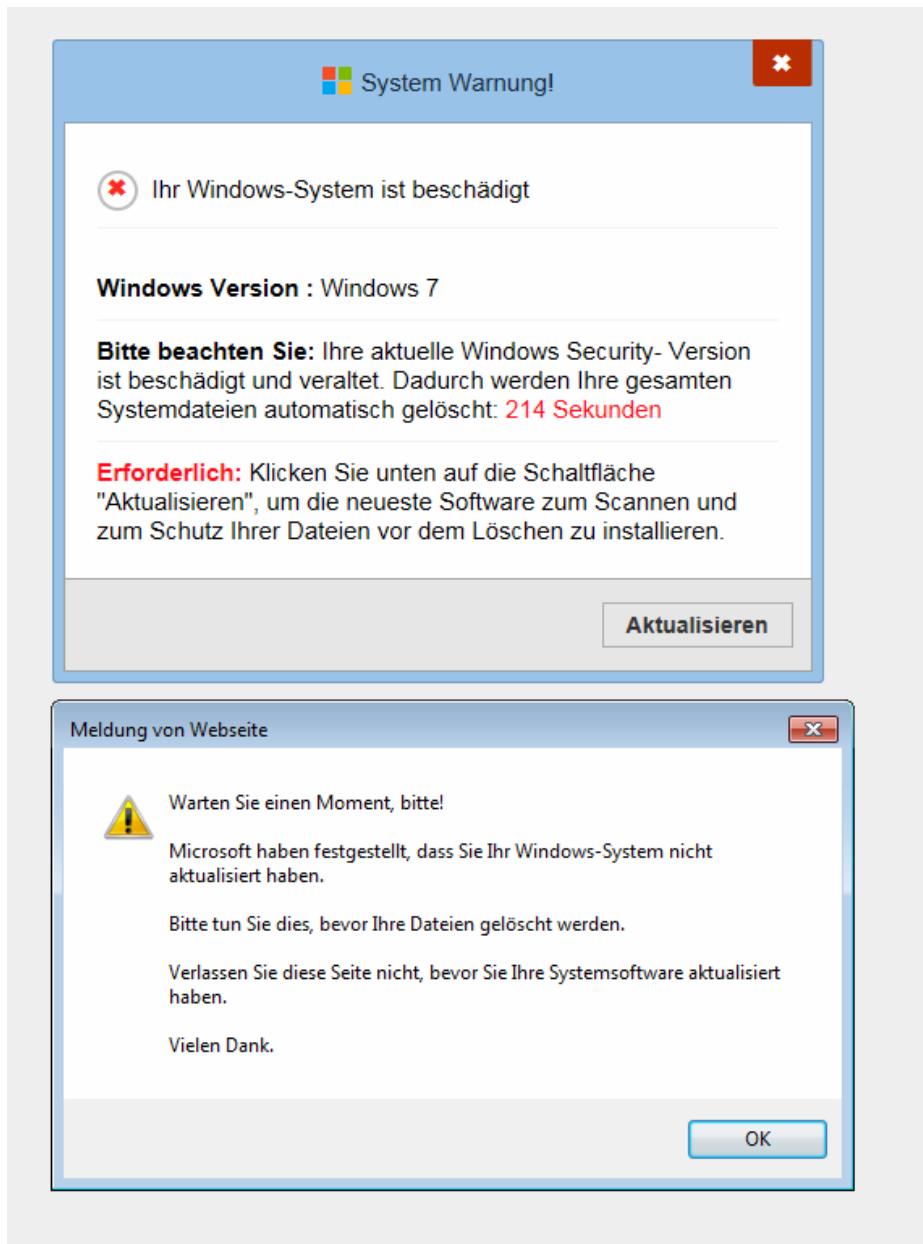




Anleitung im Browser Angriff mit nervendem Hupendem Computer Beispiel:

Man ist beispielsweise am Herunterladen einer Serie aus dem Internet, was man ja schon so oft getan hatte. Immer ohne Probleme, aber dann ...

Plötzlich geht das folgende Fenster auf und der PC hupt aus den Lautsprechern wie verrückt.



Egal wo man drauf klickt, es hört nicht auf. Das Hupen nervt und man kommt in den beabsichtigten Zugzwang.

Der Browser lässt sich nicht schliessen!

Man muss den Browser per Taskmanager beenden.



Die Analyse des Angriffs ergab folgendes:

Bibliothek	Name	Schlagwörter	Adresse
✓ Chronik			
Heute	***Attention Required*** - [http://windows.windows-gesperzt.download/firefox/index.php]		http://windows.windows-gesperzt.download/firefox/index.php
Gestern	***Attention Required***		http://windows.windows-gesperzt.download/
Letzte 7 Tage	35.184.188.211/NTTNTxMTE5LzltNtUhDe2MTMS5l8lwWowN28zaTc		http://35.184.188.211/NTTNTxMTE5LzltNtUhDe2MTMS5l8lwWowN28zaTc
In diesem Monat	Share-Links.biz - AXQ1XLPQR8 - [http://share-links.biz/_1j0ldg5fmfm]		http://share-links.biz/_1j0ldg5fmfm
April	- [http://www.boers.de/redirection-to/redirects/http://334.hcf%2fshare-links.biz/_1j0ldg5fmfm]		http://www.boers.de/redirection-to/redirects/http://334.hcf%2fshare-links.biz/_1j0ldg5fmfm
März	Relinkto - Share TNG Staffel 7 20g - [http://relinkto.view.php?id=12de7d407799e9bce68522da5b7]		http://relinkto.view.php?id=12de7d407799e9bce68522da5b7
Februar	Relinkto - Share Links for cash! - [http://relinkto.container_captcha.php?id=12de7d407799e9bce68522da5b7]		http://relinkto.container_captcha.php?id=12de7d407799e9bce68522da5b7
Januar	Container Password - [http://relinkto/container-password/?p_id=12de7d407799e9bce68522da5b7]		http://relinkto/container-password/?p_id=12de7d407799e9bce68522da5b7
Dezember 2017	- [http://www.boers.de/redirection-to/redirects/http://334.hcf%2fshare-links.biz/_1j0ldg5fmfm]		http://www.boers.de/redirection-to/redirects/http://334.hcf%2fshare-links.biz/_1j0ldg5fmfm
Altler als 6 Monate	Star TNG The Next Generation Remastered 501 - 507 COMPLETE German DL AC3 720p Bluray x264 - INO - Bours.A...		http://www.boers.de/videoebooks/serien/130622_star-tng-next-generation-remastered-501-507-complete-germa...

Der Versuch die Star Trek-Serie herunterzuladen

Star Trek TNG The Next Generation Remastered S01 - S07 COMPLETE German
<http://www.boerse.sh/boerse/videoboerse/serien/1306622-star-trek-tng-next-generation-remastered-s01-s07-complete-german-dl-ac3-720p-bluray-x264-ind.html>

führte zu der Umleitung zu Share-links.biz

<http://www.boerse.sh/redirect-to/?redirect=http%3A%2F%2Fshare-links.biz%2F1jox6p15fmf>

Diese wiederum

<http://share-links.biz/1jolx6pj5fm>

dann weiter zu

<http://35.184.188.211/NTE1NTEyNTkxMTE5LzUxNTUxNDE2MTM5Mi8wdWowN28zaTc3>

Ab hier begann dann der Angriff

Die weitere Webseite wurde aufgerufen

Attention Required

<http://windows.windows-gesperrt1.download/>

Der Browser Firefox dabei erkannt

<http://windows.windows-gesperrt1.download/firefox/index.php>

So konnte gezielt Firefox manipuliert werden!

Beim nochmaligen Direkten Aufruf der Webseite per URL warnte uns ESET DANN vor der schädlichen Webseite ...

Meist funktionieren solche Angriffe nur kurze Zeit, weil dann die o.a. Webseite schon wieder nicht erreichbar ist. Aber eines ist klar, diese Art Angriffe ist ganz neu so dass der Virenschutz nicht unbedingt anspringen wird.

Das Ganze geschah am 09.06.2018