vx-underground@vxunderground·Sep 14

Ballin' on a budget: A Quick Guide to Defining Malware with $0, Python3, and Windows

To be blunt: if you've got a bunch of binaries that you know is malware, or suspect is malware, and want to label it appropriately but don't have the ability to get an expensive VirusTotal license (or they don't want to lend you a researcher API key), don't have the ability (or skillset) to setup something like
Polish CERT MWDB
or
Canadian CCCS AssembyLine
, or any other reason not listed here, then this tutorial will show you how to ball out on a budget. Requirements: - Windows (yes, you read that correctly) - Python3 - Malware
Windows Defender comes equipt with a command line interface designed for Enterprise Users (maybe? no idea, just making that up) that allows anyone to do a quick custom scan on a file. The binary is (usually) located in:

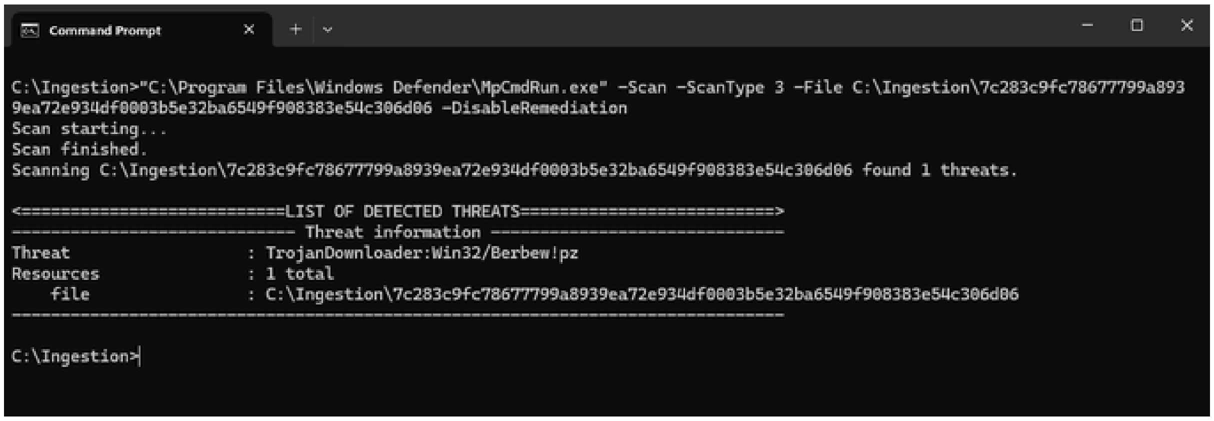
plaintext

```
C:\Program Files\Windows Defender\MpCmdRun.exe
```

MSDN offers a
pretty good guide
on how to use the command line interface. If you don't want to read, the tl;dr is the the following command line is absolute gold:
plaintext

```
MpCmdRun.exe -Scan -ScanType 3 -File "{full_file_path}" -DisableRemediation
```

This will scan a file, print the results onto the console, and do nothing thanks to the DisableRemediation flag. It looks like this:



```
C:\Ingestion>"C:\Program Files\Windows Defender\MpCmdRun.exe" -Scan -ScanType 3 -File C:\Ingestion\7c283c9fc78677799a893
9ea72e934df0003b5e32ba6549f908383e54c306d06 -DisableRemediation
Scan starting...
Scan finished.
Scanning C:\Ingestion\7c283c9fc78677799a8939ea72e934df0003b5e32ba6549f908383e54c306d06 found 1 threats.

<===========================LIST OF DETECTED THREATS==========================>
----------------------------- Threat information ------------------------------
Threat                  : TrojanDownloader:Win32/Berbew!pz
Resources               : 1 total
    file                : C:\Ingestion\7c283c9fc78677799a8939ea72e934df0003b5e32ba6549f908383e54c306d06
-------------------------------------------------------------------------------

C:\Ingestion>
```

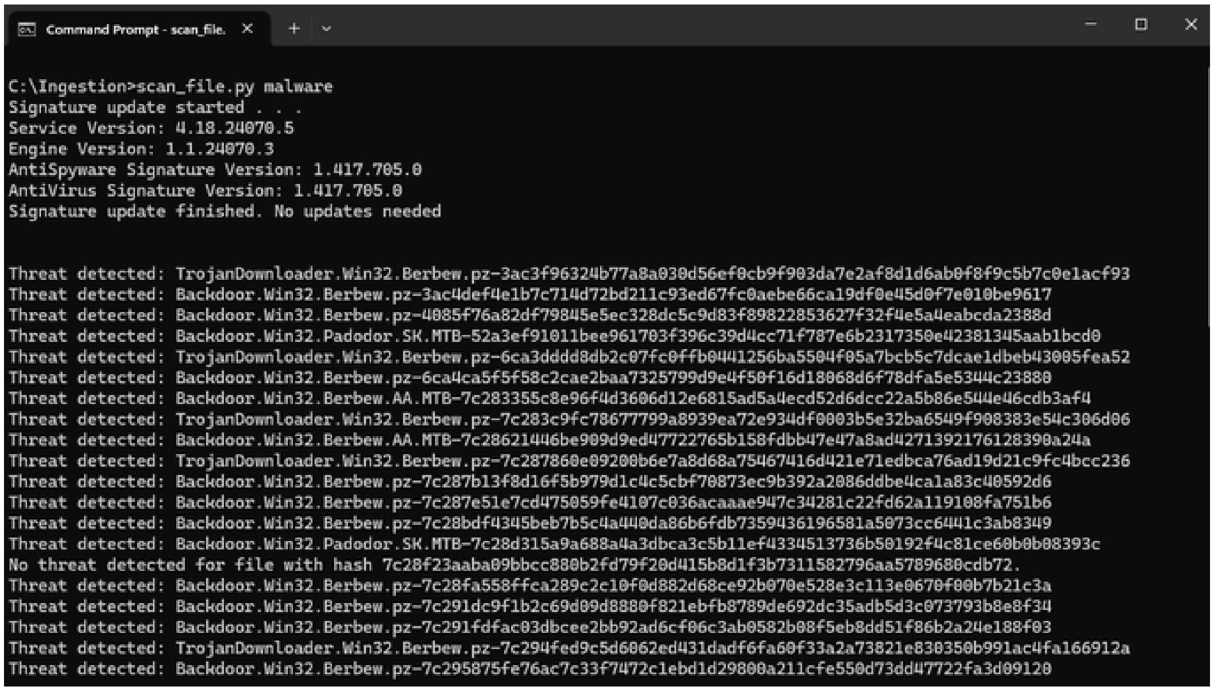
The caveat to this command line argument is the -File flag requires the full path to the file you want to scan. Anyway, here is some Python 3 code that accepts a directory as an argument. It will programmatically loop through a directory, scan the file, get the output from MpCmdRun.exe, then display the result on the console using a file path friendly definition (more on that later).

python

```
import subprocess
import os
import argparse
import hashlib

def update_defender_signatures():
    """Updates the Defender virus definitions to ensure the latest signatures are
used."""
    try:
        command = r'"C:\Program Files\Windows Defender\MpCmdRun.exe" -
SignatureUpdate'
        result = subprocess.run(command, capture_output=True, text=True, shell=True)
        print(result.stdout)  # Directly print the output from the command
        print(result.stderr)  # Directly print any errors from the command
    except Exception as e:
        print(f"An error occurred during signature update: {e}")

def calculate_sha256(file_path):
    """Calculates and returns the SHA-256 hash of a file."""
    sha256_hash = hashlib.sha256()
    try:
        with open(file_path, "rb") as f:
            # Read the file in chunks to avoid memory issues with large files
            for byte_block in iter(lambda: f.read(4096), b""):
                sha256_hash.update(byte_block)
        return sha256_hash.hexdigest()
    except Exception as e:
        print(f"Error calculating SHA-256 for {file_path}: {e}")
        return None

def extract_threat_name(output, file_hash):
    """Extracts and prints the full threat name from the Defender output, replacing
special characters."""
    lines = output.splitlines()
    threat_section_found = False
    threat_name_found = False

    for line in lines:
        if "LIST OF DETECTED THREATS" in line:
            threat_section_found = True  # Found the section with the threat list
            continue  # Move to the next line after detecting the section

        if threat_section_found and not threat_name_found:
            if "Threat" in line and ":" in line:
                # Capture everything after the first colon to ensure the full threat
name
                threat_name = line.split(":", 1)[1].strip()  # Get the threat name
                # Replace :, /, and ! with a period
                threat_name = threat_name.replace(":", ".").replace("/",
".").replace("!", ".")
                print(f"Threat detected: {threat_name}-{file_hash}")
                threat_name_found = True
                break

    if not threat_name_found:
        print(f"No threat detected for file with hash {file_hash}.")

def scan_file_with_defender(file_path):
    """Scans a single file using Windows Defender."""
    # Calculate the SHA-256 hash of the file
    file_hash = calculate_sha256(file_path)
    if not file_hash:
        return  # If hash calculation failed, skip this file

    # Define the command to run MpCmdRun.exe to scan the specific file
    command = fr'"C:\Program Files\Windows Defender\MpCmdRun.exe" -Scan -ScanType 3 -
File "{file_path}" -DisableRemediation'

    try:
        # Run the command and capture output, using shell=True
        result = subprocess.run(command, capture_output=True, text=True, shell=True)

        # Parse the result.stdout to extract and print the threat name along with the
file hash
        extract_threat_name(result.stdout, file_hash)

    except Exception as e:
        print(f"An error occurred while scanning {file_path}: {e}")

def scan_directory_with_defender(directory_path):
    """Scans all files in a directory using Windows Defender."""
    # Resolve the full path of the directory
    directory_path = os.path.abspath(directory_path)

    # Check if the directory exists
    if not os.path.isdir(directory_path):
        print(f"Directory not found: {directory_path}")
        return

    # First update signatures
    update_defender_signatures()

    # Loop through all files in the directory and scan each one
    for root, dirs, files in os.walk(directory_path):
        for file in files:
            file_path = os.path.join(root, file)
            scan_file_with_defender(file_path)

if __name__ == "__main__":
    # Parse the command line argument
    parser = argparse.ArgumentParser(description="Scan a file or a directory using
Windows Defender.")
    parser.add_argument("directory_path", help="The path to the directory you want to
scan.")
```

```
    args = parser.parse_args()
    scan_directory_with_defender(args.directory_path)
```

When you run it against a directory containing malware, the output will look like this:



```
C:\Ingestion>scan_file.py malware
Signature update started . . .
Service Version: 4.18.24070.5
Engine Version: 1.1.24070.3
AntiSpyware Signature Version: 1.417.705.0
AntiVirus Signature Version: 1.417.705.0
Signature update finished. No updates needed


Threat detected: TrojanDownloader.Win32.Berbew.pz-3ac3f96324b77a8a030d56ef0cb9f903da7e2af8d1d6ab0f8f9c5b7c0e1acf93
Threat detected: Backdoor.Win32.Berbew.pz-3ac4def4e1b7c714d72bd211c93ed67fc0aebe66ca19df0e45d0f7e010be9617
Threat detected: Backdoor.Win32.Berbew.pz-4085f76a82df79845e5ec328dc5c9d83f89822853627f32f4e5a4eabcda2388d
Threat detected: Backdoor.Win32.Padodor.SK.MTB-52a3ef91011bee961703f396c39d4cc71f787e6b2317350e42381345aab1bcd0
Threat detected: TrojanDownloader.Win32.Berbew.pz-6ca3dddd8db2c07fc0ffb0441256ba5504f05a7bcb5c7dcae1dbeb43005fea52
Threat detected: Backdoor.Win32.Berbew.pz-6ca4ca5f5f58c2cae2baa7325799d9e4f50f16d18068d6f78dfa5e5344c23880
Threat detected: Backdoor.Win32.Berbew.AA.MTB-7c283355c8e96f4d3606d12e6815ad5a4ecd52d6dcc22a5b86e544e46cdb3af4
Threat detected: TrojanDownloader.Win32.Berbew.pz-7c283c9fc78677799a8939ea72e934df0003b5e32ba6549f908383e54c306d06
Threat detected: Backdoor.Win32.Berbew.AA.MTB-7c28621446be909d9ed47722765b158fdbb47e47a8ad4271392176128390a24a
Threat detected: TrojanDownloader.Win32.Berbew.pz-7c287860e09200b6e7a8d68a75467416d421e71edbca76ad19d21c9fc4bcc236
Threat detected: Backdoor.Win32.Berbew.pz-7c287b13f8d16f5b979d1c4c5cbf70873ec9b392a2086ddbe4ca1a83c40592d6
Threat detected: Backdoor.Win32.Berbew.pz-7c287e51e7cd475059fe4107c036acaaae947c34281c22fd62a119108fa751b6
Threat detected: Backdoor.Win32.Berbew.pz-7c28bdf4345beb7b5c4a440da86b6fdb7359436196581a5073cc6441c3ab8349
Threat detected: Backdoor.Win32.Padodor.SK.MTB-7c28d315a9a688a4a3dbca3c5b11ef4334513736b50192f4c81ce60b0b08393c
No threat detected for file with hash 7c28f23aaba09bbcc880b2fd79f20d415b8d1f3b7311582796aa5789680cdb72.
Threat detected: Backdoor.Win32.Berbew.pz-7c28fa558ffca289c2c10f0d882d68ce92b070e528e3c113e0670f00b7b21c3a
Threat detected: Backdoor.Win32.Berbew.pz-7c291dc9f1b2c69d09d8880f821ebfb8789de692dc35adb5d3c073793b8e8f34
Threat detected: Backdoor.Win32.Berbew.pz-7c291fdfac03dbcee2bb92ad6cf06c3ab0582b08f5eb8dd51f86b2a24e188f03
Threat detected: TrojanDownloader.Win32.Berbew.pz-7c294fed9c5d6062ed431dadf6fa60f33a2a73821e830350b991ac4fa166912a
Threat detected: Backdoor.Win32.Berbew.pz-7c295875fe76ac7c33f7472c1ebd1d29800a211cfe550d73dd47722fa3d09120
```

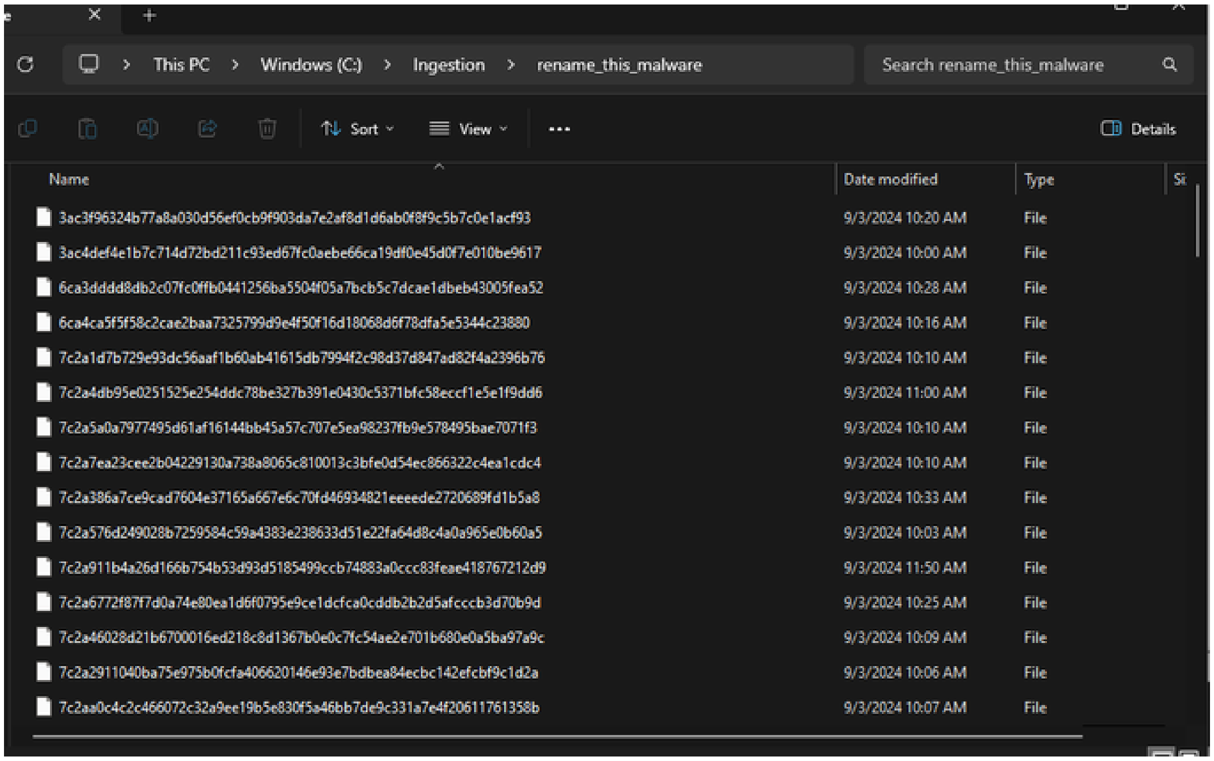
Cool beans! If you want it to rename the files using the path friendly output you can use the following code:

python

```
import subprocess
import os
import argparse
import hashlib

def update_defender_signatures():
    """Updates the Defender virus definitions to ensure the latest signatures are
used."""
    try:
        command = r'"C:\Program Files\Windows Defender\MpCmdRun.exe" -
SignatureUpdate'
        result = subprocess.run(command, capture_output=True, text=True, shell=True)
        print(result.stdout)  # Directly print the output from the command
        print(result.stderr)  # Directly print any errors from the command
    except Exception as e:
        print(f"An error occurred during signature update: {e}")

def calculate_sha256(file_path):
    """Calculates and returns the SHA-256 hash of a file."""
    sha256_hash = hashlib.sha256()
    try:
        with open(file_path, "rb") as f:
            # Read the file in chunks to avoid memory issues with large files
            for byte_block in iter(lambda: f.read(4096), b""):
                sha256_hash.update(byte_block)
        return sha256_hash.hexdigest()
    except Exception as e:
        print(f"Error calculating SHA-256 for {file_path}: {e}")
        return None

def extract_threat_name(output, file_hash):
    """Extracts and returns the full threat name from the Defender output, replacing
special characters."""
    lines = output.splitlines()
    threat_section_found = False
    threat_name_found = False

    for line in lines:
        if "LIST OF DETECTED THREATS" in line:
            threat_section_found = True  # Found the section with the threat list
            continue  # Move to the next line after detecting the section

        if threat_section_found and not threat_name_found:
            if "Threat" in line and ":" in line:
                # Capture everything after the first colon to ensure the full threat
name
                threat_name = line.split(":", 1)[1].strip()  # Get the threat name
                # Replace :, /, and ! with a period
                threat_name = threat_name.replace(":", ".").replace("/",
".").replace("!", ".")
                return f"{threat_name}-{file_hash}"
    return f"NoThreatDetected-{file_hash}"

def scan_file_with_defender(file_path):
    """Scans a single file using Windows Defender and renames it based on the threat 
and hash."""
    # Calculate the SHA-256 hash of the file
    file_hash = calculate_sha256(file_path)
    if not file_hash:
        return  # If hash calculation failed, skip this file

    # Define the command to run MpCmdRun.exe to scan the specific file
    command = fr'"C:\Program Files\Windows Defender\MpCmdRun.exe" -Scan -ScanType 3 -
File "{file_path}" -DisableRemediation'

    try:
        # Run the command and capture output, using shell=True
        result = subprocess.run(command, capture_output=True, text=True, shell=True)

        # Parse the result.stdout to extract the threat name along with the file hash
        new_file_name = extract_threat_name(result.stdout, file_hash)

        # Rename the file with the new name
        file_directory = os.path.dirname(file_path)
        file_extension = os.path.splitext(file_path)[1]  # Keep the original file 
extension
        new_file_path = os.path.join(file_directory, new_file_name + file_extension)

        os.rename(file_path, new_file_path)
        print(f"File renamed to: {new_file_path}")

    except Exception as e:
        print(f"An error occurred while scanning {file_path}: {e}")

def scan_directory_with_defender(directory_path):
    """Scans all files in a directory using Windows Defender."""
    # Resolve the full path of the directory
    directory_path = os.path.abspath(directory_path)

    # Check if the directory exists
    if not os.path.isdir(directory_path):
        print(f"Directory not found: {directory_path}")
        return

    # First update signatures
    update_defender_signatures()

    # Loop through all files in the directory and scan each one
    for root, dirs, files in os.walk(directory_path):
        for file in files:
            file_path = os.path.join(root, file)
            scan_file_with_defender(file_path)
```

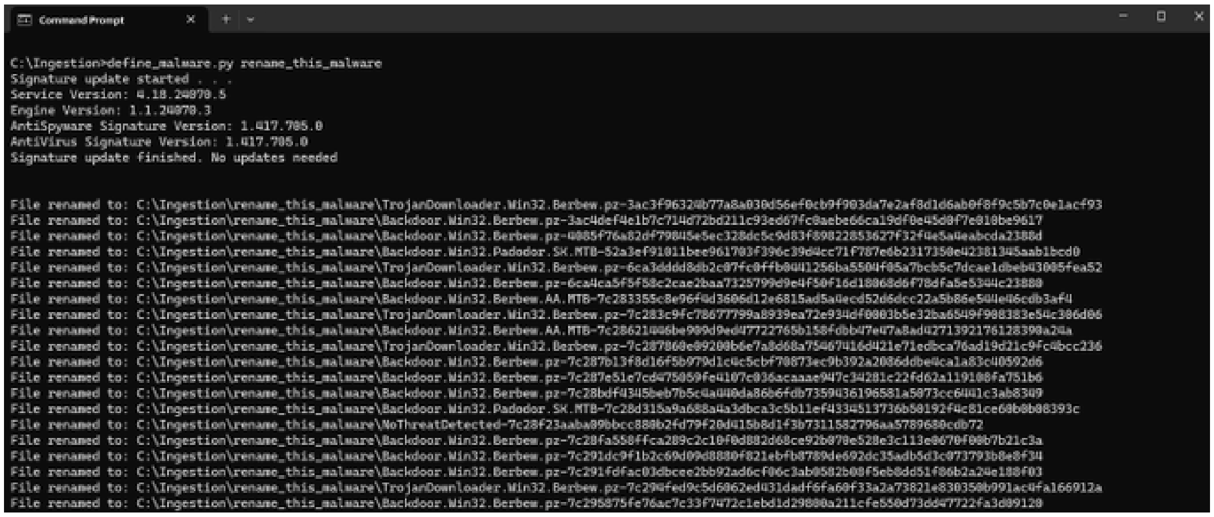
```
if __name__ == "__main__":
    # Parse the command line argument
    parser = argparse.ArgumentParser(description="Scan a file or a directory using 
Windows Defender and rename files based on detected threats.")
    parser.add_argument("directory_path", help="The path to the directory you want to 
scan.")

    args = parser.parse_args()
    scan_directory_with_defender(args.directory_path)
```

Before the script is ran, this is a picture of a directory named "rename_this_malware"


This PC > Windows (C:) > Ingestion > rename_this_malware
Search rename_this_malware
Sort
View
Details

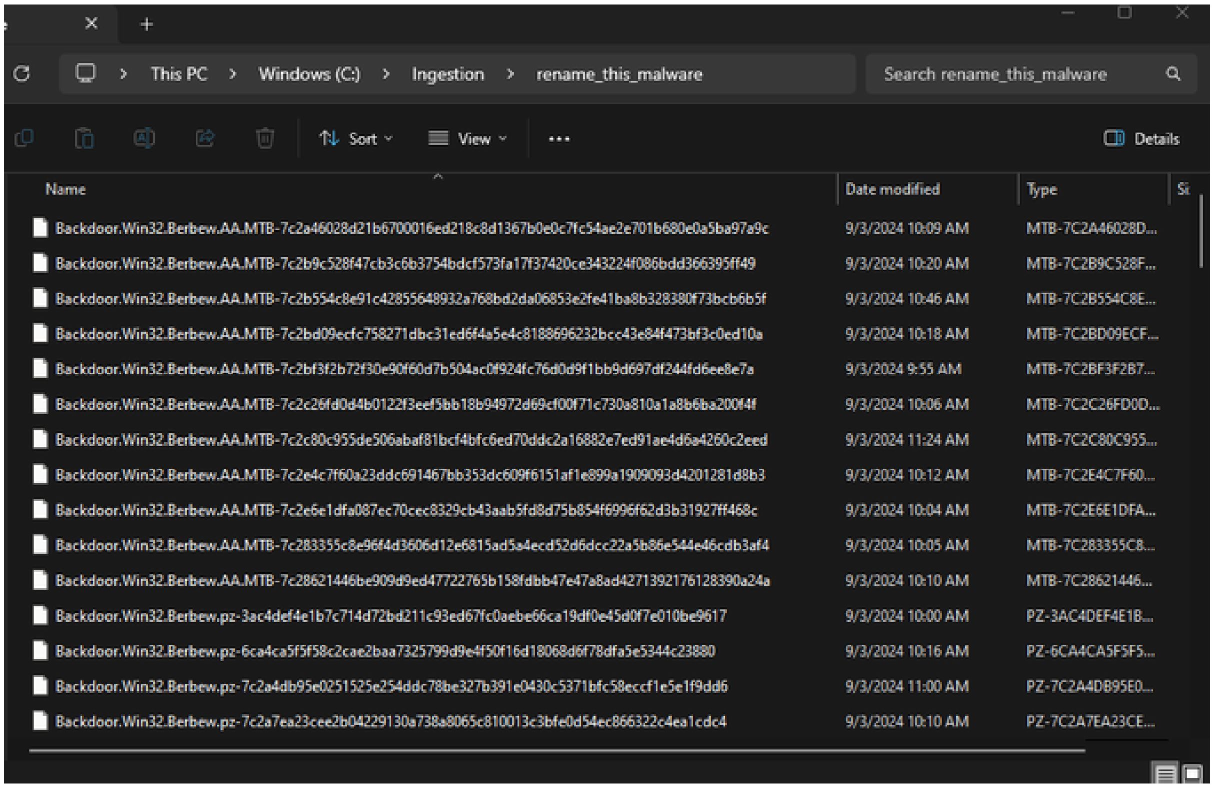
Name	Date modified	Type
3ac3f96324b77a8a030d56ef0cb9f903da7e2af8d1d6ab0f8f9c5b7c0e1acf93	9/3/2024 10:20 AM	File
3ac4def4e1b7c714d72bd211c93ed67fc0aebe66ca19df0e45d0f7e010be9617	9/3/2024 10:00 AM	File
6ca3dddd8db2c07fc0ffb0441256ba5504f05a7bcb5c7dcae1dbeb43005fea52	9/3/2024 10:28 AM	File
6ca4ca5f5f58c2cae2baa7325799d9e4f50f16d18068d6f78dfa5e5344c23880	9/3/2024 10:16 AM	File
7c2a1d7b729e93dc56aaf1b60ab41615db7994f2c98d37d847ad82f4a2396b76	9/3/2024 10:10 AM	File
7c2a4db95e0251525e254ddc78be327b391e0430c5371bfc58eccf1e5e1f9dd6	9/3/2024 11:00 AM	File
7c2a5a0a7977495d61af16144bb45a57c707e5ea98237fb9e578495bae7071f3	9/3/2024 10:10 AM	File
7c2a7ea23cee2b04229130a738a8065c810013c3bfe0d54ec866322c4ea1cdc4	9/3/2024 10:10 AM	File
7c2a386a7ce9cad7604e37165a667e6c70fd46934821eeeede2720689fd1b5a8	9/3/2024 10:33 AM	File
7c2a576d249028b7259584c59a4383e238633d51e22fa64d8c4a0a965e0b60a5	9/3/2024 10:03 AM	File
7c2a911b4a26d166b754b53d93d5185499ccb74883a0ccc83feae418767212d9	9/3/2024 11:50 AM	File
7c2a6772f87f7d0a74e80ea1d6f0795e9ce1dcfca0cddb2b2d5afcccb3d70b9d	9/3/2024 10:25 AM	File
7c2a46028d21b6700016ed218c8d1367b0e0c7fc54ae2e701b680e0a5ba97a9c	9/3/2024 10:09 AM	File
7c2a2911040ba75e975b0fcfa406620146e93e7bdbea84ecbc142efcbf9c1d2a	9/3/2024 10:06 AM	File
7c2aa0c4c2c466072c32a9ee19b5e830f5a46bb7de9c331a7e4f20611761358b	9/3/2024 10:07 AM	File

This is the output on the console from the script:



```
C:\Ingestion>define_malware.py rename_this_malware
Signature update started . . .
Service Version: 4.18.24070.5
Engine Version: 1.1.24070.3
AntiSpyware Signature Version: 1.417.705.0
AntiVirus Signature Version: 1.417.705.0
Signature update finished. No updates needed


File renamed to: C:\Ingestion\rename_this_malware\TrojanDownloader.Win32.Berbew.pz-3ac3f96324b77a8a030d56ef0cb9f903da7e2af8d1d6ab0f8f9c5b7c0e1acf93
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-3ac4def4e1b7c714d72bd211c93ed67fc0aebe66ca19df0e45d0f7e010be9617
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-4085f76a82df79845e5ec328dc5c9d83f89822853627f32f4e5a4eabcda2380d
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Padodor.SK.MTB-52a3ef91011bee961703f396c39d4cc71f787e6b2317350e42381345aab1bcd0
File renamed to: C:\Ingestion\rename_this_malware\TrojanDownloader.Win32.Berbew.pz-6ca3dddd8db2c07fc0ffb0441256ba5504f05a7bcb5c7dcae1dbeb43005fea52
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-6ca4ca5f5f58c2cae2baa7325799d9e4f50f16d18068d6f78dfa5e5344c23880
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.AA.MTB-7c283355c8e96f4d3606d12e6815ad5a4ecd52d6dcc22a5b86e544e46cdb3af4
File renamed to: C:\Ingestion\rename_this_malware\TrojanDownloader.Win32.Berbew.pz-7c283c9fc78677799a8939ea72e934df0003b5e32ba6549f988383e54c386d06
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.AA.MTB-7c28621446be909d9ed47722765b158fdbb47e47a8ad42713921761283 90a24a
File renamed to: C:\Ingestion\rename_this_malware\TrojanDownloader.Win32.Berbew.pz-7c287860e09200b6e7a8d68a75467416d421e71edbca76ad19d21c9fc4bcc236
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-7c287b13f8d16f5b979d1c4c5cbf70873ec9b392a2086ddbe4ca1a83c40592d6
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-7c287e51e7cd475059fe4107c036acaaae947c34281c22fd62a119108fa751b6
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-7c28bdf4345beb7b5c4a440da86b6fdb7359436196581a5073cc6441c3ab8309
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Padodor.SK.MTB-7c28d315a9a688a4a3dbca3c5b11ef4334513736b50192f4c81ce60b0b08393c
File renamed to: C:\Ingestion\rename_this_malware\NoThreatDetected-7c28f23aaba89bbcc888b2fd79f20d415b8d1f3b7311582796aa5789680cdb72
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-7c28fa558ffca289c2c10f0d882d68ce92b070e528e3c113e0670f00b7b21c3a
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-7c291dc9f1b2c69d09d8880f821ebfb8789de692dc35adb5d3c073793b8e8f34
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-7c291fdfac03dbcee2bb92ad6cf06c3ab0582b08f5eb8dd51f86b2a24e188f03
File renamed to: C:\Ingestion\rename_this_malware\TrojanDownloader.Win32.Berbew.pz-7c294fed9c5d6062ed431dadf6fa60f33a2a73821e830350b991ac4fa166912a
File renamed to: C:\Ingestion\rename_this_malware\Backdoor.Win32.Berbew.pz-7c295875fe76ac7c33f7472c1ebd1d29800a211cfe550d73dd47722fa3d09120
```

Here is the new file contents in the directory:


This PC > Windows (C:) > Ingestion > rename_this_malware
Search rename_this_malware
Sort
View
Details

Name	Date modified	Type	Si
Backdoor.Win32.Berbew.AA.MTB-7c2a46028d21b6700016ed218c8d1367b0e0c7fc54ae2e701b680e0a5ba97a9c	9/3/2024 10:09 AM	MTB-7C2A46028D...	
Backdoor.Win32.Berbew.AA.MTB-7c2b9c528f47cb3c6b3754bdcf573fa17f37420ce343224f086bdd366395ff49	9/3/2024 10:20 AM	MTB-7C2B9C528F...	
Backdoor.Win32.Berbew.AA.MTB-7c2b554c8e91c42855648932a768bd2da06853e2fe41ba8b328380f73bcb6b5f	9/3/2024 10:46 AM	MTB-7C2B554C8E...	
Backdoor.Win32.Berbew.AA.MTB-7c2bd09ecfc758271dbc31ed6f4a5e4c8188696232bcc43e84f473bf3c0ed10a	9/3/2024 10:18 AM	MTB-7C2BD09ECF...	
Backdoor.Win32.Berbew.AA.MTB-7c2bf3f2b72f30e90f60d7b504ac0f924fc76d0d9f1bb9d697df244fd6ee8e7a	9/3/2024 9:55 AM	MTB-7C2BF3F2B7...	
Backdoor.Win32.Berbew.AA.MTB-7c2c26fd0d4b0122f3eef5bb18b94972d69cf00f71c730a810a1a8b6ba200f4f	9/3/2024 10:06 AM	MTB-7C2C26FD0D...	
Backdoor.Win32.Berbew.AA.MTB-7c2c80c955de506abaf81bcf4bfc6ed70ddc2a16882e7ed91ae4d6a4260c2eed	9/3/2024 11:24 AM	MTB-7C2C80C955...	
Backdoor.Win32.Berbew.AA.MTB-7c2e4c7f60a23ddc691467bb353dc609f6151af1e899a1909093d4201281d8b3	9/3/2024 10:12 AM	MTB-7C2E4C7F60...	
Backdoor.Win32.Berbew.AA.MTB-7c2e6e1dfa087ec70cec8329cb43aab5fd8d75b854f6996f62d3b31927ff468c	9/3/2024 10:04 AM	MTB-7C2E6E1DFA...	
Backdoor.Win32.Berbew.AA.MTB-7c283355c8e96f4d3606d12e6815ad5a4ecd52d6dcc22a5b86e544e46cdb3af4	9/3/2024 10:05 AM	MTB-7C283355C8...	
Backdoor.Win32.Berbew.AA.MTB-7c28621446be909d9ed47722765b158fdbb47e47a8ad4271392176128390a24a	9/3/2024 10:10 AM	MTB-7C28621446...	
Backdoor.Win32.Berbew.pz-3ac4def4e1b7c714d72bd211c93ed67fc0aebe66ca19df0e45d0f7e010be9617	9/3/2024 10:00 AM	PZ-3AC4DEF4E1B...	
Backdoor.Win32.Berbew.pz-6ca4ca5f5f58c2cae2baa7325799d9e4f50f16d18068d6f78dfa5e5344c23880	9/3/2024 10:16 AM	PZ-6CA4CA5F5F5...	
Backdoor.Win32.Berbew.pz-7c2a4db95e0251525e254ddc78be327b391e0430c5371bfc58eccf1e5e1f9dd6	9/3/2024 11:00 AM	PZ-7C2A4DB95E0...	
Backdoor.Win32.Berbew.pz-7c2a7ea23cee2b04229130a738a8065c810013c3bfe0d54ec866322c4ea1cdc4	9/3/2024 10:10 AM	PZ-7C2A7EA23CE...	

Now we ballin' on a budget. -smelly