Ransomware Detection using RNN

Tianyi Zhang, Samuel Yuen, Brandon Xiao, Calvin Sun, Prof. Peter Chin   Boston University

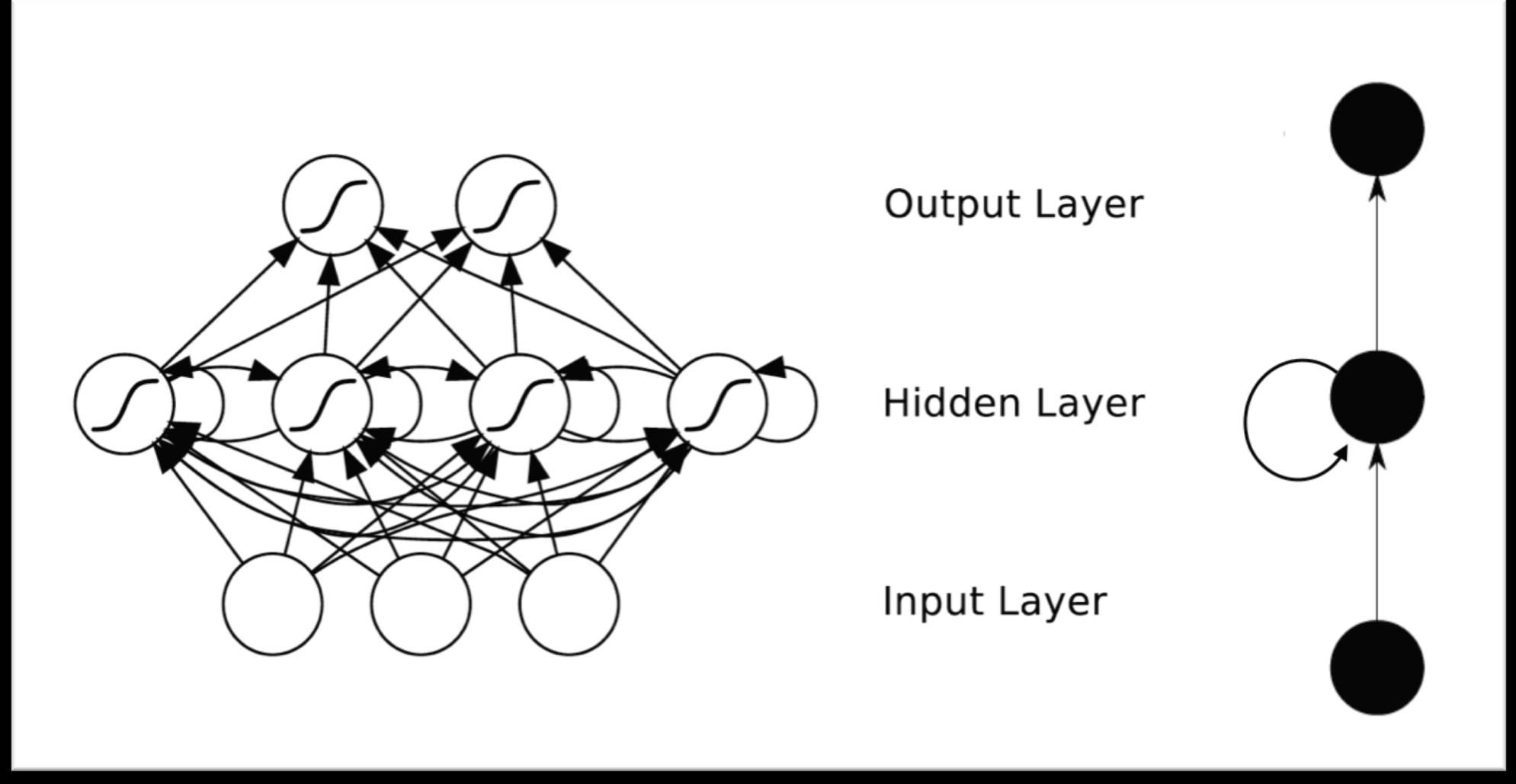
This project will apply Recurrent neural network (RNN) on ransomware detection. First, the ransomware and benign executables will be put in a virtual machine. Then, Cuckoo Sandbox will be used to analyze the behaviors of them in the virtual computer. After that, the behavior report which records the actions and their corresponding times will be translated into the inputs for RNN. After being trained with enough data, this neural network will be able to detect ransomware based on its behaviors.

Ransomware:

Ransomware is a type of malicious software. It threatens people by publishing the victim's data or perpetually blocking access to ask for money.

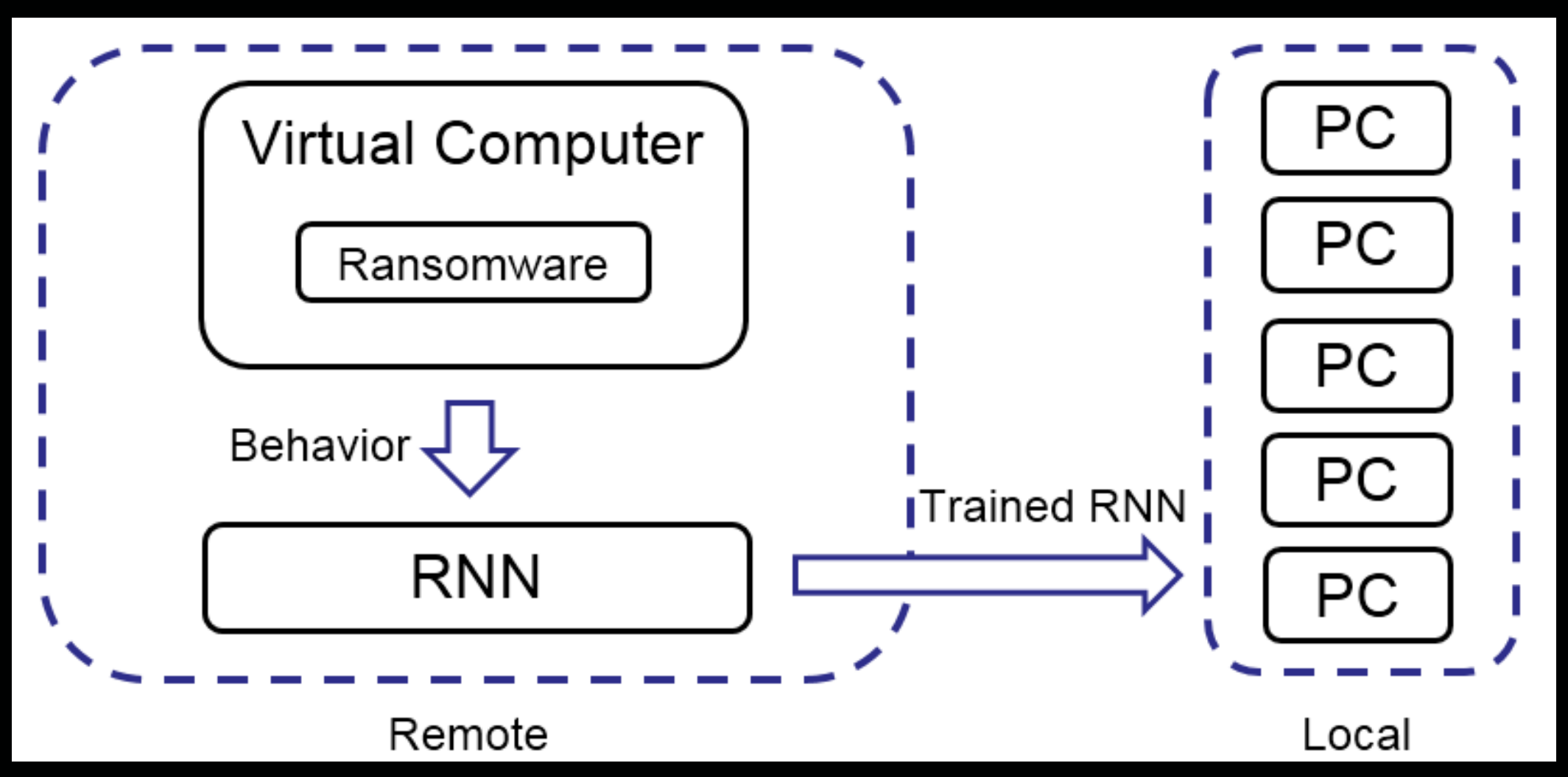
Recurrent neural network (RNN):

RNN is a class of artificial neural network. The advantage of this neural network is it has the ability to make use of sequential information.

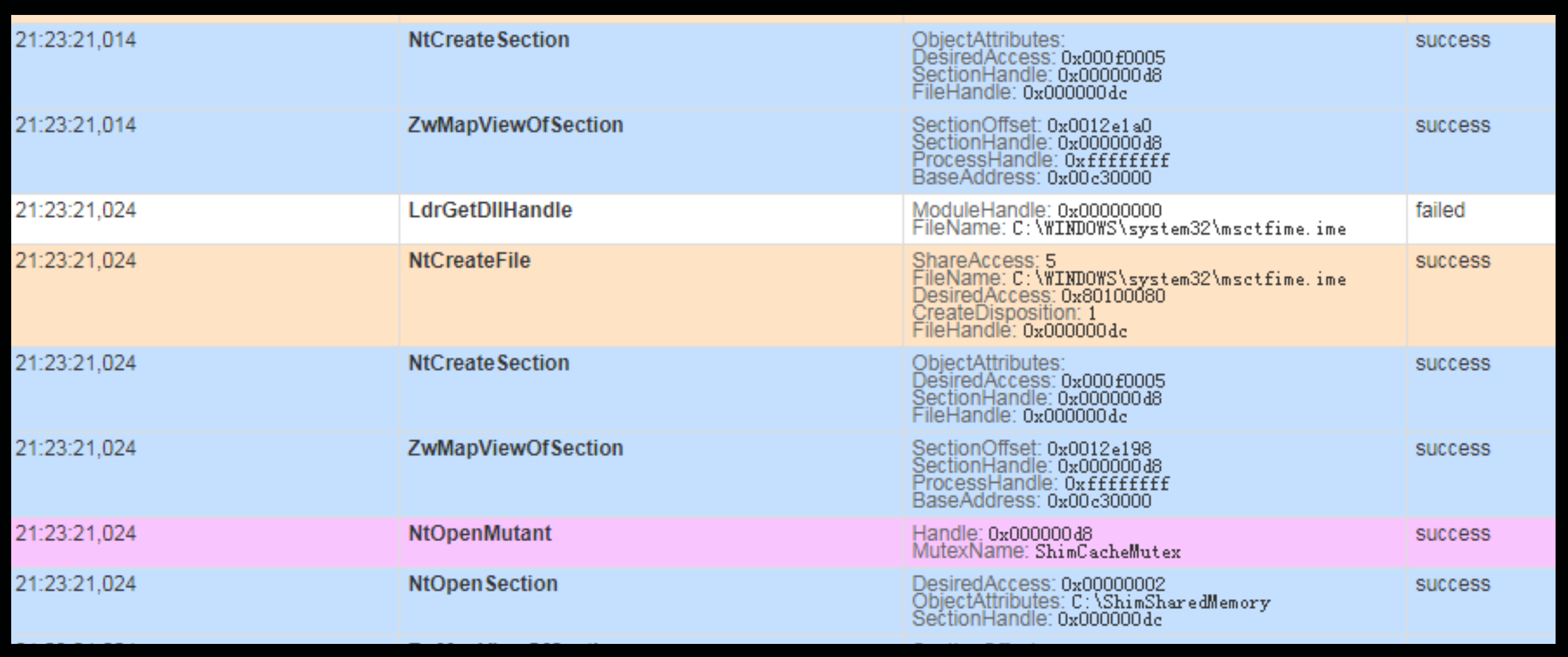


Why this project is important?

To find out ransomware, traditional anti-virus software needs to communicate with virus database, which is slow and requires the database to be updated very often. However, an RNN could be trained on a server and then be deployed to PC. What's more, the trained RNN will just analyze the behavior of the program, so even if it is not up-to-date, it still has the ability to find the newest ransomware while keeps a lower false positive rate.

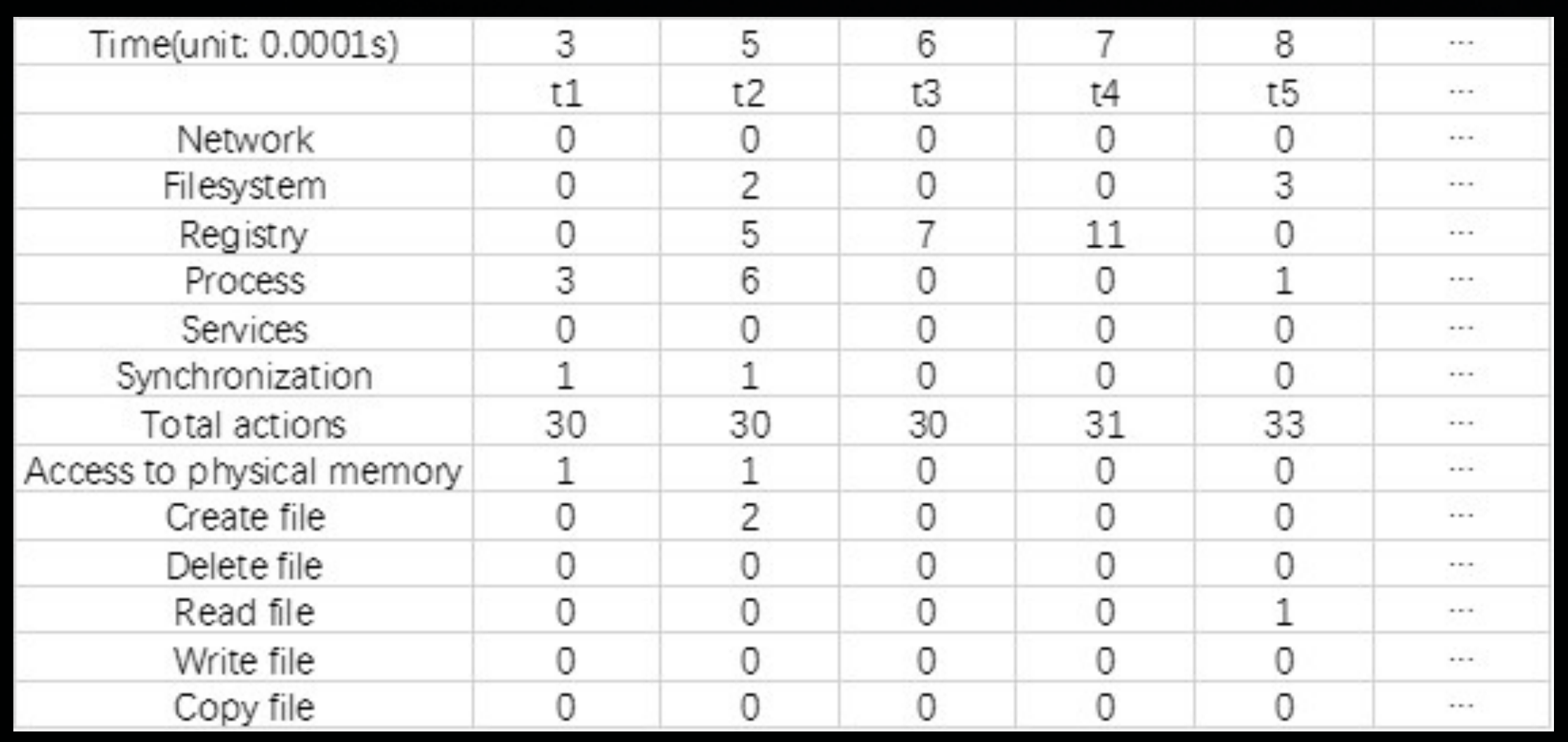


System Diagram



21:23:21,014	NtCreateSection	ObjectAttributes: DesiredAccess: 0x000f0005 SectionHandle: 0x000000d8 FileHandle: 0x000000dc	success
21:23:21,014	ZwMapViewOfSection	SectionOffset: 0x0012e1a0 SectionHandle: 0x000000d8 ProcessHandle: 0xffffffff BaseAddress: 0x00c30000	success
21:23:21,024	LdrGetDllHandle	ModuleHandle: 0x00000000 FileName: C:\WINDOWS\system32\msctfime.ime	failed
21:23:21,024	NtCreateFile	ShareAccess: 5 FileName: C:\WINDOWS\system32\msctfime.ime DesiredAccess: 0x80100080 CreateDisposition: 1 FileHandle: 0x000000dc	success
21:23:21,024	NtCreateSection	ObjectAttributes: DesiredAccess: 0x000f0005 SectionHandle: 0x000000d8 FileHandle: 0x000000dc	success
21:23:21,024	ZwMapViewOfSection	SectionOffset: 0x0012e198 SectionHandle: 0x000000d8 ProcessHandle: 0xffffffff BaseAddress: 0x00c30000	success
21:23:21,024	NtOpenMutant	Handle: 0x000000d8 MutexName: ShimCacheMutex	success
21:23:21,024	NtOpenSection	DesiredAccess: 0x00000002 ObjectAttributes: C:\ShimSharedMemory SectionHandle: 0x000000dc	success

Behavior Report



Time(unit: 0.0001s)	3	5	6	7	8	···
	t1	t2	t3	t4	t5	···
Network	0	0	0	0	0	···
Filesystem	0	2	0	0	3	···
Registry	0	5	7	11	0	···
Process	3	6	0	0	1	···
Services	0	0	0	0	0	···
Synchronization	1	1	0	0	0	···
Total actions	30	30	30	31	33	···
Access to physical memory	1	1	0	0	0	···
Create file	0	2	0	0	0	···
Delete file	0	0	0	0	0	···
Read file	0	0	0	0	1	···
Write file	0	0	0	0	0	···
Copy file	0	0	0	0	0	···

Input for RNN

SCORE
SPECIAL CYBER OPERATIONS
RESEARCH AND ENGINEERING

C3E
Computational Cybersecurity in Compromised Environments
2017 Fall Workshop | October 23-25, 2017 | Atlanta, Georgia