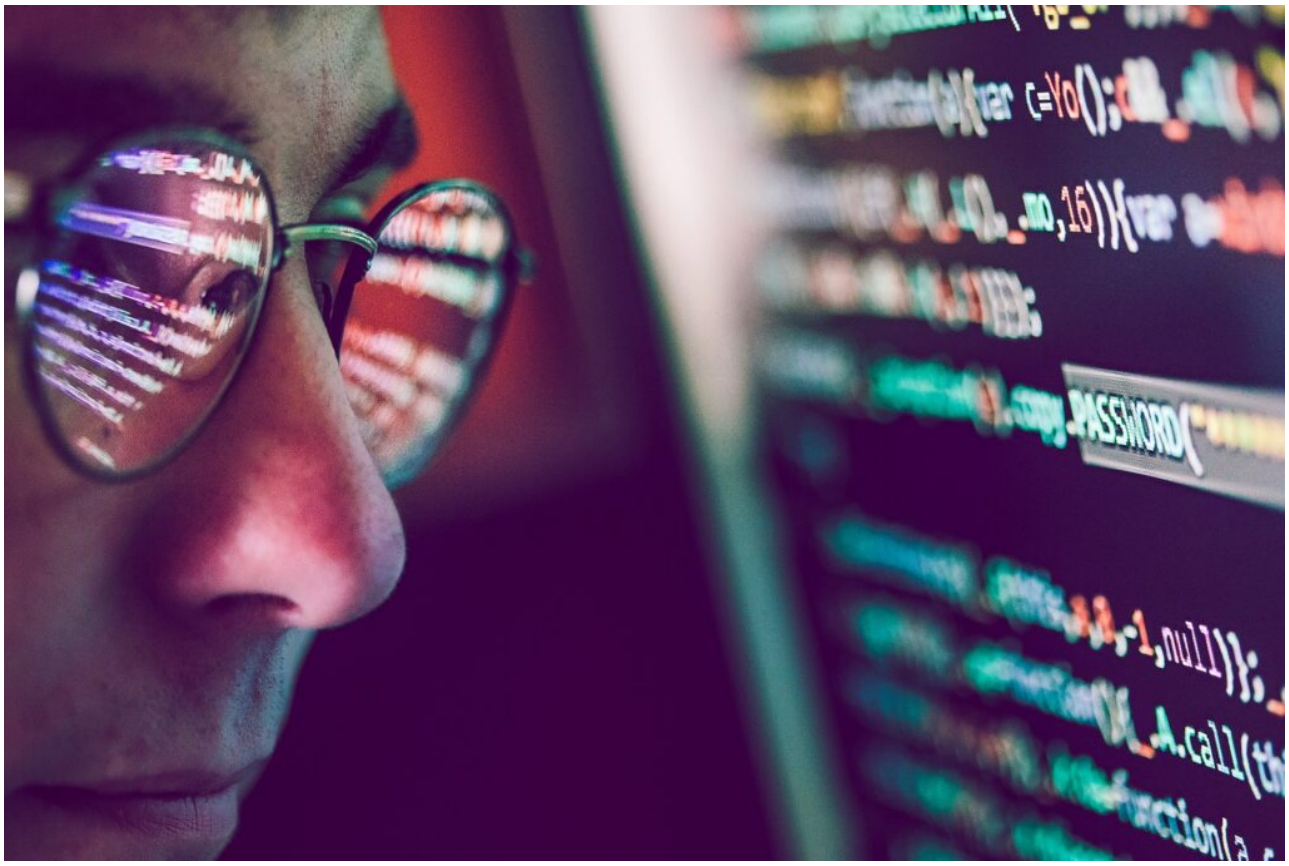
‘Zorgsector belangrijk doelwit massale cyberaanvallen’

17 mei 2019



Emotet is een breed toepasbare soort malware die is voortgekomen uit een bekend Trojaans paard, genaamd Cridex. Dit Trojaanse paard was gericht op financiële instellingen en werd voor het eerst ontdekt in 2014. Oorspronkelijk gericht op West-Europese banken, is het uitgegroeid tot een robuust botnet dat bestaat uit verschillende modules. Deze rusten Emotet uit met verschillende mogelijkheden voor spamming, e-mail logging, informatiediefstal, bankfraude, downloaden en DDoS.

Grootschalige malware-campagnes

Volgens Chris Dawson, lid van het Proofpoint Threat Insight Team, is een groot deel van deze aanvallen te wijten aan een cybercrimineel die bekend staat als TA542. Sinds begin 2019 lanceerde een persoon of groep met deze naam grootschalige campagnes die tientallen miljoenen berichten verspreidden. Die zijn voornamelijk gericht op productiebedrijven en gezondheidszorg-instellingen, aldus Proofpoint.

Vanaf midden januari 2019 verspreidde TA542 miljoenen e-mails met de Emotet-malware, zowel in het Engels als het Duits. Onderzoekers van Proofpoint konden bevestigen dat bedrijven in België en Nederland interessant gevonden worden door TA542 en dat ook Nederlandse zorginstellingen getroffen zijn.

Zorg meest getroffen branche

“Emotet is een wereldwijde bedreiging met honderdduizenden tot miljoenen van kwaadaardige berichten per dag”, legt Dawson aan ICT&health uit. “In het algemeen zijn Emotet campagnes heel breed en eerder gericht op bepaalde regio’s dan op bepaalde branches, hoewel wij zien dat de gezondheidszorg tot de meest getroffen branches hoort in de campagnes die wij zien.”

Emotet is een robust botnet dat in staat is om een extra malware te downloaden, zich over meerdere netwerken verspreidt en geïnfecteerde apparaten gebruikt om nieuwe aanvallen te lanceren. Voor zorginstellingen betekent dit volgens Dawson een groeiend aantal potentieel gecompromitteerde apparaten dat cybercriminelen toegang geeft tot een gevoelige patiëntinformatie, intellectuele eigendom, onderzoek, financiële rekeningen, netwerkgegevens en meer.”

Zorggegevens aantrekkelijk

De gezondheidszorg is om verschillende redenen een bijzonder aantrekkelijk doelwit voor bijvoorbeeld phishing-aanvallen van cybercriminelen, vervolgt Dawson. Zo zijn de gegevens uit de gezondheidszorg op de zwarte markt veel waardevoller dan bijvoorbeeld creditcards. Het rijke karakter van de gegevens ondersteunt bijvoorbeeld identiteitsdiefstal en fraude die voor een langere tijd onopgemerkt kan blijven.

“Een inbraak in een enkel ziekenhuis kan vele duizenden patiëntendossiers opleveren. Een inbreuk bij een farmaceutisch bedrijf kan daarentegen alles opleveren, van financiële fraude op grote schaal tot intellectuele eigendom. Voor TA542 betekent de flexibiliteit van Emotet dat de groep secundaire aanvallen kan plegen op besmette organisaties, of het nu gaat om een kliniek voor spoedeisende hulp, een verzekeringsmaatschappij of een onderzoeks-ziekenhuis van een grote universiteit.”

Dankbaar onderwerp cyberaanvallen

De zorgsector is al langere tijd een dankbaar onderwerp van cyber-aanvallen. Zo noemde Verizon vorig jaar de zorg meer dan elke andere sector gevoelig voor datalekken en andere digitale dreigingen. In 2017 werd onder meer een deel van de Britse zorgsector lamgelegd door malware-aanvallen, met verstrekkende gevolgen zoals uitstel van operaties.