#### MICHIGAN STATE UNIVERSITY Project Plan Next Generation Malware Detection, Clustering and Heuristics The Capstone Experience

#### Team Proofpoint

Crystal Lewis Yash Patel George Zhao Graham Thomas Brad Doherty

Department of Computer Science and Engineering Michigan State University

Spring 2018



From Students... ...to Professionals

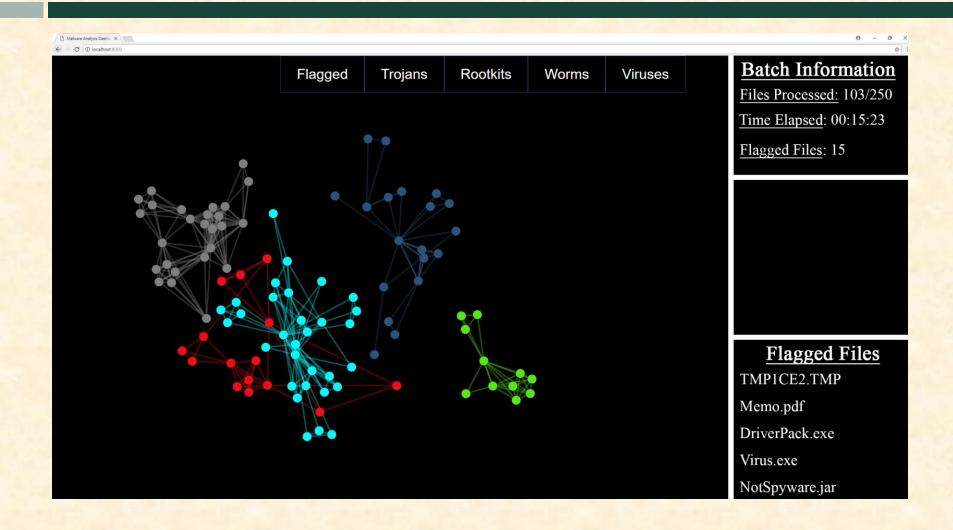
## **Functional Specifications**

- Detect and cluster malware
- Provide a Web Dashboard for analysts
- Provide a framework for assigning signatures to new malware

## **Design Specifications**

- Malware analysis tool
- Malware aggregator
- Nodal graph display
- Malware statistics applets

# Screen Mockup: Nodal Graph



# Screen Mockup: Flagged Filtering

alware Analysis Dashbi: X C ① localhost:8000						θ -
	Flagged	Trojans	Rootkits	Worms	Viruses	Batch Informatio
						Time Elapsed: 00:15:23
						Flagged Files: 15
						Cluster Analysi
						Total Number of Files:
						Behavioral Profiles: 4 files behave like Troj 6 files behave like Viru 3 files behave like Roo 2 files behave like Wor
						<b>Flagged Files</b>
						TMP1CE2.TMP
						Memo.pdf
						DriverPack.exe
						Virus.exe
						NotSpyware.jar

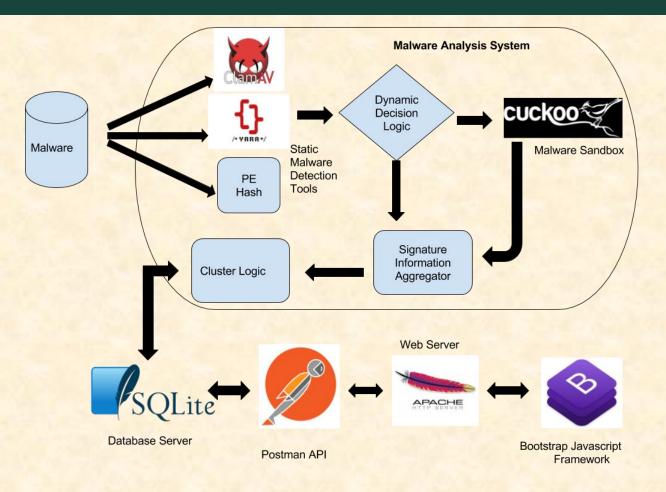
# Screen Mockup: File analysis

Malvare Analysis Dash: x → C O localhost:8000						0 - 0
	Flagged	Trojans	Rootkits	Worms	Viruses	Batch Information
						Time Elapsed: 00:15:23
						Flagged Files: 15
						File Analysis
						<u>File Name</u> : WannaCry.ex File Signature: File
		File Signature: File matched known signatur of Ransom. Wannacry				
						Behavior Profile: Behav like a trojan and a worm
						File Size: 5.65MB
						Flagged Files
						TMP1CE2.TMP
						Memo.pdf
						DriverPack.exe
						Virus.exe
						NotSpyware.jar

# **Technical Specifications**

- Static analysis module
- Dynamic analysis decision logic
- Malware sandboxing
- Signature information framework
- Malware aggregator
- Database
- Web Front End

## System Architecture



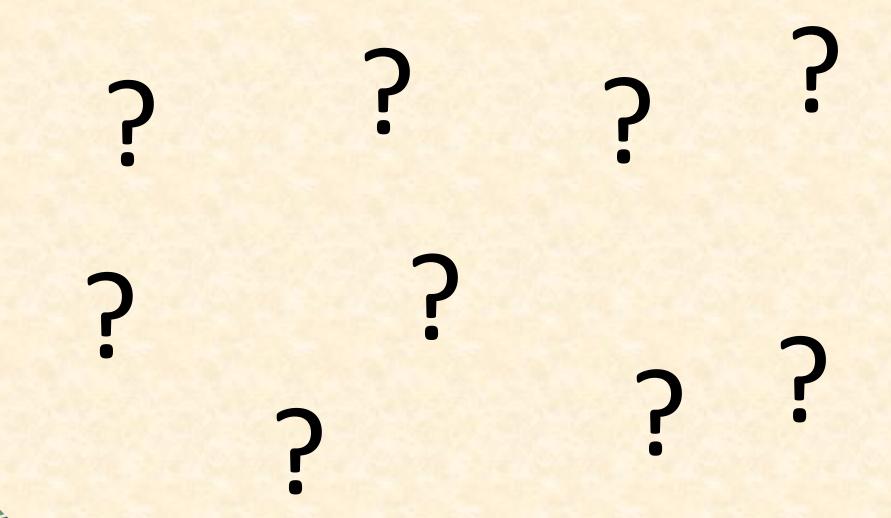
### System Components

- Hardware Platforms
  - Proofpoint hardware cluster
  - ESXi HyperVisor
  - Linux Ubuntu VMs
- Software Platforms / Technologies
  - Python, Yara, Cuckoo, ClamAV
  - SQLite, Apache
  - Postman API and Bootstrap Library

### Risks

- Malware Clustering and Categorization
  - Clustering malware based on file characteristics
  - Research the best way to cluster malware (PE Hash or Fuzzy hashing)
- Understanding Dynamic and Static Analysis Tools
  - The tools behave differently and output different formats
  - Running different malware samples and analyzing outputs
- Scalability and Speed
  - Analyzing variable amounts of malware in an efficient way
  - Properly allocate resources for
- Signature Generation Framework
  - Provide a way for analysts to easily create the signature of a malware
  - Determine what analysis information is relevant for a signature

## **Questions?**



Team Proofpoint Project Plan Presentation