Prophet Zero

Cyber Threat Intelligence Platform

Prophet Zero

Outline

- Problem Statement
- Our Solution
- Analysis Approach
- Web Platform
- Analysis of Results
- Conclusion

Our Platform

Proper
Rusty
Open
Predictions of
Hackers with
Examination
Telemetry

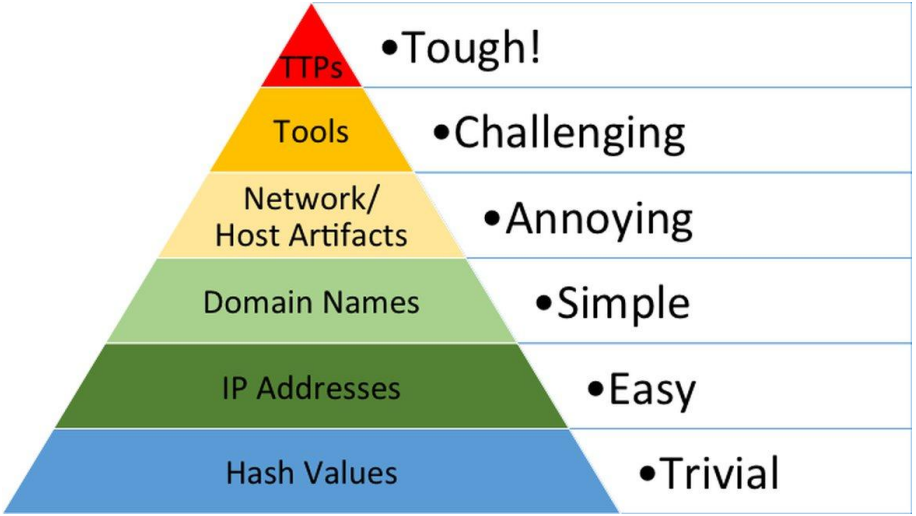
Who are we?

- Carleton Computer Science Students
- Undergrad, masters, and PhD

Prophet Zero

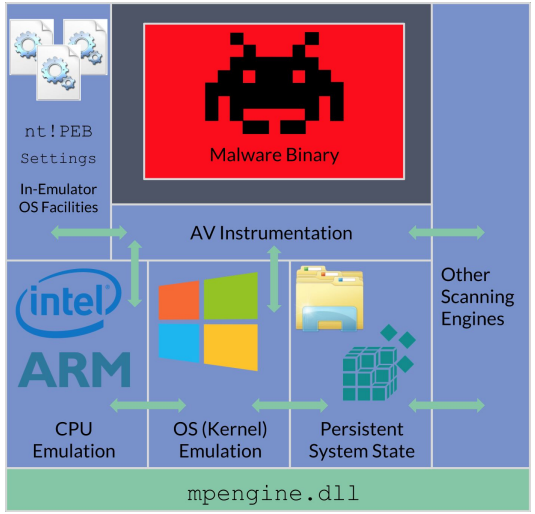
Our Problem

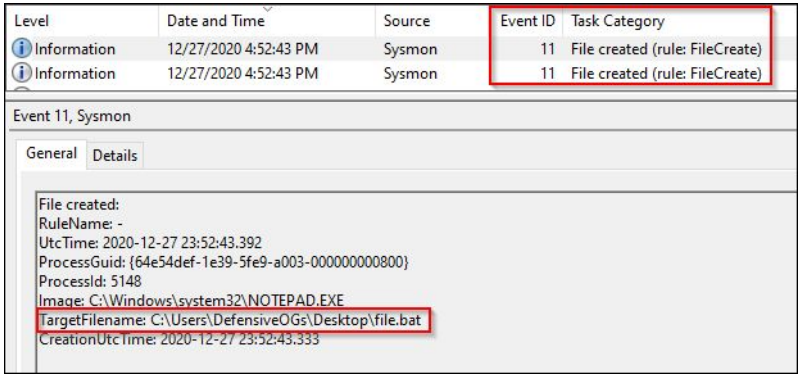
- Typical CTI focuses on IoCs and TTPs
- Would it help analysts identify threats if we created a platform that described malware behavior
- IoCs can be easily changed by attackers
- Techniques and behaviors can not



Our Problem

- Events and Sources of Data
- Data available is often limiting





Level	Date and Time	Source	Event ID	Task Category
Information	12/27/2020 4:52:43 PM	Sysmon	11	File created (rule: FileCreate)
Information	12/27/2020 4:52:43 PM	Sysmon	11	File created (rule: FileCreate)

Event 11, Sysmon

General Details

File created:
RuleName: -
UtcTime: 2020-12-27 23:52:43.392
ProcessGuid: {64e54def-1e39-5fe9-a003-000000000800}
ProcessId: 5148
Image: C:\Windows\system32\NOTEPAD.EXE
TargetFilename: C:\Users\DefensiveOGs\Desktop\file.bat
CreationUtcTime: 2020-12-27 23:52:43.333

Our Solution

- Create a queryable CTI platform
- Include behaviors in addition to IoCs
- Use dynamic and static analysis techniques
- Augment our analysis with machine learning techniques

Prophet Zero

Our Solution

1 Malware analysis pipeline

2 Web Application

Data Source:

- Used the Zoo malware repo
- Focused on Win32 samples, but our solution could handle samples for any machine/architecture

Static Analysis

- Used radare2, ioc_extract, pefile
- Extracted file info


```
"static": {
    "arch": "x86",
    "bintype": "pe",
    "class": "PE32",
    "compiled": "Fri Jun 19 18:22:17 1992",
    "os": "windows",
    "lang": "c",
    "hash": "764efa883dda1e11db47671c4a3bbd9e",
    "filesize": 1114859,
```

Imports


```
"libraries": [
    {
        "name": "LoadLibraryA",
        "lib_name": "KERNEL32.DLL"
    },
    {
        "name": "GetProcAddress",
        "lib_name": "KERNEL32.DLL"
    },
    {
        "name": "ExitProcess",
        "lib_name": "KERNEL32.DLL"
    },
    {
        "name": "RegCloseKey",
        "lib_name": "advapi32.dll"
    },
    {
        "name": "SysFreeString",
        "lib_name": "oleaut32.dll"
    },
    {
        "name": "CharNextA",
        "lib_name": "user32.dll"
    }
```

IoCs


```
"iocs": [
    {
        "indicator_type": "registry access",
        "value": "Software\\\\Microsoft\\\\Windows\\\\CurrentVersion"
    },
    {
        "indicator_type": "technique",
        "value": "Code Signing"
    },
    {
        "indicator_type": "url",
        "value": "http://nsis.sf.net/NSIS_Error"
    },
    {
        "indicator_type": "url",
        "value": "http://ocsp.thawte.com0"
    },
    {
        "indicator_type": "url",
        "value": "http://crl.thawte.com/ThawteTimestampingCA.crl0"
    },
    {
        "indicator_type": "url",
        "value": "https://www.thawte.com/cps0"
    },
    {
        "indicator_type": "url",
        "value": "http://crl.thawte.com/ThawtePremiumServerCA.crl0\\r"
    },
    {
        "indicator_type": "url",
        "value": "http://cs-g2-crl.thawte.com/ThawteCSG2.crl0"
    },
    {
        "indicator_type": "url",
        "value": "http://ocsp.thawte.com0"
    },
    {
        "indicator_type": "url",
        "value": "http://crl.thawte.com/ThawtePCA.crl0"
    }
```

```
    {
      "indicator_type": "wmi query",
      "value": "select * from Win32_BIOS"
    },
    {
      "indicator_type": "wmi query",
      "value": "Select * from Win32_ComputerSystem"
    },
    {
      "indicator_type": "wmi query",
      "value": "Select * from Win32_Processor"
    },
    {
      "indicator_type": "wmi query",
      "value": "select * from MSAcpi_ThermalZoneTemperature"
    },
    {
      "indicator_type": "wmi query",
      "value": "SELECT * FROM Win32_OperatingSystem"
    },
    {
      "indicator_type": "wmi query",
      "value": "SELECT * FROM Win32_UserAccount"
    },
    {
      "indicator_type": "registry access",
      "value": "hKU\\t"
    },
    {
      "indicator_type": "file path",
      "value": "c:\\\\sources\\\\cecil\\\\obj\\\\net_2_0_Release\\\\Mono.Cecil.pdb"
    },
    {
      "indicator_type": "file path",
      "value": "C:\\\\Users\\\\The Invincible\\\\Desktop\\\\gx\\\\gx-current-program\\\\LSASS\\\\obj\\\\Release\\\\LSASS.pdb"
    },
```

```
    {
      "indicator_type": "technique",
      "value": "detect vm"
    },
```

```
    {
        "indicator_type": "technique",
        "value": "UPX - packing"
    },
```

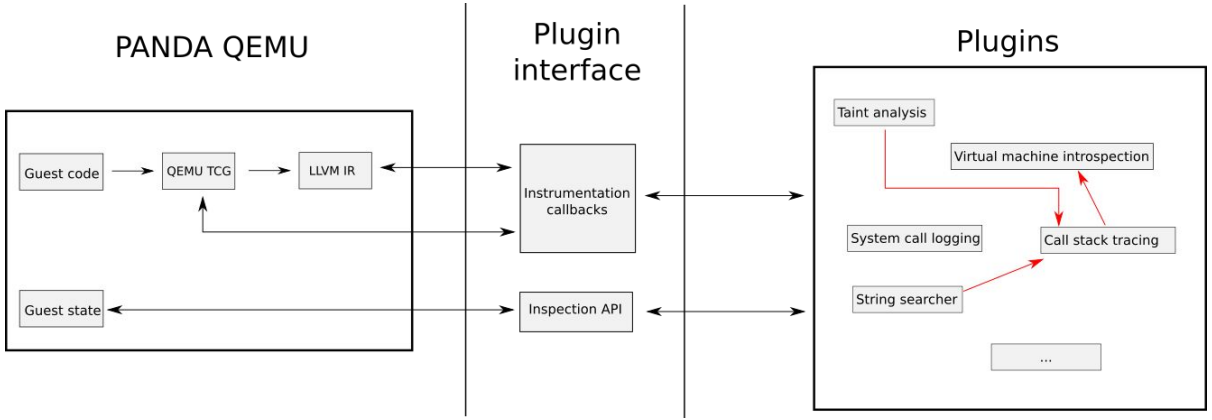
Commands and File Names

```
"cmds": [
  "Find",
  "tree",
  "Move",
  "Sort",
  "Taskkill /f /IM \"{0}\" {1}",
  "SchTasks /Delete /f /TN \"{0}\" {1}",
  "del /f \"{0}\" {1}",
  "DEL \"%~f0\"",
  "netstat -a",
  "tasklist start",
  "net start",
  "Fc w",
  "Type",
  "start",
  "type",
  "Start",
  "Sort",
  "Copy",
  "Exit",
  "Path",
  "type",
  "Type"
]
```

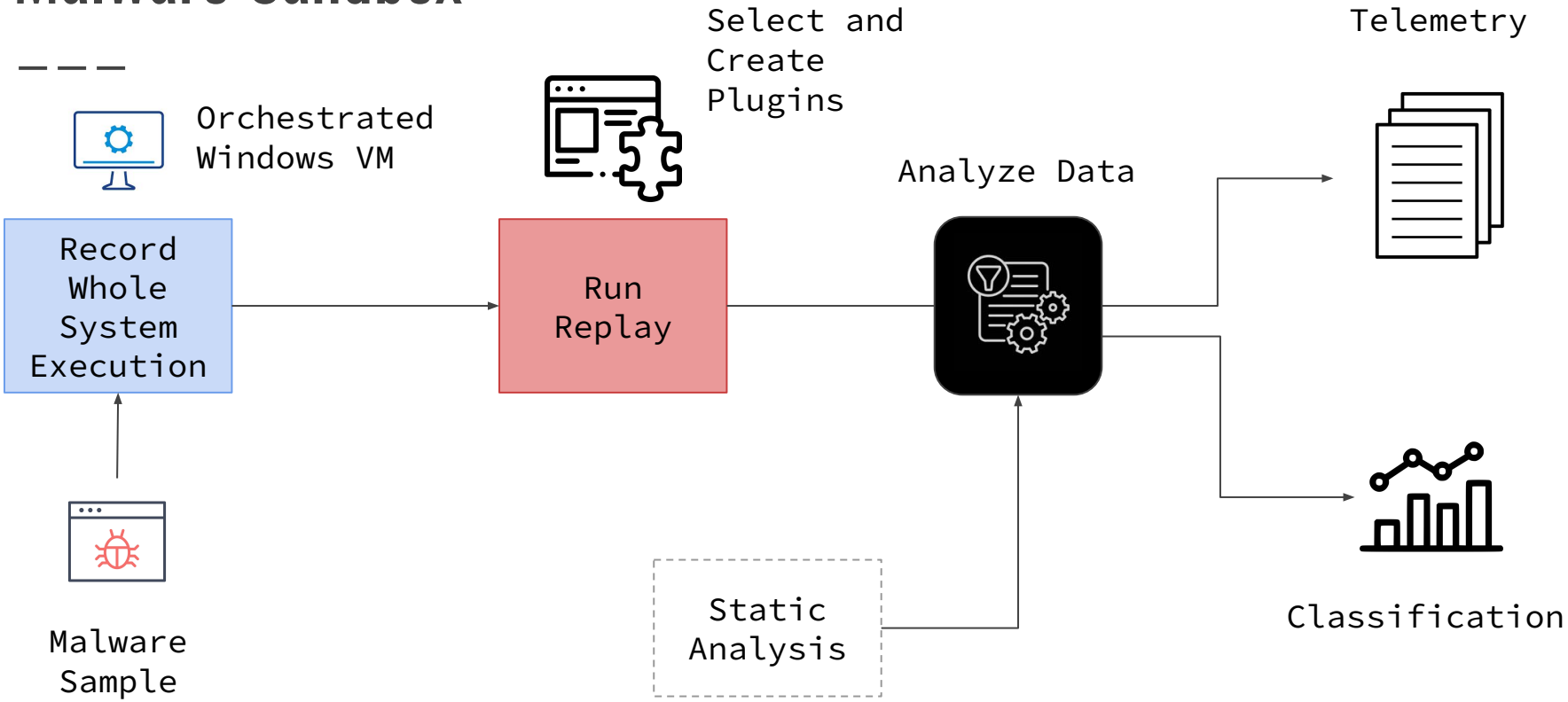
```
"files": [
  "LSASS.exe",
  "gdi32.dll",
  "kernel32.dll",
  "user32.dll",
  "LSASS.resources.Mono.Cecil.dll",
  "Win32Optimizer.bat",
  ".dll",
  "/GX/GX-Server.php",
  "/GetActiveDomains.php",
  "UserData.dat",
  "{0}.dat",
  "test.bat",
  "{0}.CMD.{1}.dat",
  "cmd.exe",
  "{0}.P.{1}.dat",
  "{0}.PM.{1}.dat",
  "{0}.SM.{1}.dat",
  "Mono.Cecil.dll",
  "Java",
  "mscoree.dll",
  ".exe",
  ".dll",
  "mscorlib.dll",
  "mscoree.dll",
  "Mono.Cecil.dll",
  "Mono.Cecil.dll",
  "mscoree.dll",
  "LSASS.exe",
  "LSASS.exe"
```

Malware Sandbox - PANDA

- Whole system reverse engineering
- Built on QEMU
- Repeatable
- Architecture Neutral
- Open-source
- Configurable

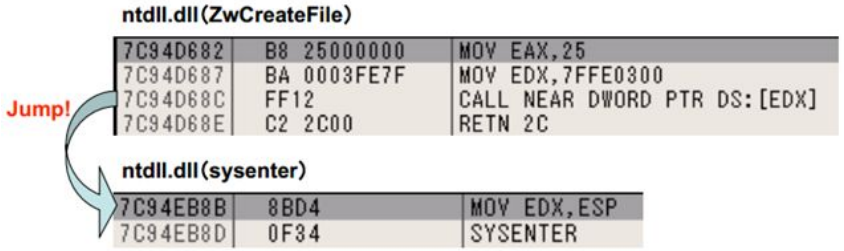


Malware Sandbox



Extending Panda

- Extended the functionality of the plugin originally created by malrec
- Collects all system calls
  - Attaches hooks on syscall instructions
  - reads syscall number and args from registers
- Stripped all arguments and only used the sequence of calls



Malware Sandbox - Data Collected

- Collected unformatted data from the entire system
- Extracted data for target process and related processes from it

Process Information

```
-----------------------------------------------

Dynamic libraries list (18 libs):
        0x49db0000      20480   csrss.exe               C:\Windows\system32\csrss.exe
        0x77580000      1314816         ntdll.dll               C:\Windows\SYSTEM32\ntdll.dll
        0x75760000      53248   CSRSRV.dll              C:\Windows\system32\CSRSRV.dll
        0x75750000      57344   basesrv.DLL             C:\Windows\system32\basesrv.DLL
                        180224  winsrv.DLL              C:\Windows\system32\winsrv.DLL
                        823296  USER32.dll              C:\Windows\system32\USER32.dll
                        319488  GDI32.dll               C:\Windows\system32\GDI32.dll
                        868352  kernel32.dll            C:\Windows\SYSTEM32\kernel32.dll
                        307200  KERNELBASE.dll          C:\Windows\system32\KERNELBASE.dll
                        40960   LPK.dll                 C:\Windows\system32\LPK.dll
                        643072  USP10.dll               C:\Windows\system32\USP10.dll
                        704512  msvcrt.dll              C:\Windows\system32\msvcrt.dll
                        36864   sxssrv.DLL              C:\Windows\system32\sxssrv.DLL
                        389120  sxs.dll                 C:\Windows\system32\sxs.dll
                        663552  RPCRT4.dll              C:\Windows\system32\RPCRT4.dll
                        49152   CRYPTBASE.dll           C:\Windows\system32\CRYPTBASE.dll
                        659456  ADVAPI32.dll            C:\Windows\system32\ADVAPI32.dll
                        102400  sechost.dll             C:\Windows\SYSTEM32\sechost.dll

 modules):
                        4235264         ntoskrnl.exe            \SystemRoot\system32\ntoskrnl.exe
                        225280  hal.dll                 \SystemRoot\system32\halmacpi.dll
                        32768   kdcom.dll               \SystemRoot\system32\kdcom.dll
                        544768  mcupdate.dll            \SystemRoot\system32\mcupdate_GenuineIntel.dll
                        69632   PSHED.dll               \SystemRoot\system32\PSHED.dll
                        32768   BOOTVID.dll             \SystemRoot\system32\BOOTVID.dll
                        270336  CLFS.SYS                \SystemRoot\system32\CLFS.SYS
                        421888  CI.dll                  \SystemRoot\system32\CI.dll
                        528384  Wdf01000.sys            \SystemRoot\system32\drivers\Wdf01000.sys
                        57344   WDFLDR.SYS              \SystemRoot\system32\drivers\WDFLDR.SYS
                        294912  ACPI.sys                \SystemRoot\system32\drivers\ACPI.sys
                        36864   WMILIB.SYS              \SystemRoot\system32\drivers\WMILIB.SYS
```


```
{
  "pc": "18446744073709551615",
  "instr": "18446744073709551615"
},
{
  "pc": "2189875776",
  "instr": "36147",
  "asidInfo": {
    "pid": 0,
    "createTime": "0",
    "ppid": 0,
    "asid": "1593344",
    "names": [
      "Idle"
    ],
    "tids": [
      0
    ],
    "startInstr": "0",
    "endInstr": "36047"
  }
},
{
  "pc": "2189905767",
  "instr": "83402",
  "asidInfo": {
    "pid": 372,
    "createTime": "0",
    "ppid": 352,
    "asid": "1748406272",
    "names": [
      "csrss.exe"
    ],
    "tids": [
      440
    ],
    "startInstr": "36187",
    "endInstr": "83302"
  }
},
{
  "pc": "2189875963",
```



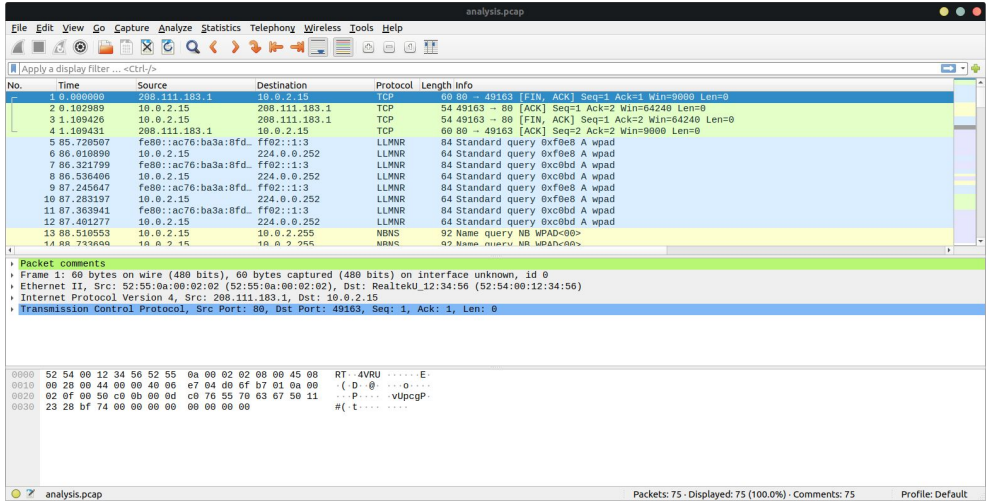
```
"dynamic": {
    "name": "zoo_samples/ed01ebfbc9eb5bbea545af4d01bf5f107166184048043 9c6e5babe8e080e41aa.exe",
    "parent": "cmd.exe",
    "pid": 2660,
    "no_threads": 2,
    "children": [
        "2796-icacls.exe",
        "2748-attrib.exe"
    ],
    "kernel_mods": {
        "2660": []
    },
    "libraries": {
        "2660": [
            "C:\\Users\\IEUser\\Desktop\\sample.exe",
            "C:\\Windows\\system32\\MSVCP60.dll"
        ]
    },
```

Files Accessed/Modified

```
600db000: Returning from NtOpenFile (success), handle=a94, filename=\??\C:\Windows\System32\hcproviders.dll, OpenOptions=60
Returning from NtOpenFile (error), return_value=c0000034, filename=\??\C:\Windows\System32\hcproviders.dll.2.Config, OpenOptions=60
68369000: Returning from NtCreateFile (success), handle=124, filename=\??\C:\Windows\WinSxS\manifests\x86_microsoft.windows.common-controls_6595b64144-
ccf1df_6.0.7601.18837_none_41e855142bd5705d.manifest, CreateOptions=20064
68369000: NtReadFile(FileHandle=124, Event=0, ApcRoutine=0, ApcContext=0, IoStatusBlock=13ef994, Buffer=13efadc, BufferLength=2, ByteOffset=0, Key=0)
Bytes Read=2
3c 3f
68369000: Returning from NtCreateFile (success), handle=124, filename=\??\C:\Windows\WinSxS\manifests\x86_microsoft.windows.common-controls_6595b64144-
ccf1df_6.0.7601.18837_none_41e855142bd5705d.manifest, CreateOptions=20064
68369000: NtReadFile(FileHandle=124, Event=0, ApcRoutine=0, ApcContext=0, IoStatusBlock=13ef884, Buffer=2f5d58, BufferLength=fff, ByteOffset=0, Key=0)
Bytes Read=e8b
3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 7
8 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 31 22 20 6d 61 6e 69 66 65 73 74 56 65-
 72 73 69 6f 6e 3d 22 31 2e 30 22 20 78 6d 6c 6e 73 3a 63 6d 69 76 32 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d-
 3a 61 73 6d 2e 76 33 22 20 63 6d 69 76 32 3a 63 6f 70 79 72 69 67 68 74 3d 22 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20-
 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 41 6c 6c 20 52 69 67 68 74 73 20 52 65 73 65 72 76 65 64 2e 22 3e 0d 0a 20 20 3c 6e 6f 49 6e 68 65 72 69 74 61-
 62 6c 65 20 2f 3e 0d 0a 20 20 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 6e 61 6d 65 3d 22 4d 69 63 72 6f 73 6f 66 74 2e 57 69 6e 64 6f 77-
 73 2e 43 6f 6d 6d 6f 6e 2d 43 6f 6e 74 72 6f 6c 73 22 20 76 65 72 73 69 6f 6e 3d 22 36 2e 30 2e 37 36 30 31 2e 31 38 38 33 37 22 20 70 72 6f 63 65 73-
 73 6f 72 41 72 63 68 69 74 65 63 74 75 72 65 3d 22 78 38 36 22 20 70 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 22 36 35 39 35 62 36 34 31 34 34 63 63-
 66 31 64 66 22 20 74 79 70 65 3d 22 77 69 6e 33 32 22 20 2f 3e 0d 0a 20 20 3c 64 65 70 65 6e 64 65 6e 63 79 20 63 6d 69 76 32 3a 64 69 73 63 6f 76 65-
 72 61 62 6c 65 3d 22 6e 6f 22 20 63 6d 69 76 32 3a 72 65 73 6f 75 72 63 65 54 79 70 65 3d 22 52 65 73 6f 75 72 63 65 73 22 3e 0d 0a 20 20 20 20 3c 64-
 65 70 65 6e 64 65 6e 74 41 73 73 65 6d 62 6c 79 3e 0d 0a 20 20 20 20 20 20 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 6e 61 6d 65 3d 22 4d-
 69 63 72 6f 73 6f 66 74 2e 57 69 6e 64 6f 77 73 2e 43 6f 6d 6d 6f 6e 2d 43 6f 6e 74 72 6f 6c 73 2e 52 65 73 6f 75 72 63 65 73 22 20 76 65 72 73 69 6f-
 6e 3d 22 36 2e 30 2e 30 2e 30 22 20 70 72 6f 63 65 73 73 6f 72 41 72 63 68 69 74 65 63 74 75 72 65 3d 22 78 38 36 22 20 6c 61 6e 67 75 61 67 65 3d 22-
 2a 22 20 70 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 22 36 35 39 35 62 36 34 31 34 34 63 63 66 31 64 66 22 20 74 79 70 65 3d 22 77 69 6e 33 32 22 20-
 2f 3e 0d 0a 20 20 20 20 3c 2f 64 65 70 65 6e 64 65 6e 74 41 73 73 65 6d 62 6c 79 3e 0d 0a 20 20 3c 2f 64 65 70 65 6e 64 65 6e 63 79 3e 0d 0a 20 20 3c-
 66 69 6c 65 20 68 61 73 68 3d 22 62 31 65 66 65 66 63 37 36 39 37 35 39 34 35 33 33 34 30 31 61 33 38 66 30 37 37 63 36 65 63 33 32 39 64 64 35 36 34-
 39 22 20 68 61 73 68 61 6c 67 3d 22 53 48 41 31 22 20 6e 61 6d 65 3d 22 63 6f 6d 63 74 6c 33 32 2e 64 6c 6c 22 20 63 6d 69 76 32 3a 73 6f 75 72 63 65-
 4e 61 6d 65 3d 22 22 20 63 6d 69 76 32 3a 69 6d 70 6f 72 74 50 61 74 68 3d 22 24 28 62 75 69 6c 64 2e 6e 74 74 72 65 65 29 5c 61 73 6d 73 5c 36 30 5c-
 6d 73 66 74 5c 77 69 6e 64 6f 77 73 5c 63 6f 6d 6d 6f 6e 5c 63 6f 6e 74 72 6f 6c 73 5c 22 3e 0d 0a 20 20 20 20 3c 77 69 6e 64 6f 77 43 6c 61 73 73 20-
 76 65 72 73 69 6f 6e 65 64 3d 22 79 65 73 22 3e 54 6f 6f 6c 62 61 72 57 69 6e 64 6f 77 33 32 3c 2f 77 69 6e 64 6f 77 43 6c 61 73 73 3e 0d 0a 20 20 20-
 20 3c 77 69 6e 64 6f 77 43 6c 61 73 73 20 76 65 72 73 69 6f 6e 65 64 3d 22 79 65 73 22 3e 43 6f 6d 62 6f 42 6f 78 45 78 33 32 3c 2f 77 69 6e 64 6f 77-
 43 6c 61 73 73 3e 0d 0a 20 20 20 20 3c 77 69 6e 64 6f 77 43 6c 61 73 73 20 76 65 72 73 69 6f 6e 65 64 3d 22 79 65 73 22 3e 6d 73 63 74 6c 73 5f 74 72-
```


```
],
"file_io": [
    {
        "call": "NtOpenFile",
        "filename": "\\??\\C:\\Users\\IEUser\\,"
    },
    {
        "call": "NtOpenFile",
        "filename": "\\??\\C:\\Windows\\SYSTEM32\\sechost.dll,"
    },
    {
        "call": "NtOpenFile",
        "filename": "\\??\\C:\\Windows\\system32\\CRYPTSP.dll,"
    },
    {
        "call": "NtOpenFile",
        "filename": "\\??\\C:\\Windows\\system32\\rsaenh.dll,"
    },
    {
        "call": "NtOpenFile",
        "filename": "\\??\\C:\\Windows\\system32\\rsaenh.dll,"
    },
    {
        "call": "NtOpenFile",
        "filename": "\\??\\C:\\Windows\\system32\\rsaenh.dll,"
    },
    {
        "call": "NtOpenFile",
        "filename": "\\??\\C:\\Windows\\system32\\rsaenh.dll,"
    },
    {
        "call": "NtCreateFile",
        "filename": "\\??\\C:\\Windows\\system32\\rsaenh.dll,"
    },
    {
        "call": "NtOpenFile",
        "filename": "\\??\\C:\\Windows\\system32\\rsaenh.dll,"
    },
    {
        "call": "NtCreateFile",
        "filename": "\\??\\C:\\Windows\\Globalization\\Sorting\\sortdefault.nls,"
```

Network Data



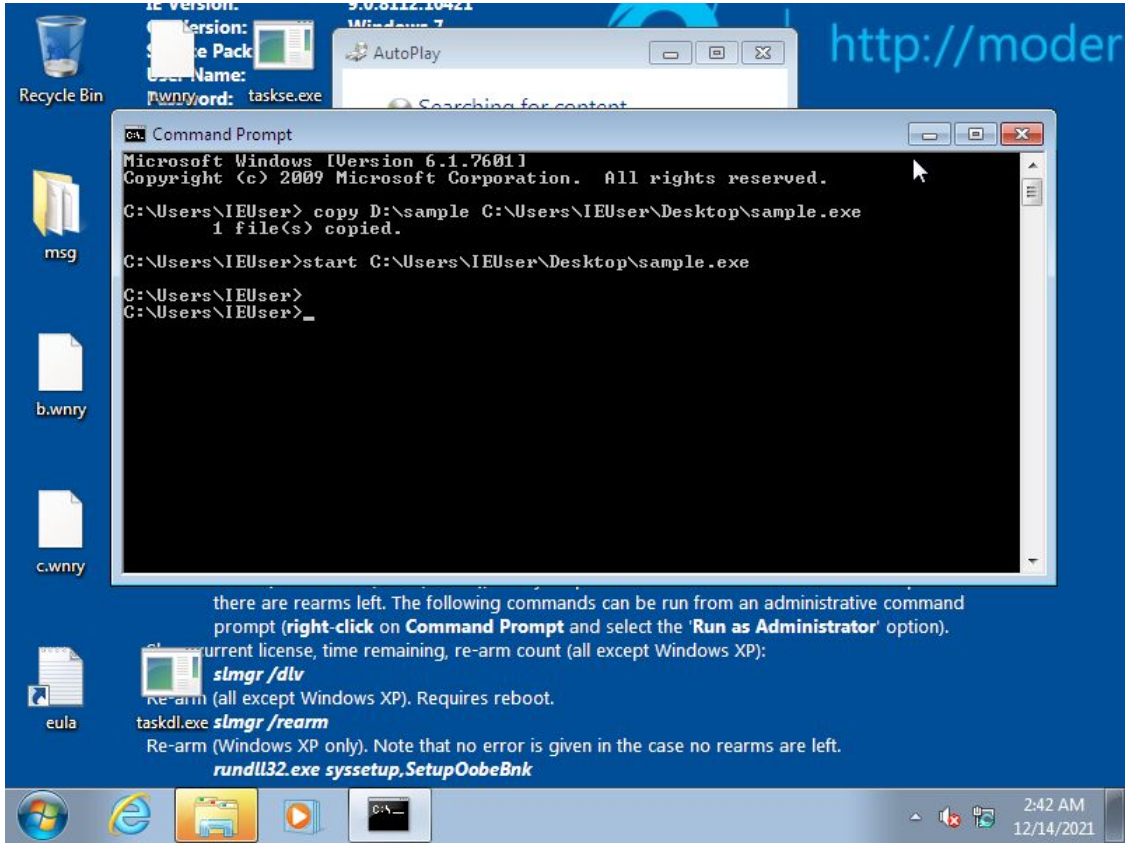

```
],
"network": [
    {
        "to": "10.0.2.15",
        "from": "64.4.54.254",
        "data": "TLSv1 464 Application Data, Application Data"
    },
    {
        "to": "64.4.54.254",
        "from": "10.0.2.15",
        "data": "TCP 60 443 \u2192 49167 [ACK] Seq=1 Ack=411 Win=9000 Len=0"
    },
    {
        "to": "10.0.2.15",
        "from": "64.4.54.254",
        "data": "TLSv1 592 Application Data, Application Data"
    },
    {
        "to": "64.4.54.254",
        "from": "10.0.2.15",
        "data": "TCP 60 443 \u2192 49167 [ACK] Seq=1 Ack=949 Win=9000 Len=0"
    },
    {
        "to": "64.4.54.254",
        "from": "10.0.2.15",
        "data": "TLSv1 384 Application Data, Application Data"
    },
    {
        "to": "10.0.2.15",
        "from": "64.4.54.254",
        "data": "TCP 54 49167 \u2192 443 [ACK] Seq=949 Ack=331 Win=64240 Len=0"
    },
    {
        "to": "10.0.2.15",
        "from": "64.4.54.254",
        "data": "TLSv1 464 Application Data, Application Data"
    },
    {
        "to": "64.4.54.254",
        "from": "10.0.2.15",
        "data": "TCP 60 443 \u2192 49167 [ACK] Seq=331 Ack=1359 Win=9000 Len=0"
```

System Calls


```
[
  {
    "asid": "0x4e43a000",
    "call": "NtQueryInformationProcess",
    "sysid": "0x00ea",
    "no_args": 5,
    "args": [
      4294967295,
      36,
      1242812,
      4,
      0
    ]
  },
  {
    "asid": "0x4e43a000",
    "call": "NtQueryInformationProcess",
    "sysid": "0x00ea",
    "no_args": 5,
    "args": [
      4294967295,
      46,
      1242936,
      4,
      1242920
    ]
  },
  {
    "asid": "0x4e43a000",
    "call": "NtOpenKey",
    "sysid": "0x00b6",
    "no_args": 3,
    "args": [
      1242700,
      2147483648,
      1242668
    ]
  },
  {
    "asid": "0x4e43a000",
    "call": "NtQueryValueKey",
    "sysid": "0x010a",
    "no_args": 6
```

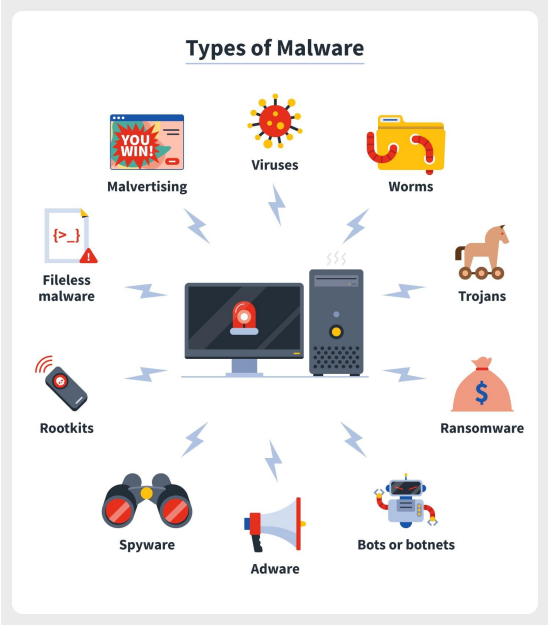
```
,
syscalls_list": [
    "NtQueryInformationProcess",
    "NtQueryInformationProcess",
    "NtOpenKey",
    "NtQueryValueKey",
    "NtClose",
    "NtQueryInformationProcess",
    "NtQueryInformationProcess",
    "NtQueryInformationProcess",
    "NtQuerySystemInformation",
    "NtQuerySystemInformation",
    "NtAllocateVirtualMemory",
    "NtFreeVirtualMemory",
    "NtAllocateVirtualMemory",
    "NtQuerySystemInformation",
    "NtAllocateVirtualMemory",
    "NtFreeVirtualMemory",
    "NtOpenDirectoryObject",
    "NtOpenSymbolicLinkObject",
    "NtQuerySymbolicLinkObject",
    "NtClose",
    "NtOpenFile",
    "NtQueryVolumeInformationFile",
    "NtOpenSection",
    "NtMapViewOfSection",
    "NtQuerySection",
    "NtClose",
    "NtProtectVirtualMemory",
    "NtOpenSection",
    "NtMapViewOfSection",
    "NtQuerySection",
    "NtClose",
    "NtProtectVirtualMemory",
    "NtProtectVirtualMemory",
    "NtProtectVirtualMemory",
    "NtQueryPerformanceCounter",
    "NtQueryPerformanceCounter",
    "NtQuerySystemInformation",
    "NtOpenSection",
```

Screenshots



Classifying Malware

- Used the following dataset to train a classifier: [octatak - malware api class]
  - Consists of sequences of API calls
  - 9 Classes - Spyware, Downloader, Trojan, Worms, Adware, Dropper, Virus Backdoor
- Reduced sequences to contain only NT syscalls

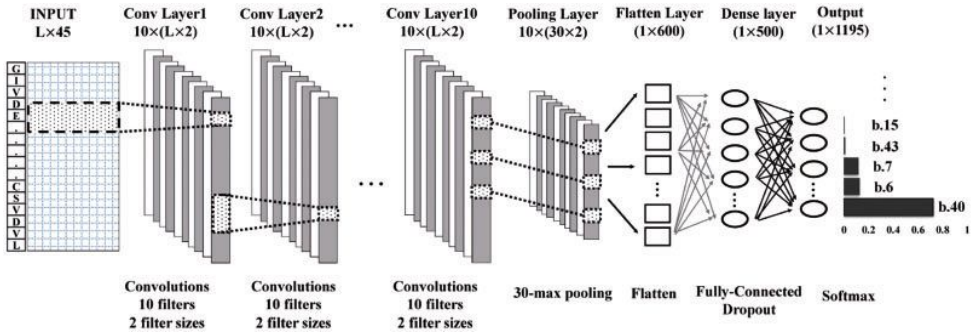



```
createthread ntallocatevirtualmemory ntfreevirtualmemory ntallocatevirtualmemory getfiletype
getfiletype getfiletype ntallocatevirtualmemory ntallocatevirtualmemory ntallocatevirtualmemory
ldrgetdllhandle ldrgetprocedureaddress ntallocatevirtualmemory setunhandledexceptionfilter
loadstringa regopenkeyexa regopenkeyexa regclosekey setunhandledexceptionfilter ntterminateprocess
ntterminateprocess ntclose ntclose ldrunloaddll ntopenkey ntqueryvaluekey ntclose ntclose ntclose
ntclose ntterminateprocess
```

An Example Sequence

Classification Method

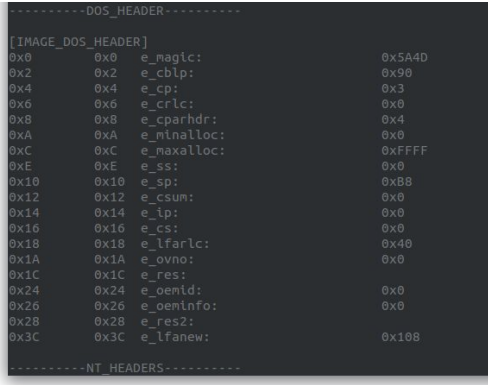
- 1D Convolutional Neural Network
  - > 95% accuracy on validation data
- Fed sequences from live samples into classifier



Example of the selected Network Architecture. Image Source: [1]

Clustering to identify similar samples

- Hybrid Features
  - Combination of static and dynamic features
- K-Means algorithm



```
----------DOS_HEADER----------

[IMAGE_DOS_HEADER]
0x0        0x0   e_magic:                    0x5A4D
0x2        0x2   e_cblp:                     0x90
0x4        0x4   e_cp:                       0x3
0x6        0x6   e_crlc:                     0x0
0x8        0x8   e_cparhdr:                  0x4
0xA        0xA   e_minalloc:                 0x0
0xC        0xC   e_maxalloc:                 0xFFFF
0xE        0xE   e_ss:                       0x0
0x10       0x10  e_sp:                       0xB8
0x12       0x12  e_csum:                     0x0
0x14       0x14  e_ip:                       0x0
0x16       0x16  e_cs:                       0x0
0x18       0x18  e_lfarlc:                   0x40
0x1A       0x1A  e_ovno:                     0x0
0x1C       0x1C  e_res:
0x24       0x24  e_oemid:                    0x0
0x26       0x26  e_oeminfo:                  0x0
0x28       0x28  e_res2:
0x3C       0x3C  e_lfanew:                   0x108

----------NT_HEADERS----------
```

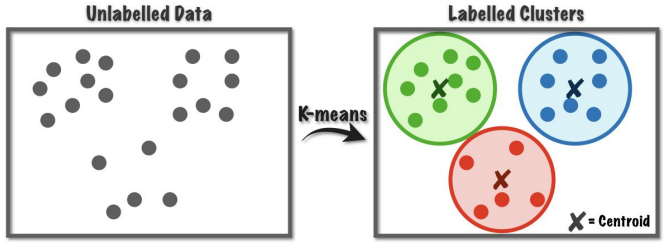
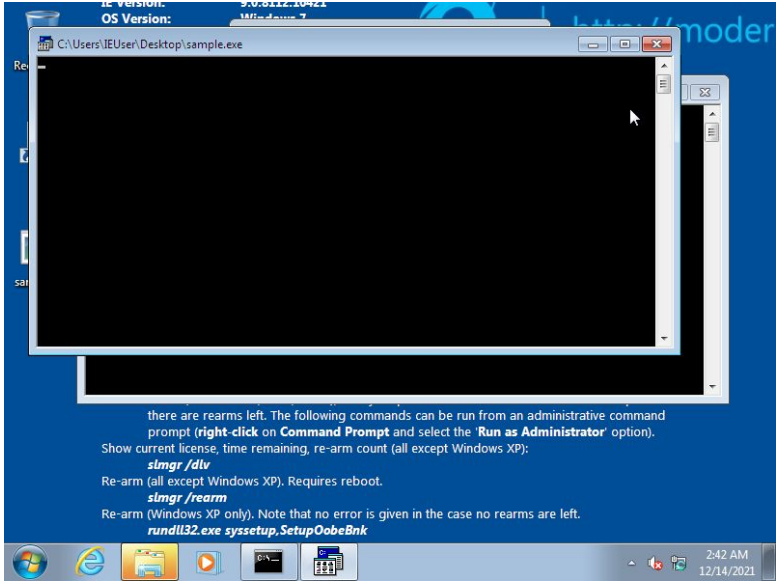


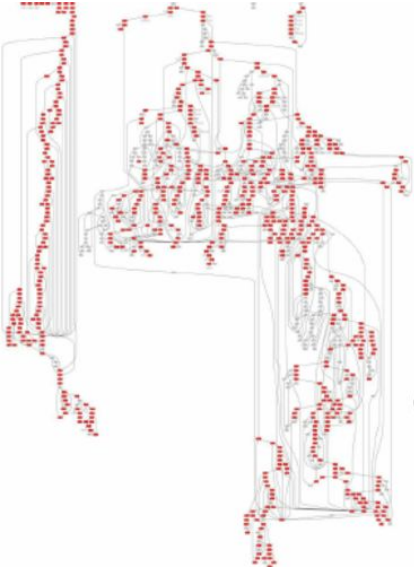
Image Source: [2]

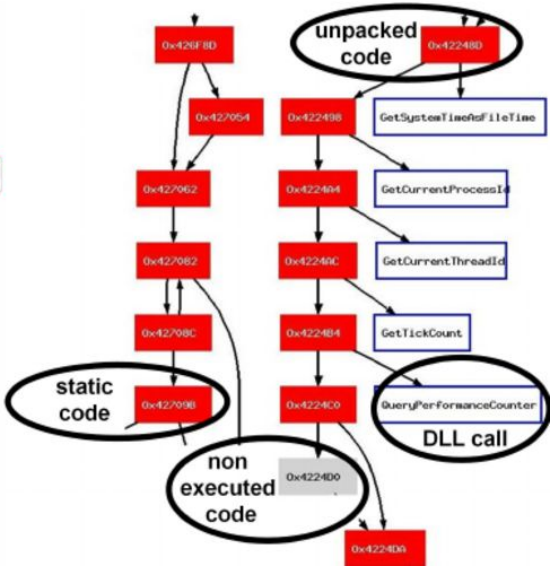
Wrap up:

- We now have:
  - Dynamic Features:
    - System Calls, File Accesses, Network Traffic, Process Information, Libraries, Screenshots of the malware running
  - Static Features:
    - IoCs, Strings, File Info



A Retrospective





Web Platform

Our Stack:

- MongoDB NoSQL database stores behavioural IoC information
- Rust back end exposes a RESTful API into the database
  - Rust type system + memory model → memory-safe and efficient code
  - Asynchronous rocket.rs webserver with the tokio runtime
  - MongoDB Rust driver to perform queries on malware data
- Quasar front end to view malware data
  - Sleek and modern design
  - Supports filtering malware by various IoCs (touched files, libraries, etc.)

PROPHET ZERO

Prophet Zero

Malware Name

Files Touched (Comma Separated)

Libraries (Comma Separated)

Keywords (Comma Separated)

Per Page
10

SUBMIT

A Discussion of Results

Were we able to achieve our goals?

- We created a malware sandbox
  - Performed Hybrid Analysis
  - Integrated ML
- We created a web platform to display our data

Yes, but there is still future work to be done

Lessons Learned

- Time
- Datasets
- Limited Sources of Data

Conclusion

- Future work
  - Augmentation of data sources
  - Refinement of Presentation

- Idea is solid

References:

[1] DeepSF: Deep Convolutional Neural Network for Mapping Protein Sequences to Folds - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/The-architecture-of-1D-deep-convolutional-neural-network-for-fold-classification-The_fig1_327213391 [accessed 16 Dec, 2021]

[2] https://towardsdatascience.com/k-means-a-complete-introduction-1702af9cd8c

Thanks
For Listening!