

## Re: blaster

**Source:**

<http://www.tech-archive.net/Archive/German/WinXP/microsoft.public.de.german.windowsxp.sonstiges/2004-02/119>

---

**From:** Michael Arm (*SEND.NO.SPAM.TO.arminator\_at\_web.de*)

**Date:** 02/06/04

Date: Fri, 6 Feb 2004 15:40:10 +0100

Norbert Müller wrote:

> *"Michael H. Fischer [MVP]" <usenet07@derfisch.de> schrieb im*  
> *Newsbeitrag news:c005ji\$108mpa\$1@ID-4092.news.uni-berlin.de...*  
>> *Norbert Müller schreibselte am 06 Feb 2004:*  
>>  
>>> *Ich brauchte aber den Virenschanner, um trotz Neuinstallation den*  
>>> *"Windows-Autoritätsmanager" zu eliminieren, der ständig mein*  
>>> *System runtergefahren hat.*  
>>  
>> *Falsch.*  
>  
> *Ob du es glaubst oder nicht:*  
> *So ist es aber!*

Keiner glaubt hier leider mehr an etwas falsches als Du.

Der Windows Autoritätsmanager ist nicht ein Virus. Das ist eine Windows Systemkomponente, die aufpasst, ob mit dem Betriebssystem alles ordnungsgemäß funktioniert. Den hast Du mit Sicherheit nicht eliminiert. Blaster ist etwas schlampig programmiert. Er sucht sich zufällig aus, ob er eine Sicherheitslücke von Win 2000 angreifen will oder ob er eine Lücke in XP angreifen will.

Wenn er ein XP System mit der XP Lücke angreift, merkst Du nichts. Wenn der 2000 Angriff auf Deinen XP Rechner ausgeführt wird, kommt der Autoritätsmanager von Windows und fährt Deinen Rechner runter. Ab diesem Zeitpunkt bist Du aber schon infiziert. Ob Du das glauben magst oder nicht.

>  
>>> *Vielleicht hatte sich der gar über den MS-Download Zutritt*  
>>> *verschafft?*  
>>  
>> *Mit Sicherheit nicht.*  
>  
> *Wollen wir es hoffen! Woher also kam er dann?*

Der Autoritätsmanager ist wie gesagt eine Windows Komponente und ist schon seit der ersten Installation auf Deinem System.

Der Blaster Wurm kommt von anderen Usern wie Dir, die ihre Rechner als "sicher" glauben und keine Lust haben auf Windowsupdate ihr System auf den Neuen Stand zu bringen.

Blaster verbreitet sich über die Netzwerke, nicht wie "normale" Viren über Dateien.

Bildlich betrachtet kannst Du Dir das so Vorstellen:

"normaler" Virus kommt über Diskette oder e-Mail Anhang, den Du auf Platte Speicherst auf Deinen Rechner und wird dort von der Platte oder einem Netzwerklaufwerk ausgeführt.

Wenn Du einen Virenschanner hast, klemmt der sich quasi zwischen Hauptspeicher und Laufwerk und kann den Virus aufhalten.

Der Blaster Virus nutzt eine Lücke im RPC aus. RPC erlaubt es, Programmstücke über das Netzwerk direkt in den Speicher eines Rechners zu schreiben und dort ausführen zu lassen. Ohne daß eine Datei dafür auf einem Laufwerk landet. Deshalb kann Dein Virenschanner auch erst den Blaster finden wenn es schon längst zu spät ist...

>

>>> *Jetzt ist der Backdoor jedenfalls weg und das System funktioniert*

>>> *wieder einwandfrei.*

>>

>> *Das glaubst du jedenfalls.*

>

> *Ich sehe es bloß an den nichtmehrvorhandenen Auswirkungen :-)*

Die nicht mehr vorhandenen Auswirkungen (NT-Autorität fährt Rechner runter) sind Zufall. Du wurdest mit Deinem XP System nur nicht mehr mit der 2000er Variante angegriffen. Oder hast Dein System mittlerweile entsprechend auf Windowsupdate gepatcht.

>

>> *Hast du eigentlich irgendeine der vielen Antworten, die du zu deinem*

>> *ursprünglichen Problem bekommen hast, wirklich gelesen und*

>> *verstanden? Ich bezweifle es so langsam.*

>

> *Hast du eigentlich mein Problem und das vom Anonymus verstanden? Daran*

> *zweifle ich auch – aber nicht langsam... ; -)*

Bitte gewöhne Dir mal an auch mal an Dir selbst zu zweifeln. Vor allem dann, wenn mehrere Leute Dir schon eindeutige Hinweise gegeben haben, daß Du lieber Deinen Standpunkt nochmal überdenken sollst.

Standhaftigkeit ist schon was positives. Aber stur auf seinem Standpunkt zu beharren, obwohl andere Leute die belegbar "richtigeren" Argumente haben ist nicht mehr so positiv...

Daß Du ihm einen kostenlosen Virenschanner empfohlen hast löst aber sein Blaster Problem nicht.

Das wäre genauso als würde sich der Poster beklagen, daß Seine Reifen Platt sind und das Auto nicht mehr so schnell fahren kann. Anstatt ihm zu sagen, er soll die Reifen wieder mit Luft füllen, empfiehlst Du ihm einfach mehr Gas zu geben oder einen stärkeren Motor einzubauen.

Der Virenschanner löst nicht das Hauptproblem des Blaster Befalls...