



Noriben

Information Security Inc.

Contents

- About Noriben
- Features
- Installing Noriben
- Running Noriben
- Troubleshooting
- References

About Noriben

- Noriben is a Python-based script that works in conjunction with Sysinternals Procmon (<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>) to automatically collect, analyze, and report on runtime indicators of malware
- Wrapper for Microsoft SysInternals Process Monitor

Noriben Malware Analysis Sandbox

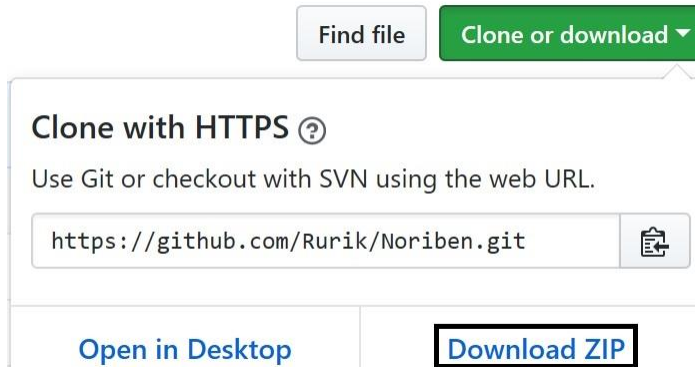
Features

- Bypassing Anti-Sandboxing => use Noriben is with malware that is VM and Sandbox aware
- Command Line-Based Applications
- General Attack Artifacts => used by pentesters to determine what system artifacts exist when launching an attack against a system or service
- Perfect for Malware Analysis on the Road
- Events filtering using Procmon Filter PMC

```
-f FILTER, --filter FILTER  
Specify alternate Procmon Filter PMC
```

Installing Noriben

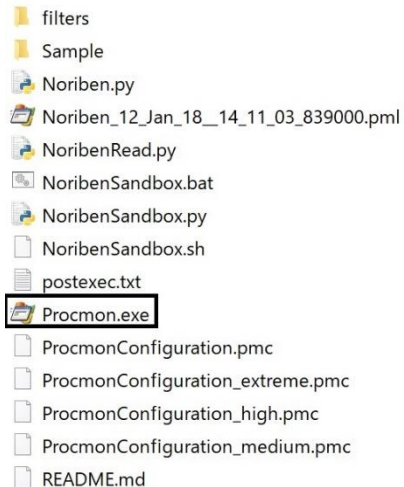
- Downloading from Github



The screenshot shows the GitHub interface for cloning a repository. At the top, there are two buttons: 'Find file' and 'Clone or download'. The 'Clone or download' button is green and has a dropdown arrow. Below it, a dropdown menu is open, showing the title 'Clone with HTTPS' with a help icon. The text below the title says 'Use Git or checkout with SVN using the web URL.' Below this text is a text input field containing the URL 'https://github.com/Rurik/Noriben.git' and a clipboard icon. At the bottom of the dropdown menu, there are two buttons: 'Open in Desktop' and 'Download ZIP'. The 'Download ZIP' button is highlighted with a black border.

Installing Noriben

- Copying Procmon.exe to the Noriben folder



Running Noriben

- Running Noriben.py

```
Noriben-master>Noriben.py
[!] Python module "requests" not found. Internet functionality is now disabled.

This is acceptable if you do not wish to upload data to VirusTotal.
====[ Noriben v1.7.3b
====[ @bbaskin
[*] Using filter file: ProcmonConfiguration.PMC
[+] Features: (Debug: False   YARA: False   VirusTotal: False)
[*] Using procmon EXE: procmon.exe
[*] Procmon session saved to: Noriben_12_Jan_18__14_17_14_215000.pml
[*] Launching Procmon ...
[*] Procmon is running. Run your executable now.
[*] When runtime is complete, press CTRL+C to stop logging.
```

Running Noriben

- Running the malware



Running Noriben

- Pressing Ctrl-C to stop the scan => Notepad then automatically opens the resulting text report shows a lot of data



The screenshot displays a terminal window on the left and a dialog box on the right. The terminal output shows the following steps:

```
[*] Using procmon EXE: procmon.exe
[*] Procmon session saved to: Noriben_12_Jan_18__14_28_53_779000.txt
[*] Launching Procmon ...
[*] Procmon is running. Run your executable now.
[*] When runtime is complete, press CTRL+C to stop logging.

[*] Termination of Procmon c...
[*] Procmon terminated
[*] Saving report to: Noriben_...
[*] Saving timeline to: Noriben_...
```

The dialog box, titled "Applying Event Filter", shows a progress bar at 90% completion with the text "90% - 0:00 remaining (2018/01/12 14:30:50)" and a "Cancel" button.

The terminal output continues with the following information:


```
--] Sandbox Analysis Report generated by Noriben v1.7.3b
--] Developed by Brian Baskin: brian @ thebaskins.com @bbaskin
--] The latest release can be found at https://github.com/Rurik/Noriben

--] Execution time: 107.11 seconds
--] Processing time: 16.64 seconds
--] Analysis time: 400.60 seconds

Processes Created:
[CreateProcess] Explorer.EXE:2716 > "%ProgramFiles% (x86)¥Java¥jre1.8.0
[CreateProcess] Explorer.EXE:2716 > "rundll32.exe %ProgramFiles% (x86)¥
```

Running Noriben

- Pressing Ctrl-C to stop the scan => Notepad then automatically opens the resulting text report shows a lot of data

 Noriben_12_Jan_18_14_28_53_779000.txt

```
--] Sandbox Analysis Report generated by Noriben v1.7.3b
--] Developed by Brian Baskin: brian @@ thebaskins.com @bbaskin
--] The latest release can be found at https://github.com/Rurik/Noriben

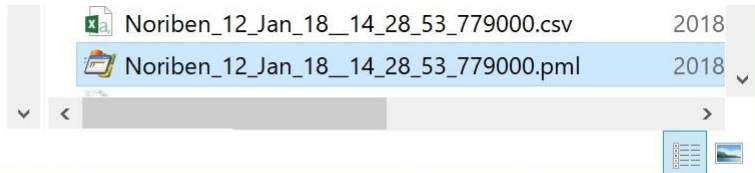
--] Execution time: 107.11 seconds
--] Processing time: 16.64 seconds
--] Analysis time: 400.60 seconds
```

Processes Created:

```
=====
[CreateProcess] Explorer.EXE:2716 > "%ProgramFiles% (x86)¥Java¥jre1.8.0
[CreateProcess] Explorer.EXE:2716 > "rundll32.exe %ProgramFiles% (x86)¥
```

Running Noriben

- Verifying the reports



Procmon session saved to: Noriben_12_Jan_18_14_28_53_779000.pml

Running Noriben

- Malware.jar modifying auto-execute functionality by setting/creating a value in the registry

Registry Activity:

```
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 121
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 122
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 123
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 124
[RegSetValue] Explorer. EXE: 2716 > HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries = 60 2F 47 BD FA 27 CF 11 B8 B4 44 45 53 54 00 00
[RegSetValue] Explorer. EXE: 2716 > HKCU\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{3C042D6D-8919-46A2-AB46-B8FC5481AE03}\LastAccessedTime =
[RegSetValue] Explorer. EXE: 2716 > HKCU\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{3C042D6D-8919-46A2-AB46-B8FC5481AE03}\LaunchCount = 4
[RegSetValue] Explorer. EXE: 2716 > HKCU\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{3C042D6D-8919-46A2-AB46-B8FC5481AE03}\AppPath =
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 125
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 126
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 127
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 128
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 129
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\SetupProgress = 54
[RegSetValue] SetupHost. Exe: 6064 > HKLM\SYSTEM\Setup\MoSetup\Volatile\InstallITicks = 130
[RegSetValue] reg.exe: 3256 > HKCU\Software\Microsoft\Windows\CurrentVersion\Run\XoKXy0BhkeB = C:\Users\BZ\AppData\Roaming\Oracle\bin\javaw.exe -jar ""C:\Users\BZ\XefifW
```

Running Noriben

- Malware.jar executing a visual basic script

```
CreateProcess] java.exe:5896 > "cmd.exe /C cscript.exe %LocalAppData%\Temp\Retrieve5636655753227972051.vbs" [Child PID: 7588]
CreateProcess] cmd.exe:7588 > "%WinDir%\system32\conhost.exe 0xffffffff -ForceV1" [Child PID: 7516]
CreateProcess] cmd.exe:7588 > "cscript.exe %LocalAppData%\Temp\Retrieve5636655753227972051.vbs" [Child PID: 4068]
```

Running Noriben

- Malware.jar creating new processes => javaw.exe creating java.exe

```
[CreateProcess] javaw.exe:7228 > "%ProgramFiles%\Java\jre1.8.0_151\bin\java.exe -jar %LocalAppData%\Temp\0.138608708372531034531126356701865275.class" [Child PID: 2416]
[CreateProcess] java.exe:2416 > "%WinDir%\system32\conhost.exe 0xffffffff -ForceV1" [Child PID: 7988]
```

Troubleshooting

- Getting rid of the following error by installing the six python module

```
File "C:\Users\BZ\Documents\Noriben-master\Noriben.py", line 365, in terminate_self
    from six.moves import input
ImportError: No module named six.moves

C:\Python27\Scripts>easy_install.exe six
Searching for six
Reading https://pypi.python.org/simple/six/
Downloading https://pypi.python.org/packages/16/d8/bc6316cf98419719bd59c91742194c111b6f2e85abac88e496adefaf7afe/six-1.11.0.tar.gz#md5=d12789f9baf7e9fb2524c0c64f1773f8
Best match: six 1.11.0
Processing six-1.11.0.tar.gz
Writing c:\users\bz\appdata\local\temp\easy_install-1amomz\six-1.11.0\setup.cfg
Running six-1.11.0\setup.py -q bdist_egg --dist-dir c:\users\bz\appdata\local\temp\easy_install-1amomz\six-1.11.0\egg-dist-tmp-wzngm
no previously-included directories found matching 'documentation\*_build'
zip_safe flag not set; analyzing archive contents...
six: module references __path__
creating c:\python27\lib\site-packages\six-1.11.0-py2.7.egg
Extracting six-1.11.0-py2.7.egg to c:\python27\lib\site-packages
Adding six 1.11.0 to easy-install.pth file

Installed c:\python27\lib\site-packages\six-1.11.0-py2.7.egg
Processing dependencies for six
Finished processing dependencies for six
```

References

- Noriben

<https://github.com/Rurik/Noriben>

- Procmon

<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>