Tekst Jolein de Rooij

Uitsmijter

Hoe een illegale marktplaats (niet) werd opgerold

Eind maart haalde de FBI de illegale marktplaats Genesis Market offline. Over het hoe en waarom spraken we met Michele Campobasso, cybercrime-onderzoeker van de TU Eindhoven.

Tijdens Operatie Cookie Monster rolde de FBI samen met enkele internationale partners, waaronder de Nederlandse politie, de illegale marktplaats Genesis op. Alleen al in Nederland werden zeventien verdachten gearresteerd. Betekent dat nu echt het einde van Genesis?

We namen contact op met cybercrime-onderzoeker aan de TU Eindhoven, de Italiaan Michele Campobasso, die samen met landgenoot en collega Luca Allodi jarenlang undercover-onderzoek deed naar de Genesis-marktplaats.

Wie: Michele Campobasso
Waar: Eindhoven
Wat: cybercrime-marktplaats Genesis
Waarom: waarschuwen

Handel in online fingerprints

Campobasso en Allodi bezochten Genesis sinds 2018 dagelijks. Door vanaf een verzameling accounts steeds opnieuw het aanbod in kaart te brengen, kregen ze een goed beeld van de handel op deze illegale marktplaats. Er werden niet alleen gestolen inloggegevens, maar ook online 'fingerprints' van computergebruikers verhandeld. Die fingerprints gaven criminelen de mogelijkheid om met gestolen wachtwoorden in te loggen zonder dat controlesystemen alarm sloegen.

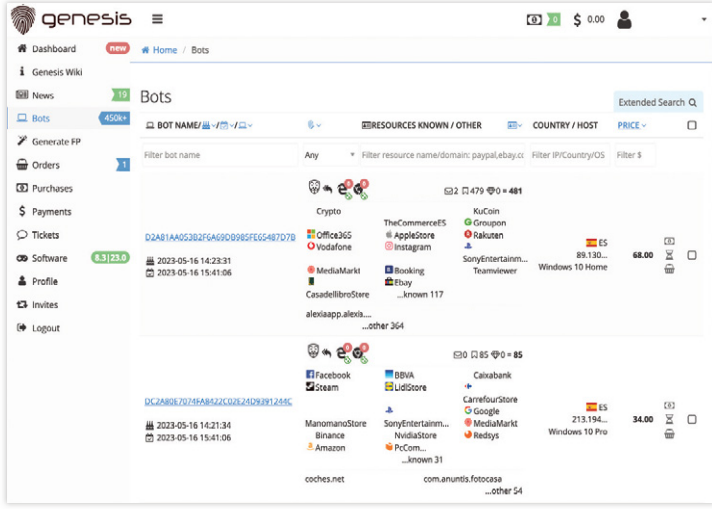
Aanbieders zoals Google, Netflix en Meta controleren de identiteit van gebruikers namelijk niet alleen op basis van hun wachtwoord, maar kijken ook naar de locatie en tijdstippen waarop iemand inlogt en de technische specificaties van iemands systeem. Wanneer ze een verdachte inlog zien, ondernemen ze actie. Ze zenden bijvoorbeeld waarschuwingsmailtjes en -sms'jes, of sluiten een account uit voorzorg zelfs tijdelijk af. Die beveiligingstechniek heet risico-gebaseerde authenticatie (RBA).

Browser plug-in

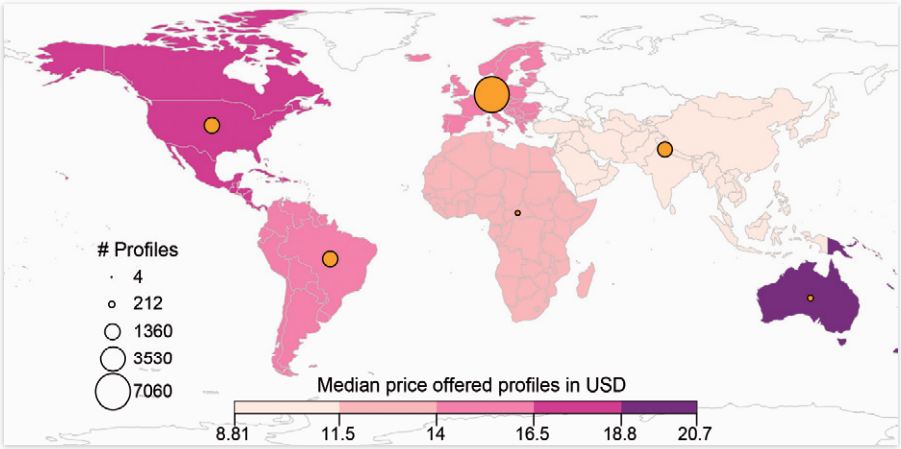
RBA is een enorme hinderpaal voor cybercriminelen bij het verzilveren van gestolen inloggegevens. Genesis bood deze criminelen echter een oplossing. Zodra die een of meer gebruikersprofielen kochten, ontvingen ze een malware-plug-in voor hun browser. Daarmee konden ze de fingerprints van de aangekochte gebruikersprofielen in hun browser 'laden'. Die nam dan alle eigenschappen over van de browser van het slachtoffer, zoals bladwijzers, zoekgeschiedenis en cookies. Vervolgens konden de criminelen zonder dat er een alarmbelletje afging, met gestolen wachtwoorden inloggen binnen allerlei diensten en daar gerichte aanvallen doen.

Is Genesis uit de lucht?

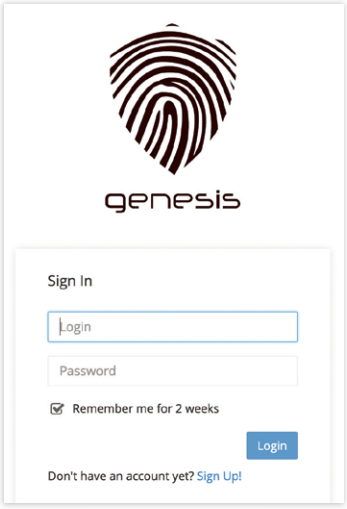
"De FBI heeft alle openbare websites van Genesis uit de lucht gehaald. Ook zijn overal ter wereld mensen opgepakt die gebruikersprofielen hadden gekocht en misbruikt. Toch is de markt zelf na ruim een maand weer volledig in bedrijf genomen. Dat wijst erop dat de



De eigenaren van Genesis beloofden hun klanten dat ze gebruikersprofielen (afkomstig van met spyware geïnfecteerde gebruikerssystemen) slechts één keer verkochten. Prijzen van profielen varieerden van twee dollar tot honderden dollars.



Uit het onderzoek van Campobasso en Allodi bleek dat gebruikersprofielen uit Australië en Noord-Amerika voor de hoogste prijzen werden aangeboden.



De beheerders van Genesis zorgden voor een gebruiksvriendelijke marktplaats.

beheerders niet opgepakt zijn. De kans is groot dat ze zich in Rusland bevinden, en dat land is sowieso niet bereid criminelen uit te leveren aan het westen.

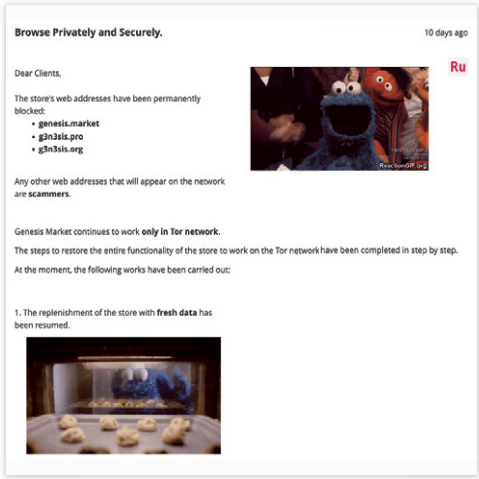
Dat hun websites uit de lucht werden gehaald, was voor de beheerders geen onoverkomelijk probleem. Om de identiteit van kopers en verkopers te beschermen, is Genesis namelijk bereikbaar via het Tor-netwerk. Klanten bezoeken Genesis met 'onion-links'. Dat zijn heel lange links, die eindigen op .onion. Je surft ermee naar servers waarvan de locatie onbekend blijft, doordat datapakketjes slim worden doorgesluisd van onion-router naar onion-router."

Is alles dus voor niets geweest?

"De FBI heeft wel degelijk iets bereikt. Zelfs voordat Operatie Cookie Monster plaatsvond, heeft de FBI de handel op de marktplaats al twee keer verstoord: een keer in december 2020 en een keer in mei 2022. Beide keren heeft de FBI waarschijnlijk de server van de marktplaats in beslag kunnen nemen. Daardoor kregen ze een databank in handen met alle transactie- en contactgegevens van de afgelopen jaren. In mei 2022 ging dat om 59.000 klanten en 200.000 verhandelde gebruikersprofielen, met een totale waarde van acht miljoen dollar, zo valt te lezen in het FBI-rapport over Operatie Cookie Monster. Die databanken hielpen de FBI om slachtoffers te benaderen. Ook konden ze achterhalen of er mogelijk overheidsorganisaties kwetsbaar waren geworden. Daarnaast hebben ze grote klanten van Genesis kunnen identificeren en kunnen arresteren. Operatie Cookie Monster zorgde er bovendien voor dat de malware-extensie tijdelijk niet bruikbaar was. Die haalde namelijk fingerprints op bij de opgerolde websites. Vanaf eind maart konden criminele gebruikers daardoor ruim een maand geen fingerprints in hun browser laden."

Dat klinkt als een tijdelijk effect?

"Klopt, maar zelfs nu de marktplaats weer in gebruik is, blijkt dat de FBI een belangrijke boodschap heeft gegeven aan alle criminele klanten die gebruikersprofielen willen kopen op Genesis: ze lopen het gevaar om gearresteerd te worden. Daarom is de handel op dit moment ingezakt. Klanten zijn blijkbaar huiverig om zaken te doen op Genesis. Ook de Genesis-beheerders worden gemeden. Ze zijn van minstens één online forum afgegooid, waar ze reclame probeerden te maken voor Genesis. Toch is de kans klein dat Genesis voor altijd opgerold is. Daarvoor is deze marktplaats simpelweg te lucratief voor criminelen."



Ruim een maand na Operatie Cookie Monster berichtten de beheerders van Genesis op hun nieuwspagina dat hun marktplaats weer in de lucht was. Campobasso: "Ze konden hun activiteiten voortzetten via het Tor-netwerk." Bij het bericht plaatsten ze afbeeldingen van 'Cookie Monster', een duidelijke verwijzing naar de gelijknamige FBI-operatie."

Hadden jullie contact met de FBI?

"Ruim twee jaar geleden zijn we benaderd door cyberrechercheurs van de Nederlandse politie. Ze waren heel nieuwsgierig naar ons wetenschappelijke onderzoek. Maar in hoeverre ons werk heeft bijgedragen aan het oprollen van Genesis weten we niet. Het is alweer even geleden, en bovendien waren er veel meer partijen bij Operatie Cookie Monster betrokken dan alleen de Nederlandse recherche."

Waar ga je nu onderzoek naar doen?

"Genesis was erg succesvol. Dat is bijzonder, want er zijn ook ontelbaar veel marktplaatsen die nooit van de grond komen. Ik wil uitvinden hoe je in een vroeg stadium marktplaatsen kunt identificeren die populair gaan worden bij criminelen. Als je dat kunt voorspellen, zie je grootschalige fraude eerder aankomen en kunnen het bedrijfsleven en de overheid bijtijds tegenmaatregelen nemen."

Checkjehack.nl

Ook de gegevens van ruim vijftigduizend Nederlanders waren op Genesis te vinden, aldus de FBI. Wil je weten of ook jouw gegevens gestolen zijn? Ga dan naar Check je hack via www.kwikr.nl/checkhack.

Oproep

Doe je iets bijzonders met jouw computer? Of heb je een handige softwareoplossing voor je hobby bedacht? Stuur dan een e-mail met als onderwerp 'Rubriek Uitsmijter' naar redactie@computeridee.nl
Wie weet kom je ermee in Computer Idee.

Sites

- www.kwikr.nl/campo
- www.twitter.com/alpha_centauri3
- www.kwikr.nl/checkhack