HORNETSECURITY OVER DE DOORONTWIKKELING VAN MALWARE

‘Malware is extreem divers geworden’

Bestaande malware is tegenwoordig veel langer dan voorheen in omloop, meldt Hornetsecurity, specialist in het beveiligen van e-mail. Wel blijven cybercriminelen bestaande schadelijke programma’s doorontwikkelen. *Tekst: Mels Dees*

Naast de problemen die bedrijven en gebruikers ondervinden als gevolg van malware en andere cybercriminaliteit, was er begin dit jaar ook goed nieuws. Internationaal samenwerkende opsporingsdiensten slaagden erin de servers waarop de schadelijke malware Emotet draaide uit de lucht te halen.

“De ontwikkeling die Emotet doormaakte illustreert hoe een schadelijk programma steeds weer wordt aangepast zodat securitymaatregelen worden omzeild”, stelt Dr. Yvonne Bernard, Head of Product Management bij de Duitse security-specialist Hornetsecurity. “We moeten niet vergeten dat Emotet al sinds 2014 actief was. Aanvankelijk kon het programma zich nog niet actief verspreiden – later wel. In 2018 kon deze malware bij geïnfecteerde computers het adresboek scannen en de adressen gebruiken.”

> **‘Nu we massaal thuiswerken slaan criminelen hun slag’**

Ook het mailbericht waarmee het schadelijke programma als bijlage werd verzonden veranderde steeds. “Dat zien we bij alle malware, er wordt continu ingespeeld op de actualiteit. Zo zagen we rond de Black Lives Matter-demonstraties berichten die daarop inspeelden, en sinds de coronacrisis ook mails die eruitzien alsof ze van het RIVM of de WHO afkomstig zijn, of waarin mond-neusmaskers tegen een actieprijs worden aangeboden.”

Yvonne Bernard

Twee fases

Het weren van attachments houdt criminelen niet tegen, maakt Bernard duidelijk: “Dan worden URL’s in de body van de mail aangeboden en is sprake van een campagne in twee fases. De scansoftware ziet bij ontvangst geen schadelijke URL maar enige uren na het verzenden wordt een schadelijke component in de URL alsnog geactiveerd.” Om dan alsnog problemen te voorkomen scant de software van Hornetsecurity de URL (ook nog) op het moment dat de gebruiker erop klikt.

Intelligente fraude

Het ‘intelligenter’ maken van de boodschap die gebruikers moet verleiden speelt ook nadrukkelijk bij CEO-fraude. “Zeker nu er massaal thuis wordt gewerkt en er minder gelegenheid is met collega’s te overleggen, slaan cybercriminelen hun slag”, is de observatie bij Hornetsecurity. “Ook hier wordt de social engineering geavanceerder. Zo zien we dat API’s van social media-platforms gebruikt worden om aan specifieke informatie te komen. LinkedIn geeft aan wat iemands functie is en wat er speelt in een onderneming, op Facebook kan automatisch gecheckt worden of iemand van een vakantie geniet. Zo wordt een mailtje waarin de baas zogenaamd opdracht geeft een betaling te doen heel overtuigend.” ■