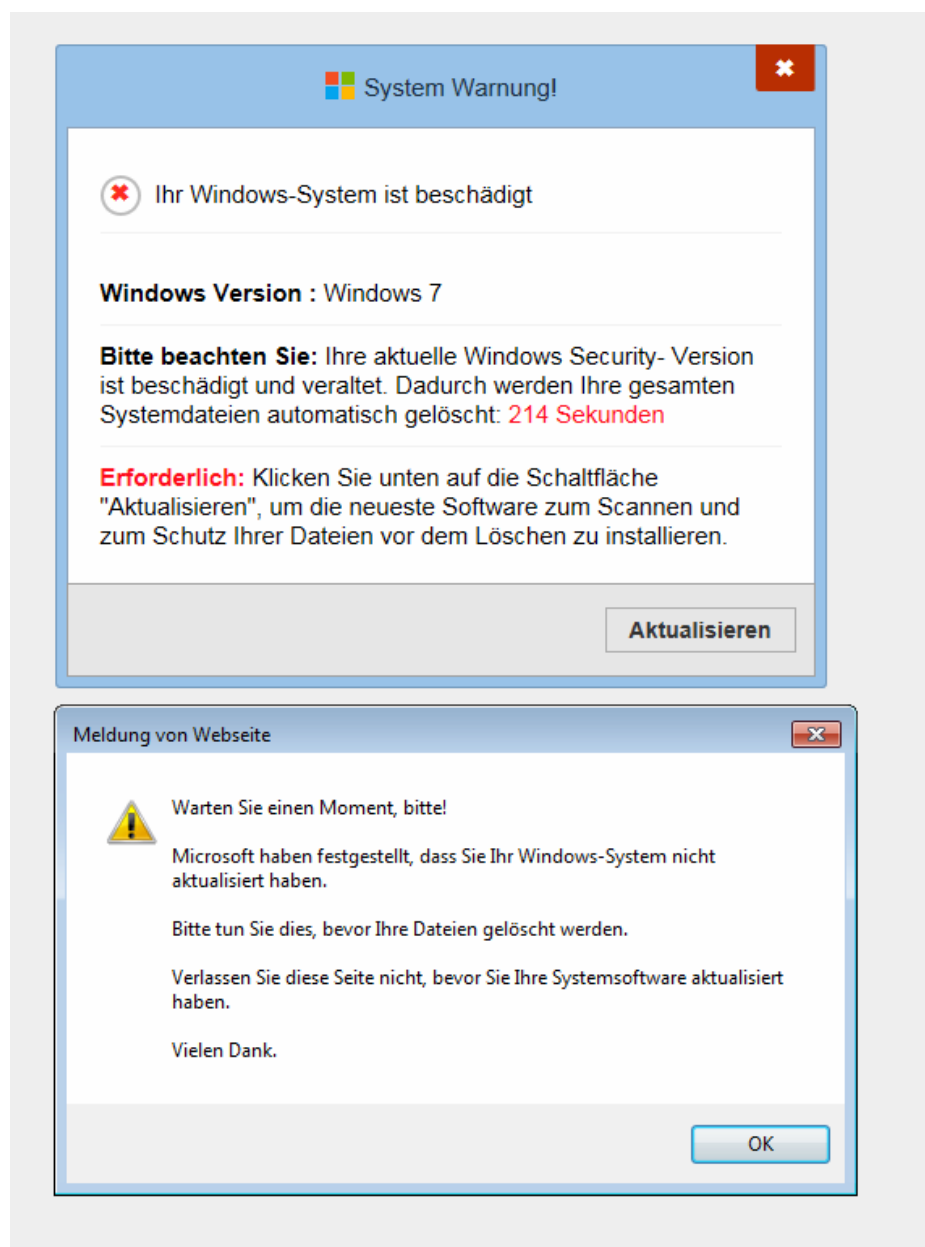




Anleitung im Browser Angriff mit nervendem Hupendem Computer Beispiel:

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:

Name	Schlüsselwörter	Adresse
Attention Required - [http://windows.windows-gesperrt1.download/firefox/index.php]		http://windows.windows-gesperrt1.download/firefox/index.php
Attention Required		http://windows.windows-gesperrt1.download/
35.184.188.211/NTE1NTEyNTkxMTE5LzUxNTUxNDE2MTM5Mi8wdWovN28zaTc3		http://35.184.188.211/NTE1NTEyNTkxMTE5LzUxNTUxNDE2MTM5Mi8wdWovN28zaTc3
Share-Links.biz - ACQUILAPRO - [http://share-links.biz/_1jolx6pj5mfm]		http://share-links.biz/_1jolx6pj5mfm
Share-Links.biz - ACQUILAPRO - [http://share-links.biz/_1jolx6pj5mfm]		http://share-links.biz/_1jolx6pj5mfm
Relink-to - Star Trek TNG Staffel 5 720p SD - [http://relink.to/view.php?id=12da7d047f769d9e5e68522da5b7]		http://relink.to/view.php?id=12da7d047f769d9e5e68522da5b7
Relink-to - Share links for cash! - [http://relink.to/container_captcha.php?id=12da7d047f769d9e5e68522da5b7]		http://relink.to/container_captcha.php?id=12da7d047f769d9e5e68522da5b7
Container Password - [http://relink.to/container-password/?pw_cid=12da7d047f769d9e5e68522da5b7]		http://relink.to/container-password/?pw_cid=12da7d047f769d9e5e68522da5b7
Star Trek TNG The Next Generation Remastered S01 - S07 COMPLETE German DL AC3 720p Blu-ray x264 - IND - Boerse.A...		http://www.boerse.sh/boerse/videoboerse/serien/1306622-star-trek-tng-next-generation-remastered-s01-s07-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%2F_1jolx6pj5mfm

Diese wiederum

http://share-links.biz/_1jolx6pj5mfm

dann weiter zu

<http://35.184.188.211/NTE1NTEyNTkxMTE5LzUxNTUxNDE2MTM5Mi8wdWovN28zaTc3>

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