



Alternative Datenströme – Zone.Identifier

Microsoft schützt uns mit dem Anlagen-Manager vor nicht sicheren Anlagen, die per E-Mail oder aus dem Internet heruntergeladen wurden. Hat der Anlagen-Manager eine mögliche potenzielle Anlage erkannt werden wir am Öffnen gehindert. Häufiger jedoch treten Probleme bei heruntergeladenen Dateien auf. Wenn wir mit dem Internet Explorer Dateien aus dem Internet herunterladen, werden für diese Dateien Streams erzeugt, sogenannte ADS (alternative Datenströme). Diese werden mit der heruntergeladenen Datei verknüpft. Diese Datei hält für den Windows Explorer eine Information namens „Zone.Identifier“ bereit. Anhand dieser Information weiß der Windows Explorer nun, dass es sich hier um eine Datei aus dem Internet handelt und potenziell gefährlich sein könnte. Also werden wir vor dem Öffnen mit einem Warnhinweis konfrontiert.

Interessant oder?

Schauen wir uns mal meinen Download Ordner an. Mit dir /r lassen wir uns den Inhalt des Ordners anzeigen inkl. eventueller ADS. Hier sehen wir auch direkt den Hinweis Zone.Identifier. \$Data bedeutet das es dazu ein Main-File gibt.

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Joern\Downloads>dir /r 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
Datenträger in Laufwerk C: ist WIN10ENT
Volumeseriennummer: 3A2F-B405

Verzeichnis von C:\Users\Joern\Downloads

05.03.2017  11:54          37.228.104 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
              26 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier:$DATA
              1 Datei(en),          37.228.104 Bytes
              0 Verzeichnis(se), 170.510.077.952 Bytes frei

C:\Users\Joern\Downloads>
```

Mark Russinovich hält dafür natürlich auch ein Tool bereit.

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Joern\Downloads>dir /r 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
Datenträger in Laufwerk C: ist WIN10ENT
Volumeseriennummer: 3A2F-B405

Verzeichnis von C:\Users\Joern\Downloads

05.03.2017  11:54          37.228.104 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
              26 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier:$DATA
              1 Datei(en),          37.228.104 Bytes
              0 Verzeichnis(se), 170.510.077.952 Bytes frei

C:\Users\Joern\Downloads>streams.exe 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe

Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:
  :Zone.Identifier:$DATA 26

C:\Users\Joern\Downloads>
```



Alternative Datenströme – Zone.Identifier

Es gibt verschieden Zonen wie z.B.:

- 0.Local Machine / Lokale Maschine
- 1.Local Intranet / Lokales Intranet
- 2.Trusted Sites / Vertrauenswürdigen Seiten
- 3.Internet / Internet
- 4.Restricted Sites / Eingeschränkte Seiten

Wenn wir uns nun den Inhalt der ADS anzeigen lassen, stellen wir fest, dass es sich hierbei tatsächlich um eine Datei aus dem Internet handelt > ZoneId=3.

```
Auswählen Administrator: Eingabeaufforderung
Datenträger in Laufwerk C: ist WIN10ENT
Volumeseriennummer: 3A2F-B405

Verzeichnis von C:\Users\Joern\Downloads

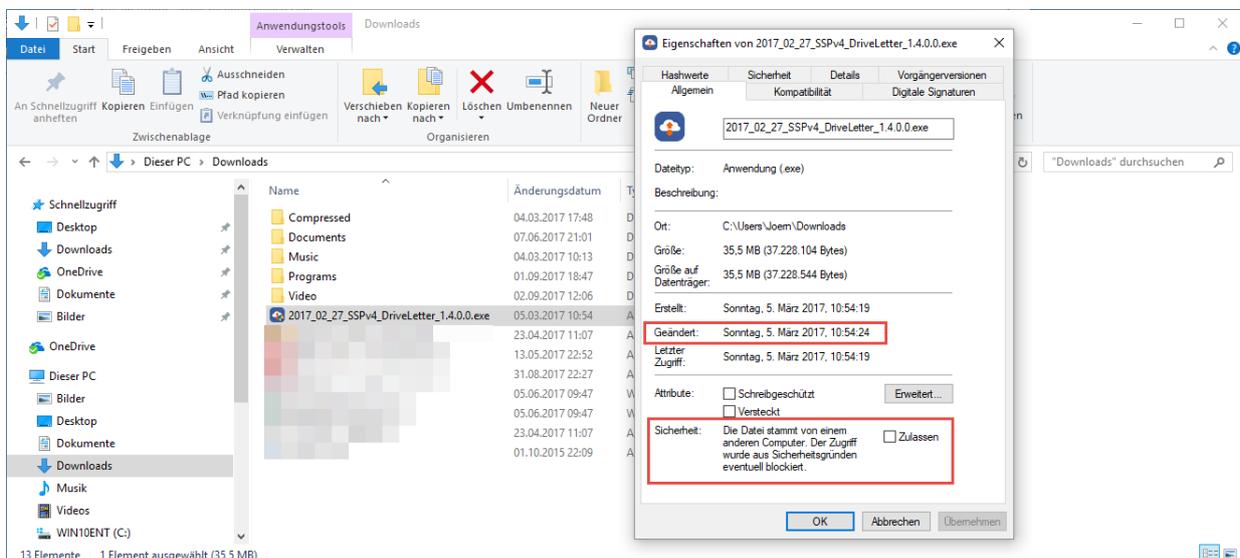
03.09.2017  15:37  <DIR>          .
03.09.2017  15:37  <DIR>          ..
05.03.2017  11:54          37.228.104 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
                26 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier:$DATA
23.04.2017  11:07
04.03.2017  18:48  <DIR>          .
07.06.2017  21:01  <DIR>          ..
13.05.2017  22:52          7
31.08.2017  22:27          7
05.06.2017  09:47          1
05.06.2017  09:47          1

04.03.2017  11:13  <DIR>          .
01.09.2017  18:47  <DIR>          ..
23.04.2017  11:07
01.10.2015  22:09
02.09.2017  12:06  <DIR>          .
                8 Datei(en),          55.754.714 Bytes
                7 Verzeichnis(se), 170.492.604.416 Bytes frei

C:\Users\Joern\Downloads> notepad 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier
C:\Users\Joern\Downloads>

2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier - Editor
Datei Bearbeiten Format Ansicht ?
[[ZoneTransfer]
ZoneId=3
```

Eigenschaften > Download am 5. März 2017 und den Sicherheitshinweis!





Alternative Datenströme – Zone.Identifier

Das Ganze können wir natürlich auch mit der Powershell.

```
Windows PowerShell
PS C:\Users\Joern\Downloads> Get-Item .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream *

PSPath           : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4
                  .0.0.exe::$DATA
PSParentPath     : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads
PSChildName     : 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe::$DATA
PSDrive         : C
PSProvider      : Microsoft.PowerShell.Core\FileSystem
PSIsContainer   : False
FileName       : C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
Stream         : :$DATA
Length        : 37228104

PSPath           : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4
                  .0.0.exe:Zone.Identifier
PSParentPath     : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads
PSChildName     : 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier
PSDrive         : C
PSProvider      : Microsoft.PowerShell.Core\FileSystem
PSIsContainer   : False
FileName       : C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
Stream         : Zone.Identifier
Length        : 26

PS C:\Users\Joern\Downloads>
```

Auch hier sehen wir die ZoneId=3.

```
Windows PowerShell
PS C:\Users\Joern\Downloads> Get-Item .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream *

PSPath           : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4
                  .0.0.exe::$DATA
PSParentPath     : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads
PSChildName     : 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe::$DATA
PSDrive         : C
PSProvider      : Microsoft.PowerShell.Core\FileSystem
PSIsContainer   : False
FileName       : C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
Stream         : :$DATA
Length        : 37228104

PSPath           : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4
                  .0.0.exe:Zone.Identifier
PSParentPath     : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads
PSChildName     : 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier
PSDrive         : C
PSProvider      : Microsoft.PowerShell.Core\FileSystem
PSIsContainer   : False
FileName       : C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
Stream         : Zone.Identifier
Length        : 26

PS C:\Users\Joern\Downloads> Get-Content .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
PS C:\Users\Joern\Downloads>
```



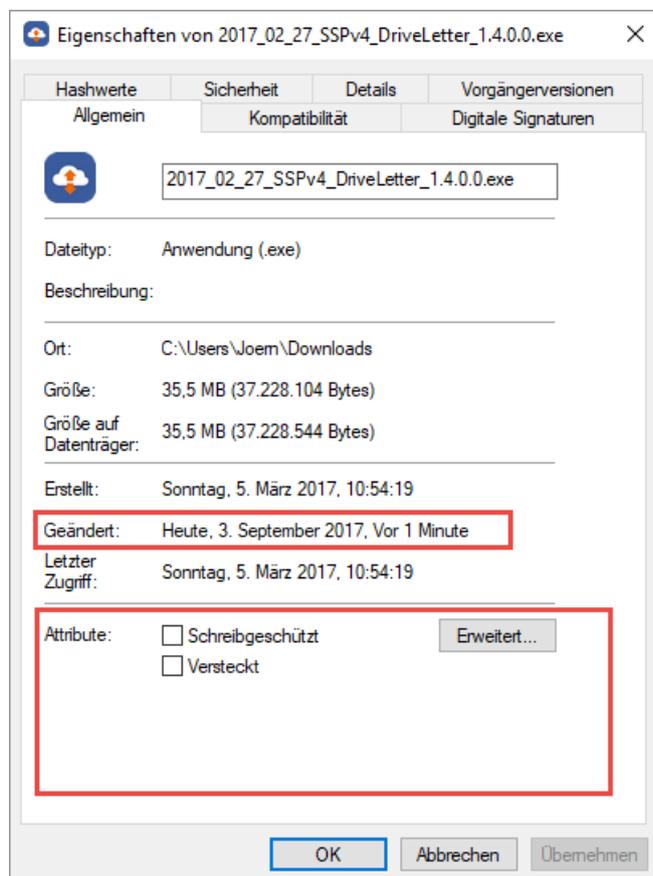
Alternative Datenströme – Zone.Identifier

Wenn ich jetzt den Inhalt der ADS lösche wird die Datei ohne Sicherheitshinweis angezeigt und ist 0 Byte groß.

```
Get-Content .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream Zone.Identifier  
Clear-Content .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream Zone.Identifier  
Get-Item .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream *
```

```
Windows PowerShell  
PS C:\Users\Joern\Downloads> Get-Content .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream Zone.Identifier  
[ZoneTransfer]  
ZoneId=3  
PS C:\Users\Joern\Downloads> Clear-Content .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream Zone.Identifier  
PS C:\Users\Joern\Downloads> Get-Content .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream Zone.Identifier  
PS C:\Users\Joern\Downloads> Get-Item .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream *  
  
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4  
.0.0.exe::$DATA  
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads  
PSChildName : 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe::$DATA  
PSDrive : C  
PSProvider : Microsoft.PowerShell.Core\FileSystem  
PSIsContainer : False  
FileName : C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe  
Stream : $DATA  
Length : 37228104  
  
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4  
.0.0.exe:Zone.Identifier  
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads  
PSChildName : 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier  
PSDrive : C  
PSProvider : Microsoft.PowerShell.Core\FileSystem  
PSIsContainer : False  
FileName : C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe  
Stream : Zone.Identifier  
Length : 0  
  
PS C:\Users\Joern\Downloads>
```

Zu erkennen, dass unter den Attributen nichts mehr steht, der Hinweis rechts fehlt.



Sicherheit: Die Datei stammt von einem anderen Computer. Der Zugriff wurde aus Sicherheitsgründen eventuell blockiert. Zulassen



Alternative Datenströme – Zone.Identifier

Wir können den ADS auch komplett löschen.

```
Remove-Item .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream Zone.Identifier  
Get-Item .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream *
```

```
Windows PowerShell  
PS C:\Users\Joern\Downloads> Remove-Item .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream Zone.Identifier  
PS C:\Users\Joern\Downloads> Get-Item .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream *  
  
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4  
.0.0.exe::$DATA  
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads  
PSChildName : 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe::$DATA  
PSDrive : C  
PSProvider : Microsoft.PowerShell.Core\FileSystem  
PSIsContainer : False  
FileName : C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe  
Stream :::$DATA  
Length : 37228104  
  
PS C:\Users\Joern\Downloads>
```

Wir haben aber auch die Möglichkeit für jede Datei einen ADS zu erstellen. Nach dem Löschen erstelle ich den ADS wieder.

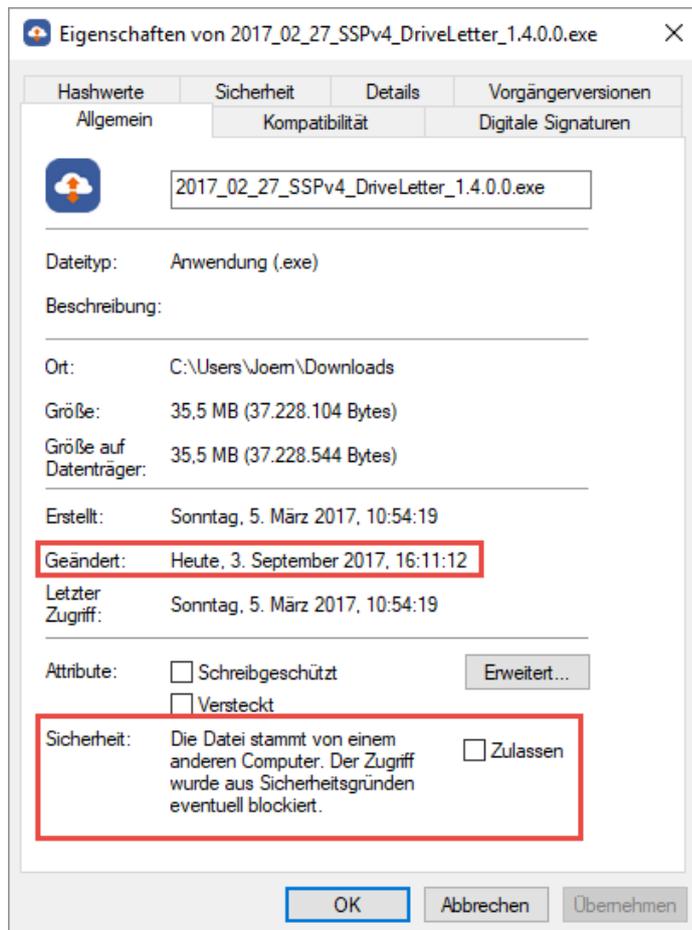
```
Add-Content .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Str Zone.Identifier  
"[ZoneTransfer]`r`nZone=3"
```

```
Windows PowerShell  
PS C:\Users\Joern\Downloads> Add-Content .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Str Zone.Identifier "[Zone  
Transfer]`r`nZone=3"  
PS C:\Users\Joern\Downloads> Get-Item .\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe -Stream *  
  
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4  
.0.0.exe::$DATA  
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads  
PSChildName : 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe::$DATA  
PSDrive : C  
PSProvider : Microsoft.PowerShell.Core\FileSystem  
PSIsContainer : False  
FileName : C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe  
Stream :::$DATA  
Length : 37228104  
  
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4  
.0.0.exe:Zone.Identifier  
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\Joern\Downloads  
PSChildName : 2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier  
PSDrive : C  
PSProvider : Microsoft.PowerShell.Core\FileSystem  
PSIsContainer : False  
FileName : C:\Users\Joern\Downloads\2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe  
Stream : Zone.Identifier  
Length : 26  
  
PS C:\Users\Joern\Downloads>
```

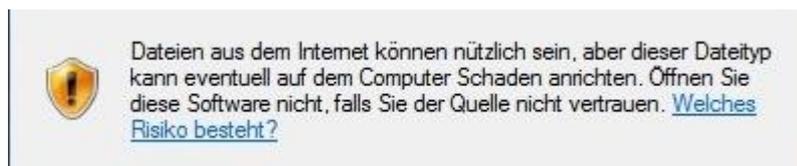


Alternative Datenströme – Zone.Identifier

Voila, auch der Sicherheitshinweis ist wieder da.



Wenn wir wissen das die Datei sicher ist, kann der Haken bei Zulassen gesetzt werden. Somit wird beim Installieren auch kein Sicherheitshinweis ausgegeben.





Alternative Datenströme – Zone.Identifier

Ein weiteres Beispiel:

Habe soeben eine .bat Datei aus dem Internet heruntergeladen. Möchte diese editieren und bekomme folgende Meldung.



ADS ist vorhanden.

```
Administrator: Eingabeaufforderung
C:\Users\Joern\Desktop>dir /r
Datenträger in Laufwerk C: ist WIN10ENT
Volumeseriennummer: 3A2F-B405

Verzeichnis von C:\Users\Joern\Desktop

04.09.2017  18:08  <DIR>          .
04.09.2017  18:08  <DIR>          ..
31.08.2017  13:42                812 DESKTOP.lnk
03.09.2017  21:05  <DIR>          fgdump-2.1.0-exeonly
02.09.2017  11:36                3.814 File to Mail.ps1
04.09.2017  18:07                99 FixMapsBrokerWin10.bat
                26 FixMapsBrokerWin10.bat:Zone.Identifier:$DATA
01.09.2017  14:40                269.775 FSUTIL 8.3.docx
03.09.2017  10:22  <DIR>          IE Trackingschutz TPL
02.09.2017  19:57                1.589 Invoke Command.ps1
03.09.2017  21:16                39.944 NTFS Berechtigungen.xlsx
01.09.2017  10:33  <DIR>          NTFSInfo
02.09.2017  18:49                3.419.698 Performance Tuning Guidelines for Windows Server 2016.pdf
04.09.2017  17:55  <DIR>          Progs
03.09.2017  21:09  <DIR>          pwdump6-2.0.0-beta-exe-only
04.03.2017  02:46                691 Total Commander 64 bit.lnk
04.03.2017  02:46                677 Total Commander.lnk
31.08.2017  18:47                780 Update AD-Users with new Phone-number and Pager via Powershell.txt
02.09.2017  18:48                490.686 Windows Server 2016 IT Pro.pdf
                11 Datei(en), 4.228.565 Bytes
                7 Verzeichnis(se), 165.447.254.016 Bytes frei

C:\Users\Joern\Desktop>
```



Alternative Datenströme – Zone.Identifier

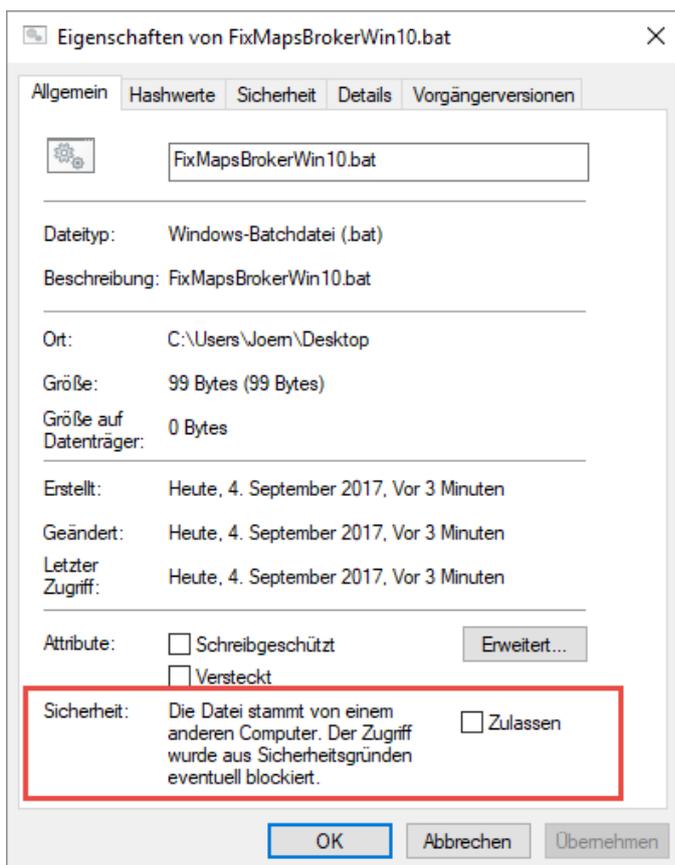
Auch hier schauen wir uns den Zone.Identifier mal an.

```
Administrator: Eingabeaufforderung
Datenträger in Laufwerk C: ist WIN10ENT
Volumeseriennummer: 3A2F-B405

Verzeichnis von C:\Users\Joern\Desktop
04.09.2017 18:08 <DIR> .
04.09.2017 18:08 <DIR> ..
31.08.2017 13:42      812 DESKTOP.lnk
03.09.2017 21:05 <DIR>      fgdump-2.1.0-exeonly
02.09.2017 11:36      3.814 File to Mail.ps1
04.09.2017 18:07      99 FixMapsBrokerWin10.bat
      26 FixMapsBrokerWin10.bat:Zone.Identifier:$DATA
01.09.2017 14:40    269.775 FSUTIL 8.3.docx
03.09.2017 10:22 <DIR>      IE Trackingschutz TPL
02.09.2017 19:57      1.589 Invoke Command.ps1
03.09.2017 21:16      39.944 NTFS Berechtigungen.xlsx
01.09.2017 10:33 <DIR>      NTFSInfo
02.09.2017 18:49    3.419.698 Performance Tuning Guidelines for Windows Server 2016.pdf
04.09.2017 17:55 <DIR>      Progs
03.09.2017 21:09 <DIR>      pwddump6-2.0.0-beta-exe-only
04.03.2017 02:46      691 Total Commander 64 bit.lnk
04.03.2017 02:46      677 Total Commander.lnk
31.08.2017 18:47      780 Update AD-Users with new Phone-number and Pager via Powershell.txt
02.09.2017 18:48    490.686 Windows Server 2016 IT Pro.pdf
      11 Datei(en),      4.228.565 Bytes
      7 Verzeichnis(se), 165.447.254.016 Bytes frei

C:\Users\Joern\Desktop>notepad FixMapsBrokerWin10.bat:Zone.Identifier
C:\Users\Joern\Desktop>
```

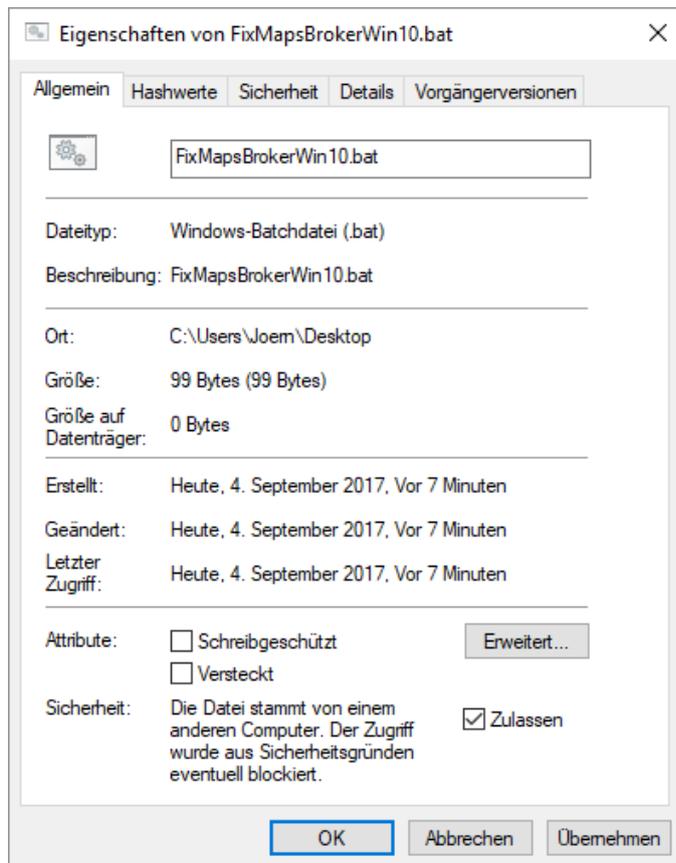
Dateieigenschaften:





Alternative Datenströme – Zone.Identifier

Setze den Haken auf Zulassen:



Und schon kann ich die Datei editieren ohne das SmartScreen eine Warnmeldung ausgibt.

```
FixMapsBrokerWin10.bat - Editor
Datei Bearbeiten Format Ansicht ?
@echo off
sc config MapsBroker start= auto
sc start MapsBroker
exit
```



Alternative Datenströme – Zone.Identifier

Aus der Community bekommen wir auch eine kleine Erweiterung für die Powershell.

<http://pscx.codeplex.com/>

```
Administrator: Windows PowerShell
PS C:\Users\Joern\Downloads> Get-Command Unblock-File -All

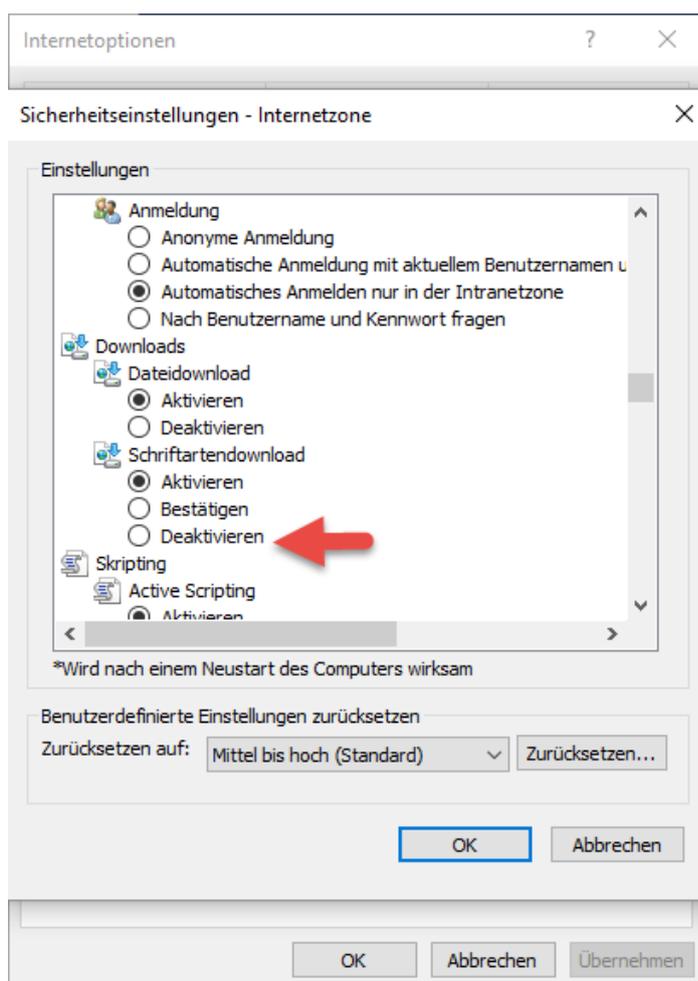
CommandType      Name                Version            Source
-----
Cmdlet           Unblock-File       3.1.0.0           Microsoft.PowerShell.Utility

PS C:\Users\Joern\Downloads> Unblock-File .\2017_02_27_S5Pv4_DriveLetter_1.4.0.0.exe
PS C:\Users\Joern\Downloads>
```

Optional:

Den Download von Dateien unterbinden.

Internetoptionen > Sicherheit > Internet > Stufen anpassen... > Downloads





Alternative Datenströme – Zone.Identifier

Eine Datei unter NTFS kann mehrere Streams (Datenströme) besitzen. Sehen können wir ohne Hilfsmittel immer nur den Stream 1. Ein Stream speichert z.B. zusätzliche Metadaten zur Datei, wie etwa die Eigenschaften einer Datei, den Autor, Interpret, Album usw. Wenn man nicht weiß, dass an einer Datei ein Stream anhängt, könnte man ihn dazu benutzen weitere Informationen zu verstecken oder sogar Schadcode!

Kurzer Einblick:

```
Administrator: Eingabeaufforderung
C:\temp>echo "Das ist ein test" > Stream.txt
C:\temp>type stream.txt
"Das ist ein test"
C:\temp>echo "Das ist ein test" > Stream.txt:GeheimeInformation
C:\temp>type stream.txt
"Das ist ein test"
C:\temp>dir /r
Datenträger in Laufwerk C: ist WIN10ENT
Volumeseriennummer: 3A2F-B405

Verzeichnis von C:\temp

03.09.2017  16:59  <DIR>          .
03.09.2017  16:59  <DIR>          ..
01.09.2017  17:17                19 1-TEST.txt
01.09.2017  14:40            269.775 FSUTIL 8.3.docx
02.09.2017  19:23                47 Services.ps1
03.09.2017  16:59                21 Stream.txt
                21 Stream.txt:GeheimeInformation:$DATA
02.09.2017  19:49                42 Test.txt
31.08.2017  18:47            780 Update AD-Users with new Phone-number and Pager via Powershell.txt
        6 Datei(en),          270.684 Bytes
        2 Verzeichnis(se), 167.059.644.416 Bytes frei

C:\temp>
```

Oder so, jetzt haben wir eine .exe Datei erzeugt.

```
Administrator: Eingabeaufforderung
C:\Users\Joern\Downloads>echo "Das ist ein Test" > testdatei.txt:testdatei.exe
C:\Users\Joern\Downloads>
```



Alternative Datenströme – Zone.Identifier

```
Administrator: Eingabeaufforderung
C:\Users\Joern\Downloads>echo "Das ist ein Test" > testdatei.txt:testdatei.exe
C:\Users\Joern\Downloads>dir /r
Datenträger in Laufwerk C: ist WIN10ENT
Volumeseriennummer: 3A2F-B405

Verzeichnis von C:\Users\Joern\Downloads

03.09.2017  18:09  <DIR>          .
03.09.2017  18:09  <DIR>          ..
03.09.2017  17:45                37.228.104  2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe
                24  2017_02_27_SSPv4_DriveLetter_1.4.0.0.exe:Zone.Identifier:$DATA
23.04.2017  11:07                515 ASCII Table  ASCII code table.website
                1.251 ASCII Table  ASCII code table.website:favicon:$DATA
04.03.2017  18:48  <DIR>          Compressed
07.06.2017  21:01  <DIR>          Documents
13.05.2017  22:52                7.013.752  FileZilla_3.25.2_win64-setup.exe
31.08.2017  22:27                7.897.776  FileZilla_3.27.1_win64-setup.exe
05.06.2017  09:47                1.810.432  MBSASetup-x64-DE.msi
05.06.2017  09:47                1.716.224  MBSASetup-x86-DE.msi
                247  MBSASetup-x86-DE.msi:Zone.Identifier:$DATA
04.03.2017  11:13  <DIR>          Music
01.09.2017  18:47  <DIR>          Programs
23.04.2017  11:07                487 QR code - Wikipedia.website
                2.734 QR code - Wikipedia.website:favicon:$DATA
01.10.2015  22:09                87.424  streams.exe
03.09.2017  18:09                0  testdatei.txt
                21  testdatei.txt:testdatei.exe:$DATA
02.09.2017  12:06  <DIR>          Video
                9 Datei(en),    55.754.714 Bytes
                7 Verzeichnis(se), 166.766.436.352 Bytes frei

C:\Users\Joern\Downloads>
```

Die Datei ist leer, wo ist der Inhalt?

```
Administrator: Eingabeaufforderung
C:\Users\Joern\Downloads>notepad testdatei.txt
C:\Users\Joern\Downloads>
```

Der Inhalt war in der testdatei.exe versteckt.

```
Administrator: Eingabeaufforderung
C:\Users\Joern\Downloads>notepad testdatei.txt
C:\Users\Joern\Downloads>notepad testdatei.txt:testdatei.exe
C:\Users\Joern\Downloads>
```