**Drie mannen aangehouden in onderzoek naar grootschalige internationale datadiefstal en datahandel**

Laatst gewijzigd op: 23-02-2023 | 16:55

Amsterdam - Het cybercrimeteam van de politie Amsterdam heeft op maandag 23 januari drie mannen aangehouden in een omvangrijk onderzoek naar computervredebreuk, datadiefstal, afpersing, afdreiging en witwassen.



De verdachten zijn een 21-jarige man uit Zandvoort (hoofdverdachte), een 21-jarige man uit Rotterdam en een 18-jarige man zonder vaste woon- en verblijfplaats. Twee van de verdachten zijn na hun aanhouding direct in alle beperkingen gegaan, wat betekent dat zij alleen contact mochten hebben met hun advocaat. Vanwege deze maatregel en om het onderzoek niet te verstoren, zijn de aanhoudingen niet eerder bekendgemaakt.

**Duizenden bedrijven slachtoffer**

Het cybercrimeteam is het onderzoek gestart in maart 2021 naar aanleiding van een aangifte van datadiefstal en afdreiging bij een groot Nederlands bedrijf. Gaandeweg het onderzoek is duidelijk geworden dat vermoedelijk duizenden kleine en grote bedrijven én instellingen, zowel nationaal als internationaal, de afgelopen jaren slachtoffer zijn geworden van computervredebreuk (hacken) en vervolgens diefstal en heling van data. Tientallen miljoenen privacygevoelige persoonsgegevens zijn als gevolg van deze diefstal en handel in handen van criminelen gekomen.

**Geraffineerd**

Het onderzoek van de recherche geeft zicht op een zeer geraffineerde werkwijze. Nadat illegaal toegang is verkregen tot de data op de systemen van de getroffen bedrijven, krijgen deze bedrijven een dreigend bericht per email met de mededeling dat ze moeten betalen in bitcoins. Betaalt een bedrijf niet, dan wordt gedreigd de digitale infrastructuur van het bedrijf te vernielen of de gegevens openbaar te maken. Veel bedrijven hebben zich gedwongen gevoeld om te betalen in de hoop hun data te beschermen. De totaalschade voor bedrijven loopt in de vele miljoenen. Voor tot dusver bekend, is het geëiste losgeld per bedrijf daarbij opgelopen tot meer dan 100.000 euro een uitschieter naar meer dan 700.000 euro. Bovendien is in veel gevallen de gestolen data alsnog online verkocht, ook al hebben de getroffen bedrijven betaald. De hoofdverdachte heeft vermoedelijk in de afgelopen jaren een crimineel inkomen gehad van 2,5 miljoen euro.

**Privacygevoelige gegevens**

Als gevolg van deze werkwijze zijn tientallen miljoenen privacygevoelige gegevens van mensen in handen van criminelen gekomen. Het gaat daarbij niet alleen om namen, adressen en telefoonnummers. Denk daarbij ook aan geboortedata, bankrekeningnummers, creditcards, wachtwoorden, kentekens, BSN-nummers of paspoortgegevens. Allemaal zeer privacygevoelige informatie. Informatie die goud waard is voor criminelen. Zoals eerder ook al is gezien in het onderzoek naar een 25-jarige verdachte uit Almere die wordt verdacht van diefstal en handel van persoonsgegevens van de Geburen Info Service GmbH (GIS) dat kijk- en luistergelden voor Oostenrijk int. Daarbij zijn vermoedelijk de gegevens van alle inwoners van Oostenrijk buit gemaakt en te koop aangeboden.

**Impact**

De impact voor de getroffen bedrijven is enorm. Het gaat daarbij niet alleen om financiële schade, maar ook om imagoschade en alle extra inspanningen om systemen weer te herstellen. Ook bedrijven die hun beveiliging goed op orde hebben, kunnen door dit soort feiten worden getroffen. Daarbovenop komen nog de gevolgen voor de mensen bij deze bedrijven op persoonlijk vlak. Zij voelen zich verantwoordelijk voor iets wat vaak buiten hun schuld om is gebeurd. Zo heeft een medewerker van een getroffen bedrijf aan de politie uitgelegd hoe hij voortdurend angst heeft dat de buitgemaakte data alsnog wordt verhandeld en bang is voor persoonlijke bedreiging als gevolg van praten met de politie.

**Samenwerking**

Het cybercrimeteam heeft in het onderzoek hulp gehad van andere politie-eenheden en diverse internationale opsporingsdiensten. Het gaat dan ook niet alleen om bedrijven in Nederland die het slachtoffer zijn geworden van datadiefstal- en handel, maar ook internationale bedrijven zijn gedupeerd. De bedrijven en andere instanties die vermoedelijk slachtoffer zijn geworden, zijn heel divers en komen voor in nagenoeg alle denkbare branches; van horeca, opleidingsinstituten, webshops tot aan softwarebedrijven, sociale media en instellingen die behoren tot de vitale infrastructuur.

**Dataraffinage**

Datadiefstal en datahandel is een enorm verdienmodel voor criminelen. Niet alleen door het afpersen van bedrijven. De buitgemaakte data wordt bewerkt om weer verhandeld te kunnen worden aan andere criminelen. Uit het onderzoek blijkt dat gebruikt wordt gemaakt van een speciale computercode om gestolen data te raffineren. Gestolen databases worden door dergelijke dataraffinage speciaal geschikt gemaakt om specifiek uitgekozen slachtoffers te benaderen voor bijvoorbeeld phishing, babbeltrucs, bankhelpdeskfraude of identiteitsfraude. Zo kan in een database bijvoorbeeld gefilterd worden op Nederlanders, geboren in de jaren 40 en 50.
De informatie die criminelen uit dit soort databases over hun slachtoffers kunnen vergaren, stelt ze in staat betrouwbaar over te komen. Het aantal slachtoffers als gevolg hiervan is enorm. Tot slot worden zoekslagen in gestolen data ook aangeboden om zaken of personen op individueel niveau heel gericht te kunnen vinden. Op straat zoeken en observeren is niet meer nodig. Een druk op de knop achter de computer is voldoende.

**Aanpak cybercrime**

Gezien de grote impact op zowel bedrijven en personen, zetten de politie en het Openbaar Ministerie nadrukkelijk in op het bestrijden van cybercrime. Niet alleen door cybercriminelen op te sporen zoals in dit onderzoek, maar ook door middel van preventie. De preventie richt zich zowel op slachtoffers als daders. Daarnaast zet de politie in op het verstoren van processen van criminelen. Een voorbeeld hiervan is het initiatief onder de naam No More Leaks. No More leaks is een samenwerking tussen politie en bedrijven waarbij politie gelekte inloggegevens gehashed verstrekt aan bedrijven met veel online accounthouders. Bedrijven kunnen deze lijst met hashes dan als controlelijst meenemen in hun inlogproces, zodat misbruik op voorhand wordt voorkomen.

**Contact politie**

Heeft u informatie die van belang kan zijn in het vervolg van dit onderzoek, of wilt u aangifte doen of melding maken van een cybercrime delict, neem dan contact op met politie via 0900-8844 of 088-9647360 (team criminele inlichtingen cybercrime). Of kijk voor meer informatie over cybercrime op <https://www.politie.nl/onderwerpen/cybercrime.html>.