Ransomware

Hoe komt cryptoware op een computer?

Bijlagen en links in spam zijn belangrijke aanvalsvectoren. Veel gebruikers downloaden en installeren zelf hun malware. De gebruiker denkt bijvoorbeeld een PDF bestand te openen maar dit blijkt in werkelijkheid het virus te zijn. In de meeste gevallen krijgt de gebruiker een waarschuwing, maar deze wordt door gebruikers vaak weg geklikt.

Het gebeurt ook dat websites, of hun advertentienetwerken, worden gehackt waardoor een betrouwbaar ogende site toch bezoekers besmet met malware. Een computer kan al ook langere tijd onderdeel uitmaken van een botnet. In dat geval is het vrij eenvoudig om de cryptoware te installeren via een backdoor. Goed patch management, actuele antivirussoftware en oplettende gebruikers verkleinen de kans op malware, maar bieden geen garanties.

Een andere, relatief nieuwe, modus operandi is het gebruik van exploitkits. Advertenties of code in gehackte websites verwijzen naar de webpagina van een exploitkit. De exploitkit heeft een webpagina die allerlei pogingen doet om de webbrowser te compromitteren middels de exploitatie van zwakheden. De meest gebruikte zwakheden zitten in Java, Flash en PDF.

Het lijkt er op dat de huidige varianten van cryptoware, na activatie, op het systeem van het slachtoffer op zoek gaan naar documenten, foto's en andere bestanden op schijven voorzien van een schijfletter (inclusief netwerkschijven en virtuele 'cloud'-disks) om deze te versleutelen.

Apple producten zijn niet immuun voor exploitkits, echter, omdat het merendeel van de gebruikers wereldwijd Windows gebruikt worden het merendeel van de exploits en mallware ook voor deze systemen geschreven.

Dit neemt niet weg dat het gebruik van een apple garant staat voor een veilig systeem, ook hier moeten de standaard stappen genomen worden om besmetting te voorkomen.

Unieke FAQ ID: #1429
Auteur: n/a
Laatst bijgewerkt:2020-01-14 10:48

© 2024 SecureOnline <helpdesk@secureonline.nl> | 28-03-2024 23:05

URL: https://faq.secureonline.nl/index.php?action=faq&cat=23&id=429&artlang=nl