

Detection of Ransomware using Immutable Anomalous Performance Data

Rajendra Boppana
Kumar Thummapudi (Student)
Palden Lama, Gregory White

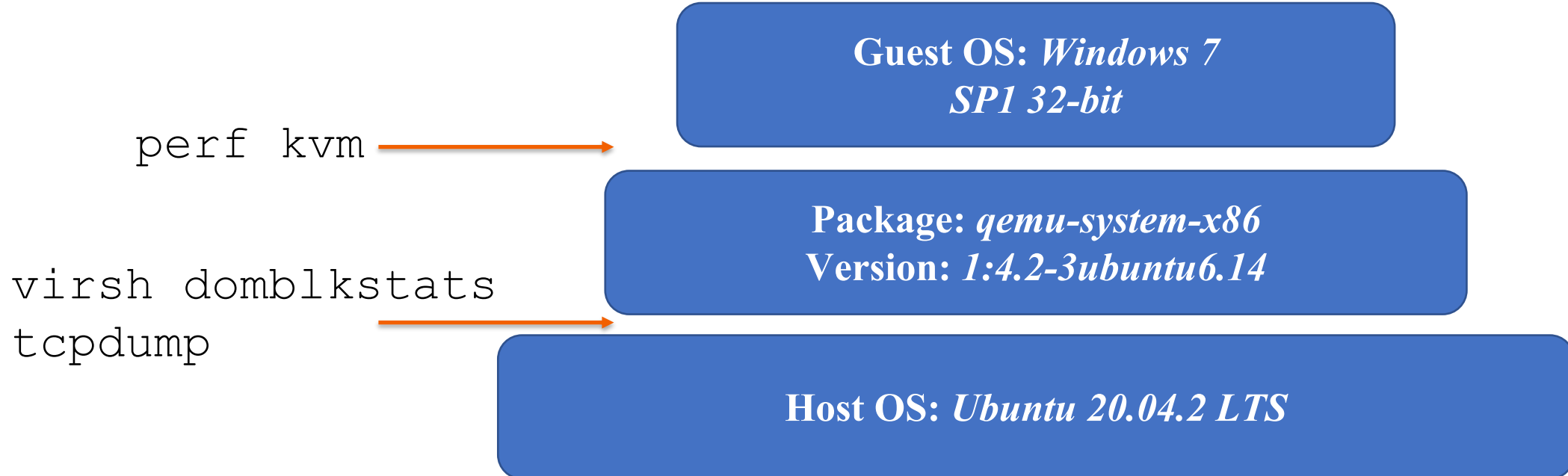


[MONITOR ACTIVATES]

Experimental Setup and Data Collection

Experimental Setup

- Chameleon cloud at TACC: a Chameleon node is configured for experiments



perf

- `sudo perf kvm stat -I <interval_in_msecs>
--interval-count <no_of_intervals>
-o <write_output_to_file> --append
-e <list_of_events_comma_separated>`
- Stats were collected for about 1 minute
 - 100 ms sampling interval $\Rightarrow$ 600 samples
 - 1 ms sampling interval $\Rightarrow$ 60,000 samples
- Up to four events of interest + instructions

Hardware Performance Counter Events

Events	Events	Events
Cycles	Instructions	Branches
Branch-misses	Mem-stores	L1-dcache-loads
L1-dcache-load-misses	L1-icache-load-misses	LLC-loads
LLC-load-misses	dTLB-loads	dTLB-load-misses
iTLB-loads	iTLB-load-misses	CPU-clock
Context-switches	Page-faults	Mem-loads

perf Raw Data

```
# started on Fri Jan 15 02:25:56 2021
```

#	time	counts	unit	events		
	0.106274293	318,119,958		instructions		
	0.106274293	117,426,826		L1-dcache-loads		
	0.106274293	1,921,114		L1-dcache-load-misses	#	1.64% of all L1-dcache hits
	0.106274293	451		context-switches		
	0.212214660	1,158,977		instructions		
	0.212214660	476,369		L1-dcache-loads		
	0.212214660	70,048		L1-dcache-load-misses	#	0.12% of all L1-dcache hits
	0.212214660	253		context-switches		
	0.318276587	2,275,197		instructions		
	0.318276587	874,941		L1-dcache-loads		
	0.318276587	94,930		L1-dcache-load-misses	#	0.24% of all L1-dcache hits
	0.318276587	246		context-switches		
	0.424265273	1,013,470		instructions		
	0.424265273	423,016		L1-dcache-loads		
	0.424265273	63,970		L1-dcache-load-misses	#	0.21% of all L1-dcache hits
	0.424265273	229		context-switches		
	0.530226164	237,117,650		instructions		
	0.530226164	84,987,565		L1-dcache-loads		

perf Data Reformatted

...4.109.79	...s — -bash ...	...— -bash	...a — -bash ...	...— -bash ...	...a — -bash ...	...a — -bash ...
instructions,L1-icache-load-misses,dTLB-load-misses,branch-misses,iTLB-load-misses						
205940	33951	2307	2525	2031		
0	0	0	0	0		
721071	20182	3515	3723	3112		
129234	19057	1810	2288	1025		
0	0	0	0	0		
1113885	36209	3855	6103	4484		
935598	11827	1281	2613	685		
1510712	6680	770	994	280		
0	0	0	0	0		
1676139	14476	1736	2604	1582		
1977447	4086	846	717	412		
99678	9259	515	1272	416		
1118104	14501	1566	2476	1851		
1967547	10765	1420	1968	588		
3623577	11653	1933	2315	1844		
854466	29191	4295	5384	5232		

domblkstat

```
for ( ( j = 1; j <= 3000; j++ ) )  
do  
    date >> domblkstats  
    virsh domblkstat Win7KVM >> domblkstats  
    echo >> domblkstats  
done
```

Disk Memory Subsystem Events

Events	Events	Events
rd_req	wr_req	flush_operations
rd_bytes	wr_bytes	
rd_total_times	wr_total_times	flush_total_times

dombldstat Raw Data

Fri 15 Jan 2021 02:25:56 AM UTC

Readings before start of 03bb4d5c0179fdceacc5df7645e6e7fa93e931ac9beb1968c7bbe40ba3499194.exe

rd_req 5631044

rd_bytes 208307542016

wr_req 12565984

wr_bytes 1398550276096

flush_operations 57891

rd_total_times 84024961512087

wr_total_times 217260993681892

flush_total_times 3056746313763

Fri 15 Jan 2021 02:25:56 AM UTC

rd_req 5631064

rd_bytes 208308118528

wr_req 12565984

wr_bytes 1398550276096

flush_operations 57891

rd_total_times 84024964295807

wr_total_times 217260993681892

flush_total_times 3056746313763

dombblkstat Data Reformatted

```
...4.109.79    ...s — -bash ...    ...— -bash    ...a — -bash ...    ...— -bash ...    ...a — -bash ...    ...a — -bash ...    ...s — -bash ...    ...—  
wr_total_times,wr_req,rd_req,flush_total_times,rd_total_times,rd_bytes,flush_operations,wr_bytes  
43230405,60,4,20045227,2874432,20480,2,3573760  
18499650,10,0,1373147,0,0,3,53760  
0,0,0,0,0,0,0,0  
622063648,20,0,3574910,0,0,2,107008  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0  
0,0,5,0,508748,135168,0,0  
0,0,8,0,425161,221184,0,0  
0,0,3,0,331244,94208,0,0  
0,0,2,0,114098,40960,0,0  
0,0,0,0,0,0,0,0  
0,0,0,0,0,0,0,0
```

Significant Events

- Identify events that give better prediction accuracy
 - Fisher scoring
 - sklearn feature_selection RFECV
- Significant processor events (hardware limit: 4)
 - L1-icache-load-misses
 - branch-misses
 - dTLB-load-misses
 - iTLB-load-misses

Events Sampled

- Processor events:
 - L1-icache-load-misses
 - branch-misses
 - dTLB-load-misses
 - iTLB-load-misses
 - Instructions (provided by perf)
- All 8 disk stats
- Network traffic

Machine Learning (ML) Models

- Support vector machine (SVM)
- Random forest (RF)
- K-nearest neighbors (KNN)
- Decision tree (DT)

Analysis Modes

- One event at a time
- Combined: all events together
 - Scales: Min-max, Max-abs, **no-scale**

Features

March 2021

- t samples = 1 instance
- k sub-instances
- Mean, std. dev. and freq-domain counter parts for each sub-instance
- $4k$ features per processor event
- $4kn$ if n events are combined

Features (2)

August 2021

- 100 samples = 1 instance
- Mean, standard deviation for each event
- $2n$ features if n events are combined
- Variations:
 - mean, fft
 - median, fft
 - median, semi-interquartile range

Target Machine States

- No background load
- Background load:
 - web browser
 - video player
 - Microsoft Office documents

Benign Applications

- Secure delete (sDel)
- AES encrypt/decrypt (aesCrypt)
- File compression (7zip)
- None (DryR)

22 Ransoms (source: virusshare.com)

File Name	Family (MalwareBytes)	Family (Microsoft)
03bb4d5c0179fdceacc5df7645e6e7fa93e931ac9beb1968c7bbe40ba3499194	Ransom.Phobos	Ransom:Win32/Phobos.SW!MSR
0a937d4fe8aa6cb947b95841c490d73e452a3cafd92645afc353006786aba76	Ransom.LockBit	Ransom:Win32/LockBit.PA!MTB
133bf8be0cf7003b83b03579970997d408a930e58ec2726715140520900c06de	Ransom.Sodinokibi	Ransom:Win32/Revil.SI!MTB
17d153a225ea04a229862875795eeec0adb8c3e2769ba0e05073baaf86850467	Ransom.Sodinokibi	Ransom:Win32/Revil.SI!MTB
3cff3197edc918d47d08f44d6dbdda157337f0ad58288d15746cf72c0e4c57	Ransom.Sodinokibi	Ransom:Win32/Revil.SI!MTB
3fdad99a17a6766fe396081f82394f5e2da0142651427da64a5b6e28c9df2fd4	Ransom.Sodinokibi	Ransom:Win32/Sodinokibi.C
42c28feb23c992a350673d63413bf11bc816d00a079462ab524934219d46430d	Ransom.Sodinokibi	Ransom:Win32/Sodinokibi.DSB!MTB
4e2554b448424859b508433e6c4a043718343febc7894a849f446dd197b47d1e	Ransom.Maze	Ransom:Win32/Maze.PA!MTB
4f7bdda79e389d6660fca8e2a90a175307a7f615fa7673b10ee820d9300b5c60	Ransom.NetWalker	Ransom:Win32/Filecoder.DD!MTB
57cf4470348e3b5da0fa3152be84a81a5e2ce5d794976387be290f528fa419fd	Ransom.NetWalker	Ransom:Win32/NetWalker!MSR
5cba3e44271279e747a67dd312d4dca18832b5a850ea6b85a460846ef0101fb6	Ransom.Sodinokibi	Undetected
5d9b75e2cb84333c6b56604ce47af75b11f80bf9079054f6619251b68357d87c	Ransom.Sodinokibi	Trojan:Win32/Occamy.C
6628de7ffbbe168a4fa9ff0a1a29b54e88a32e5963db0dd1aea4b80102c8ce01	Ransom.Sodinokibi	Ransom:Win32/Revil.SI!MTB
7c2dbad516d18d2c1c21ecc5792bc232f7b34dadcb1bc19e967190d79174131d1	Ransom.DeathRansom	Undetected
7d98972d5c78e1d4969da76856d6818942b606c267efa67fd31d39ae77497e9c	Ransom.Rapid	Ransom:Win32/Robinhood.AR!MTB
7faeb64c50cd15d036ca259a047d6c62ed491ff3729433feffa0b02c059d5ed	Ransom.Ryuk	Ransom:Win32/Sodinokibi.AD!MTB
81689f1be92c8fb7e94fe241441c7eb43cfb77c6d23592b0248566bd709ff2ed	---	Ransom:Win32/Revil.SI!MTB
d6b7b27e13700aaa7f108bf9e76473717a7a1665198e9aafc2d2227ca11bba9	Ransom.Ryuk	Ransom:Win32/Ruyk.A!ibt
e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79fc3eb42f34588bc684	Malware.AI.4262356839	Ransom:Win32/Maze
ecfb5c95d0f3d112650ef4047936e8fa5244c21c921fc7a6963e92abab4949d	Ransom.FileCryptor	Ransom:MSIL/Kelnoc.A
f2c9ae3735430b930a81148c0bb470fcb733e456a2a942f859a1b59c4a7b2150	Malware.AI.2057448532	Ransom:Win32/Locky.A
fd32cec288cec4f16dc5430cf86dc17e1d4c941d635979fc17a59c8d6d83d44	Ransom.PovIsomware	Ransom:MSIL/RnToad.SL!MTB

Benign App Experiments

- Each benign app
 - 65 rounds without background load
 - 65 rounds with background load
 - Each round: 60,000 samples of 5 hardware counter events

$$65 \times 2 \times 4 = 520 \text{ rounds}$$

Ransomware Experiments

- Each ransomware (RW)
 - 25 rounds without background load
 - 25 rounds with background load
 - Each round: 60,000 samples of 5 hardware counter events

$$25 \times 2 \times 22 = 1100 \text{ rounds}$$

Analysis

- Benign: 500 rounds out of 520 at random
- RW: 500 rounds out of 1100 at random
- 30,000 samples per round
- 200 samples/instance
- 80:20 training-testing split
- Random forest model
- 51 repetitions

Case I: Train with 11 RW, Test with 11 other RW

03bb4d5c0179fdceacc5df7645e6e7fa93e931ac9beb1968c7bbe40ba3499194	Ransom.Phobos
0a937d4fe8aa6cb947b95841c490d73e452a3cafc92645afc353006786aba76	Ransom.LockBit
133bf8be0cf7003b83b03579970997d408a930e58ec2726715140520900c06de	Ransom.Sodinokibi
17d153a225ea04a229862875795eeec0adb8c3e2769ba0e05073baaf86850467	
3cff3197edc918d47d08f44d6ddbda157337f0ad58288d15746cf72c0e4c57	
3fdad99a17a6766fe396081f82394f5e2da0142651427da64a5b6e28c9df2fd4	
42c28feb23c992a350673d63413bf11bc816d00a079462ab524934219d46430d	
5cba3e44271279e747a67dd312d4dca18832b5a850ea6b85a460846ef0101fb6	
5d9b75e2cb84333c6b56604ce47af75b11f80bf9079054f6619251b68357d87c	
6628de7ffbbe168a4fa9ffa1a29b54e88a32e5963db0dd1aea4b80102c8ce01	
4e2554b448424859b508433e6c4a043718343febc7894a849f446dd197b47d1e	Ransom.Maze
4f7bdda79e389d6660fca8e2a90a175307a7f615fa7673b10ee820d9300b5c60	Ransom.NetWalker
57cf4470348e3b5da0fa3152be84a81a5e2ce5d794976387be290f528fa419fd	Ransom.DeathRansom
7c2dbad516d18d2c1c21ecc5792bc232f7b34dad1bc19e967190d79174131d1	
7d98972d5c78e1d4969da76856d6818942b606c267efa67fd31d39ae77497e9c	Ransom.Rapid
7faeb64c50cd15d036ca259a047d6c62ed491ff3729433feba0b02c059d5ed	Ransom.Ryuk
d6b7b27e13700aaa7f108bf9e76473717a7a1665198e9aafc2d2227ca11bba9	
e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684	Malware.AI.4262356839
f2c9ae3735430b930a81148c0bb470fcb733e456a2a942f859a1b59c4a7b2150	Malware.AI.2057448532
ecfb5c95d0f3d112650ef4047936e8fa5244c21c921f6c7a6963e92abab4949d	Ransom.FileCryptor
fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44	Ransom.Povlsomware
81689f1be92c8fb7e94fe241441c7eb43cfb77c6d23592b0248566bd709ff2ed	---

Case II: Train and Test all 22 RW

File Name	Family (MalwareBytes)
03bb4d5c0179fdceacc5df7645e6e7fa93e931ac9beb1968c7bbe40ba3499194	Ransom.Phobos
0a937d4fe8aa6cb947b95841c490d73e452a3cafc92645afc353006786aba76	Ransom.LockBit
133bf8be0cf7003b83b03579970997d408a930e58ec2726715140520900c06de	Ransom.Sodinokibi
17d153a225ea04a229862875795eeec0adb8c3e2769ba0e05073baaf86850467	Ransom.Sodinokibi
3cff3197edc918d47d08f44d6ddbdda157337f0ad58288d15746cf72c0e4c57	Ransom.Sodinokibi
3fdad99a17a6766fe396081f82394f5e2da0142651427da64a5b6e28c9df2fd4	Ransom.Sodinokibi
42c28feb23c992a350673d63413bf11bc816d00a079462ab524934219d46430d	Ransom.Sodinokibi
4e2554b448424859b508433e6c4a043718343febcb7894a849f446dd197b47d1e	Ransom.Maze
4f7bdda79e389d6660fca8e2a90a175307a7f615fa7673b10ee820d9300b5c60	Ransom.NetWalker
57cf4470348e3b5da0fa3152be84a81a5e2ce5d794976387be290f528fa419fd	Ransom.NetWalker
5cba3e44271279e747a67dd312d4dca18832b5a850ea6b85a460846ef0101fb6	Ransom.Sodinokibi
5d9b75e2cb84333c6b56604ce47af75b11f80bf9079054f6619251b68357d87c	Ransom.Sodinokibi
6628de7ffbbe168a4fa9ff0a1a29b54e88a32e5963db0dd1aea4b80102c8ce01	Ransom.Sodinokibi
7c2dbad516d18d2c1c21ecc5792bc232f7b34dadcb1bc19e967190d79174131d1	Ransom.DeathRansom
7d98972d5c78e1d4969da76856d6818942b606c267efa67fd31d39ae77497e9c	Ransom.Rapid
7faeb64c50cd15d036ca259a047d6c62ed491fffb729433feffa0b02c059d5ed	Ransom.Ryuk
81689f1be92c8fb7e94fe241441c7eb43cfb77c6d23592b0248566bd709ff2ed	---
d6b7b27e13700aaa7f108bf9e76473717a7a1665198e9aafcc2d2227ca11bba9	Ransom.Ryuk
e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684	Malware.AI.4262356839
ecfb5c95d0f3d112650ef4047936e8fa5244c21c921f6c7a6963e92abab4949d	Ransom.FileCryptor
f2c9ae3735430b930a81148c0bb470fcb733e456a2a942f859a1b59c4a7b2150	Malware.AI.2057448532
fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44	Ransom.Povlsomware

Case I Results: Average of 51 Repetitions

	Acc	fpr	fnr
L1-icache-load-misses	0.729392	0.203824	0.337412
branch-misses	0.704353	0.241176	0.350098
dTLB-load-misses	0.703235	0.247961	0.345608
iTLB-load-misses	0.754373	0.198157	0.293216
instructions	0.721529	0.180588	0.376314
combined-noscale	0.875784	0.0292157	0.219235

Case II Results: Average of 51 Repetitions

	Acc	fpr	fnr
L1-icache-load-misses	0.757627	0.228137	0.256569
branch-misses	0.748294	0.255392	0.24798
dTLB-load-misses	0.727549	0.263412	0.281392
iTLB-load-misses	0.774824	0.212686	0.237569
instructions	0.783627	0.207235	0.225529
combined-noscale	0.946431	0.043098	0.0638824

Network Traffic Analysis

Network Traffic: SMB, NBNS, ARP Activity

Apply a display filter ... <96/>										
No.	Time	Source	Destination	Protocol	Length	SPort	DPort	RTO	Info	
146	2021-06-17 20:29:24.014204	192.168.122.235	192.168.122.255	BROW...	216	138	138		Get Backup List Request	
147	2021-06-17 20:29:24.014305	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1b>	
148	2021-06-17 20:29:24.754540	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1b>	
149	2021-06-17 20:29:25.510815	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1b>	
150	2021-06-17 20:29:27.255347	192.168.122.235	192.168.122.255	BROW...	216	138	138		Get Backup List Request	
151	2021-06-17 20:29:27.255440	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1b>	
152	2021-06-17 20:29:28.005159	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1b>	
153	2021-06-17 20:29:28.754726	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1b>	
154	2021-06-17 20:29:30.504578	192.168.122.235	192.168.122.255	BROW...	216	138	138		Get Backup List Request	
155	2021-06-17 20:29:30.504673	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1b>	
156	2021-06-17 20:29:31.257820	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1b>	
157	2021-06-17 20:29:32.004558	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1b>	
158	2021-06-17 20:29:33.754623	192.168.122.235	192.168.122.255	NBNS	92	137	137		Name query NB WORKGROUP<1e>	
159	2021-06-17 20:29:33.985561	RealtekU_00:a5...	Broadcast	ARP	42				Who has 192.168.122.254? Tell 192.168.122.235	
160	2021-06-17 20:29:33.986126	RealtekU_00:a5...	Broadcast	ARP	42				Who has 192.168.122.253? Tell 192.168.122.235	
161	2021-06-17 20:29:33.986258	RealtekU_00:a5...	Broadcast	ARP	42				Who has 192.168.122.252? Tell 192.168.122.235	
162	2021-06-17 20:29:33.986356	RealtekU_00:a5...	Broadcast	ARP	42				Who has 192.168.122.251? Tell 192.168.122.235	
163	2021-06-17 20:29:33.986469	RealtekU_00:a5...	Broadcast	ARP	42				Who has 192.168.122.250? Tell 192.168.122.235	
164	2021-06-17 20:29:33.986570	RealtekU_00:a5...	Broadcast	ARP	42				Who has 192.168.122.249? Tell 192.168.122.235	
165	2021-06-17 20:29:33.986690	RealtekU_00:a5...	Broadcast	ARP	42				Who has 192.168.122.248? Tell 192.168.122.235	
▶ Frame 159: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)				0000	ff ff ff ff ff ff 52 54	00 00	a5 dc 08 06 00 01	RT		
▶ Ethernet II, Src: RealtekU_00:a5:dc (52:54:00:00:a5:dc), Dst: Broad				0010	08 00 06 04 00 01 52 54	00 00	a5 dc c0 a8 7a eb	RTZ.		
▶ Address Resolution Protocol (ARP)				0020	00 00 00 00 00 00 c0 a8	7a fe		Z.		

Network Traffic: DNS Queries for Odd Domain Names

dns

Expression...

No.	Time	Source	Destination	Protocol	Length	SPort	DPort	Info													
165	2021-06-17 21:04:27.937225	192.168.122.235	192.168.122.1	DNS	72	51174	53	Standard query 0x71de A lcrjltaok.ru													
167	2021-06-17 21:04:28.623885	192.168.122.1	192.168.122.235	DNS	72	53	51174	Standard query response 0x71de No such name A lcrjltaok.r													
173	2021-06-17 21:04:30.600504	192.168.122.235	192.168.122.1	DNS	81	63530	53	Standard query 0x55d1 A spynet2.microsoft.com													
174	2021-06-17 21:04:30.635231	192.168.122.1	192.168.122.235	DNS	200	53	63530	Standard query response 0x55d1 A spynet2.microsoft.com CN													
185	2021-06-17 21:04:30.862938	192.168.122.235	192.168.122.1	DNS	82	57886	53	Standard query 0xb539 A utpjhsdhkteiaarc.click													
191	2021-06-17 21:04:31.128924	192.168.122.1	192.168.122.235	DNS	82	53	57886	Standard query response 0xb539 No such name A utpjhsdhkte													
205	2021-06-17 21:04:33.377094	192.168.122.235	192.168.122.1	DNS	76	56695	53	Standard query 0x5575 A xnsdhoteqewa.ru													
206	2021-06-17 21:04:33.932671	192.168.122.1	192.168.122.235	DNS	76	53	56695	Standard query response 0x5575 No such name A xnsdhoteqew													
207	2021-06-17 21:04:33.937668	192.168.122.235	192.168.122.1	DNS	78	61708	53	Standard query 0xac5d A eqcgycdrnffuxjf.su													
208	2021-06-17 21:04:34.415531	192.168.122.1	192.168.122.235	DNS	78	53	61708	Standard query response 0xac5d No such name A eqcgycdrnff													
209	2021-06-17 21:04:34.417723	192.168.122.235	192.168.122.1	DNS	71	53123	53	Standard query 0x997e A rhbsgve.xyz													
210	2021-06-17 21:04:34.578666	192.168.122.1	192.168.122.235	DNS	71	53	53123	Standard query response 0x997e No such name A rhbsgve.xyz													
216	2021-06-17 21:04:36.829995	192.168.122.235	192.168.122.1	DNS	80	65165	53	Standard query 0x959c A kywltldjwlpssywmq.pl													
217	2021-06-17 21:04:37.217030	192.168.122.1	192.168.122.235	DNS	80	53	65165	Standard query response 0x959c No such name A kywltldjwlp													
218	2021-06-17 21:04:37.218489	192.168.122.235	192.168.122.1	DNS	72	52026	53	Standard query 0x1132 A xphbenypf.pw													
219	2021-06-17 21:04:37.414585	192.168.122.1	192.168.122.235	DNS	72	53	52026	Standard query response 0x1132 No such name A xphbenypf.p													
227	2021-06-17 21:04:55.180732	192.168.122.235	192.168.122.1	DNS	79	52625	53	Standard query 0xe0e7 A etujxrennybylgk.su													
▶ Frame 165: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)				0000	52	54	00	2a	65	46	52	54	00	00	a5	dc	08	00	45	00	RT.*eFRTE.
▶ Ethernet II, Src: RealtekU_00:a5:dc (52:54:00:00:a5:dc), Dst: Realte				0010	00	3a	00	a8	00	00	80	11	c3	cd	c0	a8	7a	eb	c0	a8	z...
▶ Internet Protocol Version 4, Src: 192.168.122.235, Dst: 192.168.122.				0020	7a	01	c7	e6	00	35	00	26	1b	dd	71	de	01	00	00	01	z....5.& ..q....
▶ User Datagram Protocol, Src Port: 51174, Dst Port: 53				0030	00	00	00	00	00	00	09	6c	63	72	6a	6c	74	61	6f	6b	l crjltaok
▼ Domain Name System (query)				0040	02	72	75	00	00	01	00	01									.ru.....

[Response: 167]

Network Traffic: Spurious SYNs

tcp.flags.syn == 1 and ip.dst == 92.63.8.47										
No.	Time	Source	Destination	Protocol	Length	SPort	DPort	Info		
280	2021-06-17 21:01:05.293614	192.168.122.235	92.63.8.47	TCP	66	49165	80	49165 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_		
285	2021-06-17 21:01:08.295070	192.168.122.235	92.63.8.47	TCP	66	49165	80	[TCP Retransmission] 49165 → 80 [SYN] Seq=0 Win=8192 Len=0		
295	2021-06-17 21:01:14.308037	192.168.122.235	92.63.8.47	TCP	62	49165	80	[TCP Retransmission] 49165 → 80 [SYN] Seq=0 Win=8192 Len=0		
304	2021-06-17 21:01:27.024779	192.168.122.235	92.63.8.47	TCP	66	49166	80	49166 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_		
310	2021-06-17 21:01:30.026878	192.168.122.235	92.63.8.47	TCP	66	49166	80	[TCP Retransmission] 49166 → 80 [SYN] Seq=0 Win=8192 Len=0		
311	2021-06-17 21:01:36.042453	192.168.122.235	92.63.8.47	TCP	62	49166	80	[TCP Retransmission] 49166 → 80 [SYN] Seq=0 Win=8192 Len=0		
313	2021-06-17 21:01:46.886734	192.168.122.235	92.63.8.47	TCP	66	49167	80	49167 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_		
314	2021-06-17 21:01:48.042580	192.168.122.235	92.63.8.47	TCP	66	49168	80	49168 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_		
315	2021-06-17 21:01:49.901883	192.168.122.235	92.63.8.47	TCP	66	49167	80	[TCP Retransmission] 49167 → 80 [SYN] Seq=0 Win=8192 Len=0		
316	2021-06-17 21:01:51.042509	192.168.122.235	92.63.8.47	TCP	66	49168	80	[TCP Retransmission] 49168 → 80 [SYN] Seq=0 Win=8192 Len=0		

▶ Frame 280: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)	0000	52 54 00 2a 65 46 52 54	00 00 a5 dc 08 00 45 00	RT.*eFRTE.
▶ Ethernet II, Src: RealtekU_00:a5:dc (52:54:00:00:a5:dc), Dst: Realte	0010	00 34 00 e2 40 00 80 06	59 e0 c0 a8 7a eb 5c 3f	.4..@... Y...z.\?
▶ Internet Protocol Version 4, Src: 192.168.122.235, Dst: 92.63.8.47	0020	08 2f c0 0d 00 50 7d 21	e2 4c 00 00 00 00 80 02	./...P)! .L.....
▶ Transmission Control Protocol, Src Port: 49165, Dst Port: 80, Seq: 0	0030	20 00 8f 42 00 00 02 04	05 b4 01 03 03 08 01 01	..B....
	0040	04 02		..

Network Traffic: HTTP Posts with Error Response

http											Expression...										
No.	Time	Source	Destination	Protocol	Length	SPort	DPort	Info													
157	2021-06-17 21:04:27.792989	192.168.122.235	212.109.192.235	HTTP	1196	49164	80	POST /data/info.php HTTP/1.1 (application/x-www-form-urlencoded)													
161	2021-06-17 21:04:27.936161	212.109.192.235	192.168.122.235	HTTP	860	80	49164	HTTP/1.1 500 Internal Server Error (text/html)													
235	2021-06-17 21:04:55.570432	192.168.122.235	212.109.192.235	HTTP	1196	49166	80	POST /data/info.php HTTP/1.1 (application/x-www-form-urlencoded)													
238	2021-06-17 21:04:55.713650	212.109.192.235	192.168.122.235	HTTP	860	80	49166	HTTP/1.1 500 Internal Server Error (text/html)													
262	2021-06-17 21:05:15.229871	192.168.122.235	212.109.192.235	HTTP	1196	49167	80	POST /data/info.php HTTP/1.1 (application/x-www-form-urlencoded)													
265	2021-06-17 21:05:15.372820	212.109.192.235	192.168.122.235	HTTP	860	80	49167	HTTP/1.1 500 Internal Server Error (text/html)													
▶ Frame 157: 1196 bytes on wire (9568 bits), 1196 bytes captured (9568				0000	52	54	00	2a	65	46	52	54	00	00	a5	dc	08	00	45	00	RT.*eFRTE.
▶ Ethernet II, Src: RealtekU_00:a5:dc (52:54:00:00:a5:dc), Dst: Realte				0010	04	9e	00	a4	40	00	80	06	24	c9	c0	a8	7a	eb	d4	6d	@... \$...z..m
▶ Internet Protocol Version 4, Src: 192.168.122.235, Dst: 212.109.192.				0020	c0	eb	c0	0c	00	50	9a	30	97	db	78	34	a3	3b	50	18	P.0 ...x4.;P.
▶ Transmission Control Protocol, Src Port: 49164, Dst Port: 80, Seq: 4				0030	01	00	78	ae	00	00	66	4e	57	41	55	4a	79	3d	25	43	...x...fN WAUJy=%C
▶ [2 Reassembled TCP Segments (1623 bytes): #156(481), #157(1142)]				0040	35	25	46	33	25	32	42	25	33	45	25	46	42	25	46	35	5%F3%2B% 3E%FB%F5
▶ Hypertext Transfer Protocol				0050	25	46	31	25	35	43	4e	25	32	34	39	25	41	39	6d	25	%F1%5CN% 249%A9m%
▶ HTML Form URL Encoded: application/x-www-form-urlencoded				0060	44	45	25	43	45	25	33	42	36	36	25	32	31	25	32	33	DE%CE%3B 66%21%23
▶ Form item: "fNWAUJy" = "00+>000\Ns90m00;66!#0K0 E0 ds0@0000: □r0Z0				0070	25	41	45	4b	25	38	33	25	30	43	45	25	43	43	25	30	%AEK%83% 0CE%CC%0
▶ Form item: "QSlmtQEY" = "000qT40m00000E{x00@.00 000J_0MG00s0Bt00-				0080	46	25	31	33	64	73	25	42	34	25	34	30	25	39	46	25	F%13ds%B 4%40%9F%
▶ Form item: "HtAQ" = "-jb00"8: 00X000;p0C0'0				0090	39	43	25	44	32	25	44	43	25	33	41	25	31	34	25	44	9C%D2%DC %3A%14%D
▶ Form item: "TAWt" = "00<B0Z000 z0d00				00a0	46	25	39	46	72	25	42	32	5a	25	41	43	25	39	41	25	F%9Fr%B2 Z%AC%9A%
▶ Form item: "nRmdS" = "1-09 r>0FLFK0³)@8S0~0000#]]0 0 000 0{30"				00b0	41	31	25	31	33	25	32	38	25	43	41	25	39	30	26	51	A1%13%28 %CA%90&Q
▶ Form item: "KGmxHqs" = "_ k000 l0 S00o090000<0 0x0D0000 7RIud0n"				00c0	53	6c	6d	74	51	45	59	3d	25	46	34	25	43	44	25	44	SlmtQEY= %F4%CD%D
▶ Form item: "ufPBsm" = "00'"N00090u0 0w*0 00 k> V "				00d0	44	71	54	34	25	44	43	6d	25	42	41	25	45	45	25	46	DqT4%DCm %BA%EE%F
▶ Form item: "MahTfrT" = "G000mN[U[i0G000K0				00e0	32	25	43	31	25	45	41	45	25	37	42	78	25	44	41	25	2%C1%EAE %7Bx%DA%
▶ Form item: "lUjB" = "0t0 0M 0:,0k 0 0G0G0,}p0R				00f0	44	30	25	34	30	2e	25	38	46	25	39	46	25	30	35	25	D0%40.%8 F%9F%05%
▶ Form item: "qeTPpcI" = "" *000S 00@G00#5"				0100	43	37	25	46	45	25	41	39	4a	5f	25	41	45	4d	47	25	C7%FE%A9 J_%AEMG%
▶ Form item: "f0SlQnu" = "0 0 40N00n00U00V0 0"				0110	39	41	25	43	31	73	25	46	45	42	74	25	46	44	25	46	9A%C1s%F EBt%FD%F
▶ Form item: "qqXF" = "00000jdY* 00M □i"				0120	46	2d	25	30	41	25	31	35	26	48	74	41	51	3d	2d	6a	F-%0A%15 &HtAQ=-j
				0130	62	25	46	46	25	46	38	25	32	32	25	44	38	25	39	42	b%FF%F8% 22%D0%9B
				0140	38	25	30	35	25	38	31	25	42	44	58	25	42	31	25	42	8%05%81% BDX%B1%B
				0150	35	25	43	45	25	33	42	70	25	42	31	43	25	41	33	25	5%CE%3Bp %B1C%A3%
				0160	32	37	25	39	35	25	30	41	68	25	45	41	25	46	35	25	27%95%0A h%EA%F5%
				0170	45	36	25	44	43	25	30	32	25	43	46	25	35	43	25	30	E6%DC%02 %CF%5C%0
				0180	37	43	25	33	45	25	33	41	25	44	36	25	31	33	25	30	7C%3E%3A %D6%13%0
				0190	42	4e	25	43	43	25	30	30	25	38	39	36	44	26	54	41	BN%CC%00 %896D&TA
				01a0	57	74	3d	25	45	41	25	43	39	25	33	43	42	25	46	42	Wt=%EA%C 9%3CB%FB
				01b0	5a	25	45	31	25	44	35	25	45	36	25	30	46	7a	25	43	Z%E1%D5% E6%0Fz%C
				01c0	39	64	25	45	46	25	45	46	25	31	30	25	30	41	25	43	9d%EF%EF %10%0A%C
				01d0	38	25	42	31	25	46	46	25	39	35	57	25	43	30	25	46	8%B1%FF% 95W%C0%F
				01e0	36	25	46	35	25	38	44	25	45	32	25	46	33	25	45	44	6%F5%8D% E2%F3%ED
Frame (1196 bytes)				Reassembled TCP (1623 bytes)																	

Network Traffic

- No suspicious activity by some ransomwares

Category	Ransomwares
SMB Traffic; NBNS Traffic	0a93,03bb,3cff,3fda,4e25,5cba,5d9b,7c2d, 7fae, 17dl, 42c2, 133b, 6628, e8a0, F2c9
SMB and/or NBNS along with ARP	0a93, 7fae
DNS Traffic	F2c9,
HTTP Traffic	F2c9
Spurious SYNs	E8a0, 4e25
Other (DHCP) (May or may not be suspicious)	03bb, 4e25, 4f7b, 7c2d, 7d98, 57cf, 8168, e8a0, ecfb, f2c9, fd32
No suspicious activity	d6b7

Analyzed by Vasudha Vedula, Doctoral Student, UTSA

RATAFIA: Ransomware Analysis using Time And Frequency Informed Autoencoders [IEEE HOST, 2019]

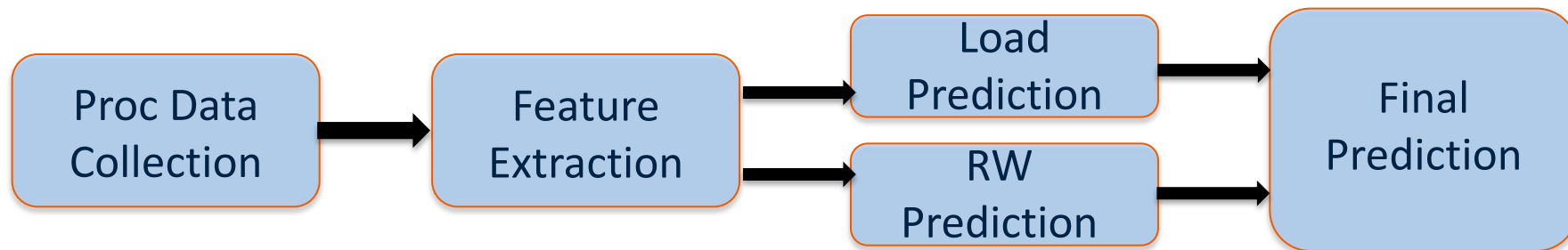
- *perf* to collect processor events
 - 10 ms sampling interval
 - 4-5 ransomwares without loads
- LSTM-based autoencoder
- Detection time: 1 second or more

RanStop: A Hardware-assisted Runtime Crypto-Ransomware Detection Technique [arXiv, 2020]

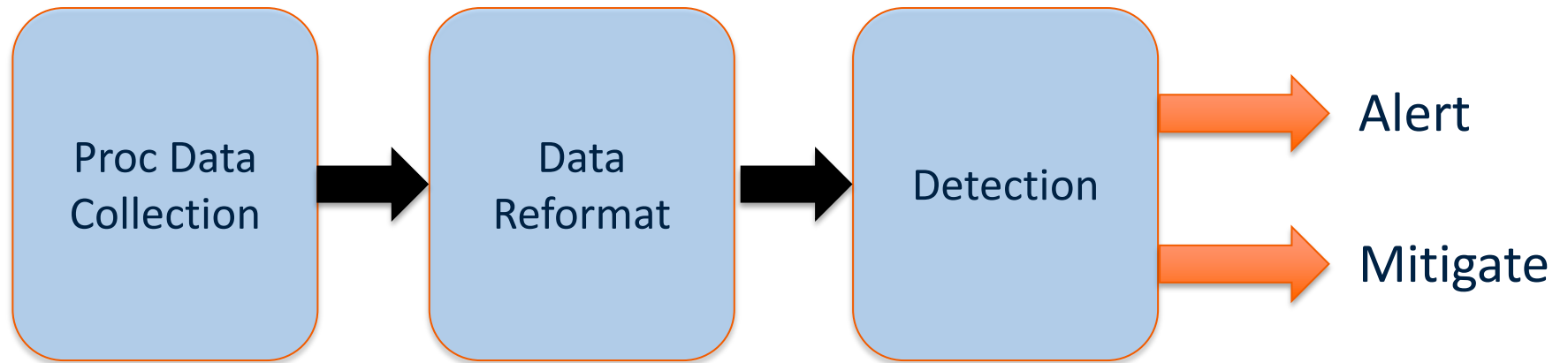
- *likwid* tool to collect processor events
 - 100 μ s sampling interval
 - Sampled first 2 ms only
 - No load case only
- LSTM model
- Detection time is 2 ms
- Ransomware with delayed action are not detected

Ongoing Work: Fine-tuning FPR and FNR

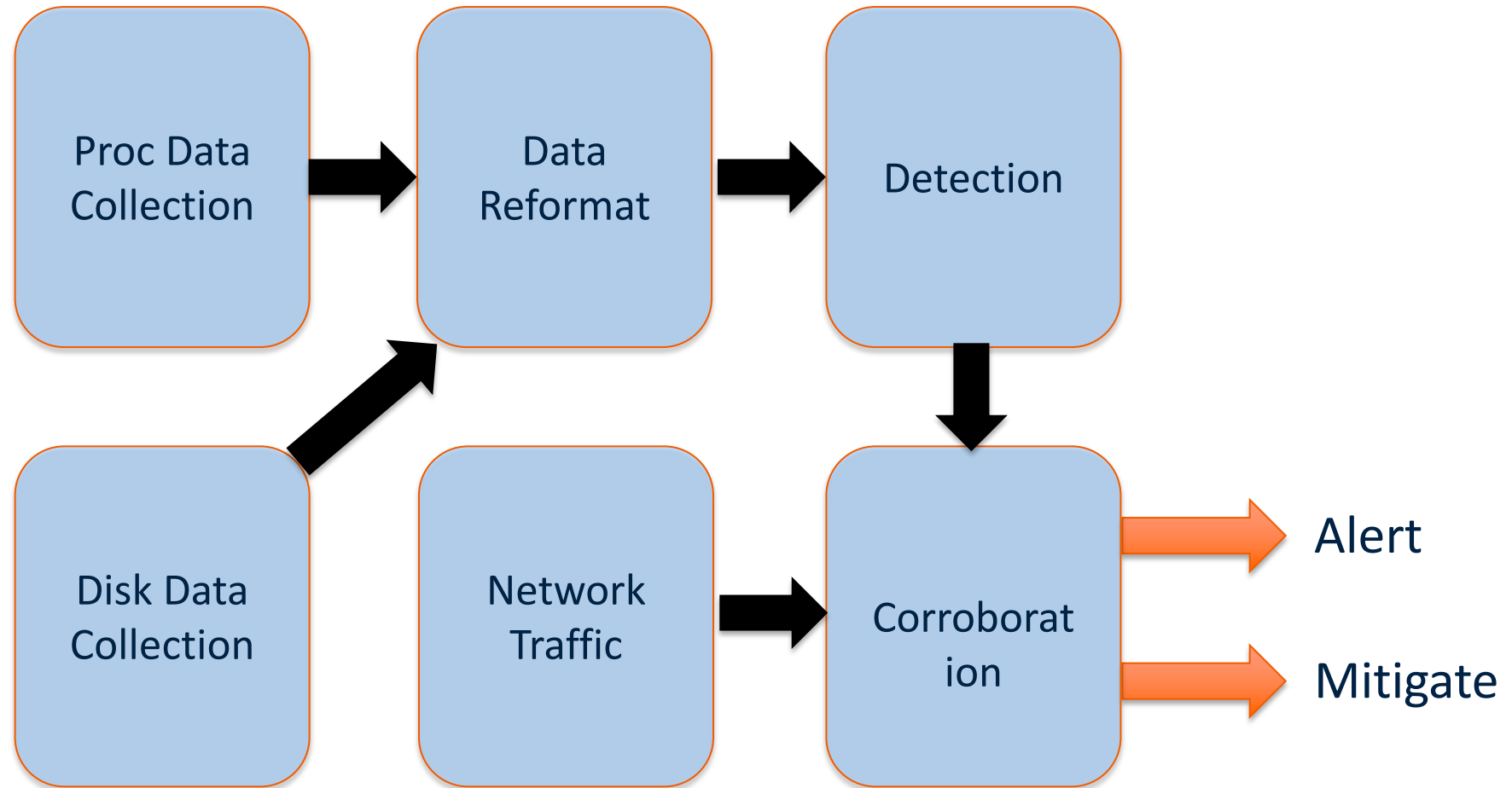
- Different probability thresholds for positive and negative predictions



Ongoing Work: Live Detection



Combine with Disk and Network Traffic Analysis



Questions?

Rajendra.Boppana@utsa.edu