NORIBEN SANDBOX

https://www.ghettoforensics.com/2013/04/noriben-your-personal-portable-malware.html

Noriben - The Portable Sandbox System

Noriben is a Python-based script that works in conjunction with SysInternals Procmon to automatically collect, analyze, and report on runtime indicators of malware and suspicious system behavior. In a nutshell, it allows you to run your malware, hit a keypress, and get a simple text report of the system's activity after running an attack.

While there are many well developed and fully featured sandboxes, such as Cuckoo, they all have various limitations that impacted the way I do malware analysis. Noriben was written specifically to fill these gaps. Noriben is an ideal solution for many unusual malware instances, such as those that would not run from within a standard sandbox environment. These files perhaps required command line arguments, or had VMware/OS detection that had to be actively debugged, or extremely long sleep cycles.

Bypassing Anti-Sandboxing

One common instance to use Noriben is with malware that is VM and Sandbox aware. Throwing the sample into any existing sandbox will most likely result in a report with no artifacts as the malware didn't run. Some applications look for manual user activity, such as mouse movement and clicking. Other malware may infect the WinHTTP stack and only trigger when a web browser is used. By just launching Noriben in the background, all of the system behavior is logged as the analyst manually controls the system to give the impression of a normal user. Once the file has been detonated, the results can be reviewed as a standard sandbox report.

Command Line-Based Applications

In rarer cases are malware samples that require command line options in order to run. Launching these executables within a sandbox would immediately fail as the malware does not have the arguments to operate. However, an analyst manually controlling the malware while Noriben is running can quickly gather all system artifacts from various command line options.

General Attack Artifacts

Even more interesting, Noriben has been used by pentesters to determine what system artifacts exist when launching an attack against a system or service. By monitoring files created or registry entries modified, a security analyst can determine all artifacts that result from running an attack, a PowerShell command, or a Javascript-based web page.

Perfect for Malware Analysis on the Road

It's commonly a scenario where an analyst may have a proper sandbox environment in a home lab but on the road has only a laptop. In working with various Sales Engineers and

Support individuals from security companies, there were many times where they needed an immediate malware answer out of their hotel room. Noriben was designed to be used with little effort, little setup, and little maintenance. Even if you don't have a dedicated malware VM, any Windows VM will do! Even <a snapshot copy of> your corporate environment!

How to Run Noriben

Noriben is simply a Python wrapper to SysInternal's Process Monitor (procmon.exe). Procmon is a system artifact collection tool that stores millions of events into a massive database. However, for many analysts, this turns into information overload. Noriben works as a filtering system to remove all activity that's known to be from legitimate activity. Therefore, whatever is left over is very likely to be related to suspicious activity from malware or an attack.

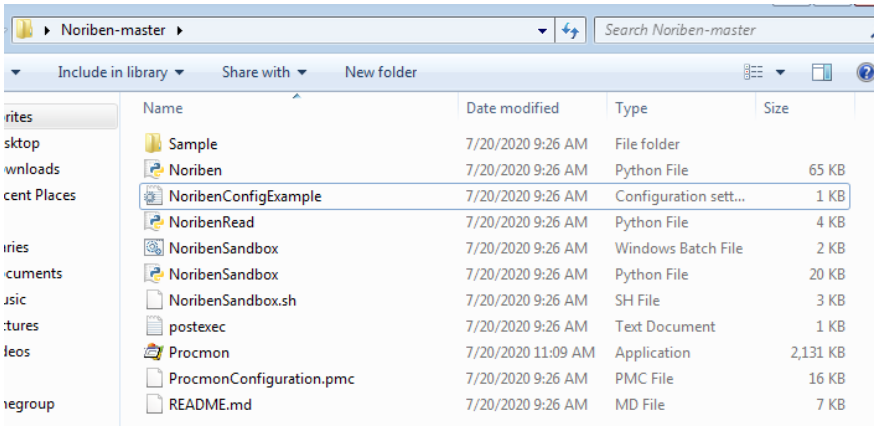
Simply run Noriben.py and wait for it to start listening to the system. Once prompted, run your malware or perform your attack actions. When the malware or attack has reached a point of activity necessary for analysis, stop Noriben by pressing Ctrl-C. Noriben will then stop the logging, gather all of the data, and process a report for you.

Noriben will actually produce multiple reports: a readable text document, a CSV separated by activity type, and a full timeline CSV.

INSTALLATION AND SETUP

- ✗ download iso file for win7: https://softlay.net/operating-system/windows-7-ultimate-full-version-free-download-iso-32-64-bit.html
- ✗ setup win7 w no recommended settings
- ✗ download and install https://www.microsoft.com/en-us/download/confirmation.aspx?id=46148 some security update for procmon driver to load.
- ✗ Download procmon https://docs.microsoft.com/en-us/sysinternals/downloads/procmon
- ✗ download python (that runs on win7) x86-64 msi installer: https://www.python.org/downloads/release/python-344/
- ✗ download noriben: https://github.com/Rurik/Noriben
- ✗ put procmon.exe in noriben-master folder.

Your noriben folder should look like this:

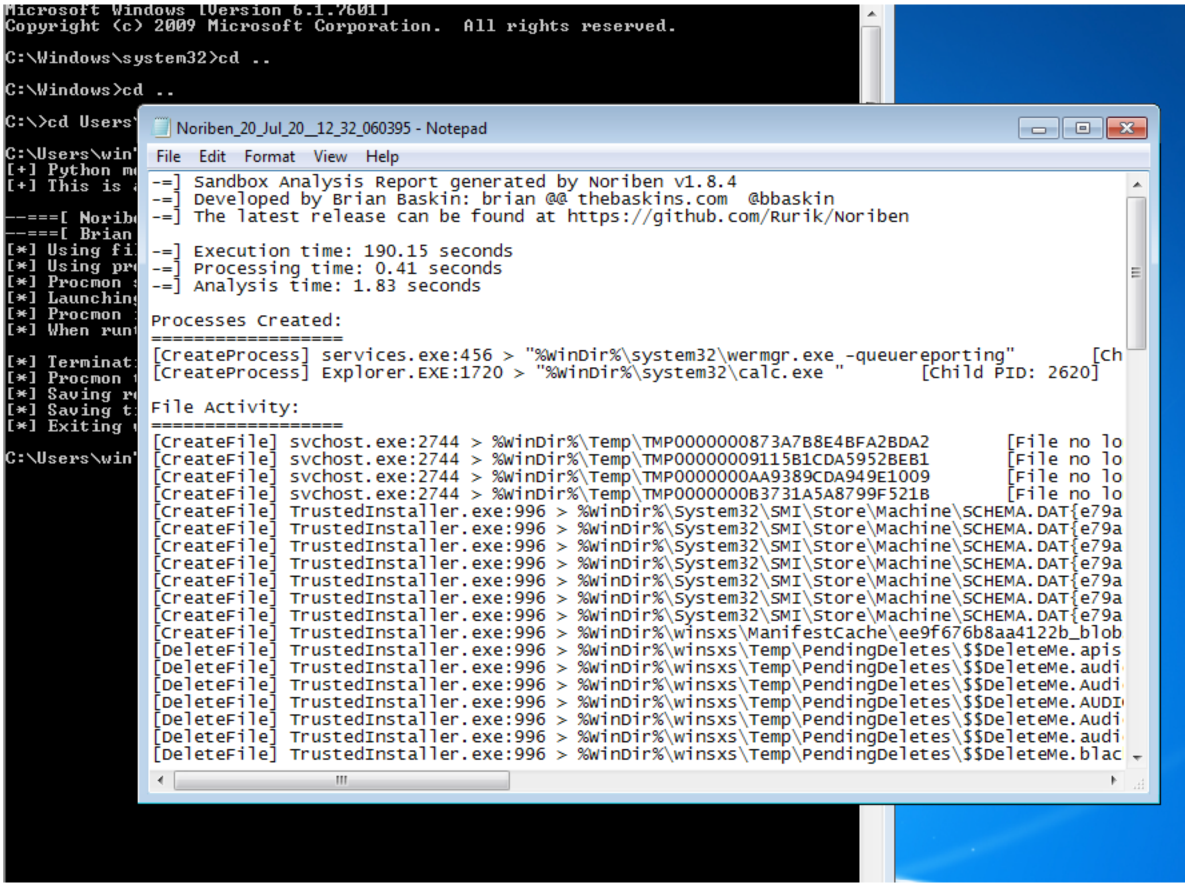


Give adminstrator rights to procmon
open command prompt as admin and cd to noriben-master folder.
Type Noriben.py

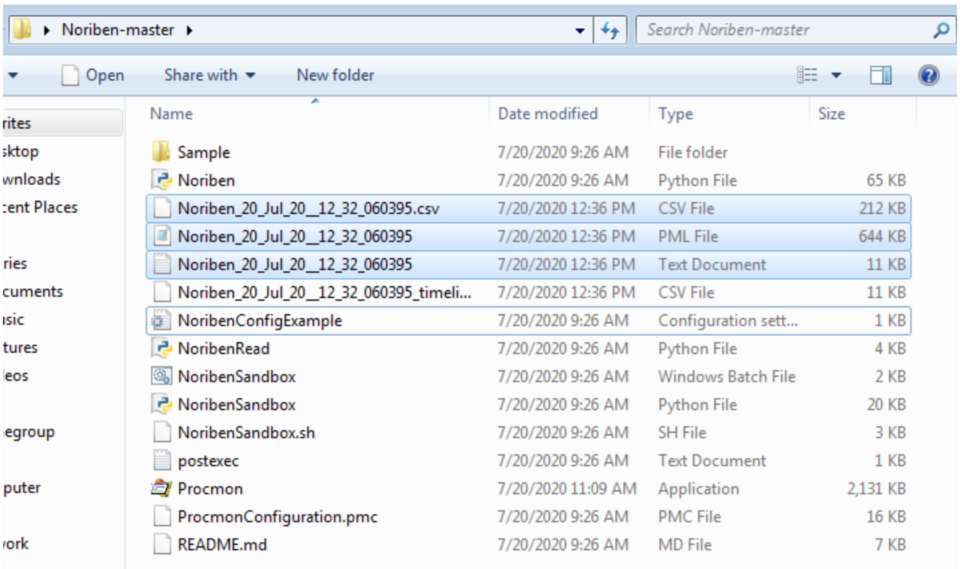
```
C:\Users\win7\Desktop\Noriben-master>Noriben.py
[+] Python module "requests" not found. Internet functionality is disabled.
[+] This is acceptable if you do not wish to upload data to VirusTotal.

--===[ Noriben v1.8.4
--===[ Brian Baskin [brian@thebaskins.com / @bbaskin]
[*] Using filter file: ProcmonConfiguration.PMC
[*] Using procmon EXE: procmon.exe
[*] Procmon session saved to: Noriben_20_Jul_20__12_32_060395.pml
[*] Launching Procmon ...
[*] Procmon is running. Run your executable now.
[*] When runtime is complete, press CTRL+C to stop logging.
```

run whatever you want, and Ctrl+C to stop scanning. Noriben will automatically open up a report on notepad.



In the folder you can see it has saved pml,csv and txt file report.



Download generic trojan malware on your VM:

https://dasmalwerk.eu/
ctrl f> 7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145bfc1af

original report for ref:
https://drive.google.com/file/d/1WgLJtFXZ2x96v9SzkoCMedJDERscdDBj/view?usp=sharing

We will study every PID and its child PIDs to undrstand the processes taking place.
These are the PIDs and child PIDs :

```
1160->3640->2364->160

3060    ->2400
        ->3484
        ->3676->3184

1912
```

pid 1160

EXPLORER.EXE is a Windows process that is run automatically at startup and remains an active process
This process is me trying to run the malware file that i downloaded.

```
[CreateProcess] Explorer.EXE:1160 >
"%WinDir%\system32\rundll32.exe %WinDir%\system32\shell32.dll,OpenAs_RunDLL %Loc
alAppData%\Temp\Temp1_7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145
bfc1af.zip\7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145bfc1af"
      [Child PID: 3640]
```

We see the SHA256 hash of file ans search it on VirusTotal. It shows that it is malicious trojan file.

```
[CreateFile]
Explorer.EXE:1160 > %LocalAppData%\Temp\Temp1_7682b842ed75b69e23c5deecf05a45ee79
c723d98cfb6746380d748145bfc1af.zip\7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6
746380d748145bfc1af     [SHA256:
7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145bfc1af]
```

I see another file with SHA256 = eacd.... it is undetected on VirusTotal.

```
[CreateFile]
Explorer.EXE:1160 > %LocalAppData%\Temp\Temp1_7682b842ed75b69e23c5deecf05a45ee79
c723d98cfb6746380d748145bfc1af.zip\7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6
746380d748145bfc1af:Zone.Identifier [SHA256:
eacd09517ce90d34ba562171d15ac40d302f0e691b439f91be1b6406e25f5913]
[CreateFile]
Explorer.EXE:1160 > %LocalAppData%\Temp\Temp1_7682b842ed75b69e23c5deecf05a45ee79
```

```
c723d98cfb6746380d748145bfc1af.zip\7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6
746380d748145bfc1af     [SHA256:
7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145bfc1af]
```

deleted Downloads.lnk file and downloaded new file (unmatched on VT).

```
[DeleteFile]
Explorer.EXE:1160 > %AppData%\Microsoft\Windows\Recent\Downloads.lnk
[CreateFile]
Explorer.EXE:1160 > %AppData%\Microsoft\Windows\Recent\Downloads.lnk   [SHA256:
cc8bf1c97171c1c1c376a5b856571eb9a2bb46c55924757d0b18435126856310]

[RegSetValue] Explorer.EXE:1160 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\Co
mponent Categories64\{56FFCC30-D398-11D0-B2AE-00A0C908FA49}\Enum\Implementing  =
1C 00 00 00 01 00 00 00 E4 07 07 00 04 00 17 00
```

pid 3640

runs 1af w rundll32.exe

```
[CreateProcess] rundll32.exe:3640 > "%ProgramFiles%
(x86)\Google\Chrome\Application\chrome.exe %LocalAppData%\Temp\Temp1_7682b842ed7
5b69e23c5deecf05a45ee79c723d98cfb6746380d748145bfc1af.zip\7682b842ed75b69e23c5de
ecf05a45ee79c723d98cfb6746380d748145bfc1af"     [Child PID: 2364]
```

changed Internet settings registry values.

```
[RegSetValue] rundll32.exe:3640 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass  =  1
[RegSetValue] rundll32.exe:3640 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName  =  1
[RegSetValue] rundll32.exe:3640 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\UNCAsIntranet  =  1
[RegSetValue] rundll32.exe:3640 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\AutoDetect  =  1
[RegSetValue] rundll32.exe:3640 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass  =  1
[RegSetValue] rundll32.exe:3640 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName  =  1
[RegSetValue] rundll32.exe:3640 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\UNCAsIntranet  =  1
[RegSetValue] rundll32.exe:3640 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\AutoDetect  =  1
```

pid 2364

chrome.exe process is created.

```
[CreateProcess] chrome.exe:2364 > "%ProgramFiles%
(x86)\Google\Chrome\Application\chrome.exe --type=crashpad-handler --user-data-
dir=%LocalAppData%\Google\Chrome\User Data /prefetch:7 --monitor-self-
```

```
annotation=ptype=crashpad-handler --database=%LocalAppData%\Google\Chrome\User
Data\Crashpad --metrics-dir=%LocalAppData%\Google\Chrome\User Data --
url=https://clients2.google.com/cr/report --annotation=channel= --
annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=84.0.4147.89 --
initial-client-
data=0xa0,0xa4,0xa8,0x74,0xac,0x7fef37eed20,0x7fef37eed30,0x7fef37eed40"
      [Child PID: 160]

[RegSetValue] chrome.exe:2364 >
HKCU\Software\Google\Chrome\BLBeacon\failed_count  =  0
[RegSetValue] chrome.exe:2364 > HKCU\Software\Google\Chrome\BLBeacon\state  =  2
[RegSetValue] chrome.exe:2364 >
HKCU\Software\Google\Chrome\ThirdParty\StatusCodes  =  01 00 00 00
[RegSetValue] chrome.exe:2364 > HKCU\Software\Google\Chrome\BLBeacon\state  =  1
```

pid 160

```
[CreateFolder] chrome.exe:160 > %LocalAppData%\Google\Chrome\User Data
```

pid 3060

```
[CreateProcess] chrome.exe:3060 > "%ProgramFiles%
(x86)\Google\Chrome\Application\chrome.exe --type=renderer --field-trial-
handle=1032,17826807827826495135,5480304491676239913,131072 --disable-gpu-
compositing --lang=en-US --enable-auto-reload --device-scale-factor=1 --num-
raster-threads=1 --renderer-client-id=47 --no-v8-untrusted-code-mitigations --
mojo-platform-channel-handle=1708 /prefetch:1" [Child PID: 2400]
[CreateProcess] chrome.exe:3060 > "%ProgramFiles%
(x86)\Google\Chrome\Application\chrome.exe --type=utility --utility-sub-
type=quarantine.mojom.Quarantine --field-trial-
handle=1032,17826807827826495135,5480304491676239913,131072 --lang=en-US --
service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-
channel-handle=2000 /prefetch:8"    [Child PID: 3484]
[CreateProcess] chrome.exe:3060 >
"%WinDir%\system32\rundll32.exe %WinDir%\system32\shell32.dll,OpenAs_RunDLL %Use
rProfile%\Downloads\7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145bf
c1af" [Child PID: 3676]
```

chrome downloads dbf.temp, renames it to 1af

```
[CreateFile] chrome.exe:3060 > %UserProfile%\Downloads\37afcac7-018f-4d7b-9572-
a94181ec5dbf.tmp  [File no longer exists]
[CreateFile] chrome.exe:3060 > %UserProfile%\Downloads\37afcac7-018f-4d7b-9572-
a94181ec5dbf.tmp  [File no longer exists]
[CreateFolder] chrome.exe:3060 > %UserProfile%\Downloads
[CreateFolder] chrome.exe:3060 > %UserProfile%\Downloads
[RenameFile] chrome.exe:3060 > %UserProfile%\Downloads\37afcac7-018f-4d7b-9572-
a94181ec5dbf.tmp
=> %UserProfile%\Downloads\7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d7
48145bfc1af.crdownload
[CreateFile]
chrome.exe:3060 > %UserProfile%\Downloads\7682b842ed75b69e23c5deecf05a45ee79c723
d98cfb6746380d748145bfc1af.crdownload    [File no longer exists]
[CreateFolder] chrome.exe:3060 > %UserProfile%\Downloads
[RenameFile]
chrome.exe:3060 > %UserProfile%\Downloads\7682b842ed75b69e23c5deecf05a45ee79c723
d98cfb6746380d748145bfc1af.crdownload
=> %UserProfile%\Downloads\7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d7
48145bfc1af

[CreateFolder] chrome.exe:3060 > %LocalAppData%\Google\Chrome\User Data\Default
```

Changes registry values.

Pid 3484

```
[CreateFile]
chrome.exe:3484 > %UserProfile%\Downloads\7682b842ed75b69e23c5deecf05a45ee79c723
d98cfb6746380d748145bfc1af:Zone.Identifier     [SHA256:
eacd09517ce90d34ba562171d15ac40d302f0e691b439f91be1b6406e25f5913]
```

some internet settings/zonemap regkey chnages

pid 3676

when I opened file with notepad

```
[CreateProcess] rundll32.exe:3676 >
"%WinDir%\system32\NOTEPAD.EXE %UserProfile%\Downloads\7682b842ed75b69e23c5deecf
05a45ee79c723d98cfb6746380d748145bfc1af" [Child PID: 3148]
```

changed registry values of zonemap.

Pid 1912

made MANY temp files which is a typical malware indication.

```
[CreateFile] svchost.exe:1912 > %WinDir%\Temp\TMP0000003EFB1BC8A7E69E6B2C
      [File no longer exists]
[CreateFile] svchost.exe:1912 > %WinDir%\Temp\TMP0000003FBB36FCB9733D49F9
      [File no longer exists]
[CreateFile] svchost.exe:1912 > %WinDir%\Temp\TMP00000040D99E6AC5842613C7
      [File no longer exists]
[CreateFile] svchost.exe:1912 > %WinDir%\Temp\TMP00000041F322CFB0B27A8937
      [File no longer exists]
[CreateFile] svchost.exe:1912 > %WinDir%\Temp\TMP00000042A754494F8C76936B
      [File no longer exists]
[CreateFile] svchost.exe:1912 > %WinDir%\Temp\TMP000000435A217BDACC141B54
      [File no longer exists]
```

So basically we had a few files downloaded and run (one of which is detected as trojan by virus total) and then deleted. Many temp files were opened by svc host which is not a good sign. Many register key values were changed (mostly internet settings/zonemap)