The Dangers of VHD and VHDX Files

WILL DORMANN

SEPTEMBER 4, 2019

Recently, I gave a presentation at BSidesPGH 2019 called Death By Thumb Drive: File System Fuzzing with CERT BFF. (The slides from my presentation are available in the SEI Digital Library.) Although my primary goal was to find bugs in kernel file-system-parsing code, a notable part of my research was investigating attack vectors. In particular, I focused on VHD and VHDX files on Windows systems. In this post, I describe some of the risks associated with these two file types.

VHD and VHDX Files

The VHD (Virtual Hard Disk) file format, originally introduced with Connectix Virtual PC, can store the contents of a hard disk drive. Eventually, Microsoft Hyper-V adopted this disk image format. Windows 7 and newer systems include the ability to manually mount VHD files. Starting with Windows 8, a user can mount a VHD by simply double-clicking on the file. Once mounted, a VHD disk image appears to Windows as a normal hard disk that's physically connected to the system. VHDX (Virtual Hard Disk v2) images are functionally equivalent to VHD images, but they include more modern features, such as support for larger sizes and disk resizing.

VHD/VHDX and File System Corruption

After fuzzing file system images with BFF, I was able to find several different ways to crash Windows as the result of it mounting a corrupted disk. Physically plugging in a USB mass storage device with a corrupted file system was the obvious attack vector. However, many security concepts are negated when physical access to a system is granted. VHD and VHDX files eliminate the requirement for physical access to a victim system. If a user simply double-clicks on a VHD or VHDX file that contains a specially crafted file system, they risk crashing Windows or worse, as illustrated below.

PUBLISHED IN

CERT/CC Vulnerabilities

CITE

Get Citation

TAGS

Vulnerability Analysis
Security Vulnerabilities
Vulnerability Discovery
Vulnerability Mitigation
CERT/CC

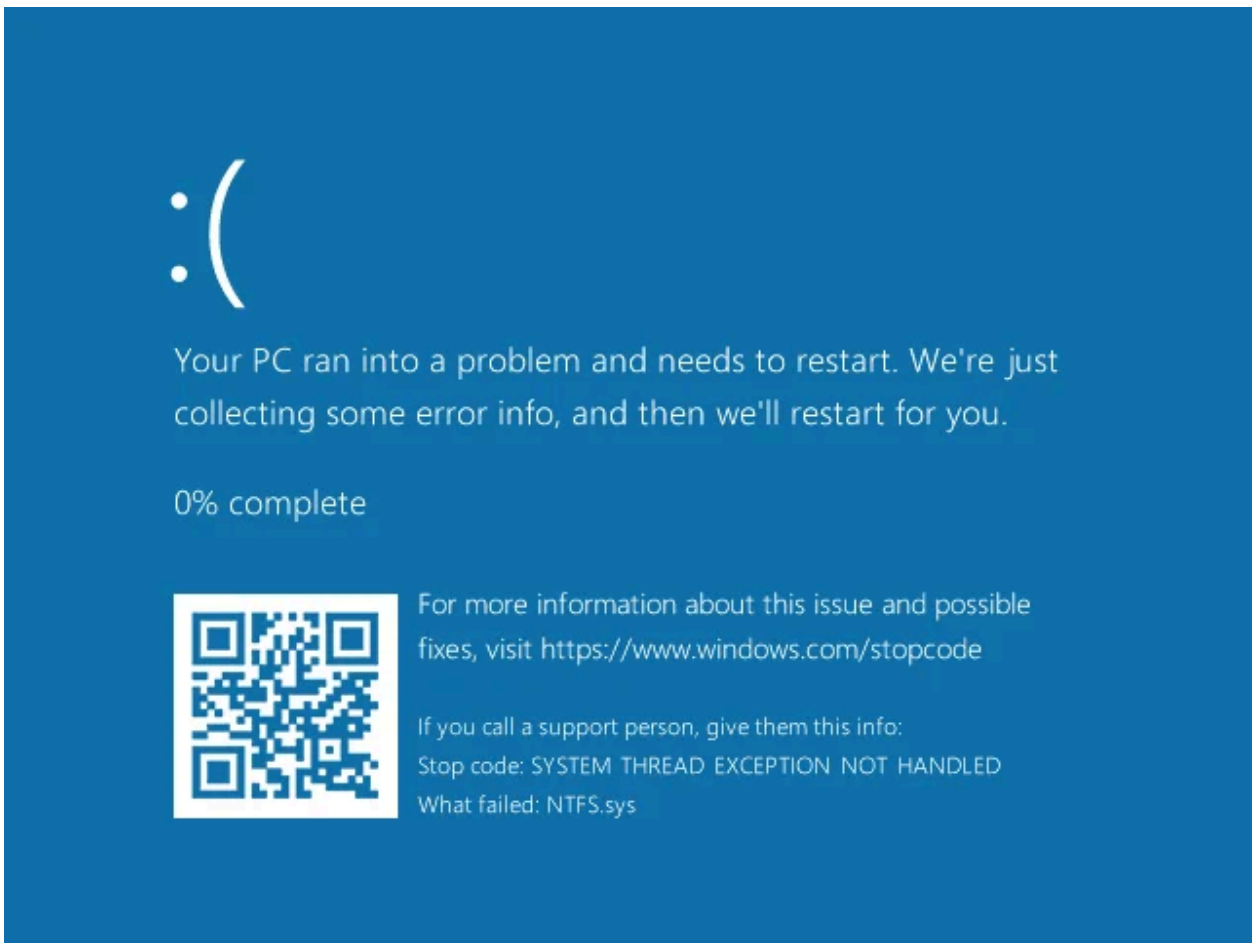
MORE IN CERT/CC VULNERABILITIES

The Threat of Deprecated BGP Attributes

JUNE 3, 2024 • BY LEIGH B. METCALF, TIMUR D. SNOKE

UEFI: 5 Recommendations for Securing and Restoring Trust

JUNE 26, 2023 • BY VIJAY S. SARVEPALLI



Vultron: A Protocol for Coordinated Vulnerability Disclosure

SEPTEMBER 26, 2022 • BY ALLEN D. HOUSEHOLDER

UEFI – Terra Firma for Attackers

AUGUST 1, 2022 • BY VIJAY S. SARVEPALLI

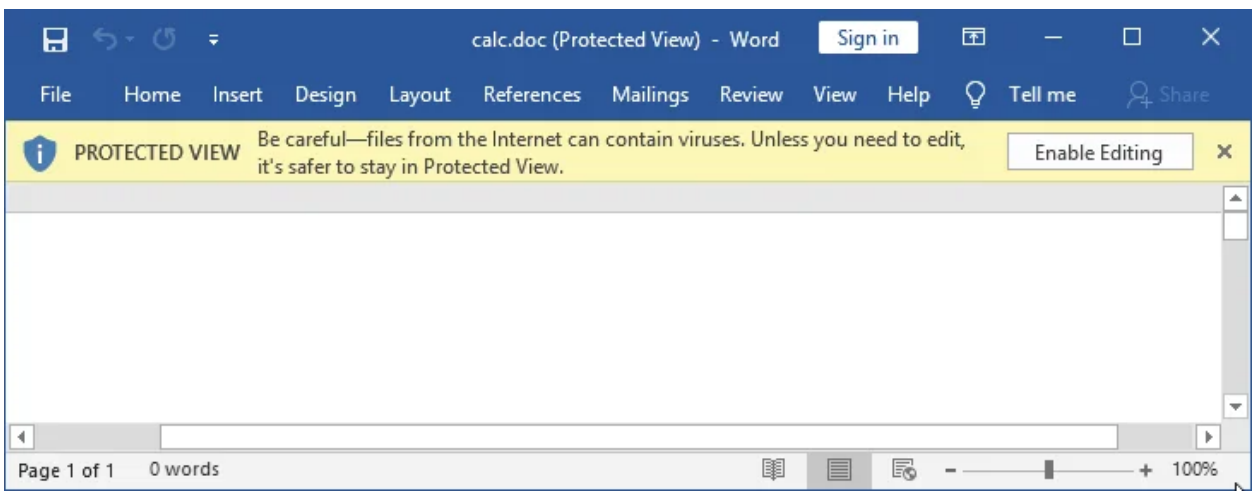
Probably Don't Rely on EPSS Yet

JUNE 6, 2022 • BY JONATHAN SPRING

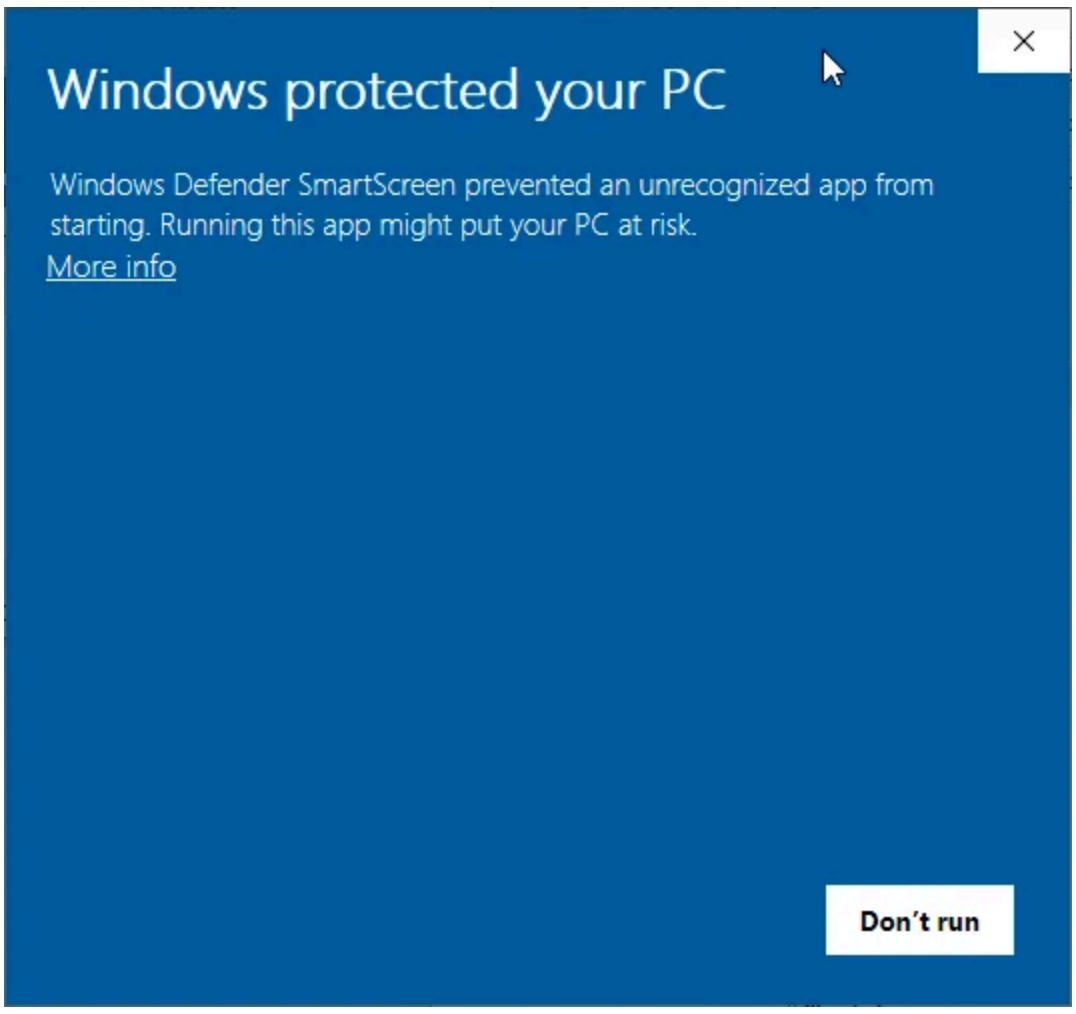
Mark of the Web

Mark of the Web (MOTW) was introduced in Windows XP SP2 and allowed Windows to tag files on the local file system with information about the Internet Explorer security zone from which the files originated. This MOTW feature has evolved to handle more and more file types and scenarios. The recurring theme is that files that came from the Internet (e.g., a web page or an email) may be dangerous, and therefore should be treated with more caution.

For example, starting with Microsoft Office 2010, documents tagged with an MOTW that indicated that they came from the Internet are opened in Microsoft Office Protected View. Documents in Protected View are restricted in what they can do, thus reducing the attack surface of potentially dangerous documents. Here's what a user might see when opening a document in Protected View:



Starting with Windows 10, Windows Defender SmartScreen restricts the execution of certain file types if they originated from the Internet. Here's what a user might see when SmartScreen blocks an unsafe executable:

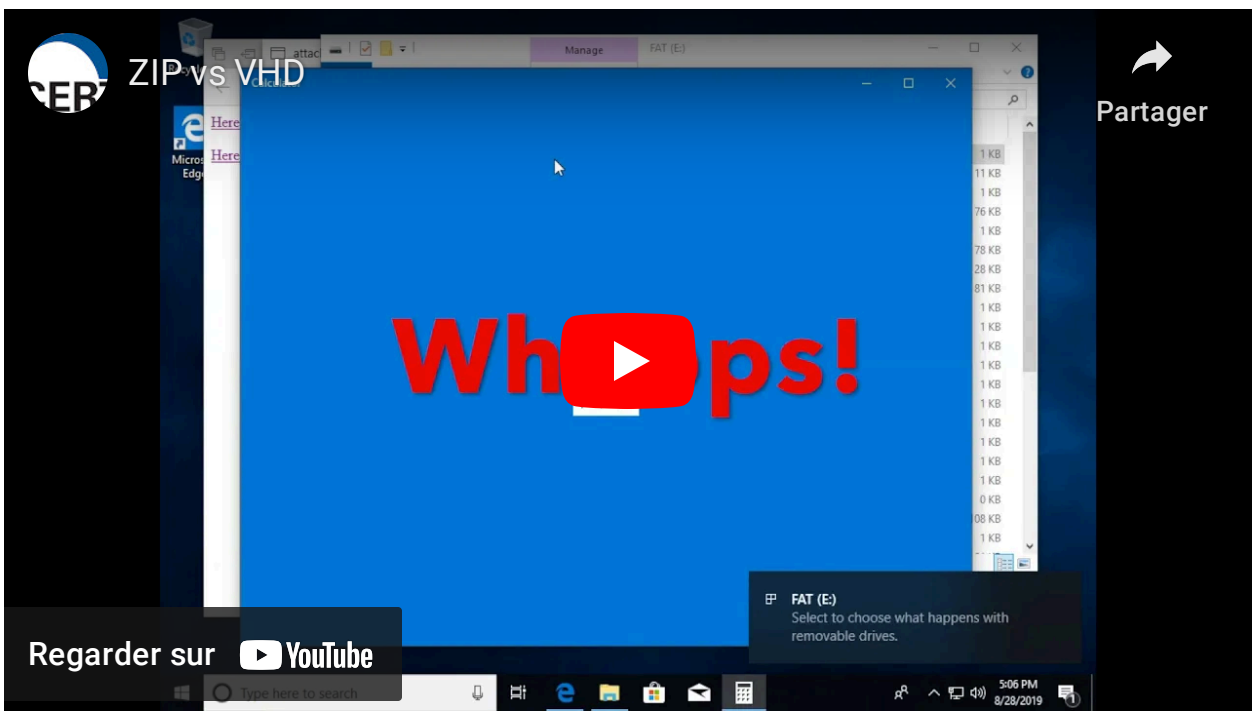


How does Windows know if a file originated from the Internet? It uses the MOTW tag associated with the file in question. If Windows Explorer or other compliant ZIP utilities are used to extract the contents of a ZIP file, each file contained within a ZIP file carries the MOTW of the ZIP file container.

VHD/VHDX Files and MOTW

From a user experience perspective, starting with Windows 8, VHD and VHDX files can have a function similar to ZIP files. That is, the user double-clicks on the file to show its contents in Windows Explorer. The important difference is that the files contained within a VHD or VHDX container do **not** retain the MOTW of the container file.

What does this mean from the end user's perspective? Any file contained within a VHD or VHDX file will not receive the same protections that Windows provides against files that originated from the Internet. To help understand what that means, I created a video that demonstrates several differences between a MOTW-tagged (in a ZIP) file and one that does not contain the MOTW tag (in a VHD):



VHD/VHDX Files and Antivirus

I have found no evidence that any currently deployed antivirus software will scan the **files contained within** a VHD or VHDX file. However, for those running an enterprise, the lack of the ability to scan these files leaves a blind spot for certain files until they arrive at the endpoint. If the contents of VHD and VHDX files are not scanned by email and web gateway security products, those products have no hope of detecting malware contained within VHD or VHDX files.

I created a VHD that contains the EICAR anti malware testfile and uploaded that file to VirusTotal. Here are the results:

There is no evidence that any of the scanners configured in VirusTotal scanned the contents of a VHD file.

ISO and IMG Files

Malware spread via ISO files is already happening in the wild. Just like VHD and VHDX files, the contents of ISO or IMG files do not carry the MOTW of the containing file. And just like VHD and VHDX files, starting with Windows 8, ISO and IMG files can be opened with a double click. Unlike VHD and VHDX files, however, there's a better chance that a deployed antivirus product may detect malware contained in an ISO or IMG file.

I performed the same EICAR test as above with VirusTotal, but this time the eicar.com file was detected within an ISO file. Here are the results:

While these results are not great, there is at least some evidence that some security products will scan the file contents of an ISO file.

Conclusion and Recommendations

VHD and VHDX files can be dangerous. Due to the combination of kernel-level file system parsing and also lack of MOTW tagging to their contents, allowing VHD or VHDX files to arrive at endpoints increases the risk presented to those systems. The following strategies can help minimize this risk:

- Block VHD, VHDX, IMG, and ISO files at email gateways.
- Unregister the VHD, VHDX, IMG, and ISO file extensions in Microsoft Windows Explorer.

- Restrict VHD, VHDX, IMG, and ISO files at web gateways. (There are some legitimate reasons for these files to be downloaded, so ensure that any restrictions do not block legitimate business needs.)

WRITTEN BY

Will Dormann

DIGITAL LIBRARY PUBLICATIONS

SEND A MESSAGE

MORE BY THE AUTHOR

It's Time to Retire Your Unsupported Things

OCTOBER 23, 2019 • BY WILL DORMANN

Expectations of Windows RDP Session Locking Behavior

JULY 29, 2019 • BY WILL DORMANN, JOSEPH TAMMARIELLO

Life Beyond Microsoft EMET

AUGUST 29, 2018 • BY WILL DORMANN

When "ASLR" Is Not Really ASLR - The Case of Incorrect Assumptions and Bad Defaults

AUGUST 3, 2018 • BY WILL DORMANN

Announcing CERT Tapioca 2.0 for Network Traffic Analysis

MAY 23, 2018 • BY WILL DORMANN

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800