Tekst Jolein de Rooij

Uitsmijter

Illegale handel in online 'fingerprints'

Onderzoekers Michele Campobasso en Luca Allodi van de TU Eindhoven (TU/e) ontdekten een nieuwe vorm van cybercrime: het verhandelen van online 'fingerprints' van computergebruikers. Inbrekers kunnen met gestolen wachtwoorden inloggen zonder dat controlesystemen alarm slaan.

Foto TU/e

Wie: Michele Campobasso
Waar: Eindhoven
Wat: nieuwe vorm van cybercrime
Waarom: waarschuwen

Krijgt u weleens een waarschuwingsmailtje van iets als Google of LinkedIn, over een verdachte inlogpoging? Online aanbieders proberen zo te voorkomen dat iemand anders misbruik maakt van uw inloggegevens. Iedere keer dat u zo'n waarschuwing krijgt, hebben ze iets geks gezien. U logt bijvoorbeeld in vanuit een ander land of vanaf een ander besturingssysteem dan normaal.

Dat valt deze dienstverleners onmiddellijk op, omdat ze met speciale beveiligingssystemen allerlei 'metadata' over u verzamelen die samen een behoorlijk unieke 'vingerafdruk' opleveren. Daarbij gaat het niet alleen om uw besturingssysteem en locatie, maar bijvoorbeeld ook om cookies op uw systeem en de lettertypes die u hebt geïnstalleerd. Ook zijn er bedrijven die een profiel opbouwen van de snelheid en het ritme waarmee u typt of de karakteristieke manier waarop u uw muis gebruikt.

Risicogebaseerde authenticatie

Deze aanbieders maken gebruik van risicogebaseerde authenticatie (RBA): iedere keer dat een gebruiker iets doet, of dat nu een inlog is of een online betaling, bekijkt een RBA-systeem op de achtergrond hoe groot het risico is dat achter deze actie een identiteitsdief schuilgaat.

Als een klant plotseling ongebruikelijk gedrag vertoont – vanuit een ander land actief is of grote bedragen naar ongebruikelijke rekeningen overmaakt – gaat er een alarm af. Vervolgens vraagt het systeem om extra bevestiging van iemands identiteit. Dat kan door een beveiligingsmelding naar het mailadres te verzenden met de vraag of de rechtmatige abonnementhouder inderdaad verantwoordelijk is voor bepaalde recente activiteit. Het kan ook door via e-mail of sms een code te versturen, waarmee iemand vervolgens kan aantonen dat hij het echt zelf is. Als het systeem zeer verontrustend gedrag ziet, kan de online aanbieder zelfs uit voorzorg het hele account tijdelijk blokkeren, totdat er meer zekerheid is over de identiteit van de gebruiker.

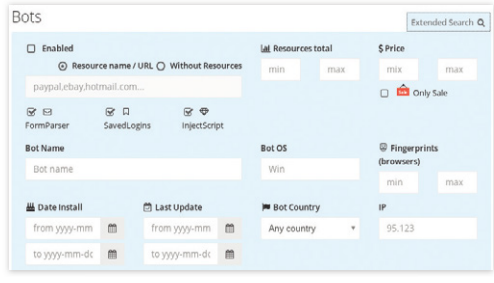
Illegale online markt

RBA is een grote hindernis voor cybercriminelen bij het verzilveren van gestolen inloggegevens. Zulke data zijn al jaren in bulkhoeveelheden te koop op online illegale markten, maar daar heb je niets aan als het RBA-systeem alarm slaat.

Cybercriminelen hebben inmiddels een geavanceerde methode ontwikkeld om die beveiliging te omzeilen, zo ontdekten twee onderzoekers van de TU/e na maandenlang, geheim onderzoek. Ze bestudeerden daarbij in detail het aanbod van een specifieke Russische marktplaats, waar in november 2020 ruim 260.000 fingerprints van nietsvermoedende gebruikers te koop werden aangeboden.

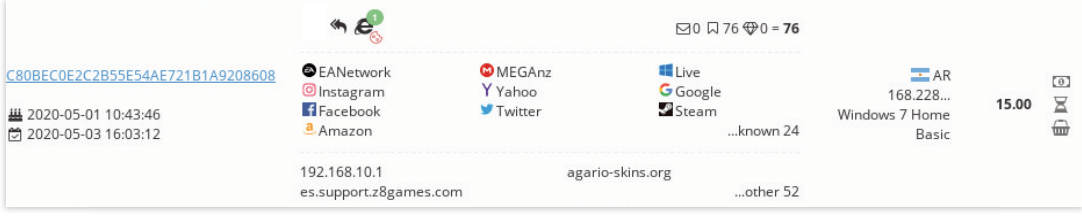
Impersonation as a Service

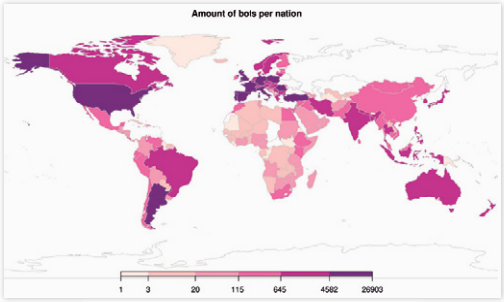
De fingerprints zijn verzameld van gebruikerssystemen die zijn



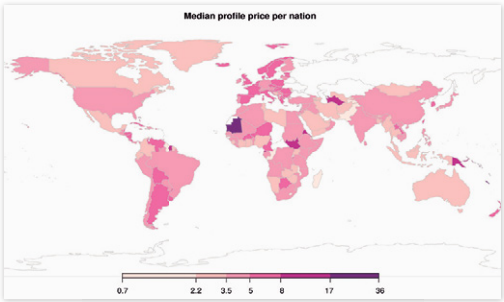
Zoekscherm voor gebruikersprofielen.

Voorbeeld van een profiel, voordat een potentiële klant overgaat tot aanschaf.





Meest voorkomende prijzen die per land worden betaald voor gebruikersprofielen.



Overzicht van de landen waar de geïnfecteerde computers staan waarop spyware continu fingerprints van gebruikers in kaart brengt.

geïnfecteerd met spyware. De eigenaren van deze marktplaats garanderen dat de profielen up-to-date zijn, doordat de spyware continu zowel de activiteiten als de technische omgeving steeds opnieuw in kaart brengt. Ook belooft de marktplaats gebruikersprofielen slechts één keer te verkopen. Prijzen van profielen variëren van twee tot honderden dollars.

De onderzoekers noemen deze geavanceerde vorm van criminele dienstverlening 'Impersonation as a Service', afgekort ImpaaS. Uit angst voor represailles delen de onderzoekers de naam van deze marktplaats niet, maar duiden die aan met ImpaaS.ru. Een van de twee onderzoekers, Michele Campobasso, vertelt erover.

Hoe kregen jullie toegang tot Impaas.ru?

"Dat kan alleen op uitnodiging. Daarom benaderden we, binnen verschillende underground-forums, een aantal personen die beweerden betrokken te zijn bij ImpaaS.ru. Omdat we aanwijzingen hadden dat de beheerders van het platform erg op hun hoede waren voor onwelkome gasten, maakten we uit voorzorg verschillende accounts aan. Zo kwamen we in totaal aan elf ImpaaS.ru-abonnementen. We verdeelden onze 'scrape'-activiteiten over de verschillende accounts om minder op te vallen. Desondanks werd een deel van onze abonnementen na verloop van tijd als verdacht aangemerkt en geblacklist. Toch slaagden we er uiteindelijk in om de hele inhoud van ImPaaS.ru in het geheim weg te 'schrapen'."

Hoe ziet ImpaaS.ru eruit?

"Heel gebruikersvriendelijk. Bezoekers kunnen een database met gebruikersprofielen doorzoeken, bijvoorbeeld op land of de aanwezigheid van gegevens over specifieke betaaldiensten, zoals PayPal of de Rabobank. Als je door resultaten scrolt, verbergt ImpaaS.ru in eerste instantie de identiteit van de slachtoffers. Als een aanvaller echter een profiel gekocht heeft, zijn gegevens in detail zichtbaar.

Een aanvaller kan dan bijvoorbeeld zien voor welke organisatie een slachtoffer werkt. Ook kan hij of zij uit een aangeschaft gebruikersprofiel afleiden welke databronnen de spyware verzamelt, zoals wachtwoorden en surfgeschiedenis. Als het daarbij gaat om extra waardevolle diensten, zoals socialmedia-platformen of online banken, dan is dat duidelijk aangegeven. Behalve inloggegevens kunnen bijvoorbeeld ook de antwoorden op beveiligingsvragen deel uitmaken van een gebruikersprofiel, net als banksaldo's, rekeningnummers en de namen van kaarthouders. Naarmate er meer gevoelige informatie beschikbaar is of de gebruiker uit een ontwikkelder land komt, is de prijs van een profiel hoger."

Is het moeilijk om deze profielen te misbruiken?

"Nee. Als je een of meer gebruikersprofielen aankoopt, ontvang je een plug-in waarmee je het profiel kunt laden in je browser. Dat is echt magisch, opeens is het alsof je echt die persoon geworden bent. De browser heeft alle eigenschappen overgenomen van de browser van het slachtoffer, inclusief de bladwijzers, zoekgeschiedenis en alle cookies. Via deze plug-in recreëer je dus de volledige gebruikersomgeving. Je brengt de volledige vingerafdruk tot leven.

Vervolgens kunnen criminelen, dankzij dat hele pakket aan gebruikersdata en zonder dat er een alarmbelletje afgaat, met gestolen wachtwoorden inloggen op allerlei diensten. Cybercriminelen kunnen zo, heel laagdrempelig, zeer gerichte aanvallen doen. En iemand met een klein beetje technische kennis kan heel eenvoudig geautomatiseerd een reeks profielen tegelijk aanvallen. Daarbij moeten inbrekers nog wel een proxy op de juiste manier configureren, om het RBAsysteem wijs te maken dat er wordt ingelogd vanuit het juiste land, de juiste stad, de juiste postcode en via de juiste provider."

Wat heeft dit voor consequenties?

"Voor diensten die gevoelige data beheren, zoals betaaldiensten, is het absoluut aan te raden om standaard gebruik te maken van sterke authenticatie, door bijvoorbeeld beveiligingscodes te verzenden, gebruik te maken van inlogapparaatjes of van biometrische beveiliging. Maar zulke extreme maatregelen zijn bijvoorbeeld niet nodig als je inlogt op je YouTube-account.

Daarnaast zou het interessant zijn om te onderzoeken hoe RBA kan worden verbeterd. Zijn er misschien toch verschillen te ontdekken tussen het profiel dat je kunt laden met aangekochte profielen op zo'n marktplaats en het echte profiel?"

Hoe kun je voorkomen dat je slachtoffer wordt?

"Als je wilt voorkomen dat je geïnfecteerd raakt, dan is het essentieel dat je de bekende voorzorgsmaatregelen neemt tijdens het surfen. Dat betekent niet klikken op verdachte links, geen verdachte websites bezoeken, niet zomaar alles downloaden en al je software, inclusief je antivirusprogramma, regelmatig updaten."

Luca Allodi **Foto** TU/e | Bart van Overbeeke

Oproep

Doet u iets bijzonders met uw pc? Of hebt u een handige softwareoplossing voor uw hobby bedacht? Stuur dan een e-mail met als onderwerp 'Creatief met de pc' naar redactie@computeridee.nl
Wie weet komt u ermee in Computer Idee.

Sites

https://michelecampobasso.github.io
https://lallodi.github.io
www.tue.nl