29. OWASP Stammtisch

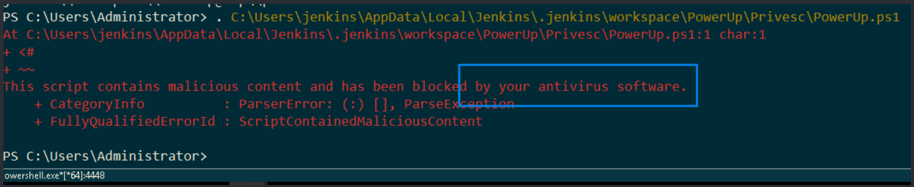
Building malicious code continuously

Marko Winkler – 19. Juli 2022

Outline

1. Introduction
2. Design and Implementation
3. Demo
4. Outlook & QA
5. Refs

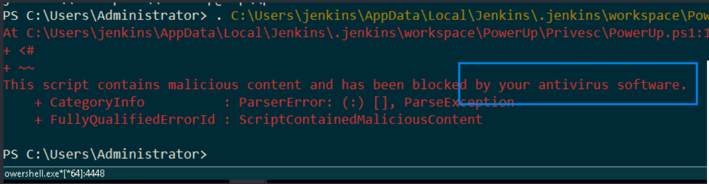
Motivation



```
PS C:\Users\Administrator> . C:\Users\jenkins\AppData\Local\Jenkins\.jenkins\workspace\PowerUp\Privesc\PowerUp.ps1
At C:\Users\jenkins\AppData\Local\Jenkins\.jenkins\workspace\PowerUp\Privesc\PowerUp.ps1:1 char:1
+ <#
+ ~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\Administrator>
```

Motivation



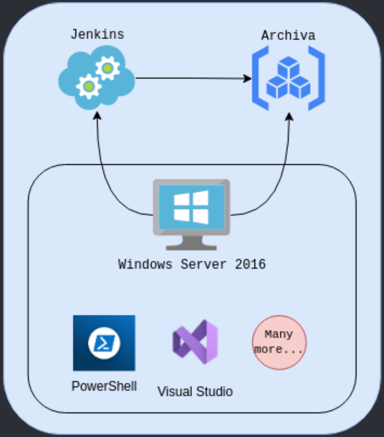
```
PS C:\Users\Administrator> . C:\Users\jenkins\AppData\Local\Jenkins\.jenkins\workspace\PowerUp\Privesc\PowerUp.ps1
At C:\Users\jenkins\AppData\Local\Jenkins\.jenkins\workspace\PowerUp\Privesc\PowerUp.ps1:1 char:1
+ <#
+ ~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\Administrator>
```

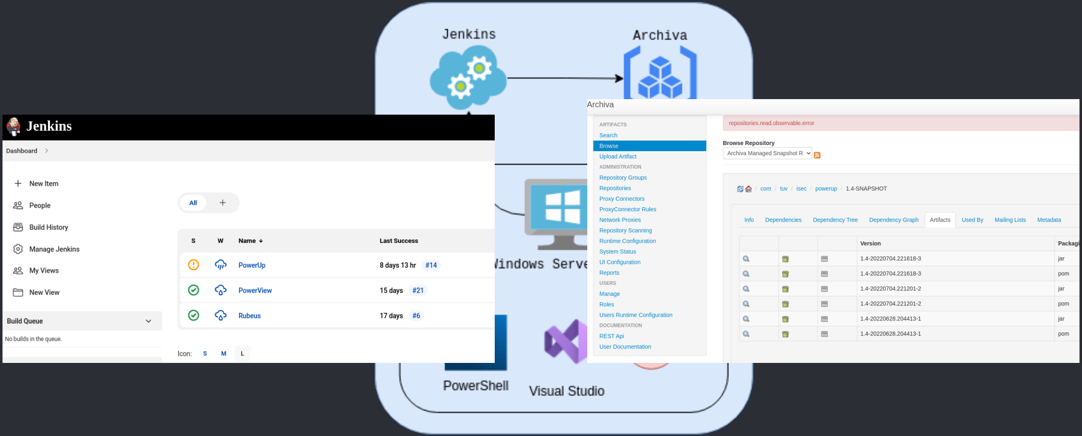
Outline

1. Introduction
2. Design and Implementation
3. Demo
4. Outlook & QA
5. Refs

Architecture



Architecture



No builds in the queue.

S	W	Name ↓	Last Success
!		PowerUp	8 days 13 hr #14
✓		PowerView	15 days #21
✓		Rubeus	17 days #6

repositories.read.observable.error

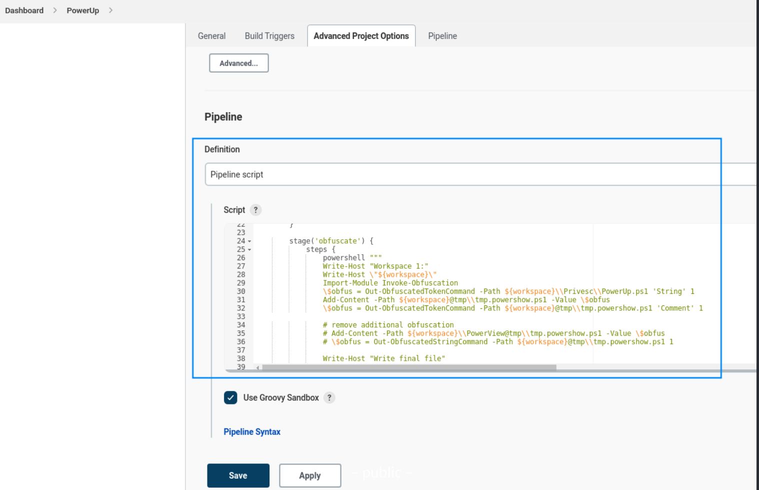
Browse Repository: Archiva Managed Snapshot R

com / tuv / isec / powerup / 1.4-SNAPSHOT

			Version	Packagi
			1.4-20220704.221618-3	jar
			1.4-20220704.221618-3	pom
			1.4-20220704.221201-2	jar
			1.4-20220704.221201-2	pom
			1.4-20220628.204413-1	jar
			1.4-20220628.204413-1	pom

Jenkins

Pipeline



Pipeline

Definition

Pipeline script

Script ?

```
        }

        stage('obfuscate') {
            steps {
                powershell """
                Write-Host "Workspace 1:"
                Write-Host \"${workspace}\"
                Import-Module Invoke-Obfuscation
                \$obfus = Out-ObfuscatedTokenCommand -Path ${workspace}\\Privesc\\PowerUp.ps1 'String' 1
                Add-Content -Path ${workspace}@tmp\\tmp.powershow.ps1 -Value \$obfus
                \$obfus = Out-ObfuscatedTokenCommand -Path ${workspace}@tmp\\tmp.powershow.ps1 'Comment' 1

                # remove additional obfuscation
                # Add-Content -Path ${workspace}\\PowerView@tmp\\tmp.powershow.ps1 -Value \$obfus
                # \$obfus = Out-ObfuscatedStringCommand -Path ${workspace}@tmp\\tmp.powershow.ps1 1

                Write-Host "Write final file"
```

☑ Use Groovy Sandbox ?

Jenkins

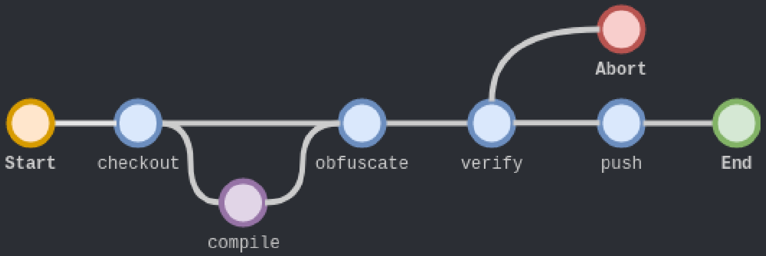
Sample Jenkins Pipeline Script

```
pipeline {
  agent any
  environment { PROJECT_NAME = "PowerSploit" }

  stages {
    stage('Checkout') {
      steps {
        git """https://github.com/PowerShellMafia/${env.PROJECT_NAME}.git"""
      }}
    stage('Obfuscate') {
      steps {
        powershell '''
        Import-Module Invoke-Obfuscation
```

Stages

Overview



Stages

Tools

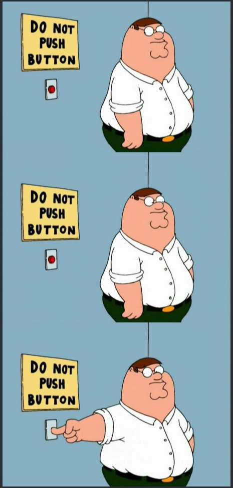
- **Checkout** – Git
- (opt.) **Compile** – msbuild
- **Obfuscate**
  - Invoke-Obfuscation [3] (PowerShell)
  - ConfuserEx [4] (.Net)

  ...
- **Verify** – ThreatCheck [5]
- **Push** – Maven

Outline

1. Introduction
2. Design and Implementation
3. Demo
4. Outlook & QA
5. Refs

Demo



Outline

1. Introduction
2. Design and Implementation
3. Demo
4. Outlook & QA
5. Refs

Outlook

- Malicious Jenkins (`pwn_jenkins`) – Alternatives?
- Adding more techniques or tools
- Other solutions?

QA

Outline

1. Introduction
2. Design and Implementation
3. Demo
4. Outlook & QA
5. Refs

References

[1] *OffSecOps: Using Jenkins For Red Team Tooling* – https://http418infosec.com/offsecops-using-jenkins-for-red-team-tooling Access on 06/07/2022

[2] Will Schroeder (Harmj0y) – *OffSecOps* – https://github.com/specterops/presentations/raw/master/Will%20Schroeder/OffSecOps_SO-CON2020.pdf Access on 06/07/2022

[3] Daniel Bohannon – *Invoke-Obfuscation* – https://github.com/danielbohannon/Invoke-Obfuscation Access on 06/07/2022

[4] Martin Karing – *ConfuserEx* – https://github.com/mkaring/ConfuserEx Access on 06/07/2022

[5] Rasta Mouse – *ThreatCheck* – https://github.com/rasta-mouse/ThreatCheck Access on 06/07/2022

[6] Marko Winkler – *Malicious Jenkins (Work in progress)* – https://github.com/no-sec-marko/malicious-jenkins.git Access on 19/07/2022