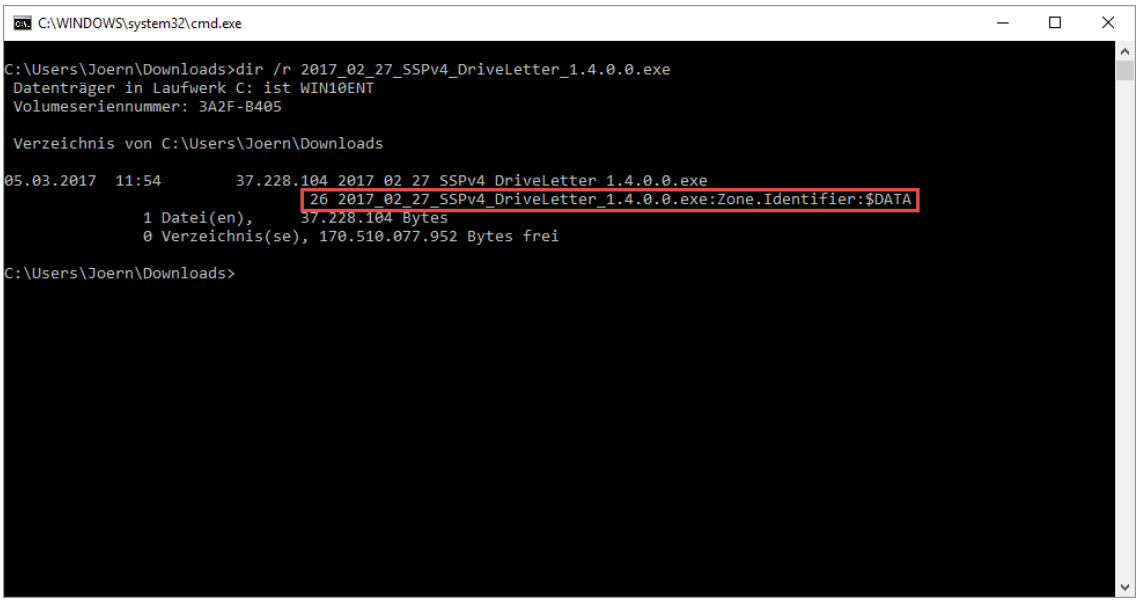
Alternative Datenströme – Zone.Identifier

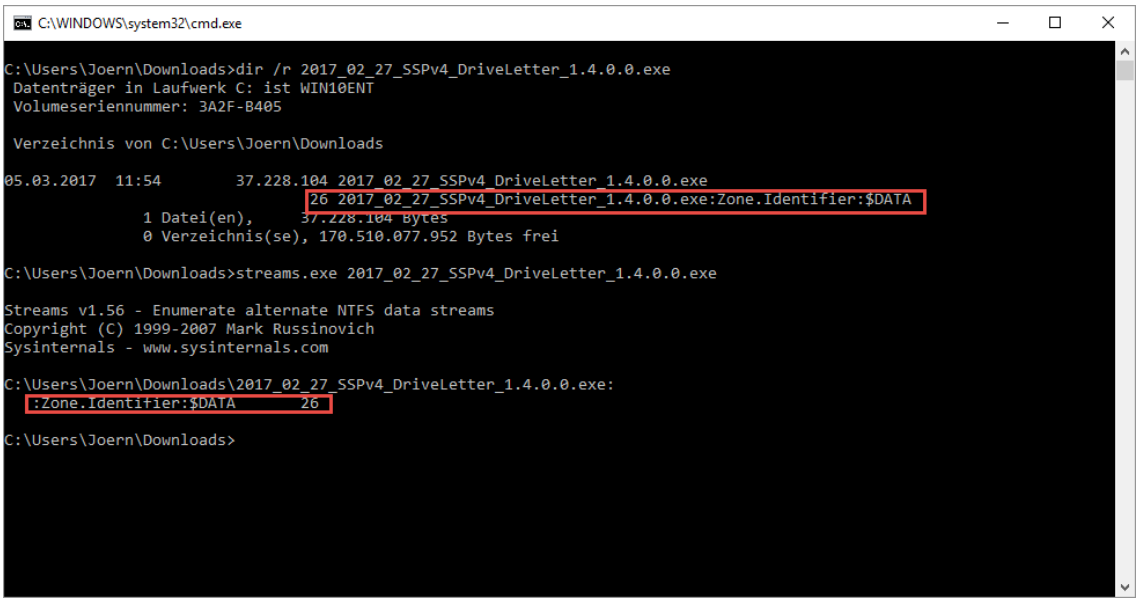
Microsoft schützt uns mit dem Anlagen-Manager vor nicht sicheren Anlagen, die per E-Mail oder aus dem Internet heruntergeladen wurden. Hat der Anlagen-Manager eine mögliche potenzielle Anlage erkannt werden wir am Öffnen gehindert. Häufiger jedoch treten Probleme bei heruntergeladenen Dateien auf. Wenn 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.



Mark Russinovich hält dafür natürlich auch ein Tool bereit.

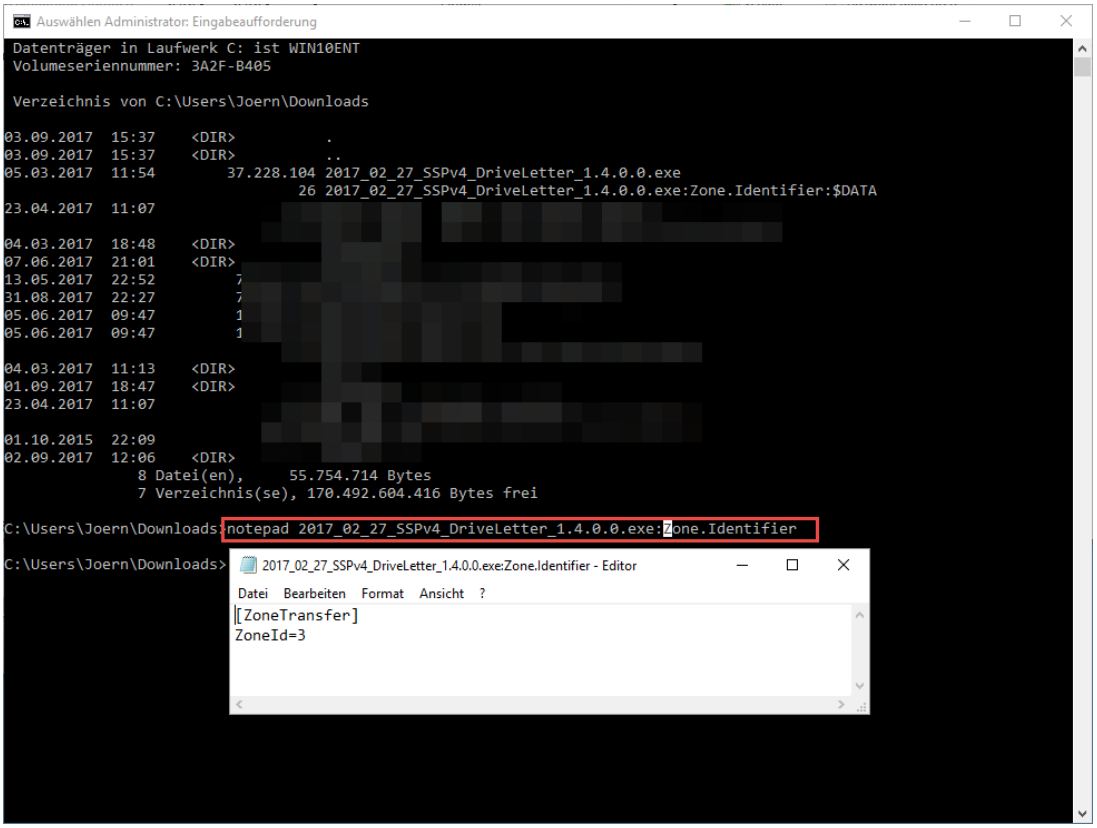


Alternative Datenströme – Zone.Identifier

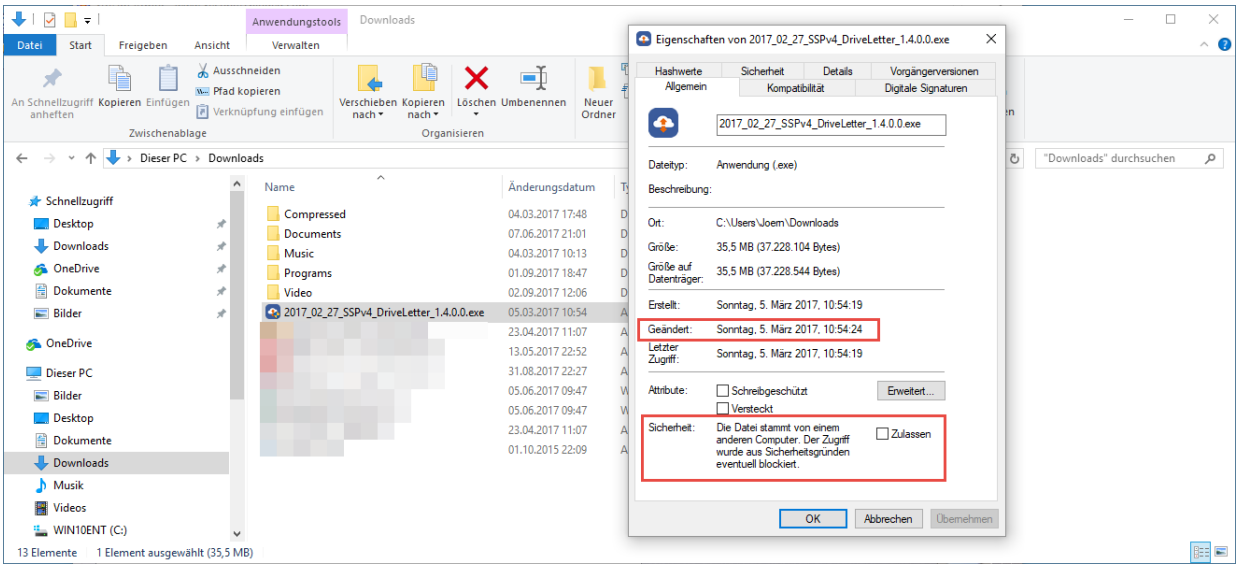
Es gibt verschieden Zonen wir z.B.:

- 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.

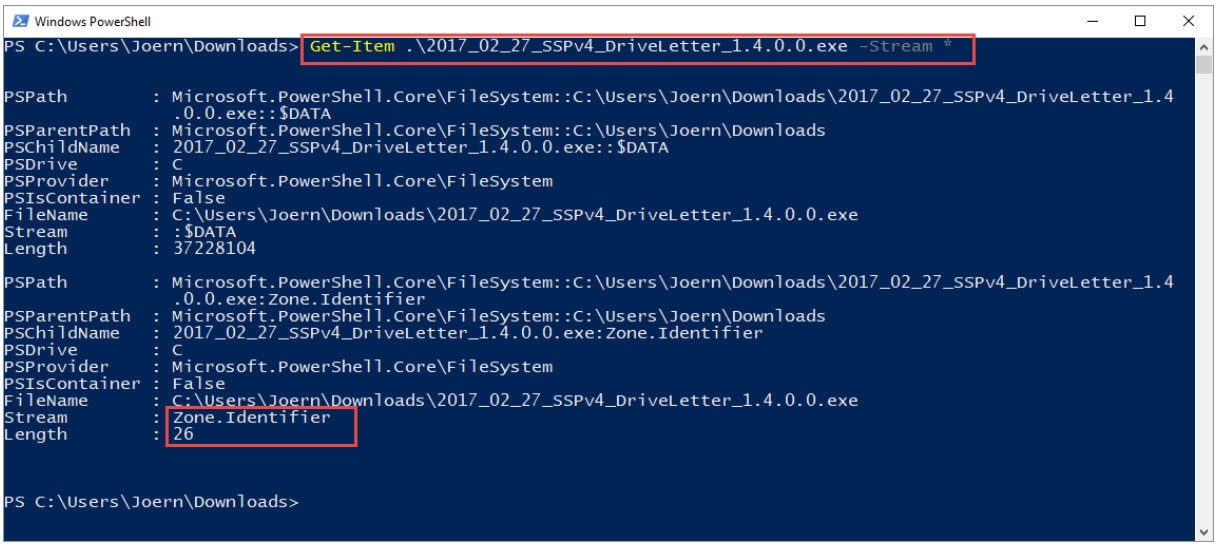


Eigenschaften > Download am 5. März 2017 und den Sicherheitshinweis!

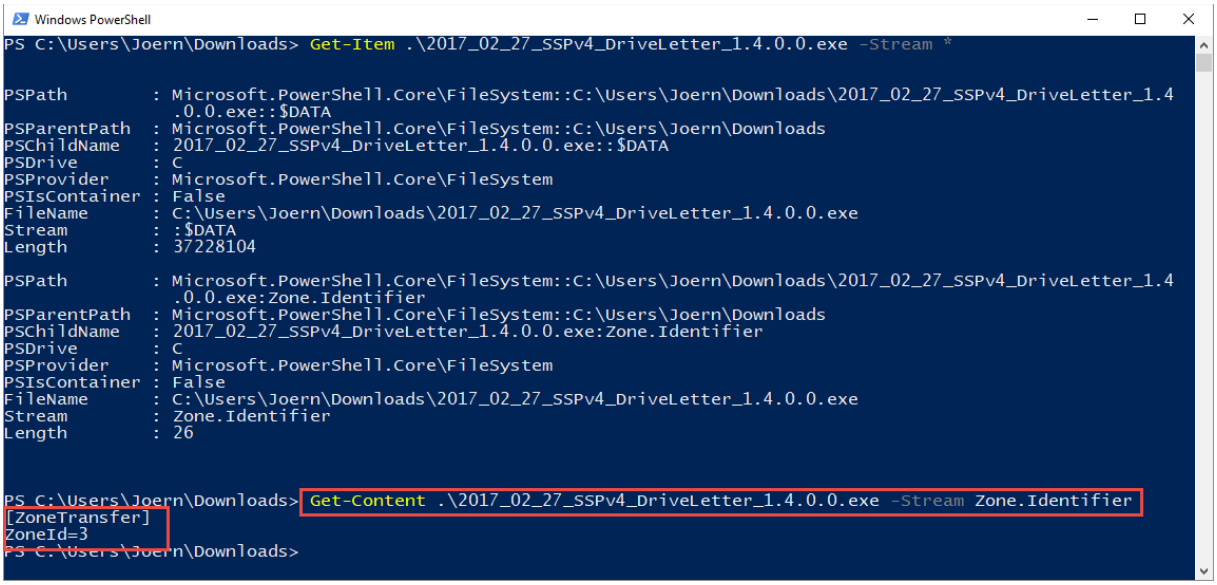


Alternative Datenströme – Zone.Identifier

Das Ganze können wir natürlich auch mit der Powershell.



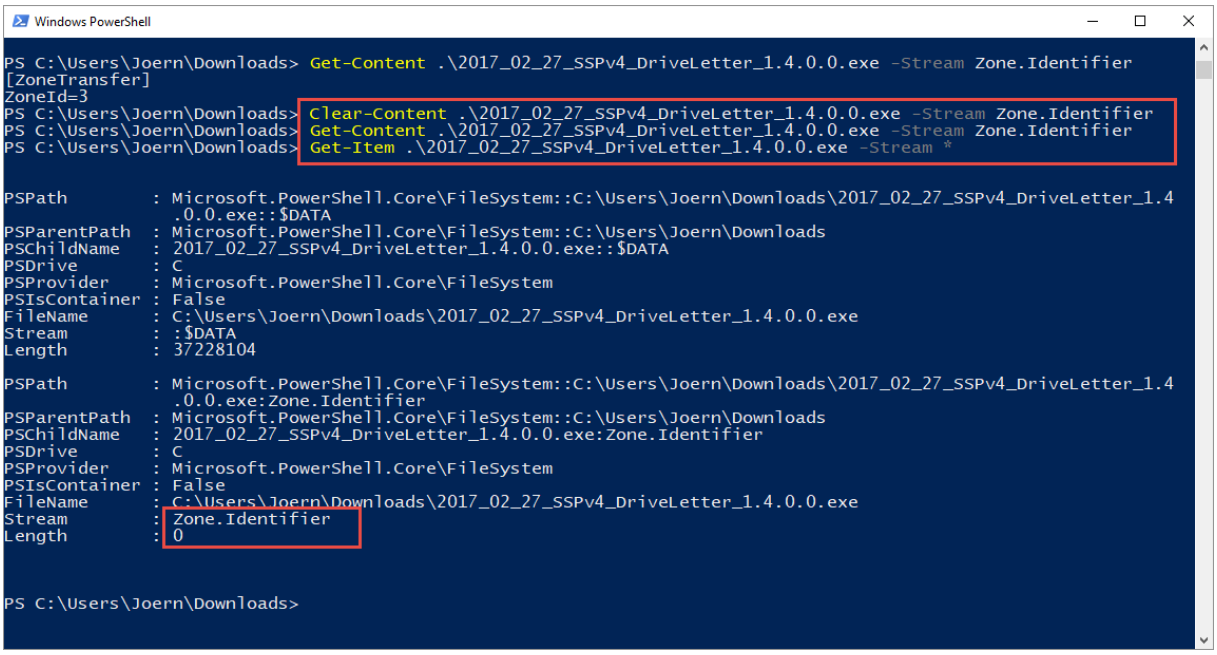
Auch hier sehen wir die ZoneId=3.



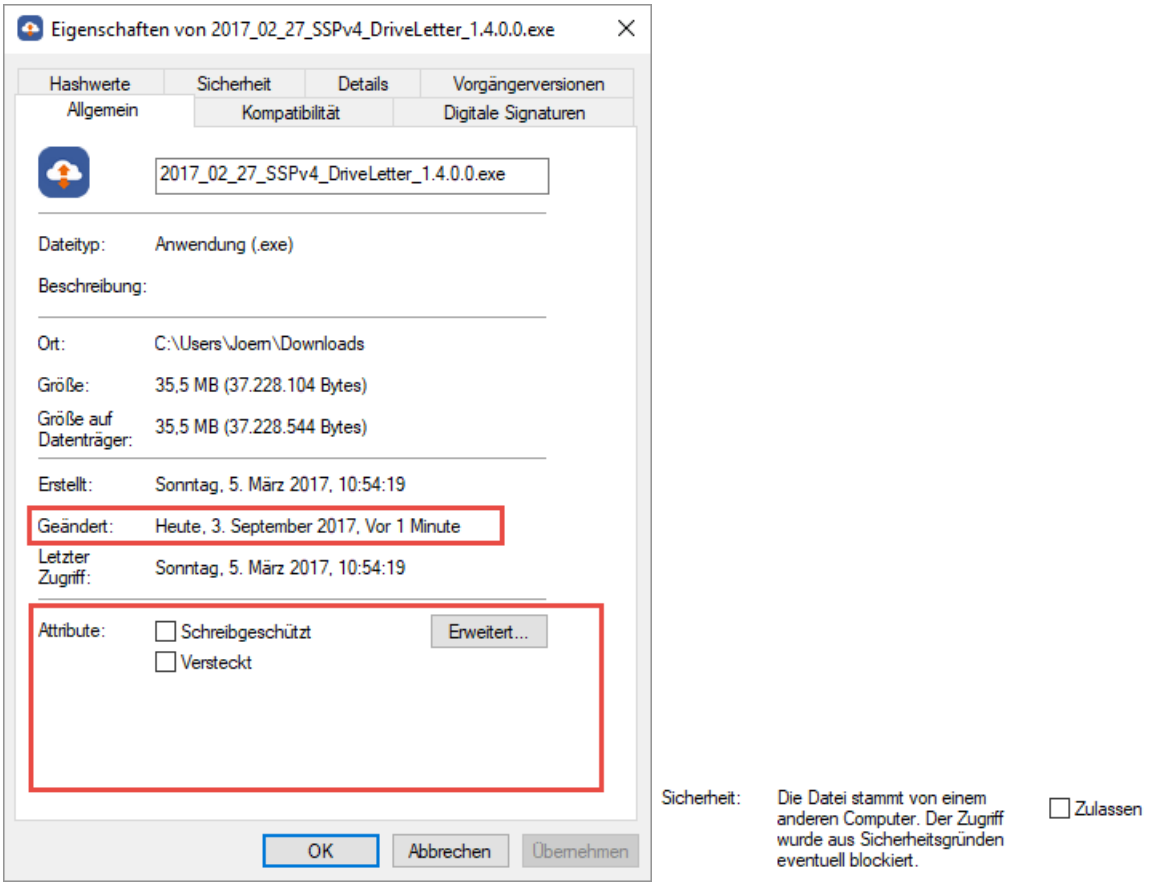
Alternative Datenströme – Zone.Identifier

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 *



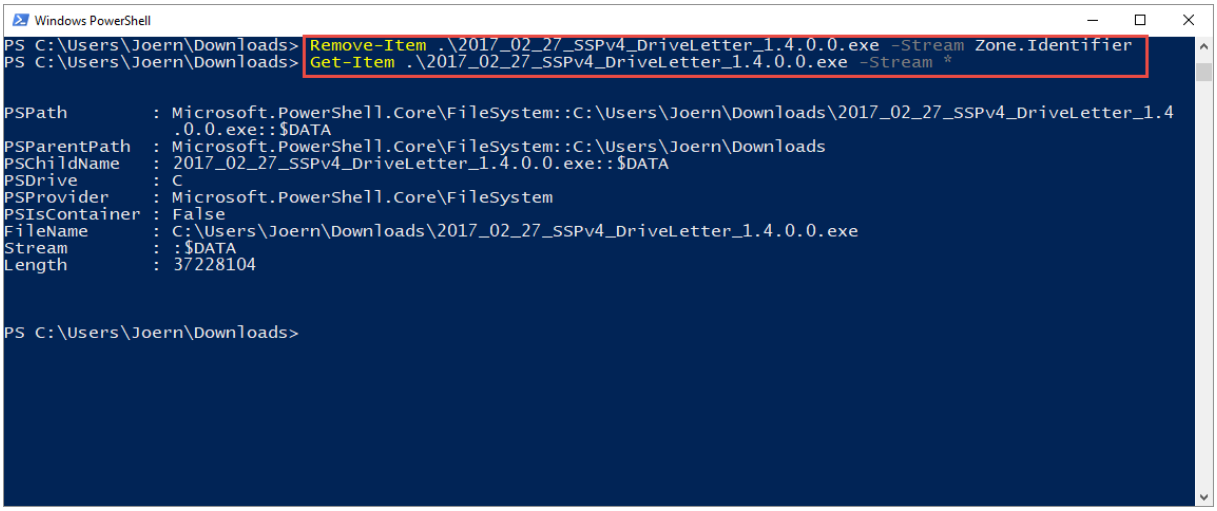
Zu erkennen, dass unter den Attributen nichts mehr steht, der Hinweis rechts fehlt.



Alternative Datenströme – Zone.Identifier

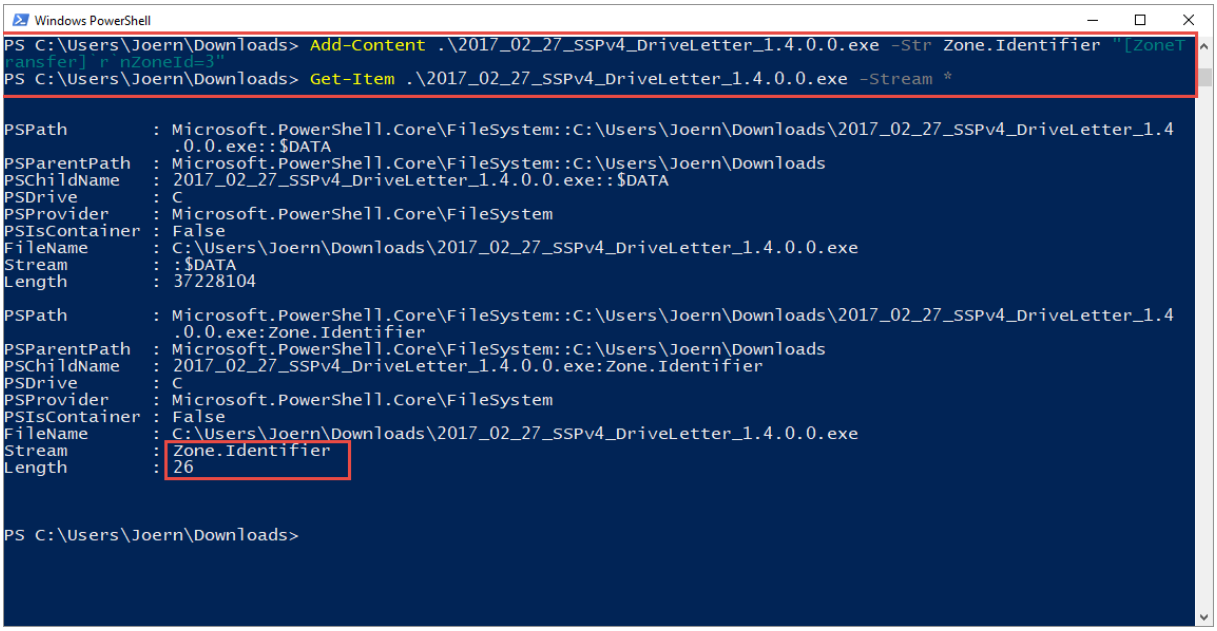
Wir können den ADS auch komplett löschen.

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 *



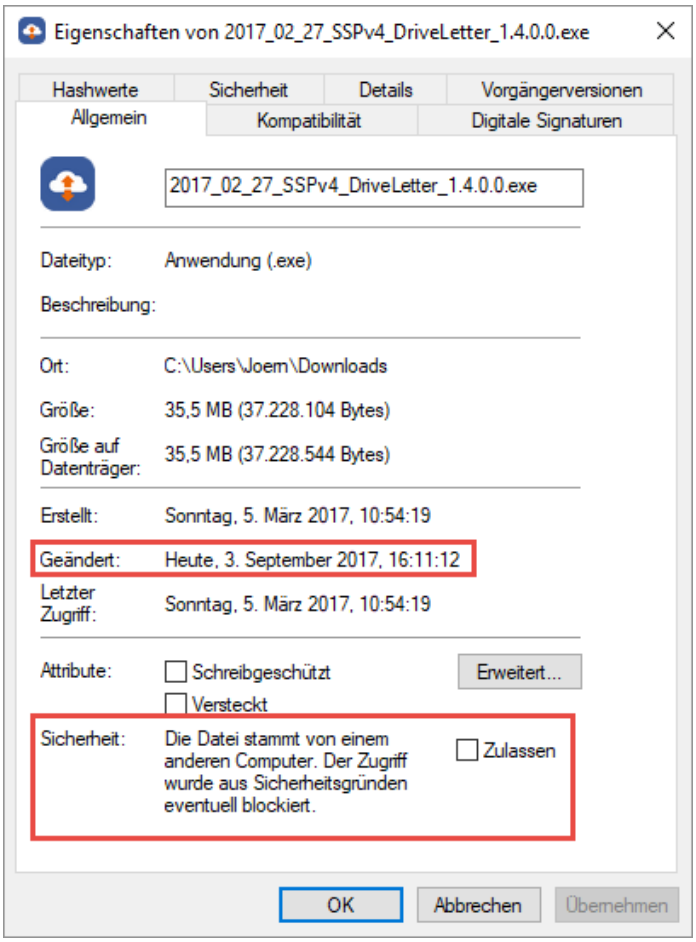
Wir haben aber auch die Möglichkeit für jede Datei einen ADS zu erstellen. Nach dem Löschen erstelle ich den ADS wieder.

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

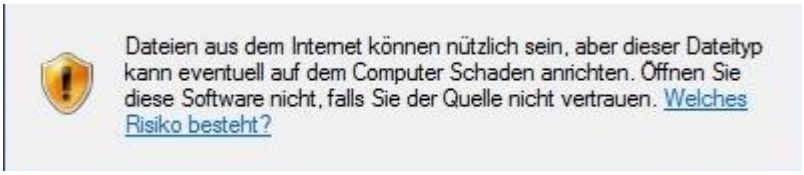


Alternative Datenströme – Zone.Identifier

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.

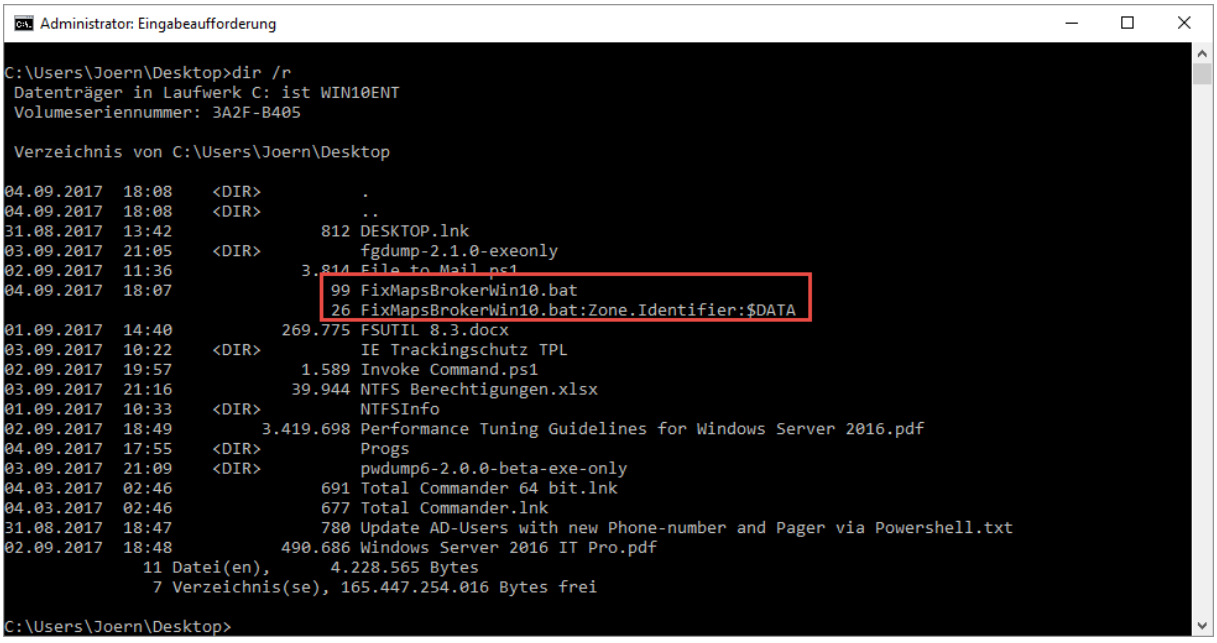


Alternative Datenströme – Zone.Identifier

Ein weiteres Beispiel:

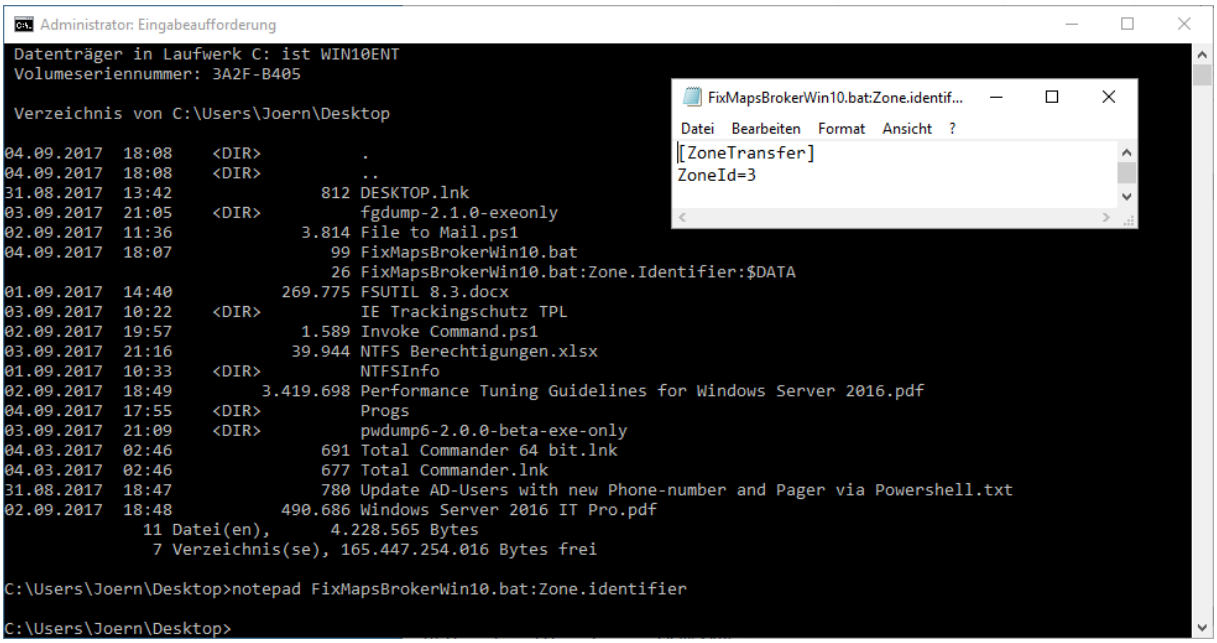
Habe soeben eine .bat Datei aus dem Internet heruntergeladen. Möchte diese editieren und bekomme folgende Meldung.

ADS ist vorhanden.

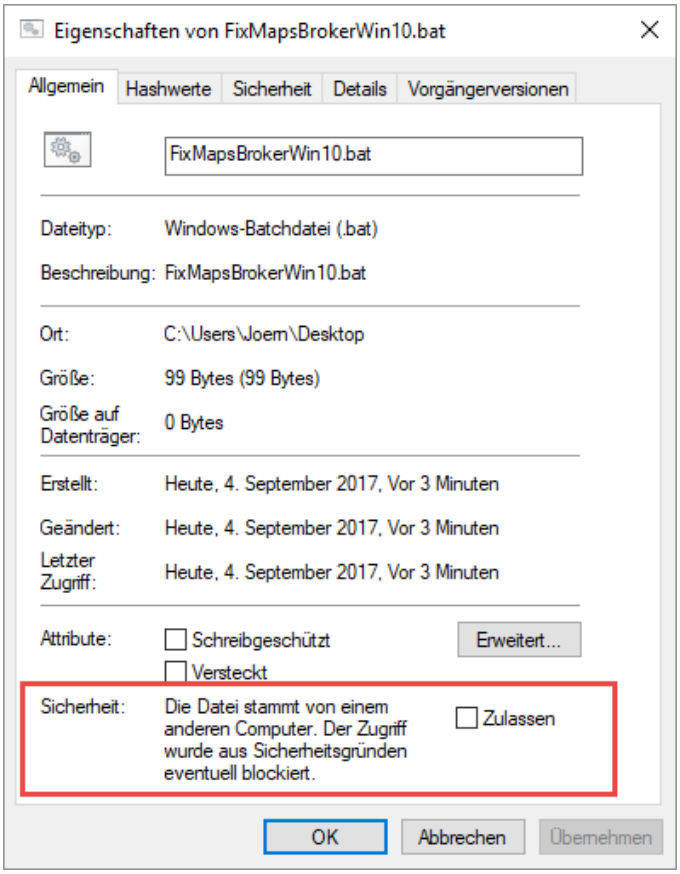


Alternative Datenströme – Zone.Identifier

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

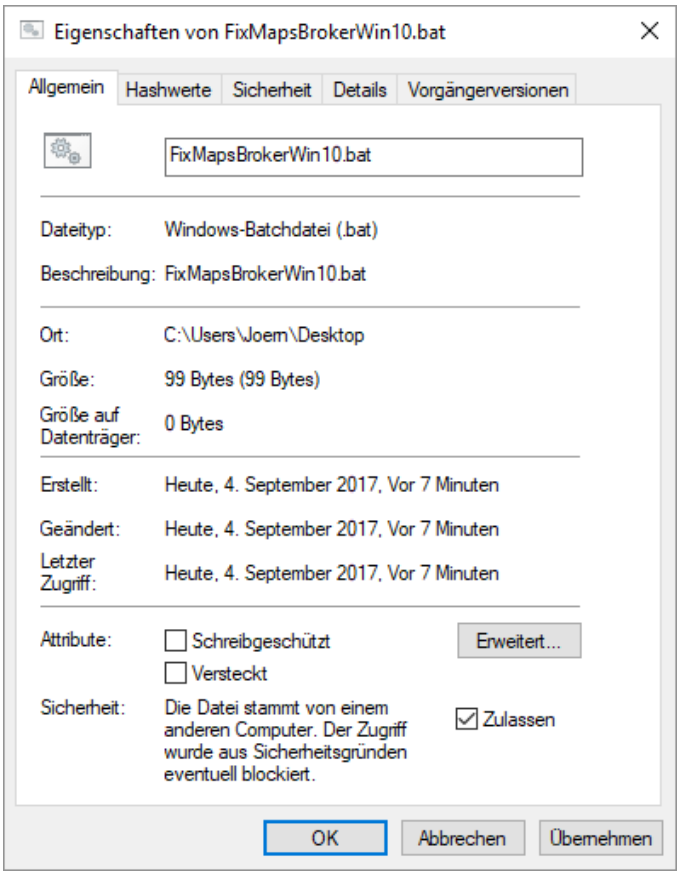


Dateieigenschaften:

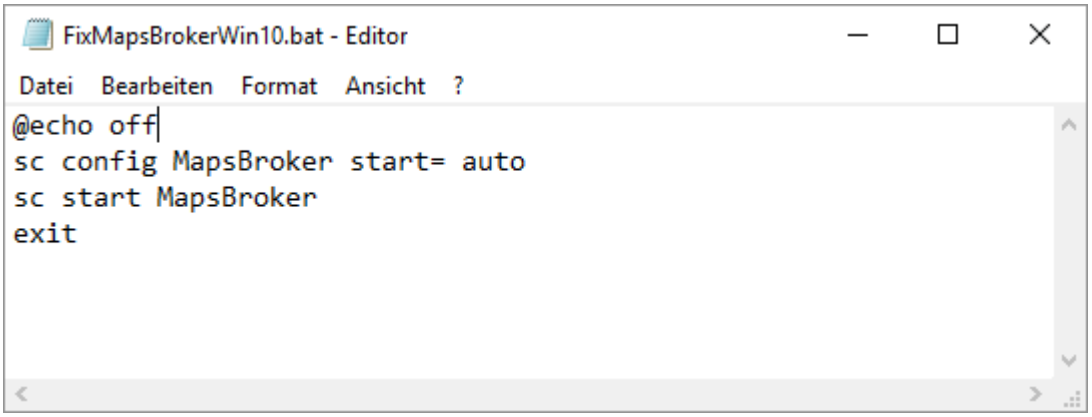


Alternative Datenströme – Zone.Identifier

Setze den Haken auf Zulassen:



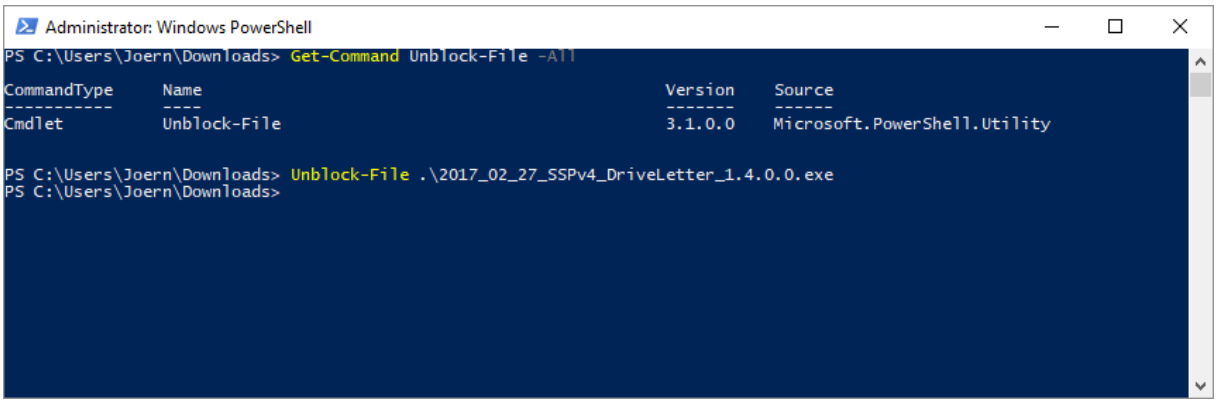
Und schon kann ich die Datei editieren ohne das SmartScreen eine Warnmeldung ausgibt.



Alternative Datenströme – Zone.Identifier

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

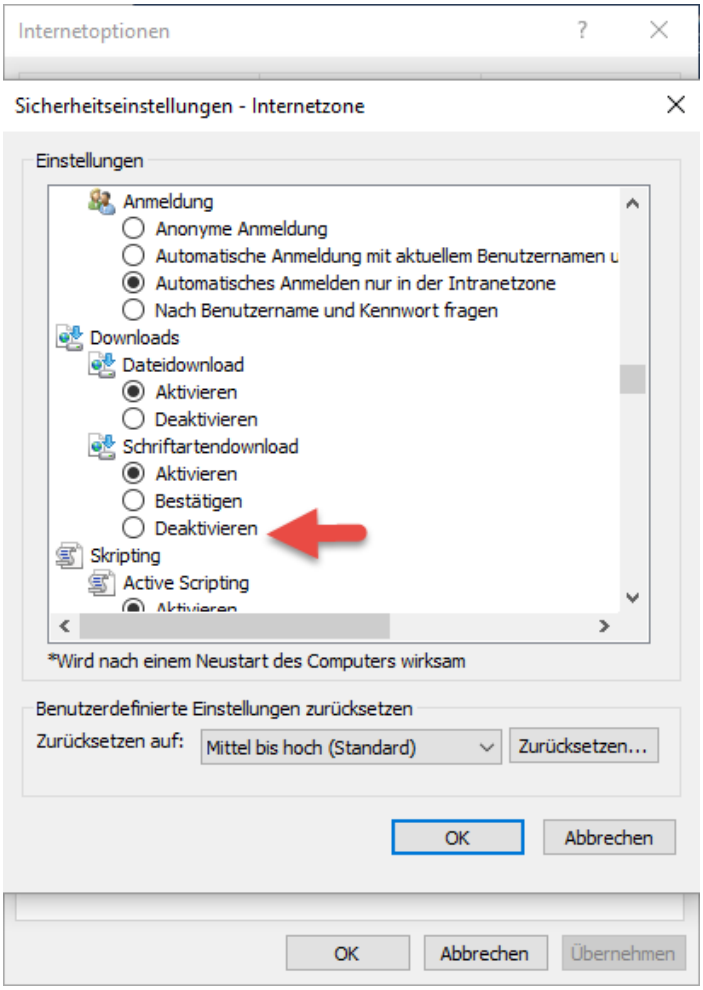
http://pscx.codeplex.com/



Optional:

Den Download von Dateien unterbinden.

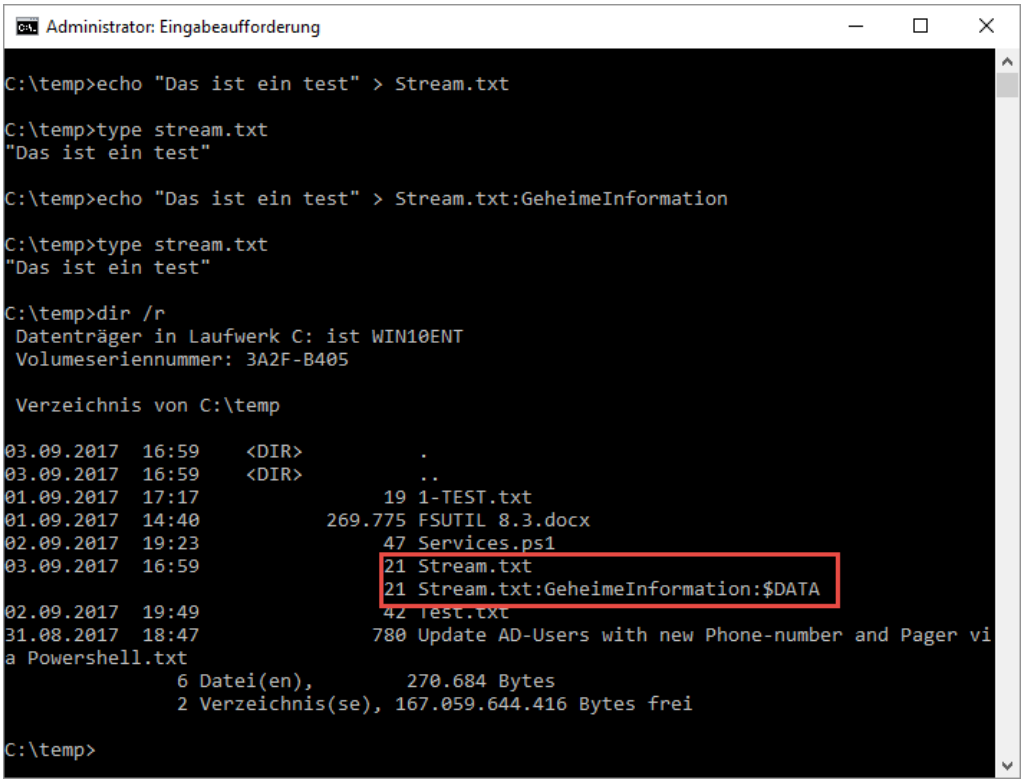
Internetoptionen > Sicherheit > Internet > Stufen anpassen… > Downloads



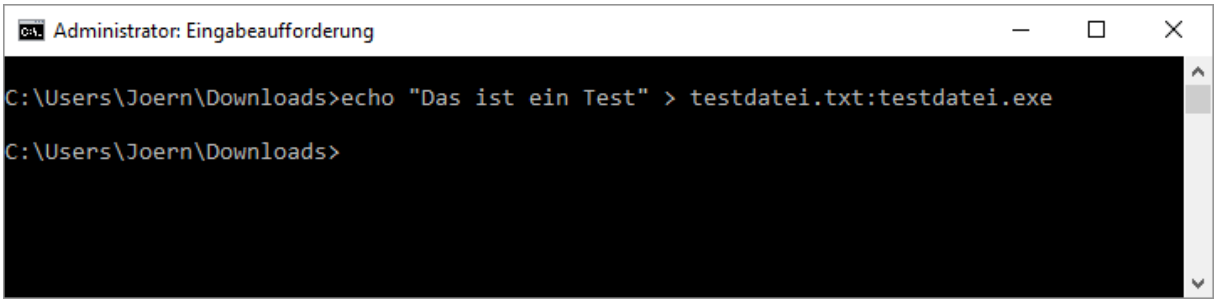
Alternative Datenströme – Zone.Identifier

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!

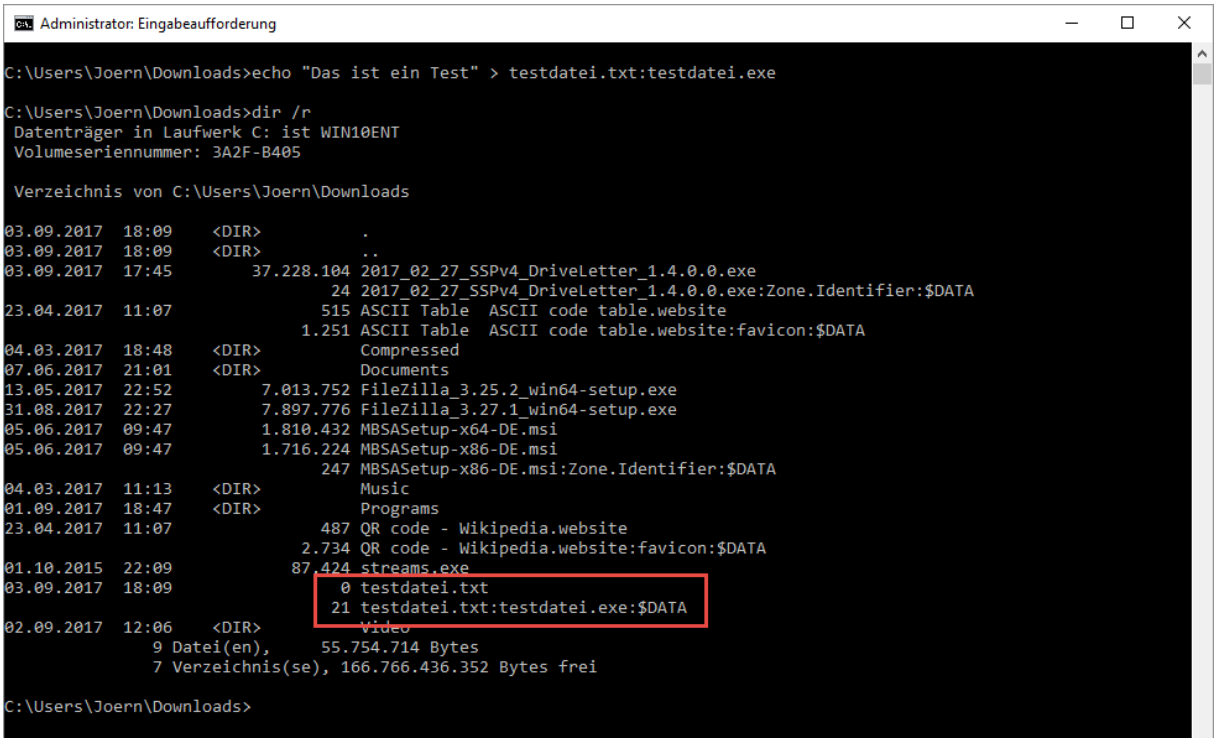
Kurzer Einblick:



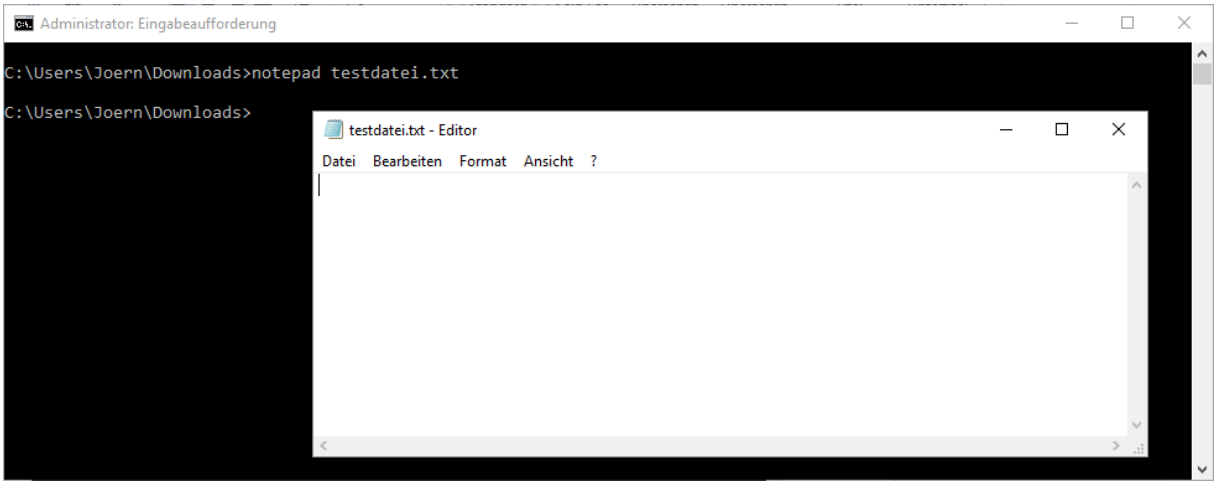
Oder so, jetzt haben wir eine .exe Datei erzeugt.



Alternative Datenströme – Zone.Identifier



Die Datei ist leer, wo ist der Inhalt?



Der Inhalt war in der tesdatei.exe versteckt.