Building malicious code continuously

Marko Winkler – 19. Juli 2022
Motivation

This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo : ParserError: (:) [], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent
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
```
Outline

1. Introduction

2. Design and Implementation

3. Demo

4. Outlook & QA

5. Refs
Architecture

- Jenkins
- Archiva
- Windows Server 2016
- PowerShell
- Visual Studio
- Many more...
Architecture
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

**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
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?
Outline

1. Introduction

2. Design and Implementation

3. Demo

4. Outlook & QA

5. Refs
References


