Regin valt ondernemingen, researchers en overheidsinstellingen aan

1 december 2014

Vorige week was Regin volop in het IT-nieuws. Regin is een vorm van spyware die vooral ingezet wordt om ondernemingen, researchers en overheidsinstellingen te bespioneren. De beveiligingsspecialisten van het Duitse G DATA concluderen na analyse van deze spyware dat die in elk geval sinds maart 2009 wordt gebruikt. G DATA heeft nu, als eerste ter wereld, een script ontwikkeld dat bestanden die door Regin zijn aangemaakt kan identificeren. Het script werkt volledig onafhankelijk van de beveiligingssoftware die op het systeem wordt gebruikt en levert geen conflicten op. Volgens de analisten van G DATA is Regin even gevaarlijk als eerder ontdekten spyware als Uroburos, Stuxnet of Duqu. De beveiligingsoplossingen van G DATA herkennen en blokkeren Regin in zijn geheel.

“Regin is een complex en hooggesofisticeerd stuk spyware dat de aanvaller de mogelijk geeft om volledige toegang tot het netwerk te krijgen en precies te monitoren wat er op dat netwerk staat en gebeurt,” legt Eddy Willems, G DATA’s Security Evangelist uit. “We vermoeden dat deze malware geschreven is door de geheime dienst van een overheid, want de ontwikkeling en implementatie van dergelijk malware kost veel tijd en geld.”

G DATA-script detecteert de spyware
Het G DATA SecurityLab heeft direct een antwoord op Regin geformuleerd door een script te ontwikkelen dat, onafhankelijk van eventueel geïnstalleerde beveiligingssoftware, bestanden kan detecteren die Regin maakt en gebruikt op geïnfecteerde systemen. Het script detecteert virtuele bestandsystemen die door Regin worden aangemaakt en slaat alarm. Voor de executie van het script is versie 2 van het Python-programma vereist: https://www.python.org/. Het script is specifiek ontwikkeld voor IT-managers en experts.

Wat is Regin?
Spyware Regin is ontwikkeld om hoogsensitieve en geheime informatie van high-potential netwerken zoals overheidsinstellingen, intelligentiediensten of grote ondernemingen en om de doelwitten te monitoren. Tot op heden is van 18 landen bekend dat zij door Regin zijn aangevallen, waaronder België, Duitsland, Rusland, Syrië en India.

Meer details over Regin en een link naar het script zijn te vinden in het G DATA SecurityBlog:

https://blog.gdatasoftware.com/blog/article/regin-an-old-but-sophisticated-cyber-espionage-toolkit-platform.html.