



Tech Support Scam: 'verbreek de verbinding'

Rapportage naar
aanleiding van de
einddatum van de
Intentieverklaring ter
verstoring van Tech
Support Scam.

Projectteam Tech Support Scam
Definitief

Inhoudsopgave

Documentinformatie.....	Fout! Bladwijzer niet gedefinieerd.
Inhoudsopgave.....	2
Voorwoord.....	3
Inleiding.....	4
Het fenomeen	5
Uitleg fenomeen	5
Modus Operandi	5
Samenwerking en maatregelen	7
Proces samenwerking	7
Verstoringsmaatregelen	7
Cijfermatige Resultaten	9
Ontwikkeling Registraties	10
Ontwikkeling schadebedragen en cash-out.....	10
Ontwikkeling (sub-)MO i.c.m. gemiddelde schadebedragen.....	12
Ontwikkeling leeftijd slachtoffers	12
Conclusie.....	13

Voorwoord

Voor u ligt de eindrapportage van het project “Verstoring van Tech Support Scam in Nederland”. Een project dat begon met de constatering dat dit de vorm van cybercrime was waarvan destijds het vaakst aangifte werd gedaan. Extra zorgelijk omdat in 2016 en 2017 het aantal Nederlandse slachtoffers snel groeide. Nu, eind 2020, kunnen we constateren dat de groei van het aantal slachtoffers tot staan is gebracht en dat de schade per slachtoffer flink is afgenomen.

Dit project toont aan dat een coalitie van overheidsinstanties en nationale en internationale private partijen kan leiden tot goede landelijke preventiecampagnes en tot het opwerpen van barrières. Daardoor wordt het voor criminelen moeilijker om slachtoffers te maken. Doordat iedere partij, vanuit een gezamenlijk gedragen doel en met respect voor ieders positie, doet wat mogelijk is om dat doel te verwezenlijken.

Wij zijn er trots op dat dit is gelukt op basis van een initiatief van de politie en het Openbaar Ministerie. Een initiatief in de beste Rotterdamse traditie van “niet lullen, maar poetsen”.

Nog één keer de oproep aan alle potentiële slachtoffers: hang op! Verbreek de verbinding!



Hugo Hillenaar
Hoofdofficier van Justitie



Fred Westerbeke
Politiechef Eenheid Rotterdam

Inleiding

In 2017 werd geconstateerd dat het aantal politie-registraties over Tech Support Scam fors toenam naar bijna 2000 registraties in dat jaar. Hierdoor bleek dit één van de vormen van cybercrime te zijn, waarvan in 2017 in Nederland het vaakst aangifte werd gedaan met in dat jaar een geschatte schade van bijna EUR 6 miljoen. Vanuit politie en OM is het initiatief genomen om meerdere partijen te benaderen om dit een halt toe te roepen.

Hoewel diverse soorten bedrijven slachtoffer kunnen worden van dit misdrijf, in die zin dat hun naam, dienst of product wordt misbruikt door fraudeurs, is in Nederland begonnen met partijen te benaderen die het vaakst door Nederlandse slachtoffers werden genoemd. Omdat Tech Support Scam internationaal is georganiseerd betrof dit ook partijen die internationaal zijn georganiseerd.

Dit heeft dan ook geresulteerd in een unieke publiek-private samenwerking. Deze samenwerking is bevestigd door het ondertekenen van de 'Intentieverklaring van de Brede Coalitie ter verstoring van Tech Support Scam in Nederland' op 28 maart 2018. De betrokken partijen hierbij waren:

1. De Minister van Justitie en Veiligheid
2. Openbaar Ministerie
3. Nationale Politie
4. Autoriteit Consument en Markt
5. Microsoft Corporation
6. TeamViewer GmbH
7. Koninklijke KPN N.V.
8. VodafoneZiggo Group Holding B.V.
9. Western Union Company
10. MoneyGram International Inc.
11. ABN AMRO Bank N.V.
12. ING Bank NV.
13. Coöperatieve Rabobank U.A. (Rabobank)
14. De Volksbank
15. Verenigde Bitcoinbedrijven Nederland (VBNL)

Later is hier nog de Betaalvereniging Nederland bij aangesloten.

In de afgelopen periode is er geïnvesteerd in een goede samenwerking, het bouwen van het netwerk en vanzelfsprekend het implementeren van maatregelen om waar mogelijk Tech Support Scam te verstoren.

De Intentieverklaring loopt op 31 december 2020 af. Met deze rapportage geven wij u een kort inzicht in de ontwikkelingen over het fenomeen, de samenwerking en wat de resultaten zijn geweest van de gezamenlijke inspanningen.

Het fenomeen

- Er is sprake van Tech Support Scam als er telefonisch contact is tussen de fraudeur (die zich voordoeft als oplosser van technische problemen met de computer) en het slachtoffer. Veelal na installatie van een Remote Access Tool wordt er geld overgeboekt zonder dat het slachtoffer hier akkoord voor heeft gegeven. Social engineering speelt een belangrijke rol.
- De hoofdlijnen van de verschijningsvormen van Tech Support Scam zijn de afgelopen jaren nauwelijks veranderd en bestaan voornamelijk uit: 'gebeld worden', 'helpdesk opgezocht' en 'pop-up-berichten'. Deze fraudevorm vindt nog steeds veelal in de Engelse taal plaats.
- Het is gecompliceerd om strafrechtelijke onderzoeken succesvol te laten zijn omdat de telecommunicatie-, de digitale én de financiële sporen, als ze al te herleiden zijn, altijd naar het buitenland leiden (en zelfs soms per zaak naar verschillende buitenlanden). Bovendien zijn dit vluchtige sporen en loopt de samenwerking met niet-Europese landen niet altijd even snel.

Uitleg fenomeen

In november 2018 is er een verdiepende analyse¹ opgesteld voor Tech Support Scam c.q. helpdeskfraude of Microsoftfraude. Hiermee is een duidelijk beeld geschetst van dit fenomeen. In 2020 is deze informatie geactualiseerd.

Tech Support Scam is een vorm van oplichting waarbij telefonisch contact plaatsvindt tussen het doelwit (het slachtoffer) en een persoon die zich voordoeft als medewerker van een softwarebedrijf, bijvoorbeeld Microsoft (de fraudeur)². Door de ongeoorloofde toegang tot de computer van een slachtoffer valt het voltooide delict meestal onder cybercrime in enge zin (criminaliteit met ICT als middel en doelwit).

De reden waarom deze fraude oorspronkelijk 'Microsoftscam' werd genoemd, is omdat deze naam het meest wordt gebruikt in de fraude. Dit hangt samen met het feit dat er door slachtoffers ook veel gebruik wordt gemaakt van deze software. Het is dus voor slachtoffers geloofwaardig als iemand zich voordoeft als helpdesk van Microsoft. Uit de informatie blijkt dit tot op de dag van vandaag nog steeds het geval te zijn.

Binnen de modus operandi wordt 'social engineering' toegepast, waarbij getracht wordt via misleiding en overtuiging toegang te krijgen tot systemen en vertrouwelijke gegevens van personen en hen actief deel te laten nemen aan de fraude. De fraudeurs misleiden slachtoffers door zich voor te doen als een vertrouwde partij, namelijk een helpdeskmedewerker, technicus of security-expert. Daarnaast gebruiken de fraudeurs sociale beïnvloeding (een verandering in de houding, overtuigingen en gedragingen van een persoon als gevolg van interne of externe druk), waarbij verschillende binnen de psychologie onderscheiden overtuigingsstechnieken worden ingezet. Het uiteindelijke doel van de fraudeur is het slachtoffer geld te laten betalen voor de zogenaamde geleverde dienst en/of het misbruiken van persoonlijke gegevens van het slachtoffer die op de computer staan, om daarmee ten laste van het slachtoffer overboekingen te doen.

Meer mensen zijn online actief en digitale hulp op afstand wordt steeds meer een gemeen goed. Aanvullend worden steeds meer gegevens digitaal bewaard waardoor de noodzaak van een beveiligde omgeving cruciaal is. Tech Support Scam zal dan ook niet meer weg te denken zijn in een steeds meer gedigitaliseerde maatschappij.

Definitie Tech Support Scam

Bij het ondertekenen van de Intentieverklaring is de onderstaande definitie van Tech Support Scam opgenomen:

- Een aantal typen frauduleuze activiteiten per telefoon, waarin een fraudeur zegt legitieme technische ondersteuningsdiensten aan te bieden. De telefoontjes gebeuren via cold calling naar nietsvermoedende gebruikers, of hebben de vorm van het verleiden van gebruikers om een bepaald telefoonnummer te bellen, bijvoorbeeld door een browser pop-up.
- In Nederland is deze fraude meestal gericht op Microsoft of Apple gebruikers, waarbij de beller vaak zegt de technische ondersteuningsdienst van deze bedrijven te vertegenwoordigen terwijl dit niet het geval is.
- De fraudeur zal in typerende gevallen proberen om het slachtoffer zover te krijgen dat deze op afstand toegang geeft tot diens computer. Nadat toegang op afstand is verkregen, probeert de fraudeur het vertrouwen van het slachtoffer te verkrijgen om te betalen voor zogenaamde ondersteuning of worden er andere listige kunstgrepen toegepast.
- Daarna wordt het slachtoffer bewogen om een geldbedrag over te maken naar de fraudeurs, bijvoorbeeld via een bankoverboeking, money transfer, giftcards, etc.

Modus Operandi

1. Het slachtoffer wordt gebeld op een vast of mobiel telefoonnummer (verschijningsvorm: 'gebeld worden')

Het slachtoffer wordt op diens vaste of (tegenwoordig steeds meer voorkomend) op het mobiele telefoonnummer gebeld, waarna de Engelssprekende beller zich voorstelt als medewerker van Microsoft of een ander softwarebedrijf. Dit wordt ook wel 'cold calling' of 'koud bellen' genoemd.

¹ Verdiepende analyse TSS, d.d. 30-11-2018, Jildau Borwell en Kirsten Bos-Riepma

² Brede coalitie ter versterking van Tech Support Fraudes in Nederland, 2018

2. Het slachtoffer zoekt online naar hulp bij computerproblemen (verschijningsvorm: 'online hulp zoeken')

Het slachtoffer zoekt online, via een zoekmachine, naar hulp bij computerproblemen. Door de fraudeurs zijn overtuigende websites opgezet die overkomen als helpdesks voor verschillende softwarebedrijven zoals Microsoft, McAfee, Avast en Skype. Deze websites verschijnen hoog in de zoekresultaten van het slachtoffer. Wanneer het slachtoffer het telefoonnummer van de 'helpdesk' uit de zoekresultaten belt, krijgt deze een fraudeurs aan de telefoon die zich voordoet als medewerker van het betreffende bedrijf.

3. Er verschijnt een pop-up in het beeldscherm van het slachtoffer (verschijningsvorm: 'pop-up')

Slachtoffers krijgen op hun computer een pop-up-scherm te zien, vaak gepaard met alarmerende geluiden of flitsen, dat zij niet (gemakkelijk) weg kunnen klikken en vaak beeldvullend is (Harteveld & Bloem, 2018). In de pop-up staat dat de computer is geïnfecteerd met een virus, de bestanden op de computer zijn versleuteld of er kinderporno op de computer is gevonden. De slachtoffers wordt gevraagd een (vaak Nederlands ogend) telefoonnummer te bellen.

Na deze bovengenoemde varianten is de manier waarop het geld afhandig wordt gemaakt op veelal dezelfde manier:

Nadat het slachtoffer ervan overtuigd is dat betaald moet worden voor de 'oplossing' van de technische ondersteuning, wordt gesproken over de prijs die hiervoor betaald zou moeten worden en wordt er ingelogd op de internetbankieromgeving. Door de Remote Access Tool heeft de fraudeur de mogelijkheid een 'zwart scherm' op te zetten of het beeld heel erg te verkleinen. Nadat er is ingelogd is op diens internetbankieromgeving heeft de fraudeur de mogelijkheid de getoonde bedragen aan te passen en zo het scherm te vervalsen. Wanneer het scherm weer wordt genormaliseerd, wordt het slachtoffer misleid over de begunstigde en het over te maken bedrag. Het geld wordt overgeboekt naar bankrekeningen in het buitenland of er worden cryptovaluta (bijvoorbeeld bitcoins) van gekocht.

Een andere veel voorkomende manier is dat er betaald wordt met giftcards (pré-paidkaarten, I-tunes, etc.). De slachtoffers kopen deze kaarten en geven vervolgens de code door.

Geografische bepalende factor

Het is algemeen bekend dat Tech Support Scam zijn oorsprong kent in India en tot op de dag van vandaag is het nog steeds zeer waarschijnlijk dat veelal vanuit dit land wordt geopereerd. De redenen hiervoor kunnen zijn:

- De historie van India als kolonie van Engeland waardoor de Engelse taal de overhand kreeg en nu in het heden nog steeds wordt gesproken.
- India was één van de eerste landen waarnaar outsourcing plaatsvond, mede doordat er Engels werd gesproken en vanwege de lage kosten. Hierdoor zijn er netwerken beschikbaar voor o.a. de communicatie met het bronland.
- India is uitgegroeid tot een IT-grootmacht met allerlei gerenommeerde opleidingsinstellingen³ op dit vlak. Door het relatief hoge opleidingsniveau in combinatie met de grote werkloosheid, wordt de keuze om hieraan mee te werken vergemakkelijkt.

Het bovenstaande kan niet 100% worden bevestigd uit de politie-informatie omdat het voor de benadeelde moeilijk te benoemen is, van welk Engelsprekend en specifiek welk accent er sprake was. Wel blijken onderzochte digitale en financiële sporen van een aantal Nederlandse politieonderzoeken inderdaad in India uit te komen.

Aanvullend is aan de hand van informatie van de domeinen en bijbehorende emailadressen uit 2020 gebleken dat ongeveer de helft van de onderzochte frauduleuze domeinen geregistreerd zijn in India. Van de andere helft is niet traceerbaar in welk land deze zijn geregistreerd omdat zij deze informatie hebben afgeschermd. Hoewel alleen een registratie van een domeinnaam niet direct impliceert dat de fraude ook vanuit India zou plaatsvinden, is ook dit een indicator dat hier wel sprake van is.

Eerdere verzoeken tot samenwerking met India op dit fenomeen zijn vooralsnog weinig succesvol gebleken. Hierdoor ontbreekt in deze rapportage ook inzicht over criminele netwerken en kan er niet altijd antwoord worden gegeven op onderliggende vragen zoals over het verdienmodel (per sub-MO) of hoe aan de data wordt gekomen om potentiële slachtoffers te benaderen.

³ <https://www.theguardian.com/news/2018/jan/02/the-scammers-gaming-indias-overcrowded-job-market>

Samenwerking en maatregelen

Door vanuit het blikveld van elke partner gezamenlijk naar het probleem Tech Support Scam te kijken, konden diverse verstoringsmaatregelen worden getroffen. Samenwerking was het sleutelwoord.

Proces samenwerking

Het belangrijkste gemeenschappelijk uitgangspunt was dat de partijen erkenden dat de onophoudelijke aanvallen door Tech Support Scam niet alleen het publieke vertrouwen bedreigen, maar ook de reputatie van de verschillende private partijen kan aantasten.

Na ondertekening van de intentieverklaring vond er onder het gedeeld voorzitterschap OM/politie eenmaal per drie maanden een overleg met de partners plaats. Dit waren voorheen fysieke bijeenkomsten, maar ten tijde van COVID-19 is dit digitaal georganiseerd. De politie stelde per kwartaal een integraal veiligheidsbeeld op. Dit op basis van data van de politie en de aangeleverde data van de overige partijen. Hierdoor werd het inzichtelijk of er wijzigingen waren in de verschijningsvormen, de ontwikkeling schadebedragen, etc. In de bijeenkomsten werden onder andere op basis van het hiervoor genoemde veiligheidsbeeld met elkaar besproken welke verstoringsmaatregelen zinvol zouden kunnen zijn om het aantal slachtoffers van Tech Support Scam te laten dalen en/of de schade te beperken. Diverse partijen hebben op basis daarvan het initiatief genomen om gedane suggesties te implementeren.

Verstoringsmaatregelen

Hoewel niet alleen in Nederland, maar over de hele wereld veel mensen slachtoffer worden van Tech Support Scam en wereldwijde maatregelen wenselijk zijn, is in het kader van haalbaarheid overeengekomen om te beginnen met maatregelen op nationaal niveau. Hieronder staat een overzicht van een groot aantal van deze maatregelen:



Een aantal van deze interventies worden op hoofdlijnen nader toegelicht:

Samenwerking

Een van de belangrijkste successen is dat er een breed netwerk is ontstaan. Deze unieke samenwerking heeft aan de basis gestaan om ook andere soortgelijke fenomenen op cybercrime integraal aan te pakken. Doordat het netwerk er al is, kan sneller met elkaar worden overlegd over mogelijke barrières en interventies.

TeamViewer

Op basis van de oorspronkelijke data bleek dat vooral TeamViewer werd gebruikt als Remote Access Tool bij Tech Support Scam. Na het delen van deze informatie, heeft TeamViewer waar mogelijk de software aangepast om misbruik hiervan te voorkomen. Na deze aanpassing is gebleken dat het gebruik van TeamViewer bij Tech Support Scam fors is afgenomen. Aanvullend heeft TeamViewer ook een site (<https://www.teamviewer.com/en/report-a-scam>) waar gebruikers fraudeleus gebruik van deze tool kan worden gemeld.

Helaas is ook gebleken dat de fraudeurs vervolgens gebruik maken van andere partijen die Remote Access Tools aanbieden waar er (nog) geen drempel is om misbruik zoveel mogelijk te voorkomen. Vanuit de coalitie is ook contact gezocht met deze partijen en hen in contact te brengen met TeamViewer om deze succesvolle aanpak te delen.

Politie

Naast strafrechtelijke onderzoeken naar de daders, is er ook geïnvesteerd naar het neerhalen van frauduleuze helpdesk-websites. Uit een aantal aangiftes is gebleken dat slachtoffers gebeld hadden naar een telefoonnummer dat zij op internet hadden opgezocht, maar dat achteraf gezien frauduleus was. Een bekend voorbeeld daarvan is klantenservicenederland.nl. Op last van de Officier van Justitie is deze website ontoegankelijk gemaakt in november 2018. Ook van deze website leidt het daderspoor naar het buitenland. Helaas is het ontoegankelijk maken van een website slechts een tijdelijke mogelijkheid; daarnaast bleken al snel weer soortgelijke websites in de lucht.

Politie haalt valse domeinnamen offline

Laatste update: 19-02-2020 | 15:52

Hoorn - Na een aantal aangiftes van oplichting en cybercrime viel het twee politiemensen op dat dezelfde telefoonnummers werden gebruikt om mensen geld afhandig te maken. De aangevers deden aangifte nadat zij een helpdesk belden bij problemen met hun computer of telefoon. De helpdesknamen waren gelijkend op site's voor het verkrijgen van een telefoonnummer, een reparatiebedrijf van een computerproducent of social media helpdesk. Zodra de aangever op het oog gebruikelijke gegevens had verstrekt werd hij bewogen of gedwongen tot het overmaken van geld.

Aanvullend heeft de politie de mogelijkheid gerealiseerd voor het doen van digitale aangifte is het voor het publiek toegankelijker geworden om aangifte te doen. Door de eenduidige en uitgebreide vraagstelling, ontstaat er een goede inzicht over deze fraude en dit bood onder andere toegevoegde waarde voor de informatievoorziening richting de partners.

Aanpassen klantidentificatieproces Verenigde Bitcoinbedrijven Nederland (VBNL)

De bedrijven hierbij aangesloten hebben op basis van de informatie hun 'due-dilligence' aangepast. Hierdoor werd de criminele cash-out bemoeilijkt en zorgde er ook voor dat de schadebedragen (vergoedingen) voor de bitcoinbedrijven fors zijn afgenomen. Ook hebben zij geïnvesteerd in het trainen van medewerkers op het tijdig kunnen signaleren van frauduleuze handelingen. Wat nog niet is gerealiseerd, maar nog op de agenda staat is niet alleen nationale, maar ook internationale samenwerking met bitcoinbedrijven.

ACM: Blokkeren telefoonnummers

De politie heeft op basis van de aangiftes periodiek frauduleus gebruikte telefoonnummers gedeeld met de Autoriteit Consument en Markt. Indien na zorgvuldig onderzoek bleek dat het telefoonnummer voor Tech Support Scam werd ingezet, zorgde de ACM in samenwerking met de telecomaانبieders ervoor dat het nummer werd geblokkeerd.

ACM gaat helpdeskfraude te lijf: 100 telefoonnummers uit de lucht

De Autoriteit Consument en Markt (ACM) probeert nep-helpdesks aan te pakken door 'foute' nummers uit de lucht te halen. Inmiddels zijn 100 Nederlandse telefoonnummers geblokkeerd. Het gaat om nummers die werden gebruikt om mensen op te lichten. Om deze vorm van fraude te bestrijden, haalt de toezichhouder de nummers tegenwoordig uit de lucht. Daarin trekt het op met telecomaانبieders, de politie en het Openbaar Ministerie.

Bron: AD: 19-02-2020

Het afsluiten van een abonnement bij een telecomprovider of het kopen van een simkaart is niet de enige manier om een telefoonnummer te gebruiken. De fraudeurs kunnen ook gebruik maken van spoofing. Dit houdt in dat het technisch mogelijk is om het te doen laten lijken alsof zij bellen met een telefoonnummer van iemand anders. Binnen het project is gekeken naar de mogelijkheid om oproepen die zijn gemaakt met 'vervalste' telefoonnummers op te sporen.

Dat is echter technisch gezien erg ingewikkeld gebleken vanwege het vaak internationale karakter van dergelijke telefoongesprekken. Door goede samenwerking tussen de telecomaandbieders kunnen zij inmiddels een gedeelte van de 'gespoofde' telefoongesprekken tegenhouden.

Microsoft

Microsoft monitort via de eigen meldingswebsite 'Avoid and report technical support scams' de ontwikkelingen. Op deze website wordt preventie advies gegeven, en informatie wat te doen als de fraude heeft plaatsgevonden.



Daarnaast ageert Microsoft vanuit de eigen kantoren in het betrokken land zeer actief tegen de fraudeurs, door daar aangifte te doen en de lokale politie desgevraagd te ondersteunen bij strafrechtelijke actie.

Banken en TeamViewer

Een interventie die zeer wenselijk is, is de koppeling van het gebruik van een Remote Access Tool en het detectiesysteem van de banken. Ook worden de mogelijkheden onderzocht om bij online bankieren een extra waarschuwing in te bouwen dat potentiële slachtoffers extra alert maakt bij het overboeken van bedragen.

Cijfermatige Resultaten

- De registraties zijn na een lange periode van daling sinds Q2 2020 weer gestaag aan het stijgen.
- De totale schade is met 59% afgenomen t.o.v. 2017 en de gemiddelde schadebedragen zijn met 62% afgenomen. Ook hier geldt wel dat de schadebedragen sinds Q2 2020 gestaag stijgen.
- Er is nog onvoldoende inzicht in het verdienmodel. Betalen met het gebruik van giftcards is toegenomen.
- De afgelopen jaren is er een verschuiving geweest van de sub-MO's. 'Gebeld worden' is afgenomen en 'Helpdesk opgezocht' is toegenomen. In de laatste twee maanden van 2020 is zichtbaar dat 'gebeld worden' wel weer aan het stijgen is. Pop-up berichten blijven onveranderd.
- De leeftijdscategorie waarin de meeste slachtoffers zijn, is onveranderd en betreft tussen 60-79 jaar.

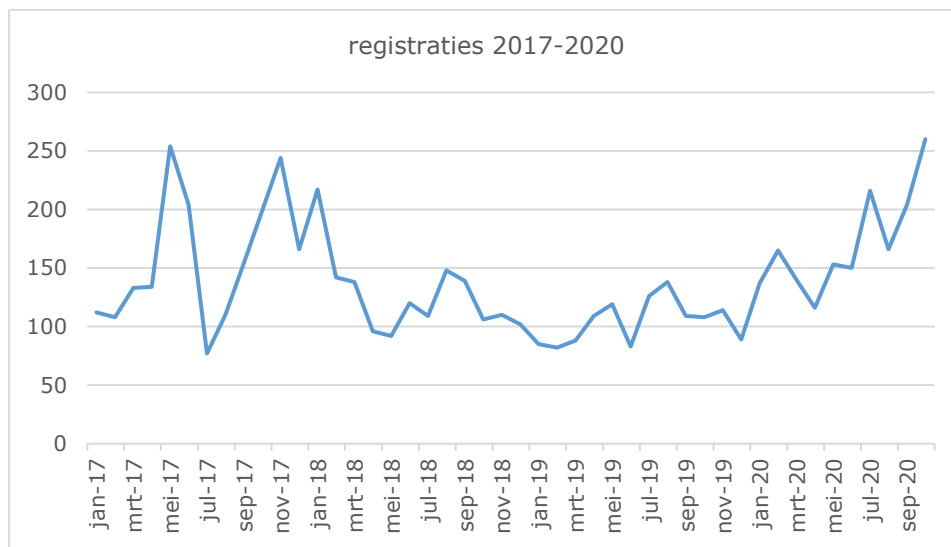
Ontwikkeling Registraties

- Sinds 2017 worden de aantallen registraties (meldingen en aangiften) van Tech Support Scam in de Nederlandse politiesystemen gemonitord. Na het van start gaan van de coalitie leverde een aantal partners ook gegevens aan ter ondersteuning van de kwartaalrapportages die sinds juli 2019 werden opgeleverd. Om de ontwikkelingen op een langere termijn inzichtelijk te maken, is ervoor gekozen om in dit onderdeel alleen de gegevens van de politie te gebruiken omdat deze sinds 2017 worden bijgehouden.
- Voor de onderstaande data geldt dat als einddatum van de gegevens 31 oktober 2020 is aangehouden, dit omdat de eindbespreking medio december plaatsvindt.
- Voor 2020 is voor de maanden november en december uitgegaan van een schatting op basis van het gemiddelde in dit jaar.

De ontwikkeling van het aantal registraties zag er als volgt uit:

Jaartal	2017	2018	2019	2020
Aantal registraties	1.933	1.540	1.807	2.116

In de afgelopen jaren was er sprake van een afname van het aantal registraties, echter medio 2020 is dit aantal weer toegenomen:



Zoals eerder genoemd wordt strafrechtelijk onderzoek bemoeilijkt door de grote internationale component in deze vorm van cybercrime. Samenwerken met landen als bijvoorbeeld India is tijdrovend en er kan nauwelijks invloed worden uitgeoefend op de voortgang. Hierdoor is er beperkt inzage in het daderschap en daardoor is het lastig om te benoemen wat nu de precieze oorzaak is van deze toename sinds maart-mei 2020. Wel zijn er aantal mogelijke verklaringen:

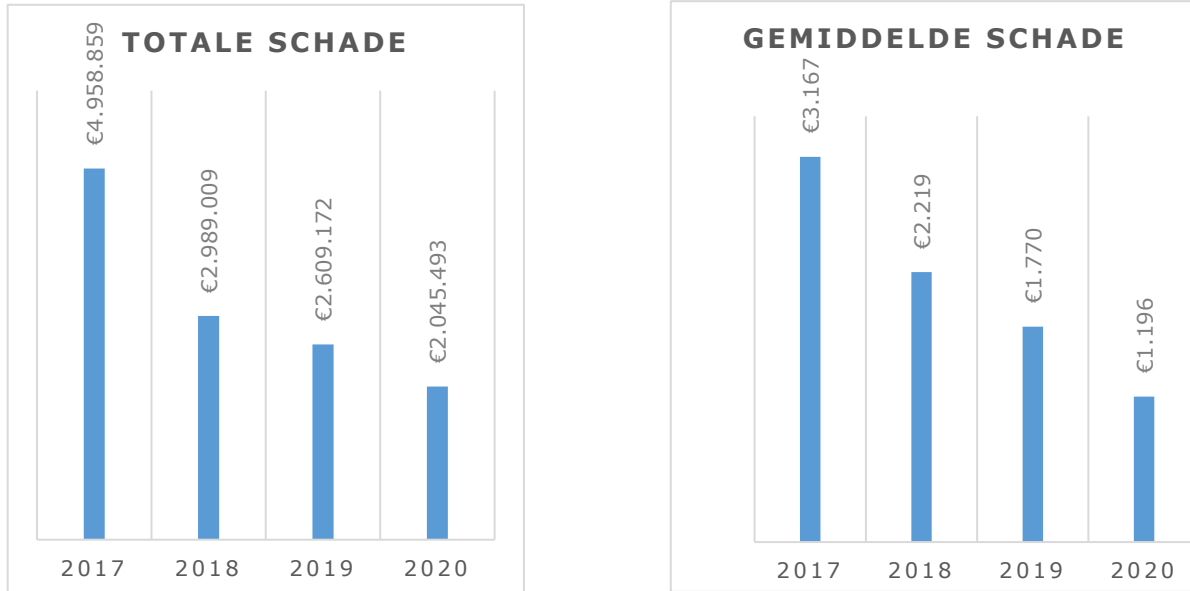
- Sinds februari 2020 is het mogelijk om digitaal aangifte te doen van Tech Support Scam. Hierdoor is het voor slachtoffers meer toegankelijk om aangifte te doen.
- Vanaf maart 2020 raakte de wereld steeds meer op slot door COVID-19. Net zoals in Nederland was er ook in India sprake van een lock-down. Echter uit berichtgeving bleek dat India al snel deze maatregelen versoepelde voor de IT-sector, aannemelijk is dat callcenters hier ook onder vielen. Een ander gevolg van COVID-19 is dat het publiek meer online actief is. Programma's moeten geüpdatet worden waardoor men sneller naar helpdesks op zoek gaat of mensen sneller geloven dat, als er gebeld wordt, er inderdaad sprake van een 'hack' zou kunnen zijn zoals de scammer beweert.
- Afnemende media-aandacht voor deze fraudevorm. In de afgelopen maanden zijn er meer fraudetechnieken op het grote publiek toegepast, zoals bankhelpdeskfraude en aan- en verkoopfraude. Ook hier is in de media aandacht voor gezocht. In de afgelopen periode is er hierdoor voor Tech Support Scam minder aandacht geweest.
- Via Europol blijkt in landen als Zwitserland en Finland Tech Support Scam een opkomend fenomeen te zijn. Dit impliceert dat deze fraudevorm nog steeds een populaire fraudevorm is en blijft.

Ontwikkeling schadebedragen en cash-out

Ten tijde van de ondertekening van de Intentieverklaring was er uitgegaan van een geschatte schade in 2017 van bijna EUR zes miljoen. Medio 2018 bleek de schade iets lager uit te vallen. Op basis van de definitieve cijfers van 2017 tot en met het heden is gebleken dat de totale schade met 59% is afgenomen. De gemiddelde schadebedragen zijn met 62% afgenomen.

Tussen de informatie over de schadebedragen die de deelnemende banken aanleverden en die van de politie zat enige discrepantie. Veelal zijn de totale schadebedragen van de banken hoger dan bij de politie. Dit is te verklaren door de lage aangiftebereidheid. Men kan in de veronderstelling zijn dat de politie geen actie onderneemt als er aangifte wordt gedaan en dit dan ook achterwege laat. De bank wordt in bijna alle gevallen wel geïnformeerd omdat er nog mogelijkheden zijn om bijvoorbeeld de rekening of een transactie te blokkeren. Doordat het nu sinds dit jaar mogelijk is om digitaal aangifte te doen bij de politie, wordt hiermee ook beoogd dat de aangiftebereidheid stijgt en er een completer beeld ontstaat van de omvang.

Onderstaande grafieken zijn weergaven van de politiecijfers:



Ten tijde van de werking van de Intentieverklaring nauwelijks inzicht verkregen in het verdienmodel. Het geld van het slachtoffer wordt in veel gevallen direct overgeboekt naar een veelal bonafide, bedrijf waar bijvoorbeeld prepaidkaarten worden gekocht. Hiermee verdwijnt de criminele opbrengst in de anonimiteit en is niet meer te traceren.

Ook is gebleken dat de overboekingen vaak niet in één keer plaatsvinden, maar dit via diverse overboekingen plaats vindt. Naar waarschijnlijkheid heeft dit te maken met het omzeilen van de fraudedetectiesystemen van bijvoorbeeld de banken. Ten tijde van de start van het project werd voor de besteding van de criminele verdiensten onder meer vooral gebruik gemaakt van Western Union en Moneygram. Op basis van onze informatie wordt van deze bedrijven nauwelijks meer gebruik van gemaakt. Ook werd er veel gebruik gemaakt van de aankoop van bitcoins. In de afgelopen periode is gebleken dat dit via de cryptocurrencybedrijven die zijn aangesloten bij de Verenigde Bitcoinbedrijven Nederland (VBNL) fors is afgenomen, wat vooral te herleiden is naar een aantal uitgevoerde verstoringsmaatregelen, zoals het verbeteren van due-dilligence.

Uit de informatie blijkt dat betalen via giftcards (zoals google playcards, iTunes tegoed, beltegoed) fors is toegenomen. Er zijn daarom ook contacten gelegd met de aanbieders van deze cards om na te gaan welke mogelijkheden er zijn om ook dit gedeelte van het criminele proces te verstoren.

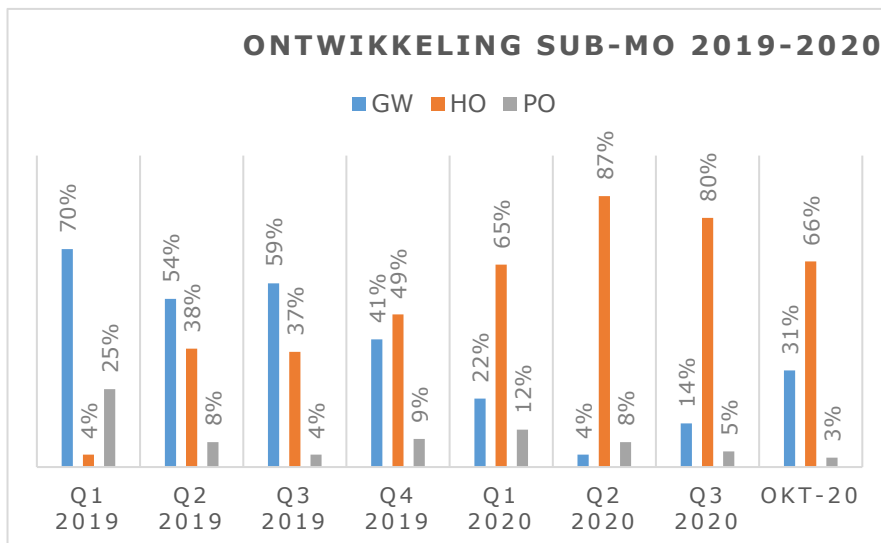
Een logische beredenering laat zien dat een gesprek tussen de fraudeur en het potentiële slachtoffer, voor zover hier inzicht in is, gemiddeld tussen de één en drie uur duurt. Dit in combinatie met het gemiddelde schadebedrag, is er sprake van een hoge verdienste per uur. Dit is snel verdiend en voor een land als Nederland in 2020 goed voor bijna EUR twee miljoen. Als dit wordt vergeleken met het algemene feit dat kapitaal en arbeid relatief goedkoop zijn in een land als bijvoorbeeld India, maakt dat Tech Support Scam een robuust verdienmodel heeft en daarom ook niet snel zal verdwijnen.

Ontwikkeling (sub-)MO i.c.m. gemiddelde schadebedragen

Uit de data (92% gescoord) is gebleken dat de sub-MO 'gebeld worden' is gedaald. Het kantelpunt bleek in Q4 2019 te hebben plaatsgevonden. Daarna is de sub-MO 'helpdesk opgezocht' toegenomen.

In 2020 blijkt dat 'gebeld worden' weer gestaag toeneemt en 'helpdesk opgezocht' daalt, maar nog wel fors hoger is ten opzichte van de andere twee sub-MO's.

Tech Support Scam via een pop-up bericht blijft onveranderd laag.



Op basis van de cijfers uit 2020 blijkt dat het gemiddelde schadebedrag bij de sub-MO 'gebeld worden' het hoogste is, namelijk: € 2.759,77. Gevolgd door sub-mo 'pop-up' met € 944,60 en sub-MO 'helpdesk opgezocht' met € 566,92. Deze cijfers kunnen licht vertekend zijn omdat ondanks dat er wel schade was, het bedrag niet altijd in de aangifte was ingevuld.

Het is niet mogelijk gebleken om te achterhalen waarom de schadebedragen bij de sub-MO 'gebeld worden', hoger zijn dan bij de andere sub-MO's. Dit vereist inzicht in daderinformatie en dit ontbreekt om eerder genoemde redenen.

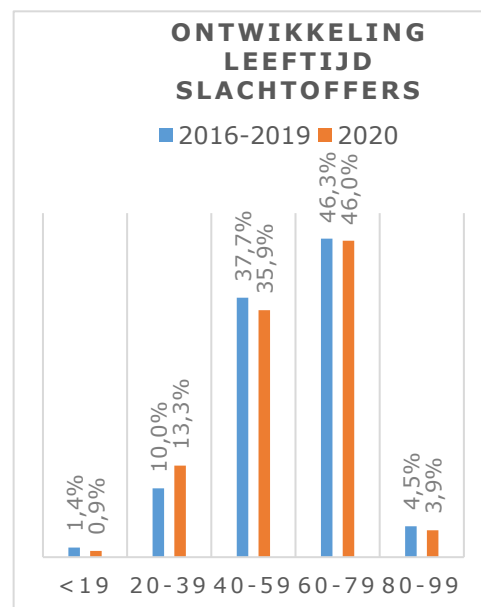
Tot slot is het opvallend dat er een toename is van Nederlandssprekende helpdesks waarbij ook technische ondersteuning wordt aangeboden. Het meest opvallende is dat er in enkele gevallen wanneer het slachtoffer aangeeft de Engelse taal niet te begrijpen, deze wordt doorverbonden met een Nederlandssprekende persoon. Dit zou kunnen betekenen dat er een samenwerking is met Nederlandse personen.

Ontwikkeling leeftijd slachtoffers

Uit de deze grafiek blijkt dat de leeftijd van de slachtoffers in de bijgehouden periode nauwelijks is veranderd. Net zoals bij andere cybercrimedelicten zijn veelal de ouderen slachtoffer, dit geldt ook voor Tech Support Scam.

Er is ook nagegaan of er een verband is tussen de leeftijdscategorieën en de verschillende sub-MO's. Hieruit is gebleken dat vooral ouderen met de leeftijd vanaf 60 jaar meer te maken krijgen met pop-up berichten dan in de andere leeftijdscategorieën.

Er geldt voor beiden dat op basis van de uitgevoerde werkzaamheden voor dit project niet onderzocht is wat hier de achterliggende reden van is. Een mogelijke verklaring is de onbekendheid vanaf deze leeftijd met de gevaren van het internet. Echter het voert voor deze rapportage te ver door, om hier dieper op in te gaan. Er is ten tijde van dit samenwerkingsverband bewust gekozen om in te zetten op actiegericht maatregelen en minder op diepgaand onderzoek.



Social engineering⁴

Daders van de Tech Support Scam maken gebruik van 'social engineering', waarmee het 'slagen' van het delict kan worden verklaard. Social engineering is een aanvalstechniek waarbij getracht wordt via **misleiding** en **overtuiging** toegang te krijgen tot systemen en vertrouwelijke gegevens van personen, en hen actief deel te laten nemen aan het delict (Bullée et al, 2018⁵). De fraudeurs misleiden hun slachtoffers door zich voor te doen als iemand anders. Zij nemen bijvoorbeeld de identiteit van helpdeskmedewerker, technicus of

⁴ Verdiepende analyse Tech Support Scam, Jildau Borwell en Kirsten Bos-Riepma

⁵ Bullée, J., Montoya, L., Junger, M. & Hartel. P. (2018). Het succes van social engineering. Tijdschrift voor Veiligheid, 1-2, 40-53.

security-expert aan; rollen die door mensen over het algemeen worden vertrouwd. Daardoor wordt de kans dat het slachtoffer meegaat met het verhaal van de fraudeur vergroot.

Uit opgenomen beelden blijkt dat slachtoffers diverse opdrachten moeten uitvoeren, de beller ook door de computer heen zoekt en tegelijkertijd de beller kalm doorpraat. Opmerkelijk is dat het slachtoffer meerdere malen de code voor het internetbankieren in moet toetsen, maar zich door die vele handelingen hier zich nauwelijks bewust van is. Stajano & Wilson beschreven dit in 2009 als volgt⁶: Op het moment dat mensen afgeleid worden door bepaalde zaken en zich hierop focussen, kan er van alles om hen heen plaatsvinden zonder dat zij dit door hebben. Mensen focussen zich op wat voor hen het meest interessant is en op wat de meest belangrijke actie lijkt te zijn. Dit betekent ook dat hierop gestuurd kan worden door de fraudeurs.

Conclusie

Met de daling van de schadebedragen is de belangrijkste doelstelling van de Intentieverklaring gehaald⁷. De ongecontroleerde groei van het fenomeen in Nederland is staande gebracht. Het aantal slachtoffers is op een stabiel niveau. De gemiddelde schade per slachtoffer is in deze periode ruimschoots gehalveerd.

Er is in samenwerking met de diverse partners gebouwd aan een betere informatiepositie. Hierdoor konden ontwikkelingen en trends sneller worden gesignaleerd om vervolgens waar mogelijk interventies en barrières op te tuigen.

Echter een winstwaarschuwing is dat in het 2^e kwartaal 2020 er sprake is van een stijging van het aantal registraties en de schadebedragen. Ook Nederlandsprekende helpdesks in relatie tot Tech Support Scam lijken toe te nemen. Dit impliceert dat met de toenemende digitalisering, deze vorm van cybercrime niet uit te bannen valt en zich blijft ontwikkelen.

Omdat vooralsnog strafrechtelijk onderzoek complex is door onder andere de internationale component, is de vervolging van daders nauwelijks mogelijk. De kansen in de aanpak aangaande Tech Support Scam is dan vooral het opwerpen van barrières in de techniek en in preventieve maatregelen voor het slachtoffers in Nederland. Echter zal wel ingezet moeten blijven worden op verbinding met India omdat dit land nog steeds een grote rol lijkt te spelen bij deze criminaliteitsvorm.

Met de huidige partners van de Intentieverklaring zijn de meest haalbare interventies beproefd en zo mogelijk in gang gezet. Dat betekent dat verlenging van de Intentieverklaring om die reden niet nodig is. Echter hebben de deelnemers laten weten het opgebouwde netwerk zeer te waarderen. Dit partnerschap blijft ook voor de toekomst zeer waardevol en niet alleen voor de aanpak van Tech Support Scam, maar ook voor andere cybercrimedelicten. Dit partnerschap kan bijvoorbeeld van belang zijn bij de aanpak van bankhelpdeskfraude, vriend-in-nood-fraude, of betaalverzoekfraude.

⁶ Stajano, F. & Wilson, P. (2009). *Understanding scam victims: seven principles for systems security*. Cambridge: University of Cambridge.

⁷ Volgens de Intentieverklaring is de belangrijkste doelstelling van het project 'Dat de Partijen ten doel hebben om de Tech Support Fraude in zijn huidige gevaarlijke vorm, in Nederland te hebben uitgebannen uiterlijk per einde 2020.