INFOSEC

Sysmon v11.10 reads Alternate Data Streams

JUNE 25, 2020

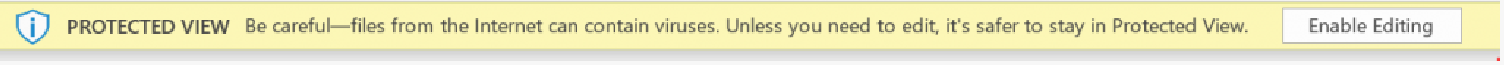
LEAVE A COMMENT

A few days ago, the new version 11.10 of Sysinternals Sysmon was released. Despite the minor version increase from 11.0 it ships with an exciting new feature: Reading NTFS Alternate Data Streams (ADS).

Why is this exciting?

Well, let's quickly recap what ADS are:

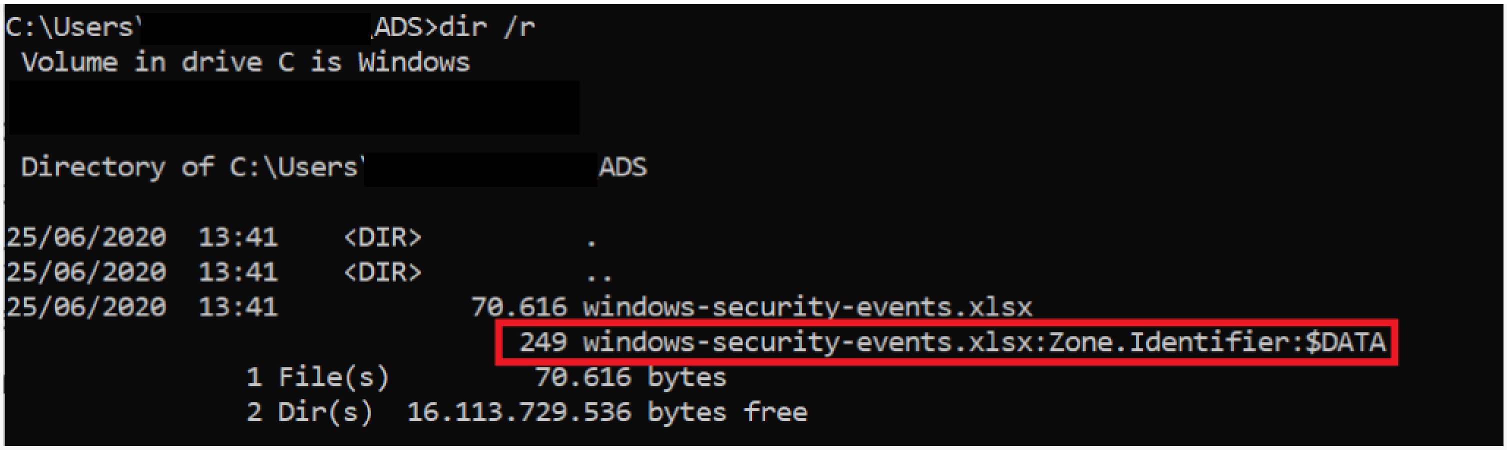
When you download a file from the internet, Windows warns you that it might be dangerous to run a file that comes from such untrusted source. If it's not an executable, the opening application might still show a warning, as is the case for Microsoft Office:



PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

How does the system know that the file was downloaded from the internet? The secret lies in so-called "Alternate Data Streams", a feature of the NT filesystem (NTFS). You will usually not see these streams when they are attached to a file (a great way for attackers to hide malicious content), but you can make it visible in the CLI, using:

```
dir /r
```

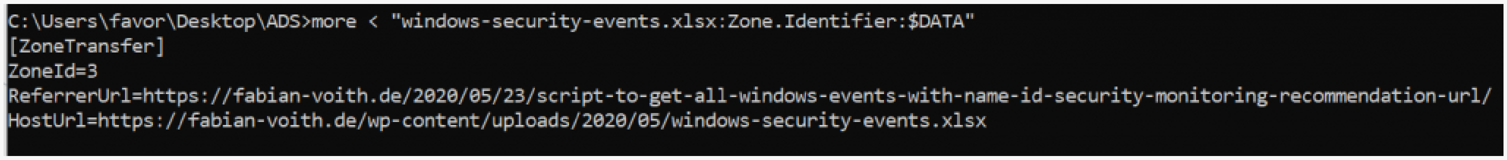


```
C:\Users\[redacted]ADS>dir /r
 Volume in drive C is Windows
[redacted]

 Directory of C:\Users\[redacted]ADS

25/06/2020  13:41    <DIR>          .
25/06/2020  13:41    <DIR>          ..
25/06/2020  13:41            70.616 windows-security-events.xlsx
                                249 windows-security-events.xlsx:Zone.Identifier:$DATA
               1 File(s)         70.616 bytes
               2 Dir(s)  16.113.729.536 bytes free
```

The data stream attached to this Excel file is a specific one called "Mark-of-the-Web" and is labeled "Zone.Identifier". It is attached by browsers to indicate where a file was downloaded from. Let's have a look into it, using:

```
more < "windows-security-events.xlsx:Zone.Identifier:$DATA"
```

So, what we can see here is not only where the file was stored remotely ("HostUrl"), but also how we got there ("ReferrerUrl"):



```
C:\Users\favor\Desktop\ADS>more < "windows-security-events.xlsx:Zone.Identifier:$DATA"
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://fabian-voith.de/2020/05/23/script-to-get-all-windows-events-with-name-id-security-monitoring-recommendation-url/
HostUrl=https://fabian-voith.de/wp-content/uploads/2020/05/windows-security-events.xlsx
```

"ZoneId=3" means that the file was downloaded from the internet and hence triggers some programs to show a warning – like we saw in the first screenshot above.

Since Sysmon is now reporting this information as part of Event 15 "File Stream Created", we can write rules that alert on untrusted HostUrls, but we can also go further and check against a list of "known good": Was chrome.exe downloaded from another domain than google.com? Do we want to allow that or rather have a closer look if that was not an infected version of Chrome then?

The author of Sysmon, Mark Russinovich, shows a quick demo on how the new feature works and looks like:

A well-known security expert who twitters as “SwiftOnSecurity” wrote that this was a feature request made by him. And since he is also the author of a widely-used Sysmon configuration file, we can expect to have a neatly adjusted Sysmon config rather sooner than later.
This article was written by Fabian

← Collection of Windows commands abused by attackers

Quick and easy setup for NetworkMiner and Suricata to perform network forensics →

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

□

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Categories

Select Category

Recent Posts

- Go Team Taiwan
- Reliable mobile Last.fm scrobbling, including Cloud streaming

Recent Comments

- Fix low volume after updating Roland TD17KV(X) to version 2 – Purple Serendipity on Make your Roland TD17 KV(X2) drums really silent while improving dynamics
- スイッチスプーフィングをやってみる – hackefy(ハカファイ) on Making a unidirectional double tagging VLAN hopping attack bidirectional