MICHIGAN STATE UNIVERSITY

Beta Presentation

Improved Detonation of Evasive Malware

The Capstone Experience

Team Proofpoint

Kyutae Park
Ian Murray
Sean Joseph
Jack Mansueti
Ryan Gallant

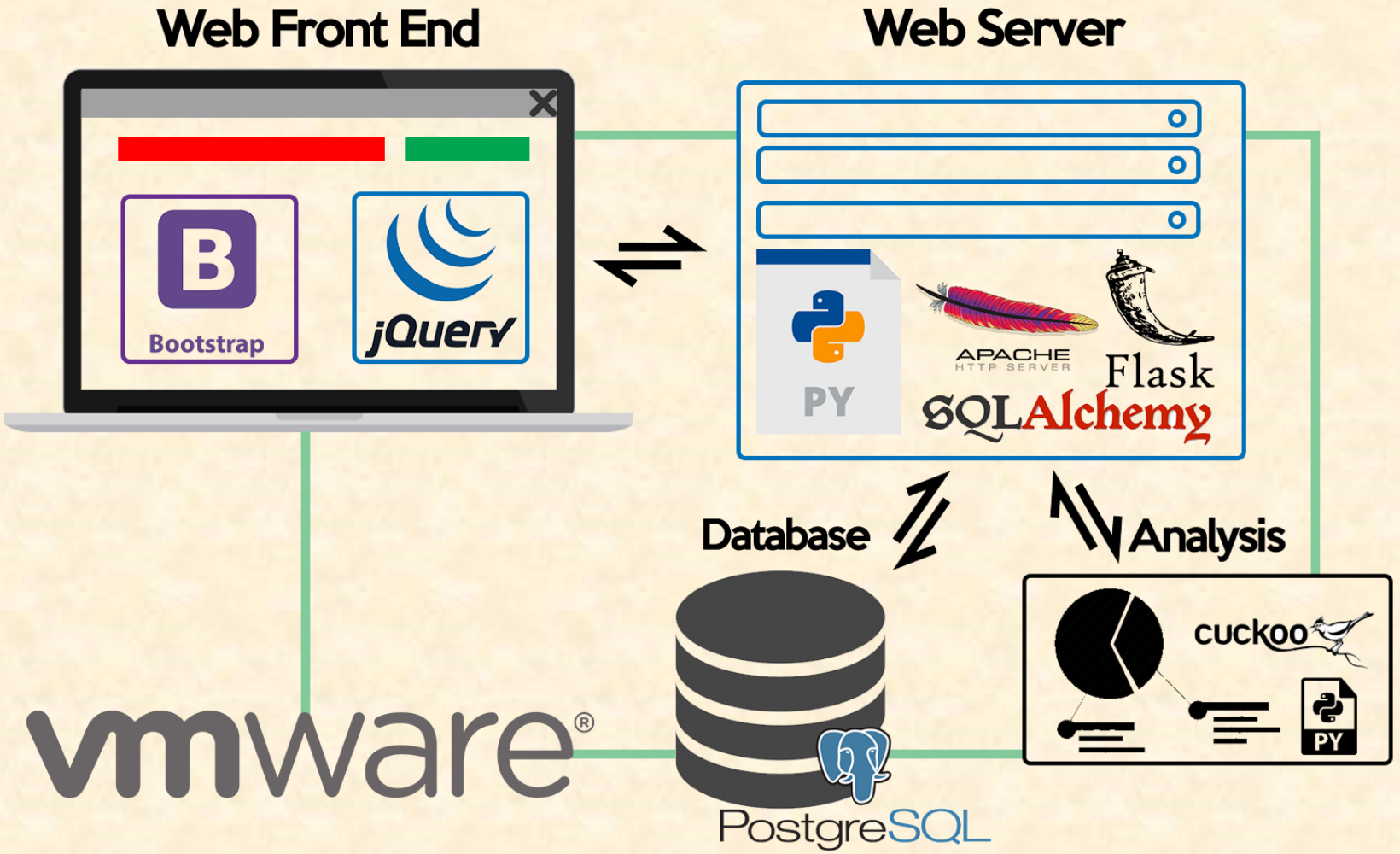
From Students…
…to Professionals

Department of Computer Science and Engineering
Michigan State University
Fall 2018

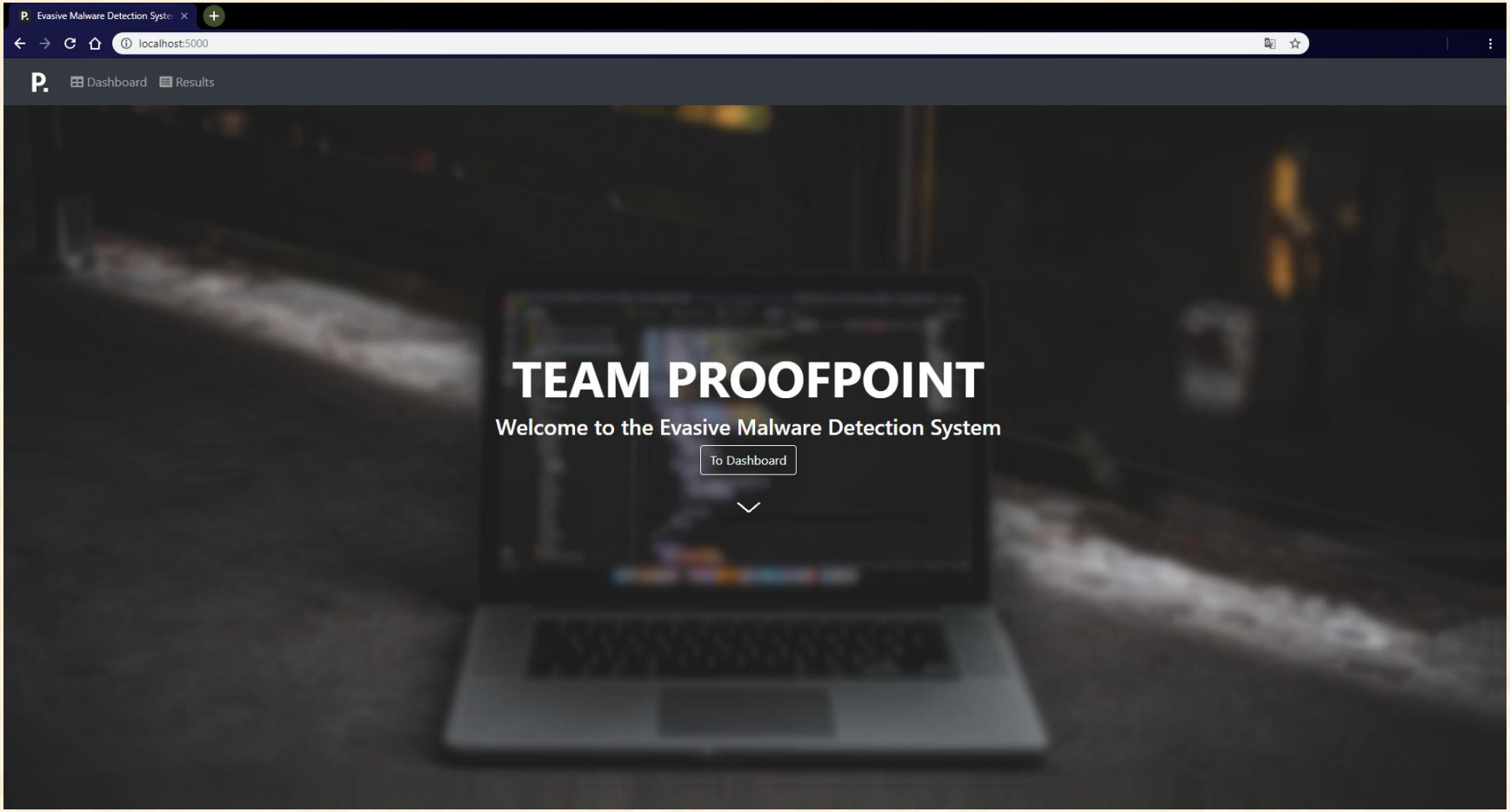
Project Overview

- Malware sample is submitted into Cuckoo
- Cuckoo runs malware sample
- If sample shows signs of evasive behavior, the sample is modified and submitted again
- Cuckoo sends results of resubmission to dashboard

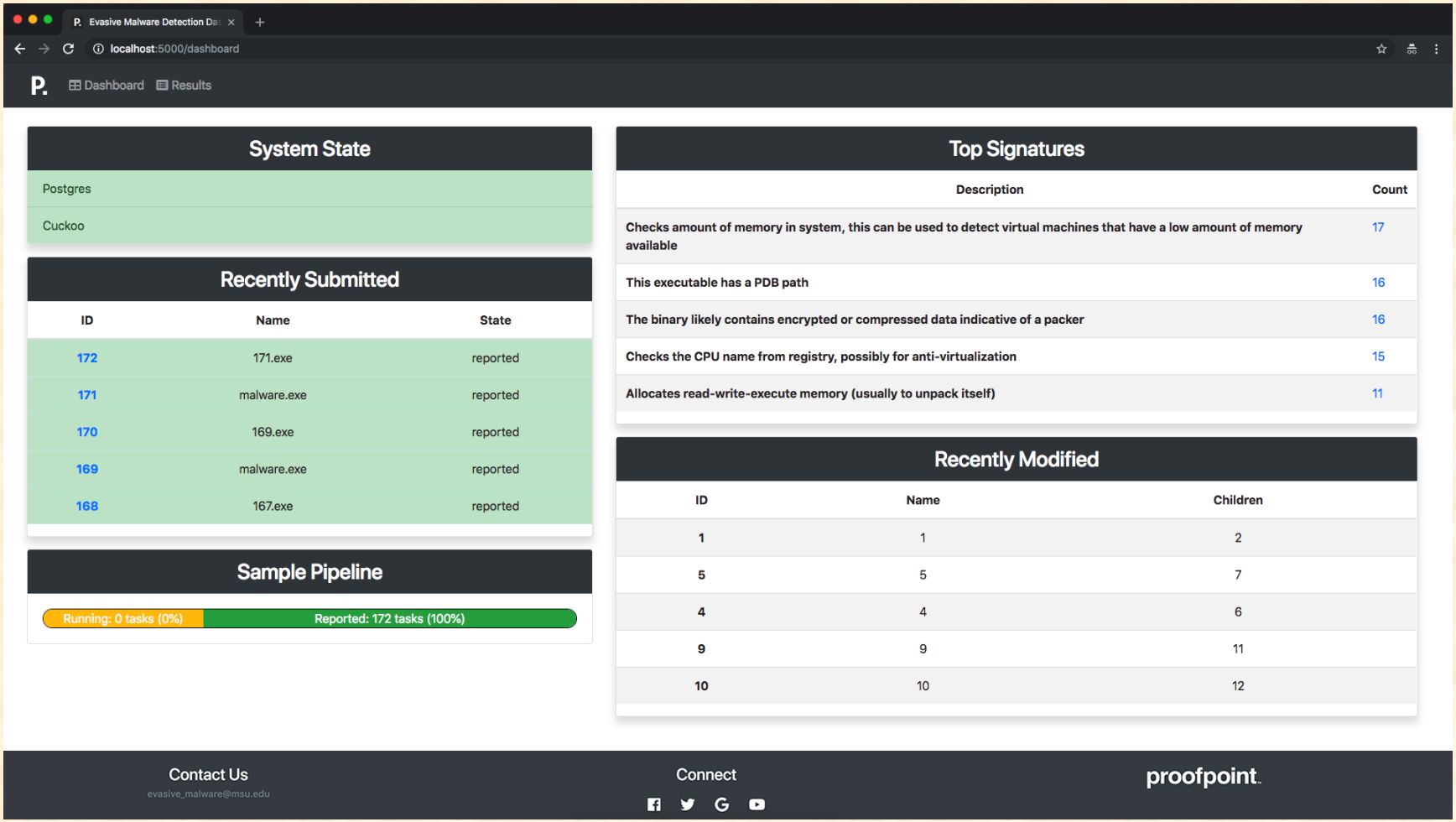
System Architecture



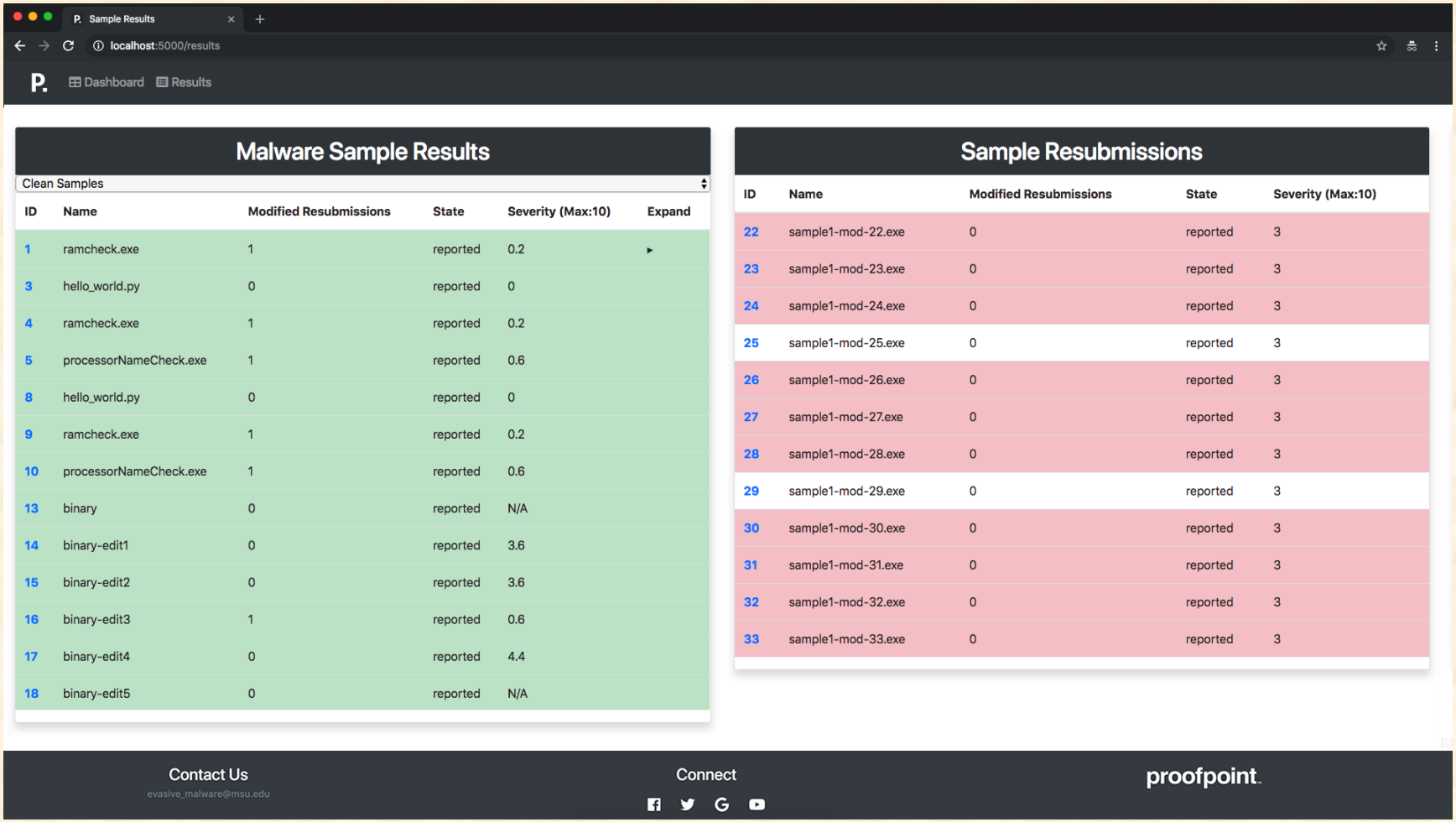
Landing Page



Dashboard


Evasive Malware Detection Da
localhost:5000/dashboard
P.
Dashboard
Results
System State
Postgres
Cuckoo
Recently Submitted
ID
Name
State
172
171.exe
reported
171
malware.exe
reported
170
169.exe
reported
169
malware.exe
reported
168
167.exe
reported
Sample Pipeline
Running: 0 tasks (0%)
Reported: 172 tasks (100%)
Top Signatures
Description
Count
Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available
17
This executable has a PDB path
16
The binary likely contains encrypted or compressed data indicative of a packer
16
Checks the CPU name from registry, possibly for anti-virtualization
15
Allocates read-write-execute memory (usually to unpack itself)
11
Recently Modified
ID
Name
Children
1
1
2
5
5
7
4
4
6
9
9
11
10
10
12
Contact Us
evasive_malware@msu.edu
Connect
proofpoint.

Results


Sample Results
localhost:5000/results
P.
Dashboard
Results
Malware Sample Results
Clean Samples
ID Name Modified Resubmissions State Severity (Max:10) Expand
1 ramcheck.exe 1 reported 0.2
3 hello_world.py 0 reported 0
4 ramcheck.exe 1 reported 0.2
5 processorNameCheck.exe 1 reported 0.6
8 hello_world.py 0 reported 0
9 ramcheck.exe 1 reported 0.2
10 processorNameCheck.exe 1 reported 0.6
13 binary 0 reported N/A
14 binary-edit1 0 reported 3.6
15 binary-edit2 0 reported 3.6
16 binary-edit3 1 reported 0.6
17 binary-edit4 0 reported 4.4
18 binary-edit5 0 reported N/A
Sample Resubmissions
ID Name Modified Resubmissions State Severity (Max:10)
22 sample1-mod-22.exe 0 reported 3
23 sample1-mod-23.exe 0 reported 3
24 sample1-mod-24.exe 0 reported 3
25 sample1-mod-25.exe 0 reported 3
26 sample1-mod-26.exe 0 reported 3
27 sample1-mod-27.exe 0 reported 3
28 sample1-mod-28.exe 0 reported 3
29 sample1-mod-29.exe 0 reported 3
30 sample1-mod-30.exe 0 reported 3
31 sample1-mod-31.exe 0 reported 3
32 sample1-mod-32.exe 0 reported 3
33 sample1-mod-33.exe 0 reported 3
Contact Us
evasive_malware@msu.edu
Connect
proofpoint.

Modification in Progress

```
teamproofpoint@CuckooNode1:~/evasive-malware-analysis/executable_modifier$ python detonator.py 205
['detonator.py', '205']
*******!!!!!!********Working on Sample 205***************
        ---Creating Assembly File---
        ---Compiling Behaviors---
        *****Working on Behavior GetDiskFreeSpaceExW: 1 of 11*****
                ---Locating Memory Addresses to Change---
                ---Evasive Behavior not Found---
        *****Working on Behavior GetComputerNameExW: 2 of 11*****
                ---Locating Memory Addresses to Change---
                ---Evasive Behavior not Found---
        *****Working on Behavior EnumServicesStatusW: 3 of 11*****
                ---Locating Memory Addresses to Change---
                ---Evasive Behavior not Found---
        *****Working on Behavior ProcessSleepNTime: 4 of 11*****
                ---Locating Memory Addresses to Change---
                ---Evasive Behavior not Found---
        *****Working on Behavior GetPhysciallyInstalledSystemMemory: 5 of 11*****
                ---Locating Memory Addresses to Change---
                ---Evasive Behavior not Found---
        *****Working on Behavior RegQueryValue: 6 of 11*****
                ---Locating Memory Addresses to Change---
                ---Evasive Behavior not Found---
        *****Working on Behavior NTWAllocateVirtualMemory: 7 of 11*****
                ---Locating Memory Addresses to Change---
                ---Evasive Behavior not Found---
        *****Working on Behavior GetAdaptersAddress: 8 of 11*****
                ---Locating Memory Addresses to Change---
                ***Modifying Code***
        *****Working on Behavior NtQuerySystemInformation: 9 of 11*****
                ---Locating Memory Addresses to Change---
                ---Evasive Behavior not Found---
        *****Working on Behavior GetSystemFirmwareTable: 10 of 11*****
                ---Locating Memory Addresses to Change---
                ***Modifying Code***
        *****Working on Behavior GlobalMemoryStatusEx: 11 of 11*****
                ---Locating Memory Addresses to Change---
                ---Evasive Behavior not Found---
********************Done********************
/home/teamproofpoint/.cuckoo/storage/modifiedExes/205.exe
```

What's left to do?

- Integration with Proofpoint's malware input stream
- Improved Detonation with Complex Samples
- Programmatically change algorithms for samples based on analysis

Questions?