Need to do setup on VM

1. Unzip logstash tar file to Desktop (path for zip file: Google drive->”GNN2023”->”SilkETW->Logstash” ) or

Download it from- <https://www.elastic.co/downloads/logstash>

1. Add “logstash-sample.conf” and “pipeline\_conf.conf” to path: “C:\Users\<user-name>\Desktop\logstash-8.10.0\config”
   * Both files should have the same content.
2. Run command in powershell with admin **(Script can do this)**
   1. go to the directory→ cd C:\Users\<username>\Desktop\logstash-8.10.0\bin
   2. run command → $env:LOGSTASH\_INDEX="any\_index\_name\_in\_small\_letters"
   3. run command → .\logstash -f C:\Users\<username>\Desktop\logstash-8.10.0\config\logstash-sample.conf
3. Download and Extract SilkETW zip-file to **“C:\Users\<username>\Downloads”** (Download - [SilkETW\_SilkService\_v8.zip](https://github.com/mandiant/SilkETW/releases/download/v0.8/SilkETW_SilkService_v8.zip)[Releases · mandiant/SilkETW (github.com)](https://github.com/mandiant/SilkETW/releases))
4. Add the “SilkServiceConfig.xml” in shared-drive to - “SilkETW\_SilkService\_v8\v8\SilkService”
5. Run command in powershell with admin
   1. sc.exe create SilkService binPath= "C:\Users\**<user-name>**\Downloads\SilkETW\_SilkService\_v8\v8\SilkService\SilkService.exe" start= demand
   2. Go to the services and look for “SilkService” and click on “start” to start the service **(Script can do this-on agent.py)**
   3. Alternative way to start the service using powershell - Start-Service SilkService **(Script can do this-on agent.py)**
6. Note: Add pipelines.yml from shared drive to “C:\Users\<username>\Desktop\logstash-8.10.0\config” file to “puma-4” instead “etw0” (i.e. correct username)

**Client.py**

1. No change.
2. (Optional)
   1. we can remove the part of the code, where we don't want to get back the PID of powershell

**Agent.py**

1. Removed the pywintrace code
2. Does not block any PID
3. Only take filename form client/host and do the following
   1. One powershell for apache
   2. Download the github source link from apache and extract it
   3. Set execution policy
   4. Terminate the first powershell
   5. Start another powershell to start logstash pipeline
      1. Run logstash commands
         1. setting elastic search index
         2. start logstash service
   6. Start another powershell to
      1. Start silkservice
      2. Run powershell scripts (.ps1)
      3. Stop silkservice
   7. Terminate silkservice powershell
   8. Terminate logstash powershell
4. Optional
   1. Get back recorded powershell PID to host

**Subgrah code path- /home/pwakodi1/tabby/STREAMLINED\_DATA\_GENERATION\_MultiGraph/STEP\_2\_Benign\_NON\_TARGETTED\_SUBGRAPH\_GENERATION\_GeneralLogCollection\_subgraphs/model\_v3\_PW**

**Malware Powershell scripts GitHub links**

**--- Collected samples ( Total: 291 samples)**

[**https://github.com/EmpireProject/Empire/tree/master/data**](https://github.com/EmpireProject/Empire/tree/master/data)

[**https://github.com/danielbohannon/Invoke-Obfuscation**](https://github.com/danielbohannon/Invoke-Obfuscation)

[**https://github.com/nettitude/PoshC2/tree/master/resources/modules**](https://github.com/nettitude/PoshC2/tree/master/resources/modules)

[**https://github.com/samratashok/nishang**](https://github.com/samratashok/nishang)

[**https://github.com/PowerShellMafia/PowerSploit**](https://github.com/PowerShellMafia/PowerSploit)

[**https://github.com/jrussellfreelance/powershell-scripts**](https://github.com/jrussellfreelance/powershell-scripts)

[**https://github.com/nullbind/Powershellery**](https://github.com/nullbind/Powershellery)

[**https://github.com/xorrior/RandomPS-Scripts**](https://github.com/xorrior/RandomPS-Scripts)

[**https://github.com/RaouzRouik/smallposh**](https://github.com/RaouzRouik/smallposh)

[**https://github.com/BlackSnufkin/PT-ToolKit/tree/f78567ce9b4701acfd6af21196b95eef44bbc9c5/PowerShell-Scripts**](https://github.com/BlackSnufkin/PT-ToolKit/tree/f78567ce9b4701acfd6af21196b95eef44bbc9c5/PowerShell-Scripts)

[**https://github.com/gtworek/PSBits**](https://github.com/gtworek/PSBits)

[**https://github.com/IAMinZoho/OFFSEC-PowerShell**](https://github.com/IAMinZoho/OFFSEC-PowerShell)

[**https://bazaar.abuse.ch/browse.php?search=tag%3Aps1**](https://bazaar.abuse.ch/browse.php?search=tag%3Aps1)

[**https://virustotal.com**](https://virustotal.com/)

**Benign Powershell Script GitHub links**

**--- Collected samples ( Total: 313 samples)**

1. [**https://github.com/LeDragoX/Win-Debloat-Tools/tree/main/src/scripts**](https://github.com/LeDragoX/Win-Debloat-Tools/tree/main/src/scripts) **(need dict)**
2. [**https://github.com/jhochwald/PowerShell-collection**](https://github.com/jhochwald/PowerShell-collection)
3. [**https://github.com/stevencohn/WindowsPowerShell**](https://github.com/stevencohn/WindowsPowerShell) **(need dict)**
4. [**https://github.com/fleschutz/PowerShell**](https://github.com/fleschutz/PowerShell)
5. [**https://github.com/farag2/Utilities**](https://github.com/farag2/Utilities)
6. [**https://github.com/nickrod518/PowerShell-Scripts**](https://github.com/nickrod518/PowerShell-Scripts)
7. [**https://github.com/nickbeau/PowerShellScripting/tree/master/scripts**](https://github.com/nickbeau/PowerShellScripting/tree/master/scripts) [**https://github.com/redlttr/scripts**](https://github.com/redlttr/scripts)
8. [**https://github.com/ErickRock/Sysadmin-Survival-Kit-Scripts**](https://github.com/ErickRock/Sysadmin-Survival-Kit-Scripts)
9. [**https://github.com/jimbrig/PSScripts**](https://github.com/jimbrig/PSScripts)
10. [**https://github.com/nickrod518/Zoom-PowerShell**](https://github.com/nickrod518/Zoom-PowerShell)
11. [**https://github.com/devblackops/Terminal-Icons**](https://github.com/devblackops/Terminal-Icons)
12. [**https://github.com/jrussellfreelance/powershell-scripts**](https://github.com/jrussellfreelance/powershell-scripts)
13. [**https://github.com/FlorianTim/autosetup\_win/tree/master**](https://github.com/FlorianTim/autosetup_win/tree/master) **(need dict)**