Wereldwijd aanhoudingen voor online identiteitsdiefstal miljoenen mensen

De FBI en Europol hebben samen met de Nederlandse politie een groot internationaal onderzoek gedaan naar de Genesis Market. Deze criminele handelswebsite is op 4 april 2023 met 'operation Cookiemonster' door de FBI offline gehaald. Op de site werden miljoenen gebruikersprofielen met daarin online fingerprints verkocht. Hiermee kunnen hackers het digitale leven van hun slachtoffers overnemen. Wereldwijd zijn in 17 landen honderden doorzoekingen gedaan. In Nederland zijn 17 aanhoudingen verricht en 23 doorzoekingen gedaan.

‘Dat op allerlei online handelsplaatsen inloggegevens worden verhandeld, is op zich bij de meeste mensen wel bekend’, zegt Ruben van Well, teamleider van het Rotterdamse cybercrimeteam. ‘Maar de criminele handelssite Genesis Market, die nu door de FBI is opgedoekt, was één van de gevaarlijkste. Deze site verkocht niet alleen accountgegevens, maar daarbij ook een kopie van iemands online fingerprint, ofwel unieke digitale vingerafdruk. Daarmee kunnen hackers iemands digitale leven overnemen. Zo was het mogelijk om op naam van slachtoffers zaken te bestellen en te betalen in webwinkels of in bepaalde gevallen zelfs volledige bank-, crypto-, of beleggingsrekeningen te plunderen.’

Besmet

´We hebben eerder met de Nederlandse politie aan veel zaken samengewerkt en de kennis en ondersteuning van Nederland was ook ditmaal van groot belang´, zegt juridisch attaché Andrew Ne van de FBI in Den Haag.
Na het eerste contact met de FBI over Genesis Market zagen de Nederlandse cybercrimerechercherchercheurs al vrij snel dat zich ook in ons land zowel slachtoffers als verdachten bevonden.
Genesis Market was volgens Europol wereldwijd een van de grootste facilitatoren voor cybercriminelen. Uitgebreid onderzoek naar de nu opgerolde handelswebsite wees uit dat het aantal verhandelde gebruikersaccounts wereldwijd tenminste 1,5 miljoen informatiepakketjes omvat en dat er vermoedelijk meer dan twee miljoen slachtoffers besmet zijn, waaronder zo’n 50.000 Nederlanders.

Slachtoffers

´Een aantal daarvan is ook daadwerkelijk slachtoffer geworden van oplichting’, zegt Van Well. ‘Er zijn gevallen waarin een social-media-profiel werd gestolen of pakketjes op iemands account bij een webwinkel werden besteld. Maar we hebben ook slachtoffers waarbij hele beleggingsportefeuilles zijn geleegd of complete bankrekeningen en cryptowallets zijn geplunderd. Kort gezegd: je raakt de controle over je hele online leven kwijt.’
Als voorbeeld noemt Van Well een 71-jarig slachtoffer uit Almere. ‘Deze man deed meerdere keren aangifte bij de politie van totaal verschillende feiten. ‘Er werden allerlei spullen op zijn naam besteld in webwinkels. Er verdween bijna 70.000 euro van zijn beleggingsrekening. Ook werden op zijn naam bankrekeningen geopend bij meerdere banken. Je kunt je voorstellen dat zoiets ongelofelijk veel impact heeft. Dit slachtoffer vertelde tegen ons dat hij het gevoel had alsof hij in een groot zwembad alleen lag te trappelen en geen idee had hoe hij eruit moest komen.’

Oplossing

‘Normaal gesproken raden we mensen in dit soort zaken aan om meteen al hun wachtwoorden te vervangen. Maar deze malware zit zo in elkaar dat dit alleen niet helpt’, vertelt Van Well. ‘De crimineel die jouw gegevens heeft aangekocht, krijgt dan gewoon een update van jouw nieuwe wachtwoord.’
De politie en de cybersecuritysector hebben elkaar hard nodig om digitaal Nederland zo veilig mogelijk te maken en houden. Daarom werkt de politie intensief samen met publieke en private partijen. Vanuit het netwerk van Team High Tech Crime (THTC) zijn anti-virusbedrijven Trellix en Computest bij dit onderzoek aangesloten.
‘Samen hebben we ervoor gezorgd dat deze malware door iedere virusscanner kan worden gedetecteerd’, legt Van Well uit. ‘Door ook samen te werken met Microsoft is daarnaast een software-update gemaakt, zodat Windows Defender de kwaadaardige software van de computer kan verwijderen. Zorg dus dat je tijdig je computer update. Om te voorkomen dat iemand opnieuw wordt opgelicht is het belangrijk om daarna alle wachtwoorden te wijzigen.’

Ben ik besmet?

Deze malware kan op meerdere manieren op je computer zijn gekomen, bijvoorbeeld nadat je iets hebt gedownload waar het virus in zat. Ook zijn er valse websites in omloop waar cybercriminelen je naar toe lokken om op het eerste oog legale software te downloaden. Het is mogelijk om te controleren of jouw gegevens op de Genesis Market zijn aangeboden. Word geen slachtoffer en doe vandaag nog de check op

www.politie.nl/checkjehack. Als jouw e-mailadres is aangeboden op de Genesis Market, dan krijg je binnen enkele minuten een mail van de politie op het ingevoerde e-mailadres. Deze e-mail krijg je alleen als je bent besmet. Kijk vervolgens zowel in je inbox als spambox of je de mail van de politie hebt ontvangen. In de e-mail staat uitleg wat je moet doen. Van Well benadrukt: “Het is echt belangrijk dat iedereen de controle doet. De aankomende tijd zullen we ook met video’s op social media iedereen oproepen: Check Je Hack.´

Meer aanhoudingen

De Genesis Market profileerde zich onder criminelen als een betrouwbaar platform. Van Well: ‘Dit bleek niet zo te zijn, de markt hield zich niet aan hun eigen opgestelde voorwaarden en was meermaals slecht bereikbaar. Gebruikers waanden zich onterecht anoniem op het platform. Op het internet laat je altijd sporen achter, ook als je gebruik maakt van een VPN.’

De politie spreekt gebruikers van het platform aan en waarschuwt ze met zowel online als persoonlijke confrontaties. Van Well benadrukt dat de Nederlandse politie en de FBI een schat aan informatie hebben over de kopers van de markt. In Nederland is een deel van hen al aangehouden, daarbij zijn meerdere gegevensdragers in beslag genomen, ook werd bij een van de verdachten een automatisch wapen en verdovende middelen aangetroffen.

Van Well: 'Personen die de markt gebruikt hebben om mensen op te lichten zullen worden aangehouden. We hebben de kopers gewaarschuwd die nog niet daadwerkelijk mensen hebben opgelicht. Ze moeten niet denken dat wij ze vergeten. Het onderzoek is in volle gang.’

Meer informatie

Ga voor meer informatie en tips naar de themapagina ‘Online fingerprint fraude’ op onze website politie.nl.

Involved countries and partners

United States

EuroJust
Europe

Europol
Europe

The Netherlands

Canada

Australia

United Kingdom

Germany

Denmark

Poland

Sweden

Spain

France

Italy

Romania

Switzerland

Estonia

New Zealand

Finland

Partners

Trellix
The Netherlands

Computest
The Netherlands

Microsoft
USA