'Omvangrijke malware-aanval trof ook geheime diensten'

Het Turla-virus, dat al eerder aan het licht kwam, trof twee geheime diensten in Europa en het Midden-Oosten. Dat blijkt uit onderzoek van Kaspersky. Ook honderden andere overheidsinstellingen zijn getroffen door de malware.

Vorig jaar kwam het bestaan van de malware al aan het licht en in maartmeldde Kaspersky al dat honderden overheidsinstellingen met de malware zijn besmet. Daaronder zijn echter ook twee geheime diensten, zo blijkt nu. Het zou gaan om één geheime dienst in het Midden-Oosten en een in de Europese Unie,meldt persbureau Reuters. Volgens Kaspersky is het de eerste digitale spionagecampagne waarbij geheime diensten zijn geïnfecteerd.

Kaspersky vermoedt dat een overheid achter de aanval zit. De aanval richtte zich op geheime diensten en overheidsinstellingen als ministeries en ambassades, maar ook toeleveranciers van het leger en farmaceutische bedrijven. De grootste aantallen slachtoffers zouden zich bevinden in Frankrijk, het Verenigd Koninkrijk, Rusland, Wit-Rusland, Duitsland, Roemenië en Polen.

Het is onbekend waar de aanval precies vandaan komt. Een rapport van Kaspersky, dat tijdens de Black Hat-beveiligingsconferentie in Las Vegas wordt vrijgegeven, zou suggereren dat de hackers Russisch spraken, maar dat betekent niet per se dat ze uit Rusland komen. Kaspersky wil niet aangeven waar het denkt dat de hackers vandaan komen; Symantec, dat later ook met een rapport over de aanval komt, eveneens niet.

Bij de aanval zouden tools zijn gebruikt die bij twee eerdere aanvallen zijn ingezet, en die volgens Westerse geheime diensten aan Rusland zouden zijn toe te schrijven. Dat onder de slachtoffers ook instellingen uit Rusland waren, is geen tegenargument voor betrokkenheid van Rusland: het kan gaan om diplomatieke posten van andere landen en vestigingen van buitenlandse bedrijven in Rusland.

De malware werd verspreid door websites die waarschijnlijk door slachtoffers zouden worden bezocht, te infecteren. Daaronder waren opvallend genoeg ook overheidswebsites. Na infectie zou de malware proberen in te schatten of het slachtoffer interessant genoeg is, bijvoorbeeld als hij of zij werkzaam is bij een overheidsinstelling. De malware die de aanvallers gebruikten zou specifiek op zoek zijn gegaan naar documenten met termen als 'Navo', 'EU-energiedialoog' en 'Boedapest'.