OPENBAAR MINISTERIE

# Klap voor communicatie criminelen: DoubleVPN uit de lucht

Nieuwsbericht | 30-06-2021 | 13:00

Een grootschalige, internationale actie van politie en justitie heeft de communicatie tussen criminelen opnieuw een slag toegebracht. DoubleVPN is uit de lucht gehaald. Dit bedrijf leverde VPN-diensten (Virtual Private Network); beveiligde en afgeschermde internetverbindingen die cybercriminelen een veilige haven boden om hun slachtoffers aan te vallen.

In tal van Europese landen, waaronder Nederland en Duitsland, en in de Verenigde Staten en Canada zijn vandaag servers van DoubleVPN in beslag genomen en is de infrastructuur uitgeschakeld. Op de websites van DoubleVPN is nu een splashpage zichtbaar van politie en justitie: facilitators van cybercriminaliteit zijn niet anoniem.

Het grote, internationale onderzoek naar DoubleVPN gebeurde onder leiding van de Landelijke Eenheid van de Nederlandse politie, onder gezag van het Landelijk Parket van het Openbaar Ministerie. Binnen dit onderzoek werkte het Team High Tech Crime (THTC) van de Landelijke Eenheid, Dienst Landelijke Recherche, samen met buitenlandse partners in de strijd tegen (inter)nationale zware criminaliteit.

Belangrijke partners van het eerste uur waren Duitsland, de Verenigde Staten, het Verenigd Koninkrijk en Canada. Later sloten ook Italië, Bulgarije, Zweden en Zwitserland

aan. Europol en Eurojust hadden een belangrijke coördinerende rol tijdens het onderzoek.

**Hackbevoegdheid**

De Nederlandse politie en het Openbaar Ministerie hebben in dit onderzoek gebruik gemaakt van hun hackbevoegdheid om de infrastructuur van DoubleVPN binnen te dringen. In Nederland zijn politie en justitie wettelijk bevoegd om heimelijk en op afstand computers binnen te gaan voor de opsporing van ernstige delicten. Het Digital Intrusion Team (DIGIT) van de Landelijke Eenheid, Dienst Specialistische Operaties, is het enige team dat deze bevoegdheid heeft. Het team bestaat uit medewerkers van de (regionale) politie-eenheden, de Koninklijke Marechaussee en de Fiscale Inlichtingen- en Opsporingsdienst.

**Ransomware en Phishing**

DoubleVPN was een kleine VPN-provider, maar heel belangrijk voor cybercriminelen. Er werd op verschillende fora veel over gesproken. De dienst maakte zelf ook reclame op deze fora; vooral op Russisch- en Engelstalige ondergrondse cybercriminele fora.
DoubleVPN werd onder meer gebruikt door ransomware verspreiders en phishing fraudeurs.

De dienst bood klanten maximale anonimiteit door niet alleen enkelvoudige, maar ook dubbele, driedubbele en zelfs quad-VPN-verbindingen aan te bieden. De goedkoopste VPN-verbinding kostte 22 euro per maand.

**Witwassen en deelname criminele organisatie**

DoubleVPN wordt ervan verdacht een criminele organisatie te zijn. Het bedrijf wordt ook verdacht en van witwassen en medeplichtigheid of betrokkenheid bij de strafbare feiten die zijn klanten pleegden door gebruik te maken van de diensten van DoubleVPN. Denk aan hacken, het verkopen

en/of verspreiden van malware, zoals ransomware en het verkopen van de gegevens die de klanten van DoubleVPN kregen door te hacken.

**Wereldwijde krachtenbundeling**

"Criminele facilitators als DoubleVPN hebben een wereldwijd bereik. Hun servers staan in vrijwel alle landen. De strijd aanbinden met dit soort criminelen kan dan ook alleen maar succesvol als we internationaal de handen inéén slaan en gebruikmaken van elkaars kennis, kunde en netwerken. De Landelijke Eenheid heeft voortdurend een belangrijke rol in dit soort internationale onderzoeken vanwege haar specialisaties op het gebied van cyber, intelligence en tactiek', aldus Andy Kraag, hoofd Dienst Landelijke Recherche van de Landelijke Eenheid. 'Dit onderzoek laat opnieuw zien dat facilitators van cybercrime niet onaantastbaar zijn."

**Geen veilige haven**

"De personen achter DoubleVPN denken anoniem te kunnen blijven bij het faciliteren van grootschalige cybercrime-operaties, maar dat zijn ze zeker niet', aldus officier van justitie Wieteke Koorn. 'Door gerechtelijke stappen te ondernemen, en digitaal in te breken op hun infrastructuur, maken we één ding heel duidelijk: er is geen veilige haven voor dit soort criminelen. Deze criminele daden schaden de gedigitaliseerde maatschappij. Ze tasten het vertrouwen aan van burgers en bedrijven in digitale technologie. Om die reden moeten we hun gedrag stoppen."

**Wat is een Virtual Private Network?**

Een VPN-dienst versleutelt het internetverkeer vanaf het IP-adres van de gebruiker naar de VPN-dienst. Voor de buitenwereld lijkt het internetverkeer hierdoor niet afkomstig te zijn van de gebruiker, maar van het IP-adres van de VPN-dienst. Het IP-adres van de gebruiker wordt

dus afgeschermd. Op deze manier weet een internetprovider of een netwerkbeheerder niet welke websites een gebruiker bezoekt.

Een beveiligde VPN-internetverbinding is legaal. Personen en bedrijven maken er gebruik van omdat ze vertrouwelijk met elkaar willen communiceren. Misbruik van VPN-internetverbindingen voor criminele activiteiten is uiteraard strafbaar.

**Deelnemende landen en instanties:**

- Nederland: politie (Landelijke Eenheid), Landelijk Parket (Openbaar Ministerie)
- Duitsland: federale recherche (Bundeskriminalamt), parket van de procureur-generaal Frankfurt am Main – Centrum voor cybercriminaliteit
- Verenigd Koninkrijk: National Crime Agency (NCA)
- Canada: Royal Canadian Mounted Police (RCMP)
- Verenigde Staten: Federal Bureau of Investigation (FBI), Amerikaanse geheime dienst (USSS), Amerikaanse ministerie van Justitie
- Zweden: Zweedse politieautoriteit (Polisen)
- Italië: Staatspolitie (Polizia di Stato)
- Bulgarije: directoraat-generaal voor de bestrijding van de georganiseerde misdaad van het Bulgaarse ministerie van Binnenlandse Zaken (Главна дирекция "Борба с организираната престъпност" при Министерството на вътрешните аботеа а ешните аот)
- Europol: Europees Centrum voor Cybercriminaliteit (EC3)
- Eurojust