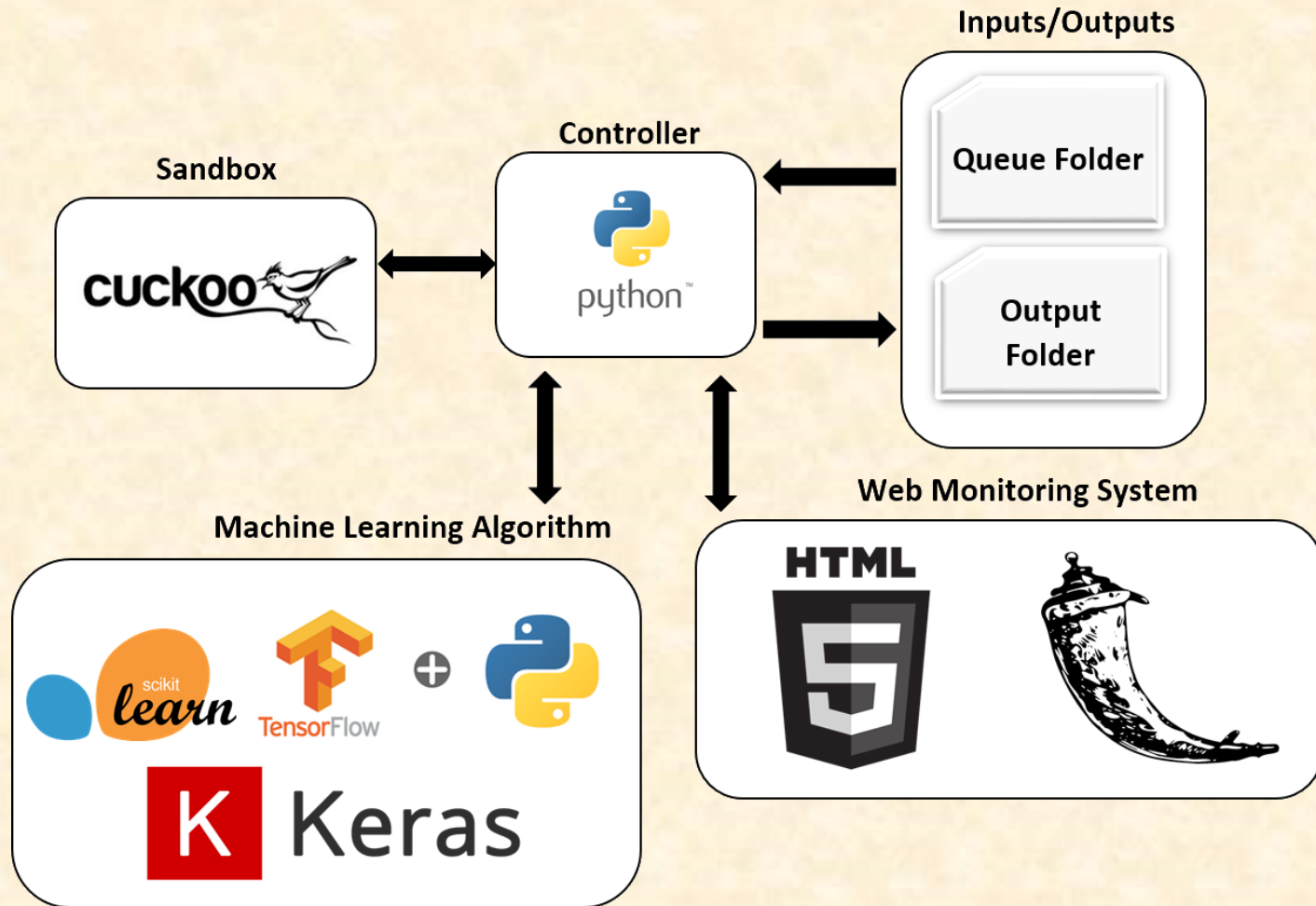
Department of Computer Science and Engineering  
Michigan State University  
Spring 2019

# Project Overview

- Create a machine learning system to classify files as malicious or benign
  - Accuracy goal: have at least the same accuracy as sandbox detonation
  - Performance goal: be at least 50% faster than detonation in Cuckoo
- Display information in web dashboard
  - High level system information
  - Ability to look at details for individual files



# System Architecture



# Dashboard

Dashboard - Mozilla Firefox

Dashboard

## File Classification

### Queue

#	File Name	MD5 Hash	Cancel
1	WannaCry.exe	0cc175b9c0f1b6a831c399e269772661	✗
2	MyDox.docx	e1671797c52e15f763380b45e841ec32	✗
3	win.bin	92eb5ffee6ae2fec3ad71c777531578f	✗
4	app.dmg	4a8a08f09d37b73795649038408b5f33	✗
5	ProjProp.pdf	8277e0910d750195b448797616e091ad	✗

### Processed

#	File Name	MD5 Hash	Classifi
1	cpuz_x64.exe	3c5f00ab1f353018a23f7771def20457	Malicious
2	PortRptr.exe	f40f6243e7c93ad1c1777ea5437da0ac	Malicious
3	cpuz_x32.exe	cfcaa51061f80c07128156edcfd9eff5	Benign
4	LockCrypt2.0.bin	f1927e7f90416bf39fc7991bbc57e1b3	Malicious
5	WannaCry.exe	f42d29367786af1b8919a9d0cbdfdf3f	Malicious
6	SpaceSniffer.exe	b310e7335eae66a533e985b377e81612	Malicious
7	vlc.exe	b2a4b2f0623cb4b661e731b768c57dd6	Malicious
8	Diablo III Launcher.exe	27074219307e30ee4fdb5c64e71eadfc	Benign
9	NanocoreRAT.bin	9319231e507d66161a60eacc23958923	Malicious



# File Drill Down – Malicious File

queue/WannaCry.exe : Proofpoint Analysis - Mozilla Firefox

queue/WannaCry.exe : Proof X +


10.55.200.109:5000/reports/f42d29367786af1b8919a9d0cbefd3f

File Drill Down: WannaCry.exe

### File Classification


File Name	WannaCry.exe
MD5 Hash	f42d29367786af1b8919a9d0cbefd3f
Classification	Malicious

Classification Confidence (%)



### File Attributes

File Type	Windows Executable File
Size	3514368 KB

Open file in  
**cuckoo** 



# File Drill Down – Benign File

queue/Diablo III Launcher.exe : Proofpoint Analysis - Mozilla Firefox

queue/Diablo III Launcher.exe X +


10.55.200.109:5000/reports/27074219307e30ee4fdb5c64e71eadfc

File Drill Down: Diablo III Launcher.exe

### File Classification


File Name	Diablo III Launcher.exe
MD5 Hash	27074219307e30ee4fdb5c64e71eadfc
Classification	Benign

Classification Confidence (%)



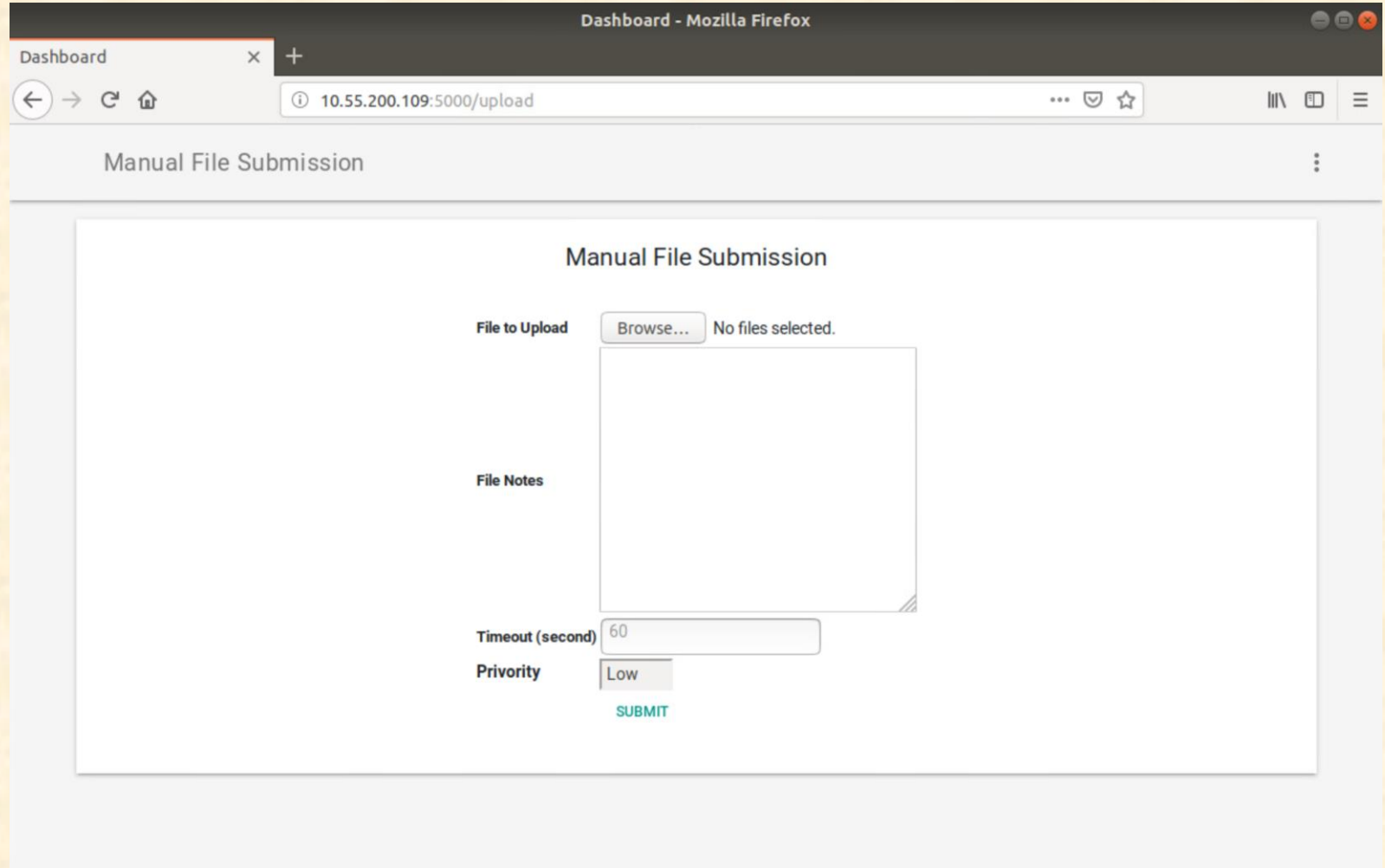
### File Attributes

File Type	Windows Executable File
Size	3353576 KB

Open file in  
**cuckoo** 



# File Upload



The screenshot shows a Mozilla Firefox browser window with the title "Dashboard - Mozilla Firefox". The address bar displays "10.55.200.109:5000/upload". The page content is titled "Manual File Submission" and includes a form with the following fields:

- File to Upload:** A button labeled "Browse..." and the text "No files selected." below it.
- File Notes:** A large, empty text area.
- Timeout (second):** A text input field containing the value "60".
- Priority:** A dropdown menu currently showing "Low".
- SUBMIT:** A green button located below the priority dropdown.



# What's left to do?

---

- Handle additional file types
- Create feedback loops for Machine Learning
- Send low confidence files to Cuckoo
- Display system health information
- Improve main dashboard



# Questions?

---

?

?

?

?

?

?

?

?

?

