Hello 1994:

Abusing Windows Explorer via Component Object Model in 2023

Mike Harbison
Unit 42, Distinguished Engineer

REcon June 2023

Whoami /all

USER INFORMATION

Name	**Occupation**
Mike Harbison	**6+ years with Palo Alto Networks Unit 42 Threat Intel Team**

USER BACKGROUND

- Computer Forensic Examiner w. DC3/Mandiant
- Vulnerability Researcher
- Reverse Engineer since SoftICE

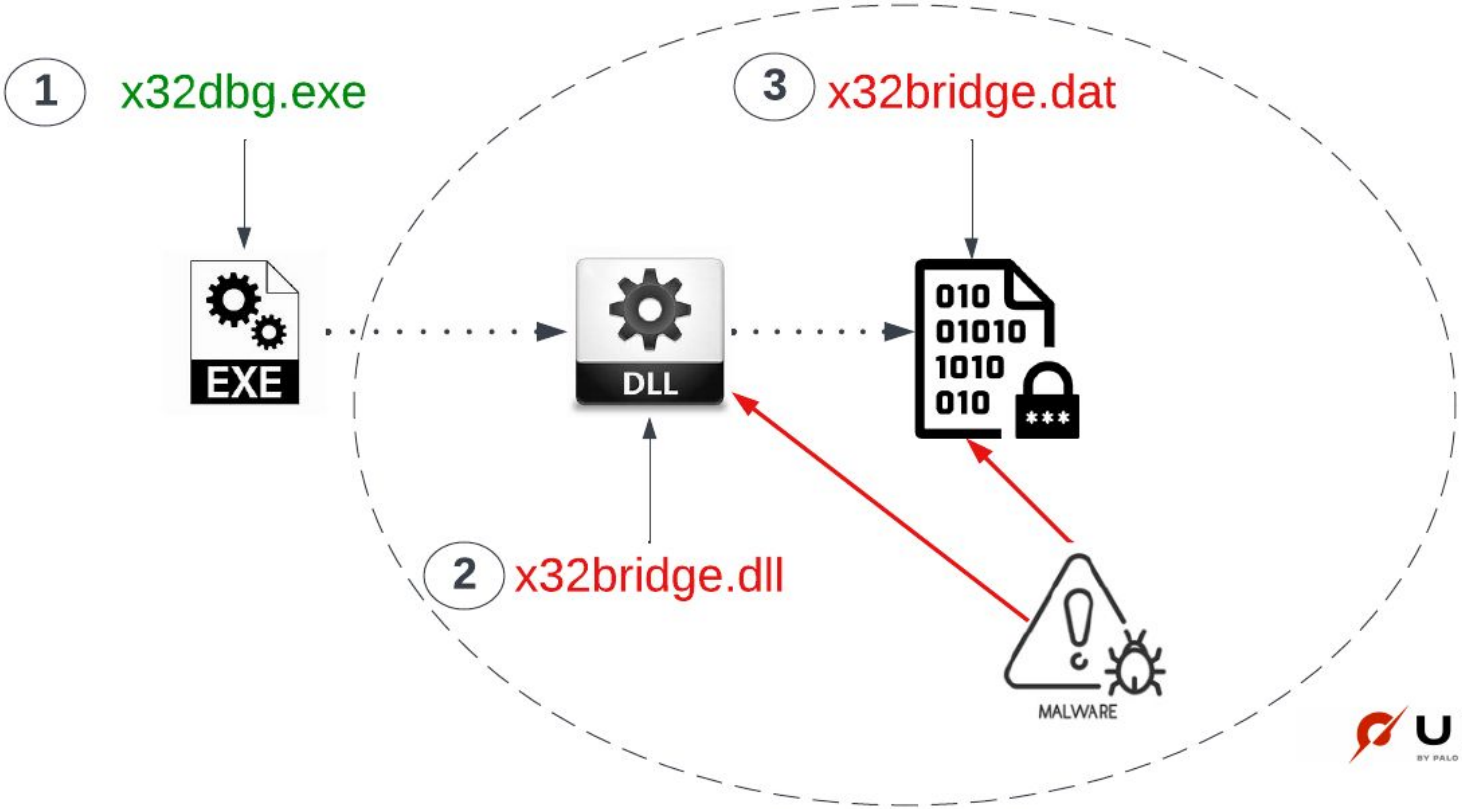
Agenda

- PlugX Malware Discovery
- Overview of COM
- USB Infection Technique
- Microsoft's Response
- Q & A

What is PlugX?

- Fully-featured remote access tool (RAT) that targets Windows OS
- First seen in 2008
- Chinese nexus but used by various nation state threat actors
- Historically abuses trusted software to DLL side load an **encrypted** payload in-memory
- Considered one of the oldest, evolving malware families

PlugX Infection Method - DLL Sideloading



Journey into the IUnknown: Discovery Timeline

- **January 2023** - Discovered interesting PlugX malware sample while investigating a Black Basta ransomware case: **x32bridge.dat**
- **January 22, 2021** - **x32bridge.dat** first uploaded to VirusTotal from Thailand*
    - 4 / 60 AV engines identified the sample as malware at that time
- **July 4, 2019** - PE Compilation date and time

*** No prior mention or detection of USB capabilities**

USB Infection and Concealment Key Components

1. Targets all type 2 DRIVE_REMOVABLE devices attached to a host
2. Implementation of Shortcut COM object
3. Implementation of Recycle Bin COM object
4. Use of a Unicode character (**N**on-**B**reaking **SP**ace) as a directory name

The combination of the Recycle Bin + the NBSP prevents the Windows OS from accessing the directory

What is COM?

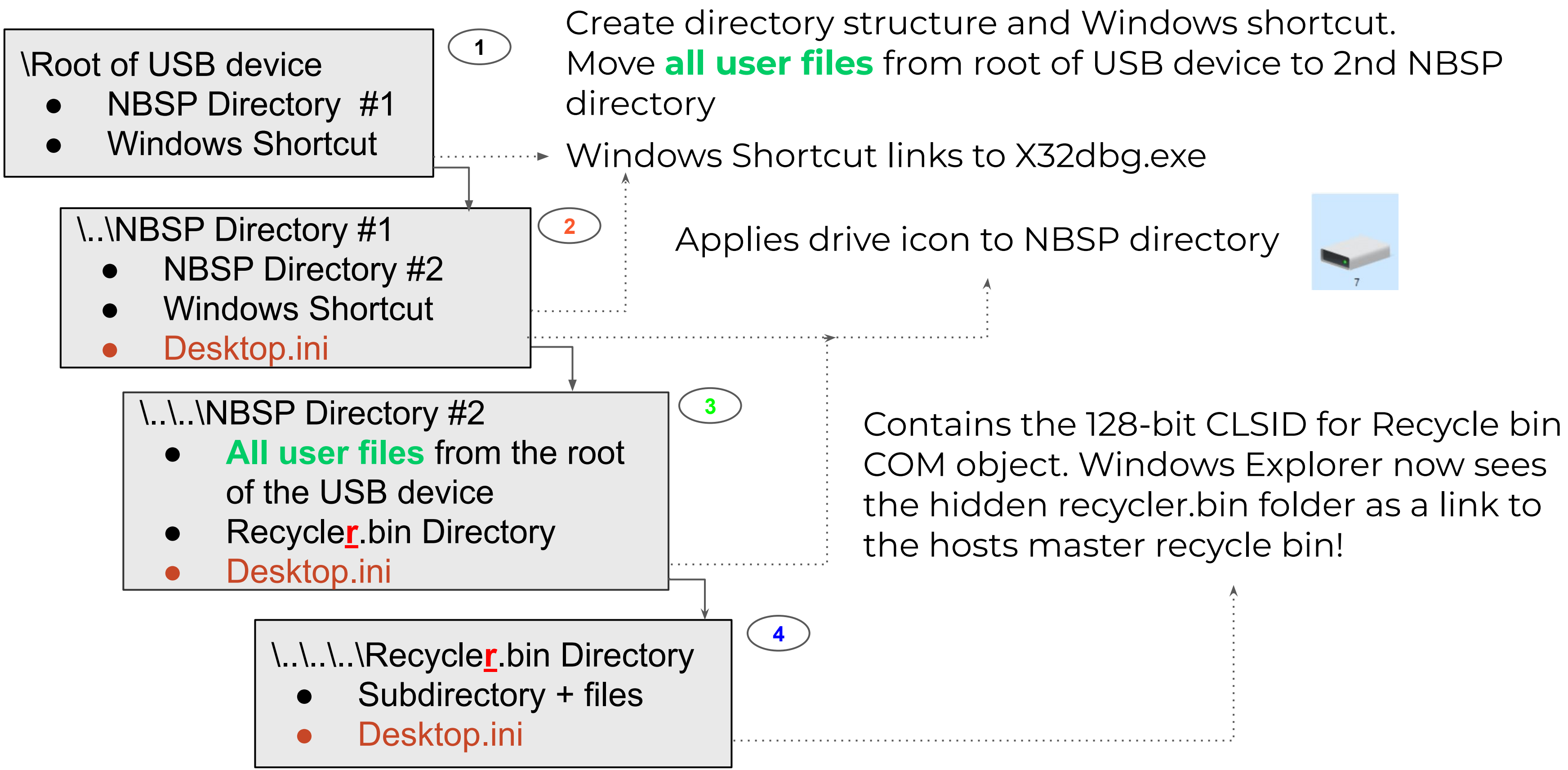
Microsoft Definition -

"COM is a platform-independent, distributed, object-oriented system for creating binary software components that can interact. COM is the foundation technology for Microsoft's OLE (compound documents) and ActiveX (Internet-enabled components) technologies."

Component Object Model (COM) is a binary interface standard for software components introduced by Microsoft in late **1993 early 1994**!

Programming COM involves the use of COM-aware components. Components are identified by a unique ID 128-bit CLSID, which are globally unique identifiers. The components expose their functionality through one or more interfaces.

USB Infection Stages



\Root of USB device
- NBSP Directory #1
- Windows Shortcut

1

Create directory structure and Windows shortcut. Move **all user files** from root of USB device to 2nd NBSP directory

Windows Shortcut links to X32dbg.exe

\..\NBSP Directory #1
- NBSP Directory #2
- Windows Shortcut
- Desktop.ini

2

Applies drive icon to NBSP directory

\..\..\NBSP Directory #2
- **All user files** from the root of the USB device
- Recycle**r**.bin Directory
- Desktop.ini

3

Contains the 128-bit CLSID for Recycle bin COM object. Windows Explorer now sees the hidden recycler.bin folder as a link to the hosts master recycle bin!

\..\..\..\Recycle**r**.bin Directory
- Subdirectory + files
- Desktop.ini

4

COM Class Factories

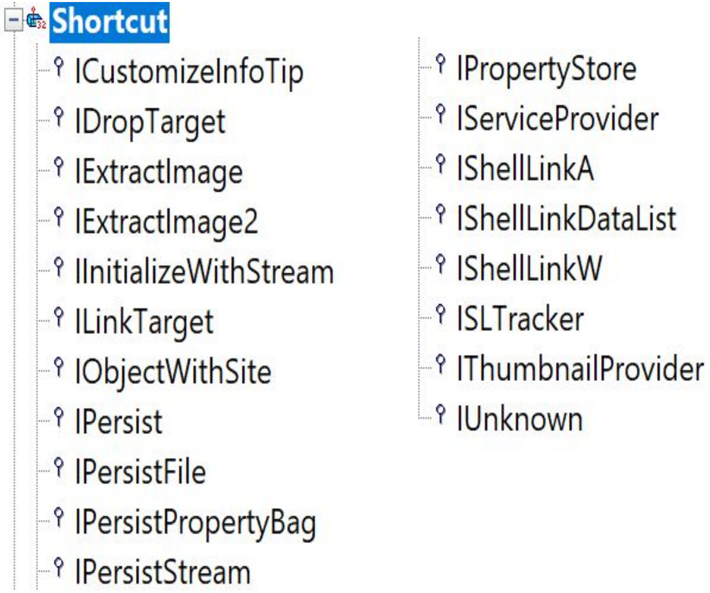
- Used to create the Windows shortcut file(s)
  - 128-bit CLSID (RIID) of **`00021401-0000-0000-C000-000000000046`**
  - “Shortcut”

- Used to turn a folder to link to the master Recycle bin
  - 128-bit CLSID (RIID) of **`645FF040-5081-101B-9F08-00AA002F954E`**
  - “Recycle Bin”

COM Class Factories - Shortcut

- 128-bit CLSID (RIID) of **00021401-0000-0000-C000-000000000046**

- CLSID_ShellLink (Shortcut) class implements the following interfaces in windows.storage.dll version 10.0 taken from Windows 10 version 21H2



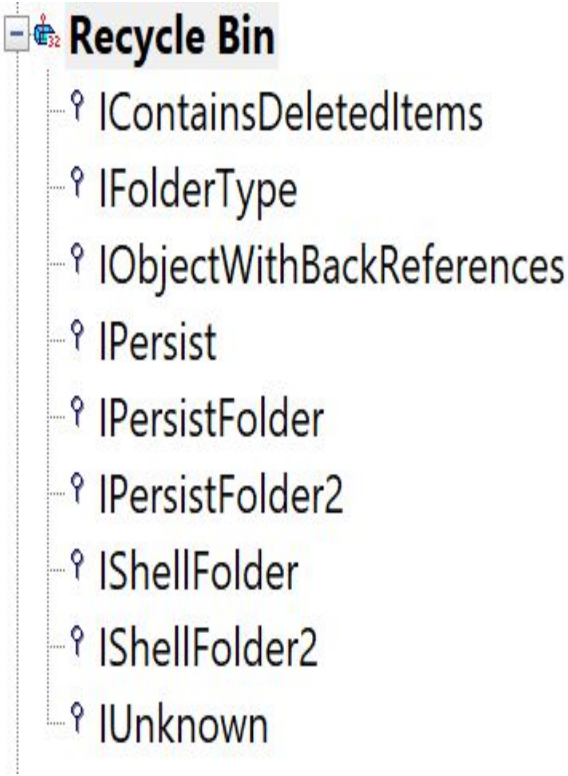
Shortcut

- ICustomizeInfoTip
- IDropTarget
- IExtractImage
- IExtractImage2
- IInitializeWithStream
- ILinkTarget
- IObjectWithSite
- IPersist
- IPersistFile
- IPersistPropertyBag
- IPersistStream
- IPropertyStore
- IServiceProvider
- IShellLinkA
- IShellLinkDataList
- IShellLinkW
- ISLTracker
- IThumbnailProvider
- IUnknown

COM Class Factories - Recycle Bin

- 128-bit CLSID (RIID) of **645FF040-5081-101B-9F08-00AA 002F954E**

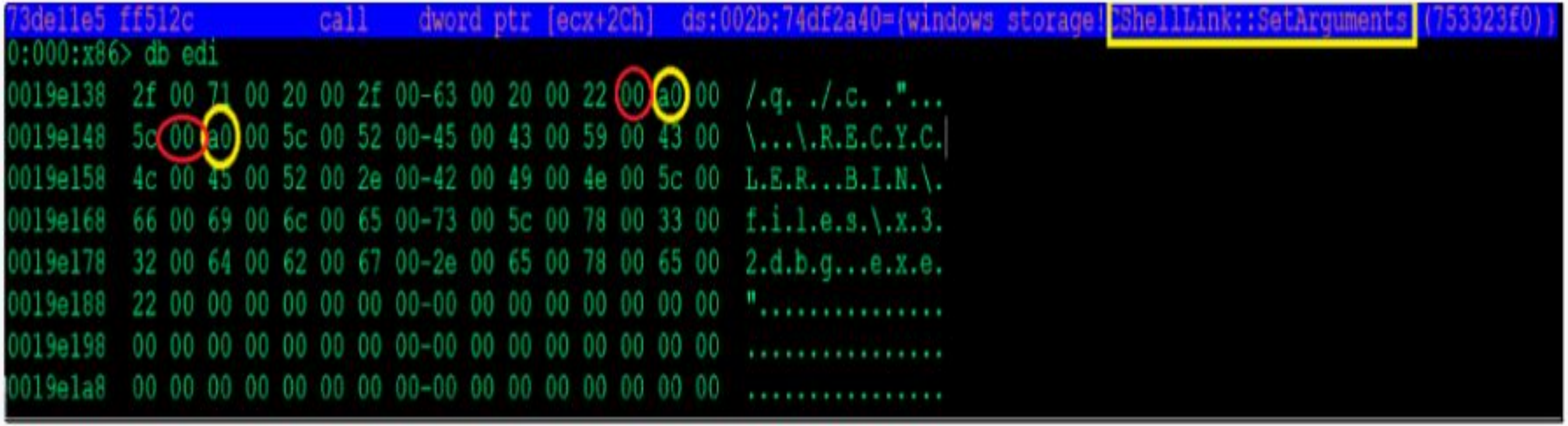
- CLSID_Recyle Bin class implements the following interfaces in shell32.dll version 10.0 taken from Windows 10 version 21H2



Recycle Bin
- IContainsDeletedItems
- IFolderType
- IObjectWithBackReferences
- IPersist
- IPersistFolder
- IPersistFolder2
- IShellFolder
- IShellFolder2
- IUnknown

Shortcut File Creation

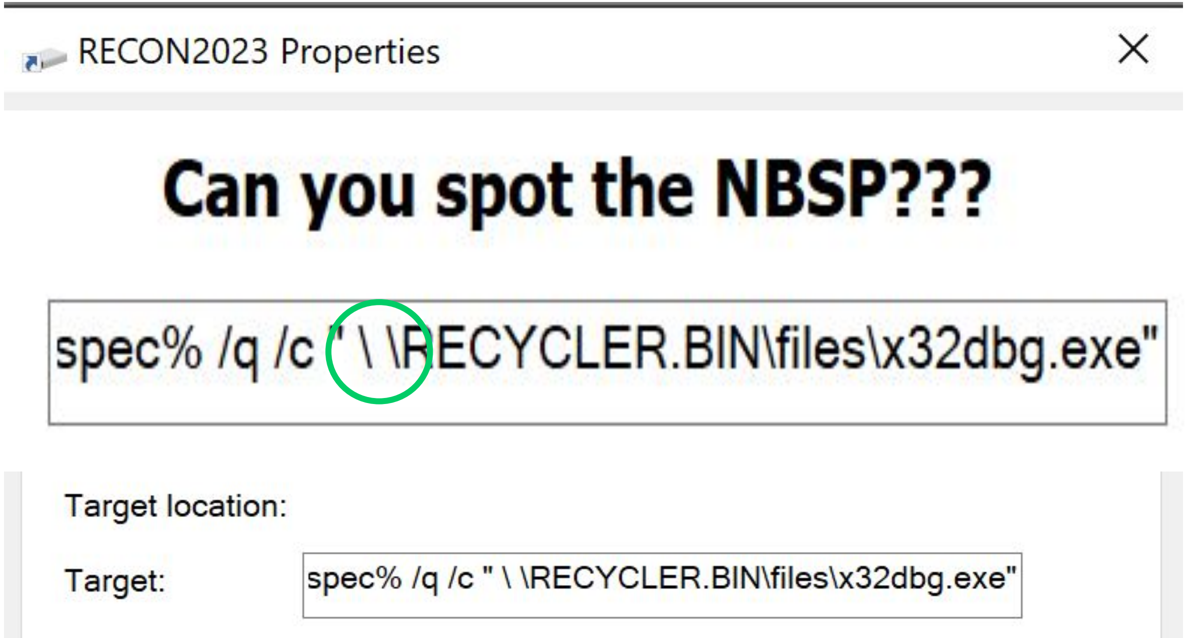
- The shortcut COM object uses the Windows.Storage namespace
- This class allows for the managing of files, folders, and application



```
73de11e5 ff512c          call    dword ptr [ecx+2Ch]  ds:002b:74df2a40={windows_storage!CShellLink::SetArguments (753323f0)}
0:000:x86> db edi
0019e138  2f 00 71 00 20 00 2f 00-63 00 20 00 22 00 a0 00  /.q. ./.c. ."...
0019e148  5c 00 a0 00 5c 00 52 00-45 00 43 00 59 00 43 00  \...\.R.E.C.Y.C.
0019e158  4c 00 45 00 52 00 2e 00-42 00 49 00 4e 00 5c 00  L.E.R...B.I.N.\.
0019e168  66 00 69 00 6c 00 65 00-73 00 5c 00 78 00 33 00  f.i.l.e.s.\.x.3.
0019e178  32 00 64 00 62 00 67 00-2e 00 65 00 78 00 65 00  2.d.b.g...e.x.e.
0019e188  22 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  "...............
0019e198  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0019e1a8  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
```

  - Sets the ICON file for the new object to shell32.dll number 7
  - Finally calling IPersistFile::Save to save the **object** to disk

Shortcut File On USB Device



RECON2023 Properties

Can you spot the NBSP???

```
spec% /q /c " \ \RECYCLER.BIN\files\x32dbg.exe"
```

Target location:

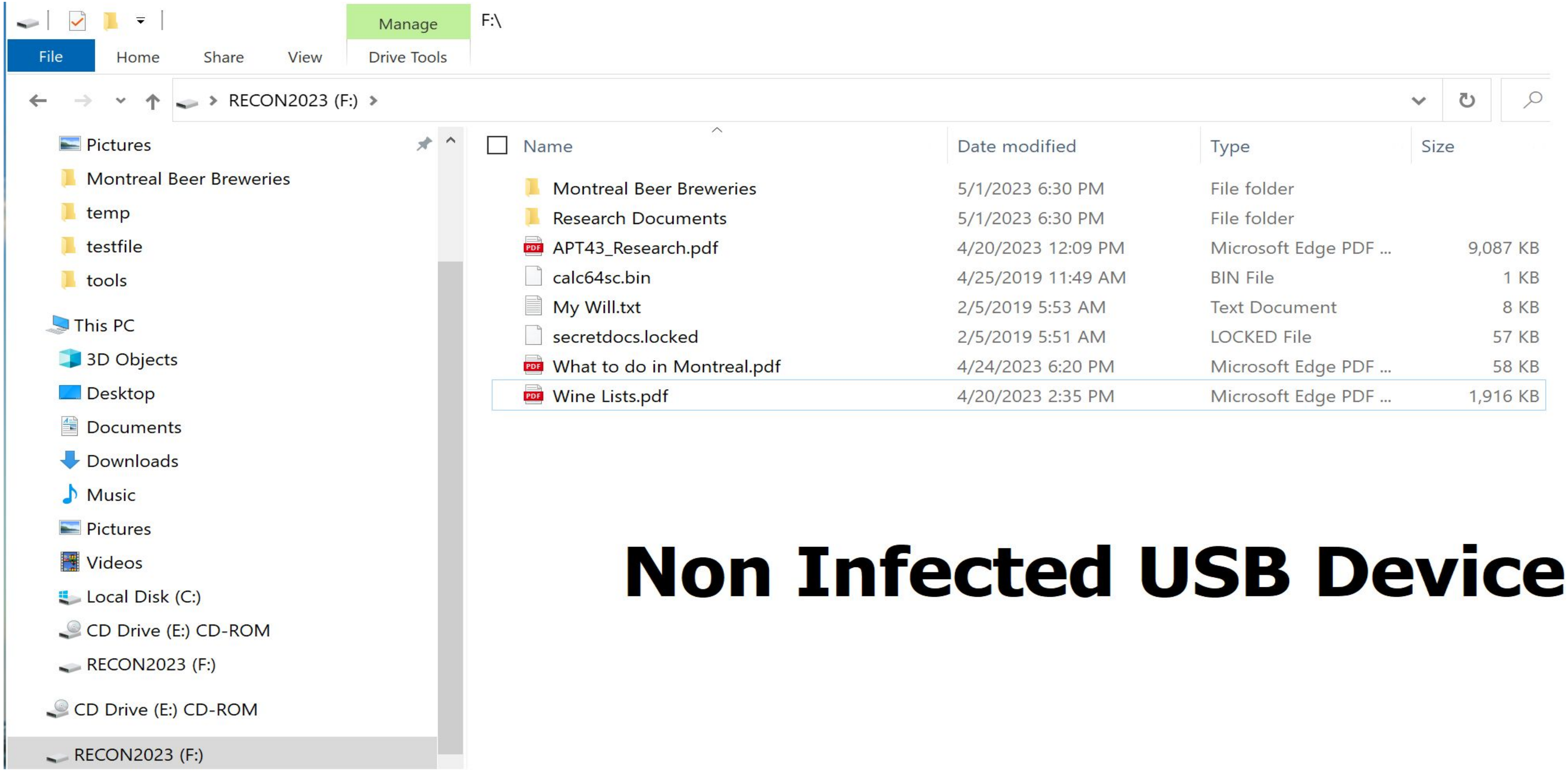
Target: `spec% /q /c " \ \RECYCLER.BIN\files\x32dbg.exe"`

Significance of the NBSP Directory (0x00A0)

- Windows Explorer and the command console (cmd.exe) are unable to traverse into the NBSP directory located in the recycler.bin directory
- The whitespace character is preventing the OS from rendering the directory name, making the folder invisible (rather than leaving a nameless folder in Windows Explorer).
- If an NBSP directory wasn't used in the recycler.bin directory, a user would be able to traverse the path and delete the corresponding file(s).

Walk-Through Demo

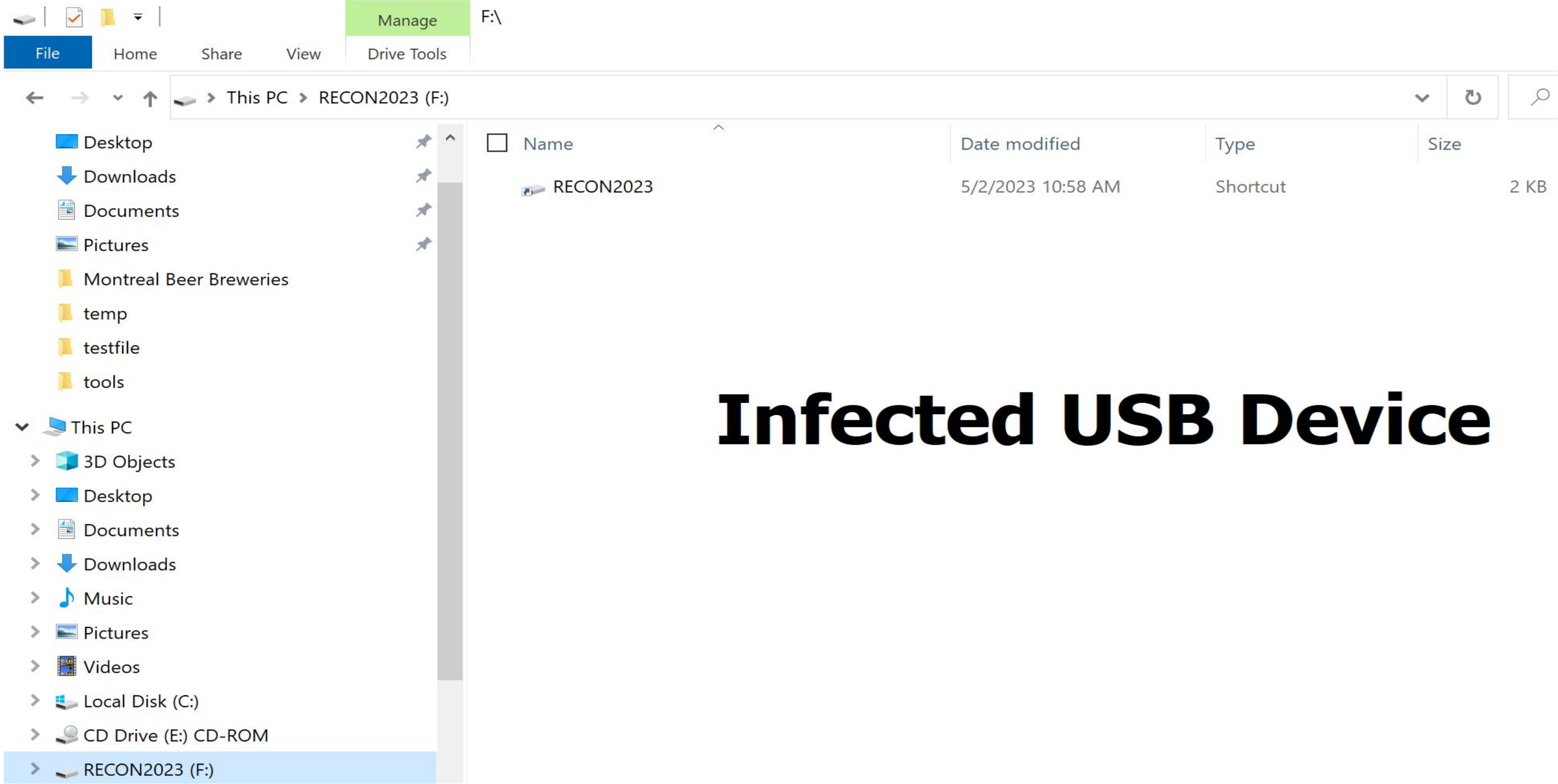
Pre and Post USB Infection



Name	Date modified	Type	Size
Montreal Beer Breweries	5/1/2023 6:30 PM	File folder	
Research Documents	5/1/2023 6:30 PM	File folder	
APT43_Research.pdf	4/20/2023 12:09 PM	Microsoft Edge PDF ...	9,087 KB
calc64sc.bin	4/25/2019 11:49 AM	BIN File	1 KB
My Will.txt	2/5/2019 5:53 AM	Text Document	8 KB
secretdocs.locked	2/5/2019 5:51 AM	LOCKED File	57 KB
What to do in Montreal.pdf	4/24/2023 6:20 PM	Microsoft Edge PDF ...	58 KB
Wine Lists.pdf	4/20/2023 2:35 PM	Microsoft Edge PDF ...	1,916 KB

Non Infected USB Device

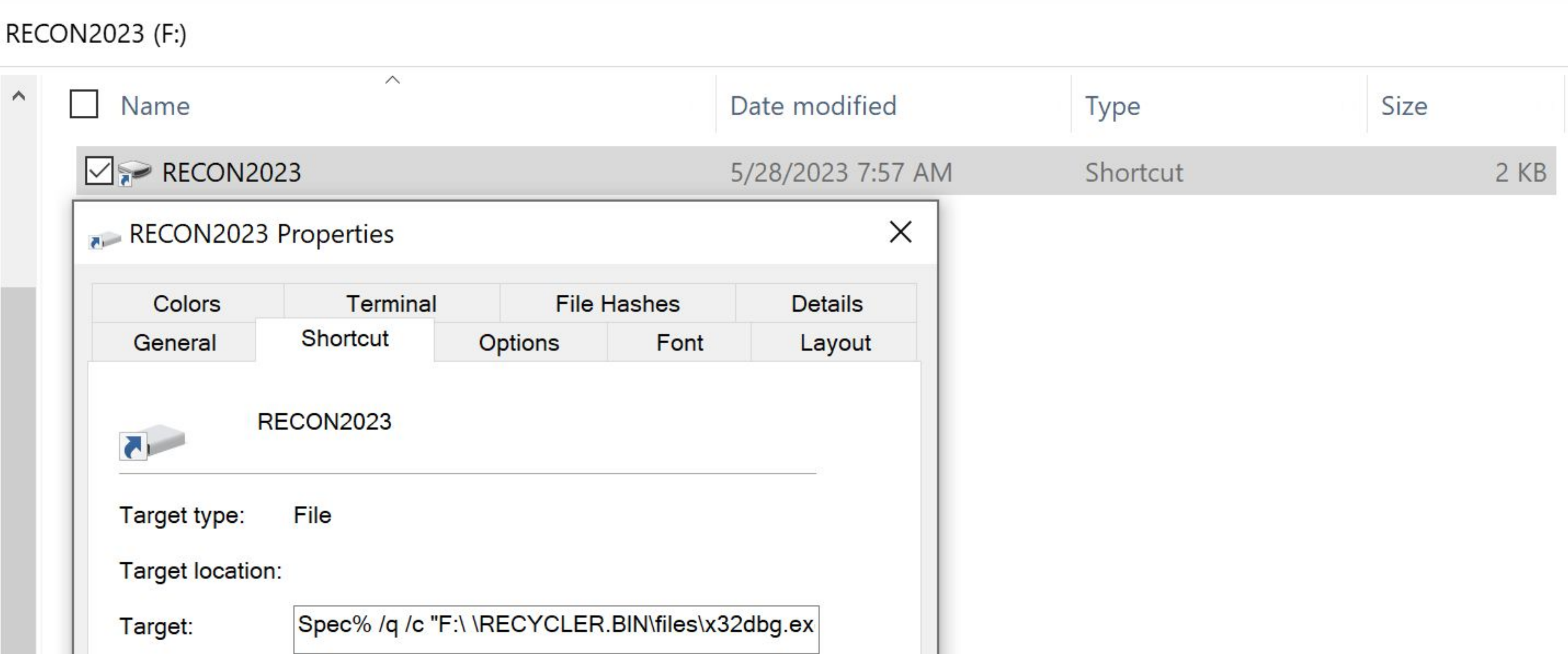
Post USB Infection



Name	Date modified	Type	Size
RECON2023	5/2/2023 10:58 AM	Shortcut	2 KB

Infected USB Device

Post USB Infection Shortcut



RECON2023 (F:)

□ Name	Date modified	Type	Size
☑ RECON2023	5/28/2023 7:57 AM	Shortcut	2 KB

RECON2023 Properties

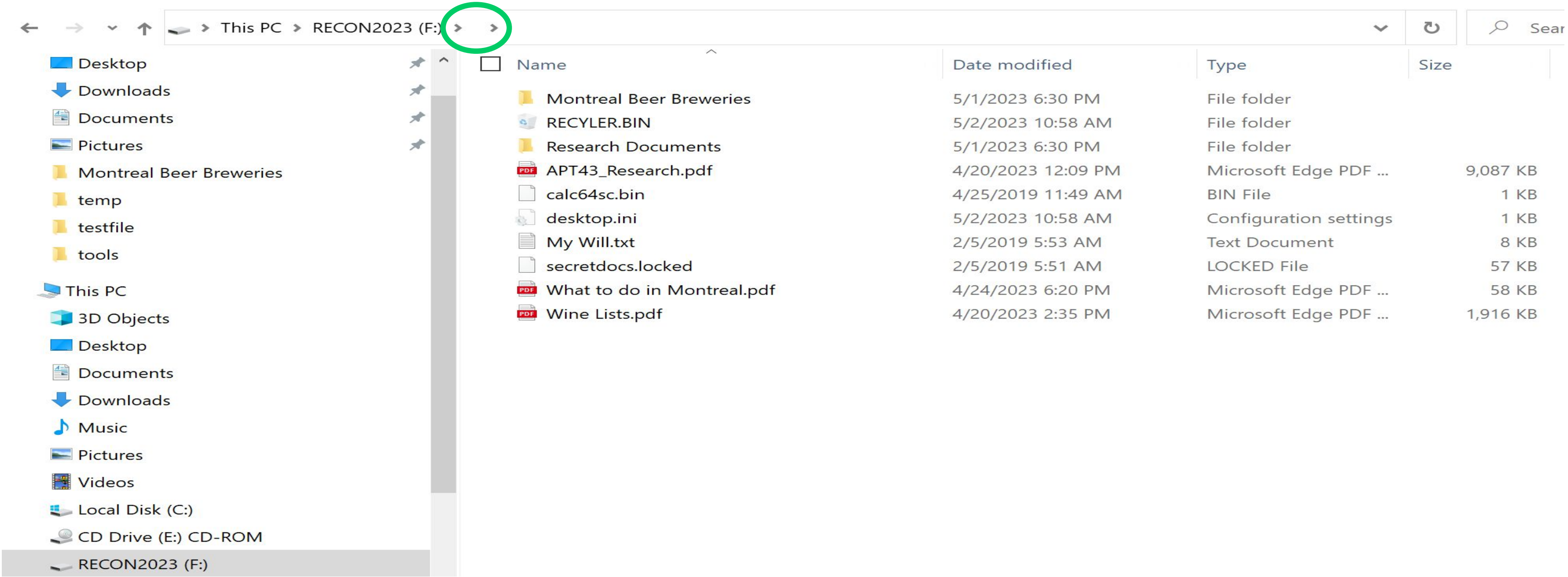
RECON2023

Target type: File

Target location:

Target: Spec% /q /c "F:\ \RECYCLER.BIN\files\x32dbg.ex

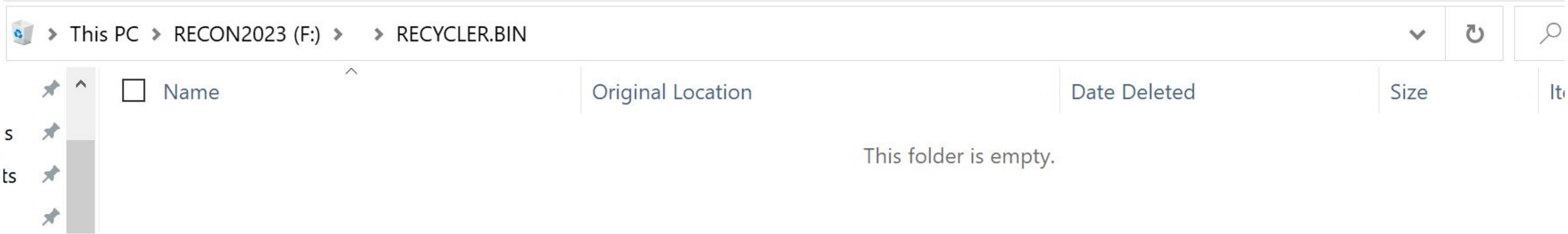
Post USB Infection - Hiding in Plain Sight



Name	Date modified	Type	Size
Montreal Beer Breweries	5/1/2023 6:30 PM	File folder	
RECYLER.BIN	5/2/2023 10:58 AM	File folder	
Research Documents	5/1/2023 6:30 PM	File folder	
APT43_Research.pdf	4/20/2023 12:09 PM	Microsoft Edge PDF ...	9,087 KB
calc64sc.bin	4/25/2019 11:49 AM	BIN File	1 KB
desktop.ini	5/2/2023 10:58 AM	Configuration settings	1 KB
My Will.txt	2/5/2019 5:53 AM	Text Document	8 KB
secretdocs.locked	2/5/2019 5:51 AM	LOCKED File	57 KB
What to do in Montreal.pdf	4/24/2023 6:20 PM	Microsoft Edge PDF ...	58 KB
Wine Lists.pdf	4/20/2023 2:35 PM	Microsoft Edge PDF ...	1,916 KB

Can you spot the NBSP?

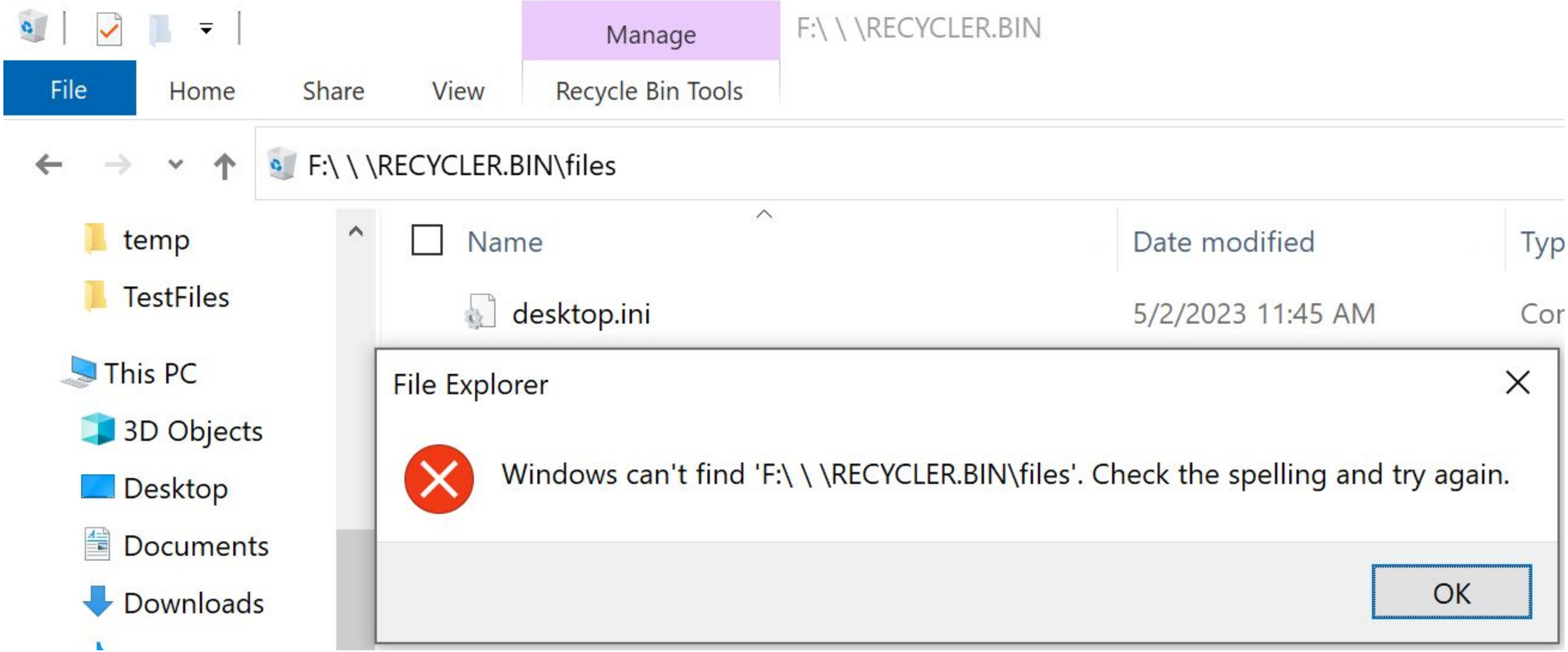
USB Recycler Bin Folder



This folder is empty.

- Not showing directories / files that were created
- Links to host master recycle bin on the root directory and not the USB device
- NBSP visibility makes it hard to detect as it looks like the F drive

Windows File Explorer - Not Found

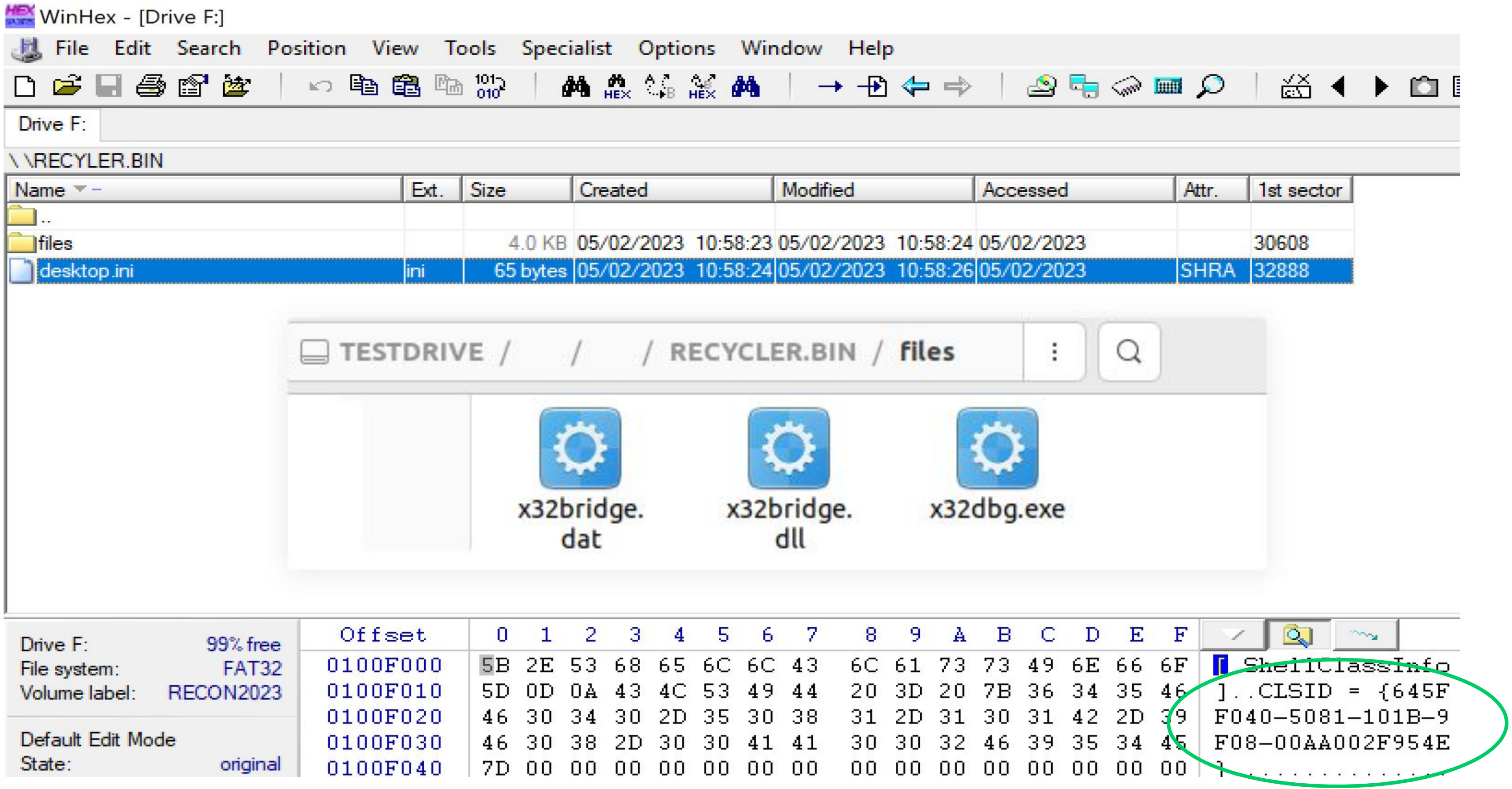


File Explorer

Windows can't find 'F:\ \ \RECYCLER.BIN\files'. Check the spelling and try again.

OK

USB Device Recycler bin folder



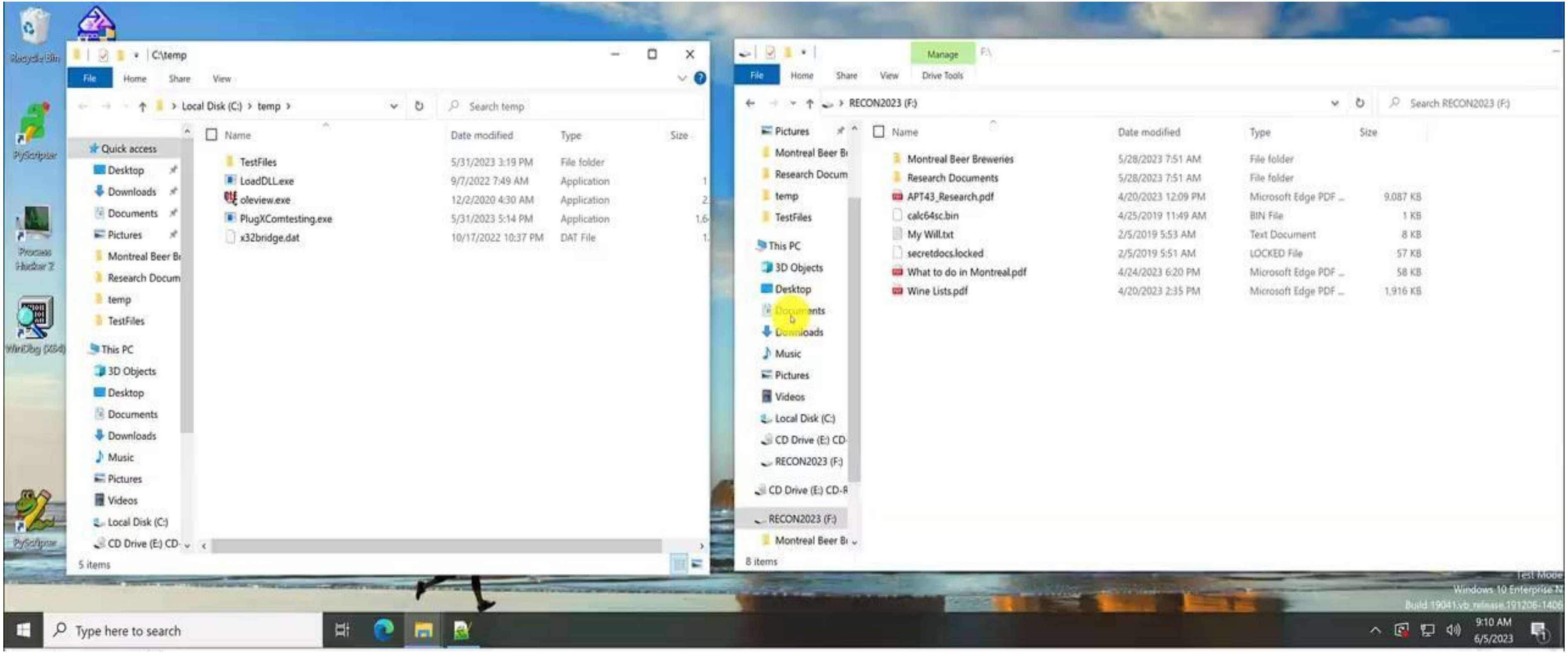
\ \RECYLER.BIN

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
..							
files		4.0 KB	05/02/2023 10:58:23	05/02/2023 10:58:24	05/02/2023		30608
desktop.ini	ini	65 bytes	05/02/2023 10:58:24	05/02/2023 10:58:26	05/02/2023	SHRA	32888

Drive F:	99% free
File system:	FAT32
Volume label:	RECON2023
Default Edit Mode	
State:	original

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0100F000   5B 2E 53 68 65 6C 6C 43  6C 61 73 73 49 6E 66 6F   [.ShellClassInfo
0100F010   5D 0D 0A 43 4C 53 49 44  20 3D 20 7B 36 34 35 46   ]..CLSID = {645F
0100F020   46 30 34 30 2D 35 30 38  31 2D 31 30 31 42 2D 39   F040-5081-101B-9
0100F030   46 30 38 2D 30 30 41 41  30 30 32 46 39 35 34 45   F08-00AA002F954E
0100F040   7D 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   }...............
```

Video Demo



Name	Date modified	Type	Size
TestFiles	5/31/2023 3:19 PM	File folder	
LoadDLL.exe	9/7/2022 7:49 AM	Application	1
oleview.exe	12/2/2020 4:30 AM	Application	2
PlugXComtesting.exe	5/31/2023 5:14 PM	Application	1,6
x32bridge.dat	10/17/2022 10:37 PM	DAT File	1.

5 items

Name	Date modified	Type	Size
Montreal Beer Breweries	5/28/2023 7:51 AM	File folder	
Research Documents	5/28/2023 7:51 AM	File folder	
APT43_Research.pdf	4/20/2023 12:09 PM	Microsoft Edge PDF ...	9,087 KB
calc64sc.bin	4/25/2019 11:49 AM	BIN File	1 KB
My Will.txt	2/5/2019 5:53 AM	Text Document	8 KB
secretdocs.locked	2/5/2019 5:51 AM	LOCKED File	57 KB
What to do in Montreal.pdf	4/24/2023 6:20 PM	Microsoft Edge PDF ...	58 KB
Wine Lists.pdf	4/20/2023 2:35 PM	Microsoft Edge PDF ...	1,916 KB

8 items

Vendor Notification

MSRC Submission

“Hey Microsoft, we are seeing in the wild exploitation of USB devices by the PlugX malware using a novel technique to conceal the payload. Additionally, we are concerned that Windows Defender is not scanning the files.”

- January 4th, 2023

MSRC Response

“Our developers have looked into possible changes in the OS, but based on designed functionality, there are **no opportunities** to improve on the design which would help against this particular malware campaign”.

- January 20th, 2023

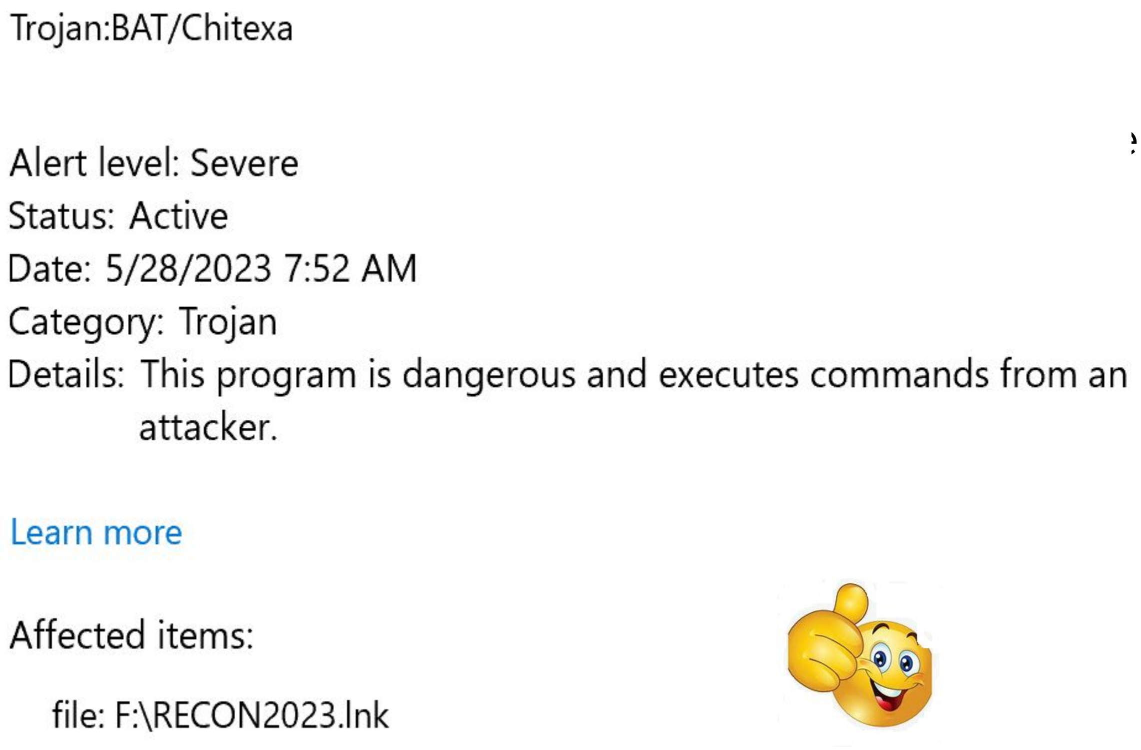
But then...

- The Wi
- While b er

  started

  malwar

  - ~ Februar



Trojan:BAT/Chitexa

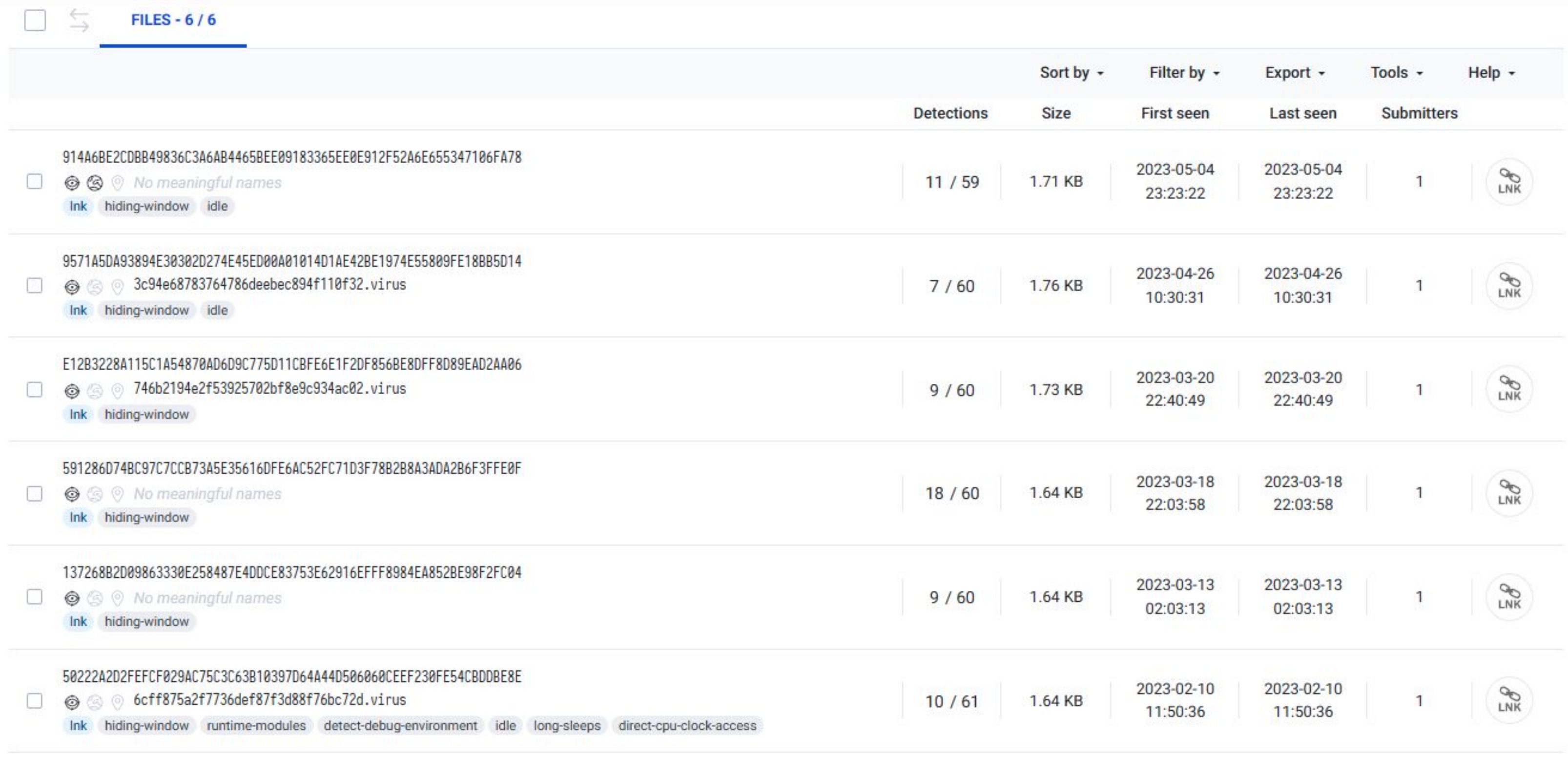
Alert level: Severe
Status: Active
Date: 5/28/2023 7:52 AM
Category: Trojan
Details: This program is dangerous and executes commands from an attacker.

Learn more

Affected items:

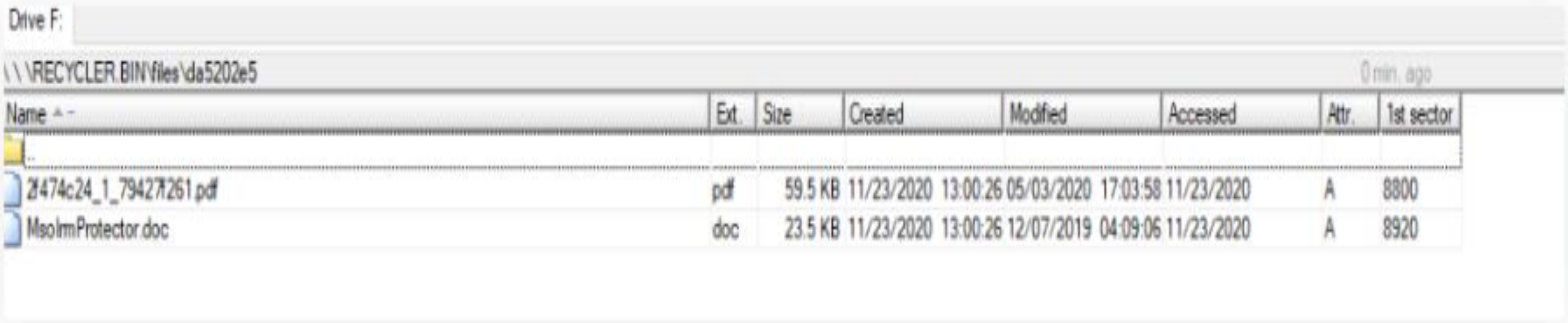
file: F:\RECON2023.lnk

Chitexa VirusTotal Hits



	Detections	Size	First seen	Last seen	Submitters
914A6BE2CDBB49836C3A6AB4465BEE09183365EE0E912F52A6E655347106FA78 *No meaningful names* lnk hiding-window idle	11 / 59	1.71 KB	2023-05-04 23:23:22	2023-05-04 23:23:22	1
9571A5DA93894E30302D274E45ED00A01014D1AE42BE1974E55809FE18BB5D14 3c94e68783764786deebec894f110f32.virus lnk hiding-window idle	7 / 60	1.76 KB	2023-04-26 10:30:31	2023-04-26 10:30:31	1
E12B3228A115C1A54870AD6D9C775D11CBFE6E1F2DF856BE8DFF8D89EAD2AA06 746b2194e2f53925702bf8e9c934ac02.virus lnk hiding-window	9 / 60	1.73 KB	2023-03-20 22:40:49	2023-03-20 22:40:49	1
591286D74BC97C7CCB73A5E35616DFE6AC52FC71D3F78B2B8A3ADA2B6F3FFE0F *No meaningful names* lnk hiding-window	18 / 60	1.64 KB	2023-03-18 22:03:58	2023-03-18 22:03:58	1
137268B2D09863330E258487E4DDCE83753E62916EFFF8984EA852BE98F2FC04 *No meaningful names* lnk hiding-window	9 / 60	1.64 KB	2023-03-13 02:03:13	2023-03-13 02:03:13	1
50222A2D2FEFCF029AC75C3C63B10397D64A44D506060CEEF230FE54CBDDBE8E 6cff875a2f7736def87f3d88f76bc72d.virus lnk hiding-window runtime-modules detect-debug-environment idle long-sleeps direct-cpu-clock-access	10 / 61	1.64 KB	2023-02-10 11:50:36	2023-02-10 11:50:36	1

Discovery of 2nd USB Variant



Drive F:

\\ \RECYCLER.BIN\files\da5202e5

0 min. ago

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
..							
2f474c24_1_79427f261.pdf	pdf	59.5 KB	11/23/2020 13:00:26	05/03/2020 17:03:58	11/23/2020	A	8800
MsoIrmProtector.doc	doc	23.5 KB	11/23/2020 13:00:26	12/07/2019 04:09:06	11/23/2020	A	8920

Future Research

paloalto NETWORKS

Future Research Opportunities

- Test AV vendors to ensure that they can scan files stored in the NBSP + recycler.bin folder
- Can a Recycle Bin folder exist on non USB devices such as a physical drive
- What other Unicode characters can be abused to conceal folders
- What other Desktop.ini entries can be used to masquerade folders and files
- Little to no research on how the master Recycle Bin folder works. Maybe a chapter in the Windows Internals?

Thank you!

Learning is doing. I've re-purposed the techniques outlined in this talk and will make them publicly available. Enjoy, learn, and I welcome any feedback you may have. The POC can be found here:

https://github.com/mjharbison/plugxUSBPOC/tree/master