Tech Support Scam Schade en RATs

04 januari 2018

Inhoudsopgave

Overzicht

Aanleiding:
Deze analyse wordt uitgevoerd om de brede coalitie ter verstoring van Tech Support Scams (TSS) in Nederland te ondersteunen. De vraag is om over de TSS (voorheen Microsoftfraude) het volgende in kaart te brengen: 1) Hoe groot is de financiële schade (bij benadering) en 2) Welke Remote Access Tools (RATs) worden gebruikt en hoe vaak.

Methode:
Voor het beantwoorden van deze vragen is het noodzakelijk om registraties (aangiften plus meldingen) door te nemen en te scoren op de gewenste kenmerken. Dit zijn financiële schadebedragen van de slachtoffers en gebruikte Remote Access Tools (RAT). Aangezien het om een groot aantal registraties gaat en het teveel tijd en capaciteit vergt om alle registraties door te nemen, is een aantal maanden uit 2017 geselecteerd, namelijk februari, juni en oktober. De registraties zijn verspreid over het jaar en omvatten ongeveer een derde van het totaal aantal registraties. Een voordeel van deze spreiding is dat eventuele veranderingen in modus operandi of schadebedragen gedurende het jaar kunnen worden waargenomen. Daarnaast zijn de aantallen groot genoeg om een redelijk betrouwbare schatting van de totale schade over het hele jaar te maken.

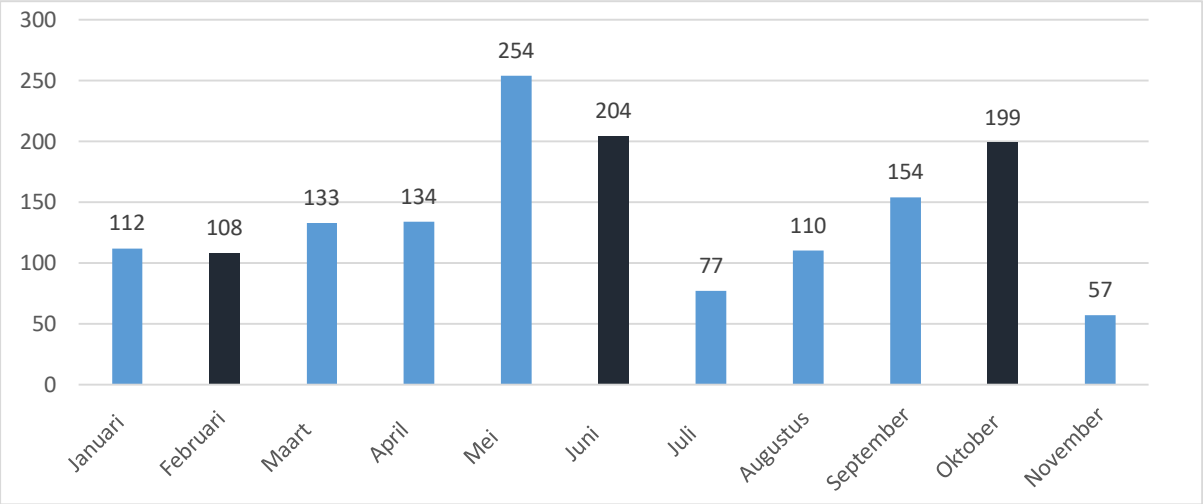
Uitkomst:
De opgetelde schade op basis van de registraties over drie maanden is iets meer dan 1,5 miljoen euro. Gemiddeld zijn de slachtoffers ongeveer 4000 euro kwijtgeraakt. Wanneer we een en ander extrapoleren naar alle registraties over 2017, dan komt de financiële schade uit op meer dan 5 miljoen euro. Over de gebruikte RATs komt naar voren dat vooral Teamviewer wordt gebruikt en andere RATs nagenoeg geen rol spelen.

Leeswijzer:
Dit rapport bestaat uit vijf korte hoofdstukken. In het eerste hoofdstuk wordt de achtergrond en nauwkeurigheid van de query beschreven, die voor de TSS is ontwikkeld. In de twee daaropvolgende hoofdstukken wordt ingegaan op de twee vragen, specifiek de schade bij de slachtoffers (hst. 2) en het gebruik van Remote Access Tools (hst. 3). In hoofdstuk 4 is aandacht voor de beperkingen van de resultaten. In het laatste hoofdstuk wordt een aantal opvallende zaken belicht en is aandacht voor een mogelijk nieuw opkomende modus operandi.

1. Achtergrond

Het fenomeen TSS wordt, zoals veel vormen van cybercrime, niet apart geregistreerd in de politiesystemen, maar komt terug in verschillende Maatschappelijke Klassen (MKs). Om inzicht hierin te krijgen, is een query ontwikkeld die de benodigde registraties naar boven haalt. Deze query is het uitgangspunt voor het beeld in dit rapport.

In 2017 zijn (tot half november) in totaal 1542 registraties uit de TSS-query naar voren gekomen. Ten behoeve van de analyse zijn de maanden februari, juni en oktober doorgenomen en gescoord. Dit zijn in totaal 511 registraties; ongeveer een derde van het totaal in 2017.



Op basis van deze analyse kan een uitspraak worden gedaan over de nauwkeurigheid van de ontwikkelde query. Een totaal van 458 registraties (van de 511) blijkt daadwerkelijk TSS te betreffen en dat is bijna 90%. Wanneer het geen TSS betreft, is het in de meeste gevallen (44) een andere vorm van (cyber)criminaliteit, onder andere fraude via Marktplaats, phishing of creditcardfraude. Deze vormen komen naar boven omdat in de query termen worden gebruikt die ook voorkomen in deze registraties. Tot slot is in de overige gevallen (9) sprake van dubbele registraties of is niet duidelijk waar de registratie betrekking op heeft. De query is daarom behoorlijk nauwkeurig te noemen.

TSS	Aantal	Percentage
Ja	458	89,6
Nee	44	8,6
Onbekend of dubbel	9	1,8
Totaal	511	100

In het vervolg zullen we ingaan op de twee gestelde vragen en gebruiken daarvoor de 458 registraties die betrekking hebben op TSS.

2. Schade

De 458 registraties over TSS zijn onderzocht op schade voor de slachtoffers. Er is sprake van schade wanneer geld is overgemaakt aan de fraudeur, dat niet of slechts gedeeltelijk is teruggekomen bij de aangever. In 386 van de 458 gevallen (84 procent) blijkt de aangever schade te hebben geleden.

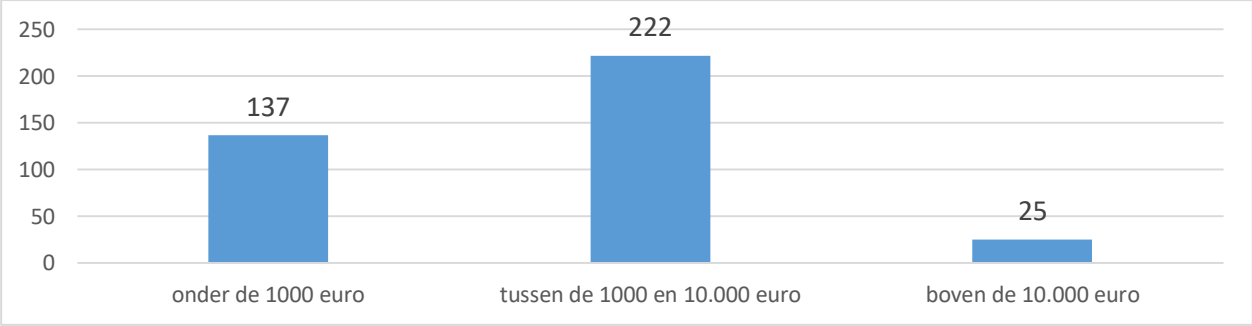
	Aangifte		
Schade	Ja	Nee	Totaal
Ja	381	5	386
Nee	48	24	72
Totaal	429	29	458

In totaal 72 aangevers hadden geen schade. Dit zijn gevallen waarin geen geld is overgemaakt, de aangever geen schade heeft geleden, betalingen zijn geblokkeerd voor versturen of het totale bedrag is teruggestort aan het slachtoffer. Van alle TSS-registraties betreft 94% een aangifte. Dit loopt zelfs op tot 99% de gevallen waarin financiële schade is geleden.

Schadebedragen
Van de 386 gevallen met schade, is bij twee aangevers wel schade geleden, maar was (nog) geen informatie over het bedrag dat is buitgemaakt. Daarom gaan we in deze analyse uit van 384 gevallen met schade.

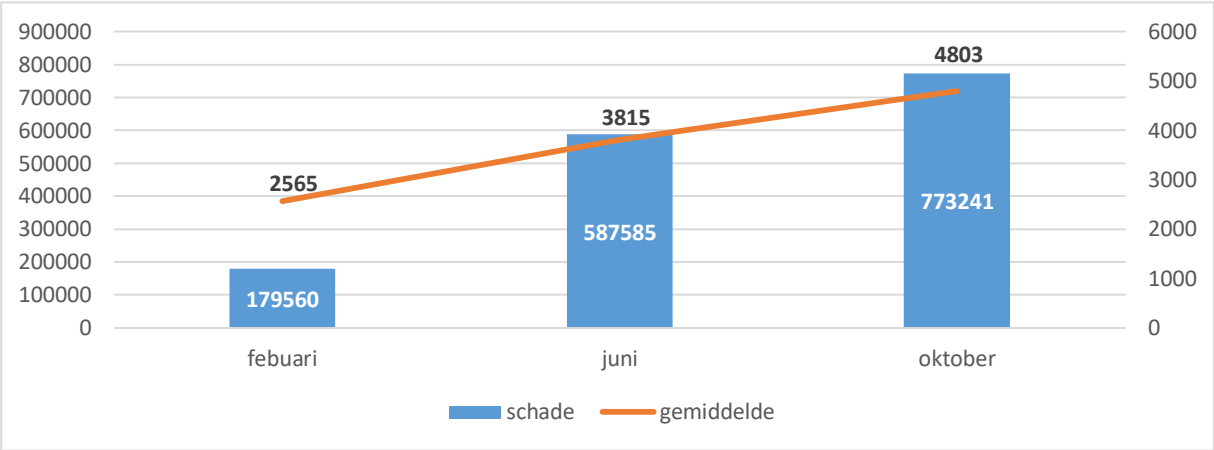
De schadebedragen blijken zeer uiteen te lopen. In ongeveer 10% van de gevallen (38 van de 384 registraties) wordt 250 euro of minder buitgemaakt. Het laagste schadebedrag is 50 euro. Aan de andere kant van het schadespectrum zien we extreme gevallen, waarin drie slachtoffers rond de 50.000 euro zijn kwijtgeraakt.

Wanneer we de registraties in drie grove categorieën verdelen, dan zien we dat in 58% van de registraties de schadebedragen variëren tussen 1000 en 10.000 euro. In 137 van de 384 registraties (36%) betreft de schade minder dan 1000 euro. In slechts 6,5 % van de registraties is meer dan 10.000 euro betaald.



Trend
Naast een groot verschil tussen de minimum - en maximumschade, komt uit de data ook een trend naar voren. Op basis van de maanden die zijn gescoord, lijken zowel de gemiddelde als de totale buitgemaakte bedragen te stijgen gedurende 2017. Was in februari de gemiddelde schade nog 2565 euro. In de maanden juni en oktober steeg dit naar respectievelijk 3815 en 4803 euro.

Omdat het slechts om drie maanden gaat en daarom toeval (als gevolg van de gemaakte selectie) niet kan worden uitgesloten, is het monitoren hiervan noodzakelijk om te zien of deze trend in de toekomst doorzet.



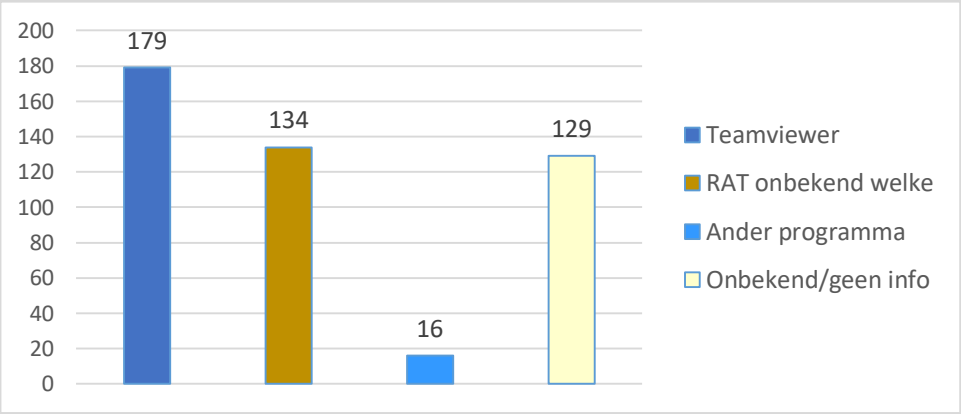
Totale schade
Bij 384 van de 386 slachtoffers is een schadebedrag vastgesteld en dit leverde in totaal 1.540.386 euro schade op, dat is gemiddeld 4000 euro per slachtoffer.

Voor een schatting van de totale schade extrapoleren we deze bedragen naar alle TSS-slachtoffers in 2017. Uitgangspunt zijn alle registraties die met de TSS-query naar boven komen (1542). Bij eenzelfde nauwkeurigheid van de query (89,6%) en het percentage betalende slachtoffers (84%), komen we uit op een totaal van 1168 slachtoffers die schade hebben geleden. De totale schade wordt dan geschat op 4.672.000 euro en dat is berekend tot en met half november. Wanneer we de laatste anderhalve maand zouden meenemen, komt de totale schade in 2017 waarschijnlijk boven de 5 miljoen euro uit.

De schade die hierin niet is meegenomen, zijn de kosten die de slachtoffers hebben gemaakt voor het opschonen en herstellen van hun computer en daarnaast iTunes-kaarten of Steam Cards waarmee de slachtoffers zijn blijven zitten, omdat de codes niet zijn doorgegeven. Kaarten worden niet altijd teruggenomen door de verkopende partij. Hoewel de kaarten een waarde vertegenwoordigen, kunnen de slachtoffers deze alleen inwisselen voor online aankopen en niet voor contant geld. Een deel hiervan zou ook als schade beschouwd kunnen worden.

3. Remote Access Tools

De 458 registraties die over TSS gaan, zijn ook onderzocht op het gebruik van een Remote Access Tool (RAT). Meestal wordt hiervan gebruik gemaakt, hoewel dit niet altijd duidelijk naar voren komt. Dit is in 129 gevallen niet duidelijk, maar het is wel aannemelijk dat in een deel daarvan ook een RAT is gebruikt. Van de overige 329 registraties is in 134 gevallen sprake van een RAT, maar wordt niet gespecificeerd welke. In de meeste gevallen wordt het gebruik van de RAT indirect opgemaakt uit de aangifte. Dit kan bijvoorbeeld gebeuren op basis van de volgende zinsneden: “De computer werd nadien op afstand overgenomen”, “Op dat moment zag ik dat hij de controle had over mijn computer”, “Hij wees met de cursor zaken aan op mijn pc die mogelijk besmet zouden zijn” of “Ik heb toen via mijn computer toestemming gegeven aan deze man om in mijn computer te kunnen kijken”. In minder dan de helft van de registraties wordt de RAT bij naam genoemd, in totaal 196 keer. In meer dan 90 procent van de gevallen (179) betreft het dan Teamviewer.



In slechts 16 gevallen is een ander programma dan Teamviewer genoemd en de tekst in de registraties suggereerde dat het om een RAT ging. Dat waren Anydesk (3 maal), Showmypc (2), Microsoft Remote Desktop Assistent, PClink, Re-image Repair, (Micro) Event Viewer (2), TshareII. Van de eerste drie programma’s is duidelijk dat het een RAT betreft, maar van de andere is dat onduidelijk of werd het voor andere doeleinden gebruikt door de fraudeurs. Overigens moet worden vermeld dat in een aantal van deze 16 registraties ook Teamviewer naar voren komt.

Samengevat is Teamviewer de meest voorkomende RAT (179) en volgt op afstand Anydesk met drie registraties. Hierbij tekenen we aan dat in veel gevallen niet duidelijk is welke RAT is gebruikt. Het is zeer waarschijnlijk dat deze verdeling ook van toepassing is op de categorie *RAT onbekend welke*. De conclusie is daarom dat buiten Teamviewer andere RATs nagenoeg geen rol spelen.

4. Beperkingen resultaten

De analyse die we uitgevoerd hebben, kent een aantal beperkingen. Dit speelt vooral bij het vaststellen van de schadebedragen, dat soms door een aantal zaken is bemoeilijkt:

- In de registratie worden overboekingen genoemd, waarbij niet altijd duidelijk is geformuleerd welke bedragen (definitief) zijn buitgemaakt en welke niet. Soms is gemeld dat het bedrag waarschijnlijk wordt teruggestort, maar dat is op het moment van de registratie nog niet gebeurd. De uiteindelijke schade is dan moeilijk te bepalen.

- Verschillende registraties lopen in elkaar over waardoor dubbeltelling mogelijk is. Een voorbeeld is het afschrijven van bedragen van de bankrekening van het ene slachtoffer naar de rekening van een ander slachtoffer. Daarbij wordt de laatste overgehaald om de fraudeurs met iTunes-kaarten te betalen. In zo'n geval wordt via de rekening van het tweede slachtoffer geld van meerdere slachtoffers doorgesluisd naar de fraudeurs. Dit kan leiden tot het dubbeltellen van schadebedragen, maar is niet altijd te voorkomen aangezien in de aangifte niet altijd voldoende informatie aanwezig is.

Getracht is om de invloed hiervan zoveel mogelijk te beperken. Bij de eerste beperking is deze schade meegeteld en bij de tweede zijn (indien dit werd opgemerkt) de dubbeltellingen ongedaan gemaakt. Omdat het om een gering aantal gaat, is de invloed op de (geschatte) schadebedragen waarschijnlijk klein.

5. Opvallende zaken

Tijdens het doornemen van de registraties zagen we geregeld opvallende zaken naar voren komen. Een aantal wordt hierna beschreven. Hoewel ze niet bijdragen aan de beantwoording van de vragen, geven ze wel een completer beeld van de modus operandi.

Werkwijze criminelen:

- Om de schade bij de slachtoffers te maximaliseren, hebben de fraudeurs in veel gevallen de daglimieten bij de banken verhoogd.
- De fraudeurs zijn hun slachtoffers vaak 'behulpzaam' met het vinden van de lokale Jumbo, Albert Heijn, Primera of andere nabije locatie waar iTunes-kaarten bemachtigd kunnen worden.
- Een groot deel van de betalingen vindt plaats via iDEAL (zeker 103 registraties). In deze registraties zijn bijna altijd bij verschillende bedrijven tegoedkaarten online aangekocht. De betalingen worden overgemaakt naar de rekeningen van een beperkt aantal bedrijven: HEMA, Alpha Com Digital Commerce, Primera, Stichting Derdengelden Buckaroo, KorsIT, Pay.nl en Top Up BV. De tegoedkaarten (Gift Cards) die worden aangekocht zijn vooral iTunes-kaarten, maar daarnaast ook Steam Cards en beltegoed. Hoewel het afzonderlijk om relatief kleine bedragen (vaak 300 euro) gaat, zien we door het totaal aantal transacties en aangekochte kaarten het schadebedrag flink oplopen. In twee gevallen ging het om meer dan 100 betalingen via iDEAL, wat leidde tot schadebedragen van enkele tienduizenden euro's.
- De schadebedragen worden regelmatig naar buitenlandse rekeningen overgemaakt, waarbij Groot-Brittannië eruit springt met minstens 19 registraties. Het gaat dan om relatief hoge bedragen, die meestal per transactie net onder de 5000 euro blijven.
  Daarnaast zijn Roemenië, Duitsland en Portugal een aantal keren genoemd als landen waar bedragen naar zijn overgemaakt.

De slachtoffers:

Op basis van de registraties is ook gekeken naar de gemiddelde leeftijd en bijna 70% van de slachtoffers is ouder dan 50 jaar. In een behoorlijk aantal gevallen ontdekten ze tijdig dat ze opgelicht werden en kon de schade beperkt blijven. Regelmatig werden slachtoffers gewaarschuwd door anderen, zoals hun partner of ander familielid, een buurman of medewerkers van winkels waar ze tegoedkaarten probeerden te kopen. Tot slot is in veel gevallen meer schade voorkomen, doordat banken de rekening hadden geblokkeerd of contact opnamen met het slachtoffer.

De banken:

- De banken kunnen het overgemaakte geld meestal niet meer terughalen of terugstorten.
- Vaak adviseren de banken om aangifte te doen.
- Veel slachtoffers overleggen bankafschriften en daarom is er weinig reden om aan de schadebedragen te twijfelen (behoudens als gevolg van de al genoemde beperkingen).

Nieuwe modus operandi:

We zagen bij een aantal recente registraties opvallende afwijkingen van de modus operandi en dan vooral in de wijze van benaderen en betalen:
Slachtoffers krijgen op hun computer een pop-up scherm te zien die zij niet weg kunnen klikken. Op het scherm staat een melding dat *ransomware* op de computer is geïnstalleerd en wordt een (vals) telefoonnummer van Microsoft getoond. Wanneer zij dit nummer bellen, vindt de gebruikelijke modus operandi plaats waarbij onder andere de computer wordt overgenomen. Opvallend is de wijze waarop de betalingen plaatsvinden, namelijk via PayPal waar de creditcard of bankrekening van de slachtoffers aan zijn gekoppeld. In deze casussen hadden de slachtoffers nog geen PayPal account, deze is door de fraudeurs aangemaakt. Vervolgens wordt via iDEAL het PayPal account opgewaardeerd. Omdat we dit in de laatste maand zagen (oktober 2017), wijst het misschien op een nieuwe trend. Op dit moment zijn de bedragen die worden buitgemaakt nog laag (100 en 250 euro) en is de schade van de slachtoffers

vergoed door de banken. Dit blijft wellicht niet zo en mogelijk wordt deze werkwijze de komende tijd geperfectioneerd en lukt het om meer schade te maken.