MICHIGAN STATE UNIVERSITY

Alpha Presentation

Next Generation Malware Detection, Clustering and Heuristics

The Capstone Experience

Team Proofpoint

George Zhao
Yash Patel
Graham Thomas
Brad Doherty
Crystal Lewis

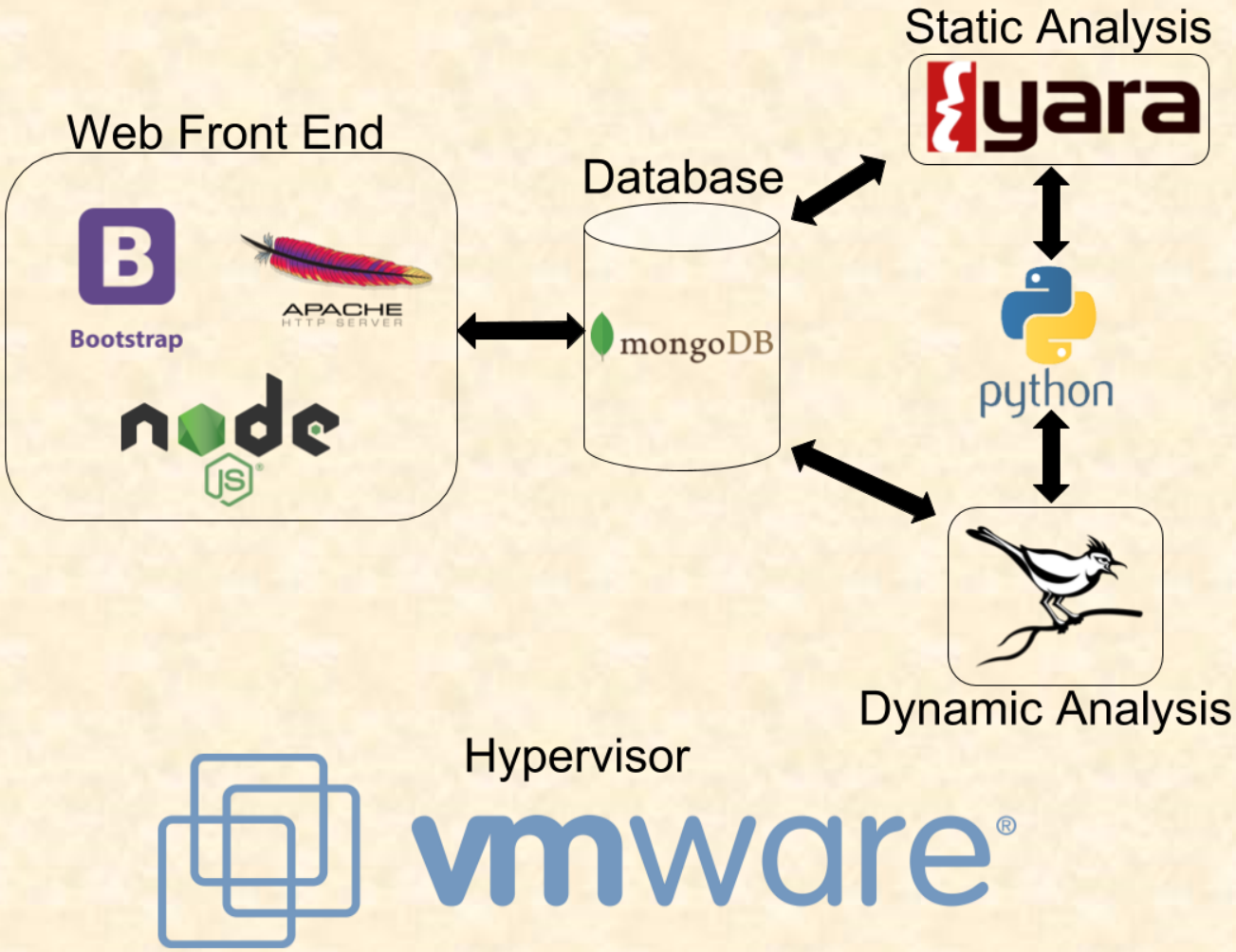
From Students…
…to Professionals

Department of Computer Science and Engineering
Michigan State University
Spring 2018

Project Overview

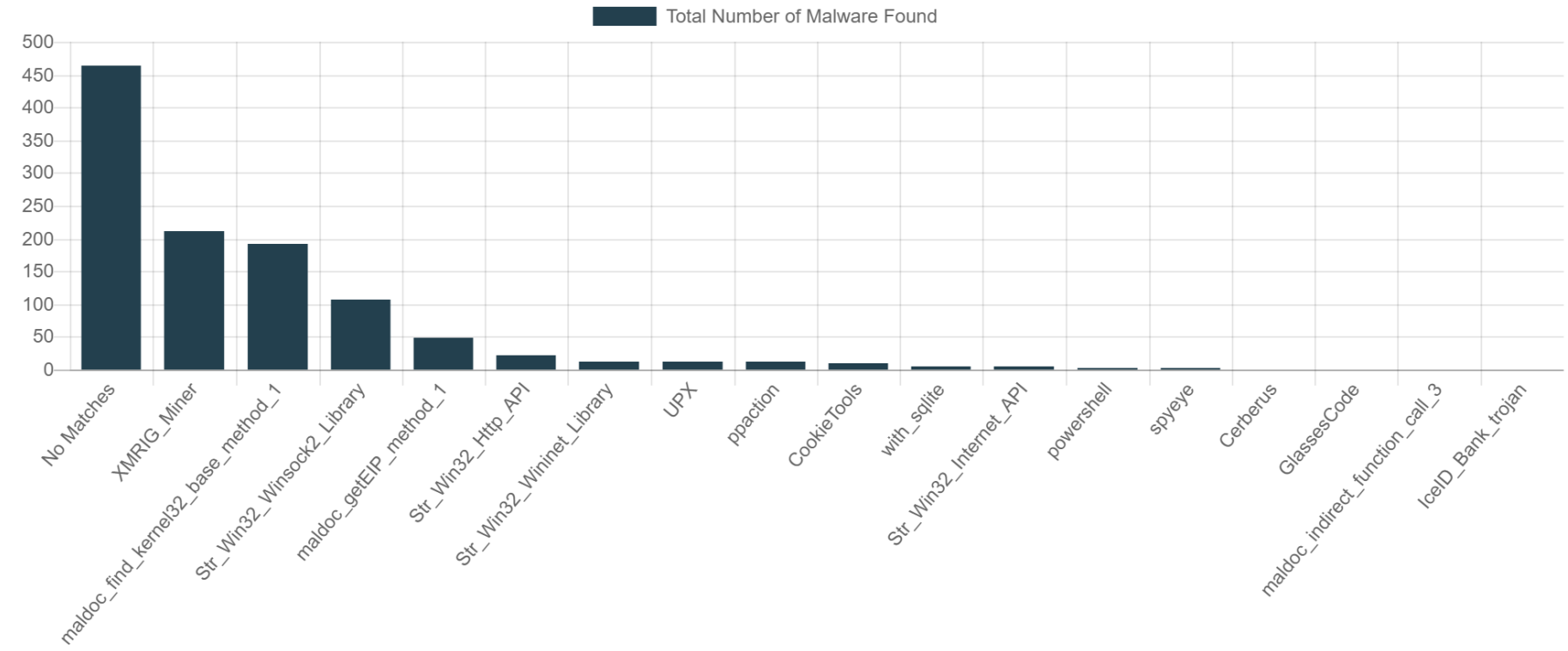
- Efficiently analyze different types of malware
- Cluster similar malware
- Provide dashboard for malware analysis data
- Provide framework for signature generation

System Architecture



Bar Graph on Dashboard

Dashboard



Filtered Results for Table

Analyzed Malware

Show 50 entries

Search: XMRIG_Miner

SID	File Name	File Type	Flagged?	YARA Match
1	C6A13AFC5831096B0CCB54FBB2B3D14E4BA06E9C7A363C884B1383C5EE81FAA	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows	No	XMRIG_Miner
8	48678EC33D22C571774ACE303C4C771B46C8121FBE46AFA807E54787671DE13	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows	No	XMRIG_Miner

In Depth Analysis of a File

In-Depth Analysis of 6BDE693CE8EB45445C0B38E3DE3AF97E0D21C8D33E8408B52E711EA67ABFD27

File Statistics and Information

File Information	Statistic Information
File Extension	PE32+ executable (console) x86-64, for MS Windows
File Size	330.8 KB (330752 bytes)
Total Analysis Time	0:00:00.286
Static Analysis Time	0:00:00.286
Dynamic Analysis Time	00:00:00

File Hashes

Hash Types	File Hash
PE Hash	3:N9K8gKRTEJ3HXKTn2QhgER4QmNWdtTqoEqhRYR+Ngk7n4R:N7TENXbQTR45iTqolhR8+yF
SHA256	6BDE693CE8EB45445C0B38E3DE3AF97E0D21C8D33E8408B52E711EA67ABFD274
SHA1	8200F58FC04B9731F20EB436E7D9C29ABB74D676
MD5	08C8682AB609AB30F189EC06EEE3CBD3

Similar Malware

File Name	PE Hash
517E899D1F9EB8656F3683E9216C904BD1061E0DFB26308C1A4E35ABB913167	3:N9K8gKRTEJ3HXKQLxchQndTGz6VXU55VtDSdmUkRgWQkMKSR:N7TENXL1HRPXsOmm1JR
4E33D223ED5CC0ADEE5612589A3AB69720321CFF9335F627430E2C73E9833E4	3:N9K8gKRTEJ3HXKRqHnhzQTUXhfkQnXUmjjnWQvXSRWVg26cPUn:N7TENX7HhzGOhVPjTWQtK238n
695C7B02EB9F73BB5E736C7088693D013CD84CE5F778CAF9F93537739427178	3:N9K8gKRTEJ3HXKThlnVXgSSWn1ITHQWlt/SIQWSS1XSUSVn:N7TENXvg1ljyMGCUSVn

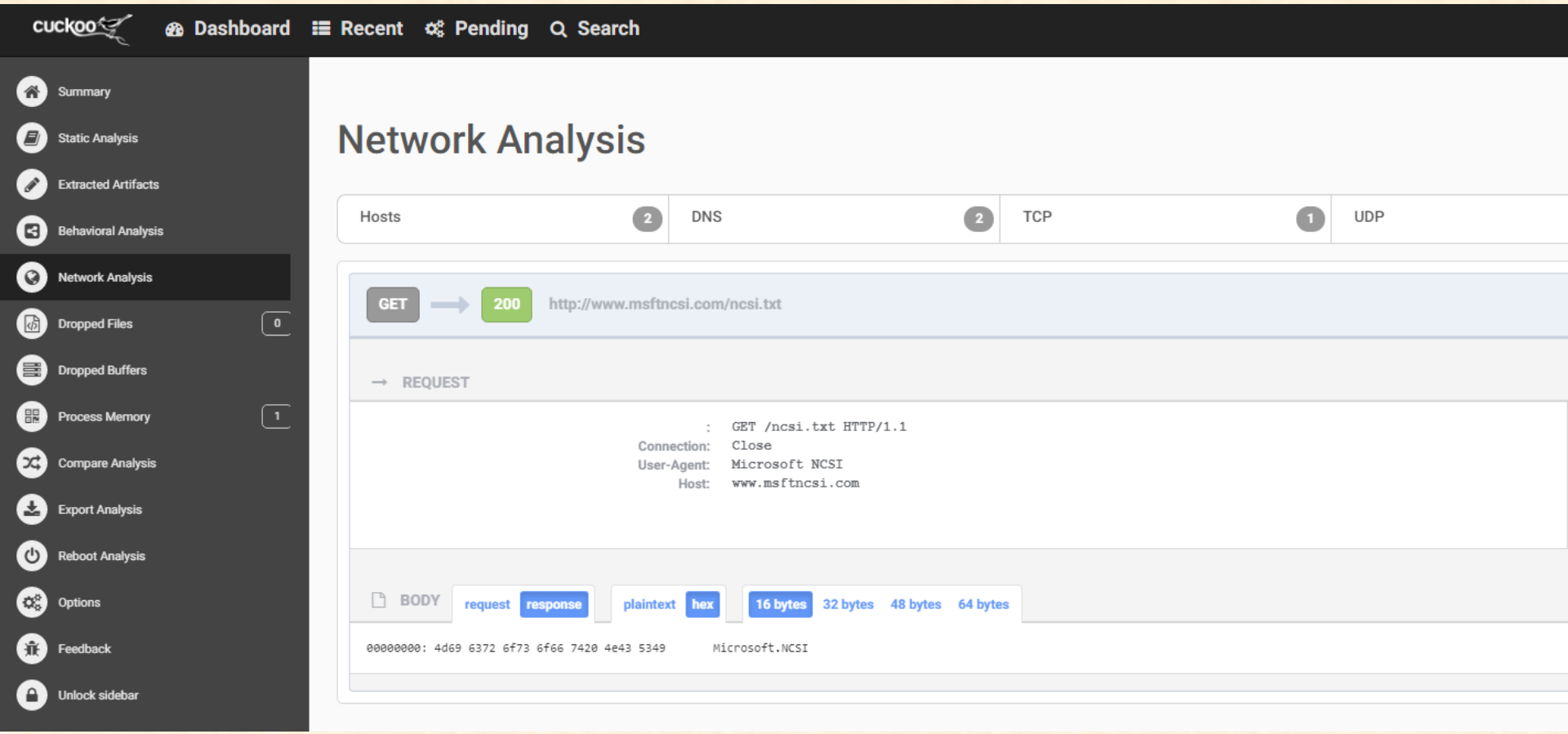
Similar Malware to a File

Similar Malware

File Name	PE Hash
517E899D1F9EB8656F3683E9216C904BD1061E0DFB26308C1A4E35ABB913167	3:N9K8gKRTEJ3HXKQLxchQndTGz6VXU55VtDSdmUkRgWQkMKSR:N7TENXL1HRPXsOmm1JR
4E33D223ED5CC0ADEE5612589A3AB69720321CFF9335F627430E2C73E9833E4	3:N9K8gKRTEJ3HXKRqHnhzQTUXhfkQnXUmjjnWQvXSRWVg26cPUn:N7TENX7HhzGOhVPjTWQtK238n
695C7B02EB9F73BB5E736C7088693D013CD84CE5F778CAF9F93537739427178	3:N9K8gKRTEJ3HXKThlnVXgSSWn1lTHQWIt/SIQWSS1XSUSVn:N7TENXvg1ljyMGCUSVn
1564EB85D5375925DDF81B7B879756B586B12C75DD902B02081BE0F6A03333C	3:N9K8gKRTEJ3HXKUG+QBSJEhhU7cSQEdTncQhhkX3ggJIWTd:N7TENXPG+4gEhkjQERnc0heQg1Td
0A33AC9B6EB9B66AC8366B3335AC18E923B354D3156A516124E95CBDD244938	3:N9K8gKRTEJ3HXKVfjmWG/tTTlk2mWnWQRAUQoQvRuQhn/W:N7TENXpWgFlk2hBxQ1Ru6/W

PE Hash
3:N9K8gKRTEJ3HXKQLxchQndTGz6VXU55VtDSdmUkRgWQkMKSR:N7TENXL1HRPXsOmm1JR
3:N9K8gKRTEJ3HXKRqHnhzQTUXhfkQnXUmjjnWQvXSRWVg26cPUn:N7TENX7HhzGOhVPjTWQtK238n
3:N9K8gKRTEJ3HXKThlnVXgSSWn1lTHQWIt/SIQWSS1XSUSVn:N7TENXvg1ljyMGCUSVn

Cuckoo Webpage



What's left to do?

- Dynamic analysis decision logic
- Automated signature generation
- Develop more robust clustering
- Automate Cuckoo node generation
- Seamlessly integrate Cuckoo web interface with ours
- Finalize website functionality and design

Questions?