

## Rootkit is mogelijke aanleiding bsod's in Windows XP

*Na het installeren van Windows-updates van 9 februari werden sommige Windows XP-gebruikers geconfronteerd met een blue screen of death. Inmiddels is duidelijk geworden dat de foutmeldingen mogelijk ontstaan naar aanleiding van een rootkit.*

Computer-expert Patrick W. Barnes ontdekte een overeenkomst in de door hem geanalyseerde systemen die last hadden van de bsod's. Hij vond bij alle drie een geïnfecteerd atapi.sys-bestand. Dit bestand is een systeemdriver voor opslagapparaten. Na het vervangen van de driver voor een schone versie, verdwenen de foutmeldingen en startten de pc's weer normaal op.

De rootkit waar het om gaat, heet onder andere 'Tdss' en is bij Microsoft bekend onder de naam 'Alureon.A'. Deze malware wordt in verband gebracht met zombie-machines en botnets. Het is voor virusscanners moeilijk om infecties in atapi.sys te detecteren, omdat het zo vroeg in het opstartproces geladen wordt. Volgens Barnes waren de systemen voor het updaten al besmet en zorgt de update, in combinatie met het corrupte atapi.sys-bestand, voor de foutmeldingen.

Barnes heeft op zijn site gepost hoe via de recovery-console het corrupte bestand vervangen kan worden. Ook adviseert hij het systeem verder goed te controleren op andere malware, aangezien de infectie slechts een voorbode is van meer problemen. De Tdss-rootkit is mogelijk niet de enige aanleiding voor de bsod's. Wellicht zijn er andere corrupte drivers die in combinatie met de update problemen veroorzaken. Microsoft verricht momenteel onderzoek en heeft update MS10-015 uit voorzorg uit Windows Update gehaald.