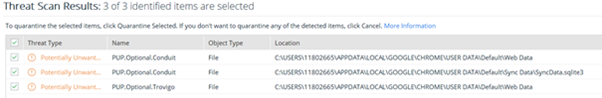
**Opdracht 3A Deel 1**

**3.2: Malwarebytes**

Bij 3 van de toestellen werd er geen malware aangetroffen. Bij 1 van de 4 toestellen werden er 3 unwanted programs aangetroffen:



De eerste 2 zijn geclassificeerd met .Conduit, dit betekent dat deze bestanden geen virus of malware zijn, maar gewoon bestanden met een slechte reputatie of slecht gedrag. Deze ‘programma’s’ zijn meestal geïnstalleerd zonder weten van de eigenaar van het toestel.

Het bestand met de .Trovigo mark is een bestand wat je standaardbrowser gaat aanpassen, maar dus niet per-sé schadelijk is voor je computer.

In MalwareBytes staan deze bestanden niet automatisch op om te verwijderen na een scan, maar dit is wel advised.

**3.3: Malicious Javascript Code**

Het script zal onderstaande website openen, dit script is ‘onnodig’ ingewikkeld gemaakt in een poging om het te encrypteren.

http://enjoyyourhaircut.com/5.html

**3.4: Confusion Matrix**

**False positive**

Een false positive, of languit een false positive error, gebeurt wanneer er wordt aangegeven dat een bepaalde conditie voldaan is, terwijl het in werkelijkheid niet zo is. Dit geval wordt ook een “false alarm” of vals alarm genoemd. Een false positive error is een type I error, waarbij de test bestaat uit 1 conditie en deze onterecht als “waar” wordt beschouwd. Ook is het belangrijk een onderscheid te maken tussen het foutenfrequentie en de waarschijnlijkheid dat er een fout plaatsvindt. Het laatstgenoemde staat bekend als een false positive risk.

**False negative**

Een false negative, of languit een false negative error, gebeurd wanneer er wordt aangegeven dat een bepaalde conditie er niet is, terwijl het in werkelijkheid er wel is. Een duidelijk voorbeeld hiervan is bijvoorbeeld een zwangerschapstest die aanduidt dat een vrouw niet zwanger is, terwijl ze in werkelijkheid wel zwanger is. Een false negative error is een type II error, waarbij de test bestaat uit 1 conditie en deze foutief resultaat geeft dat die conditie afwezig is.

**True positive**

Een true positive neemt plaats wanneer er aangegeven wordt dat een bepaalde conditie aanwezig is, en deze er in werkelijkheid ook is. Dit wilt zeggen dat het systeem goed zijn werk heeft gedaan en de test juist is verlopen. Een voorbeeld hiervan is dat een thermostaat aangeeft dat een persoon koorts heeft en de persoon ook echt koorts heeft.

**True negative**

Een true negative neemt plaats wanneer er aangegeven wordt dat een bepaalde conditie afwezig is, en deze in werkelijkheid ook afwezig is. Een voorbeeld hiervan is een zwangerschapstest die aangeeft dat de vrouw niet zwanger is, en dat deze test ook correct is.

**3.5: CC Cleaner Infectie**

Een bepaalde versie van CCleaner is aangetast en geïnfecteerd met een trojan met als resultaat dat er meerdere multi-stage backdoors worden geïnstalleerd die in staat zijn instructies te verwerken van de threat actors op de aangetaste systemen. De betreffende versies zijn version 5.33.6162 en Cloud version 1.07.3191. Het verdelen van de aangetaste versies van CCleaner kwamen van de reële website Piriform. De Threat actors waren in staat de CCleaner binary aan te tasten met de trojan. Hierdoor konden de Threat actors het trojan efficiënt verdelen naar de computers. Omdat de versie van een legitieme bron kwam zou het bijna onmogelijk zijn door de gebruikers om er achter te komen dat ze een ‘slechte’ versie hebben gedownload.

De websites die ik getest heb:

Instagram.com -> safe

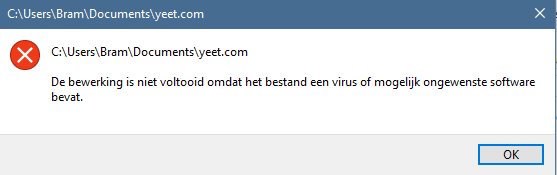
G2A.com -> safe

Wikipedia.org -> safe

Spotify.com -> safe

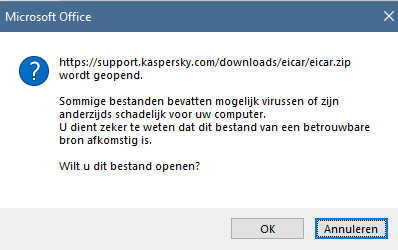
**3.6: Antivirus**

Bij het openen van het bestand vermeld in de opgave wordt de volgende pop up getoond.



Direct na de pop up werd het bestand zelf ook gedelete. Dit was zonder extra antivirus dus gewoon met windows defender.

Dit wilt dus zeggen dat de anti virus tussenbeide komt en het bestand zelfs delete.



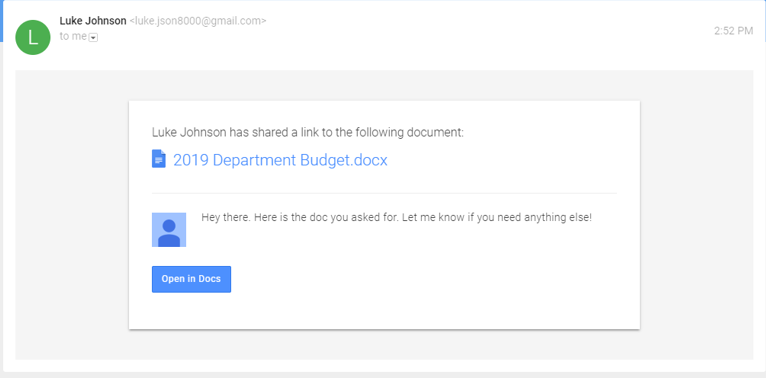
Meteen bij het klikken op de link in de opgave, werd er al een melding weergegeven. De download was nog niet begonnen en de anti virus gaf al een waarschuwing dat er mogelijk een virus was.

Tijdsraming

|  |  |  |  |
| --- | --- | --- | --- |
| Naam | Opdrachten | Tijd per opdracht | Totaal |
| Bram | 3.6 | 1 uur | 1 uur |
| Vincent | 3.4, 3.5 | 30 min, 30 min | 1 uur |
| Vicky | 3.3, opmaak,  Nakijken | 45 min,  30 min,  15 min | 1.30 uur |
| Igor | 3.3, nakijken | 45 min,  15 min | 1 uur |

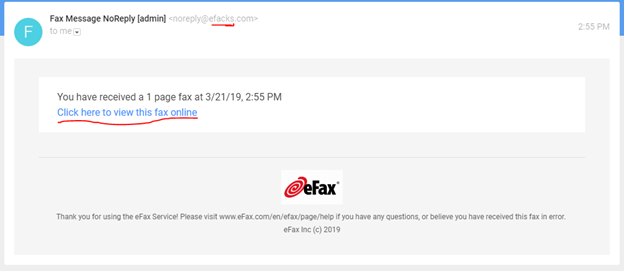
Opdracht 3A Deel 2

**3.7: Phishing Quiz**

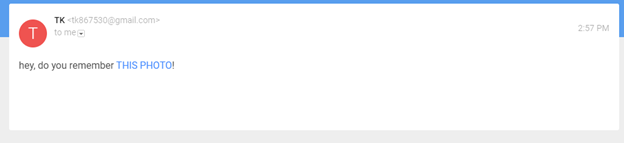


Link verwijst naar een phishing adres.

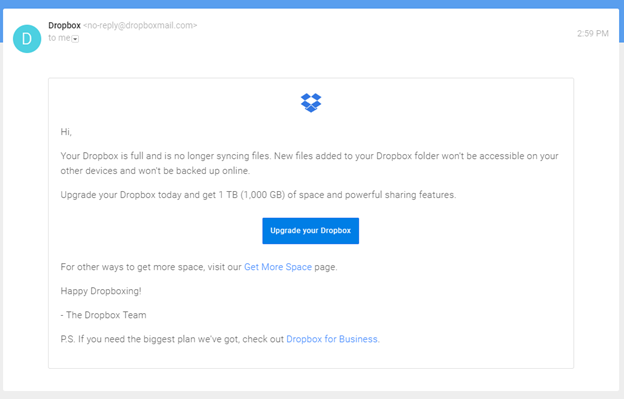




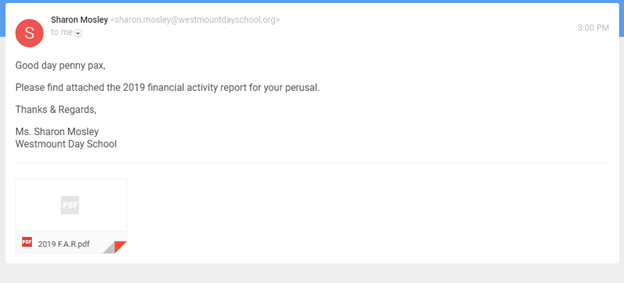
Daarnaast eindigt het mailadres op efaCKS ipv eFax zoals het bedrijf heet.



Raar mailadres, maar de link en inhoud van de mail zijn zeer onpersoonlijk.

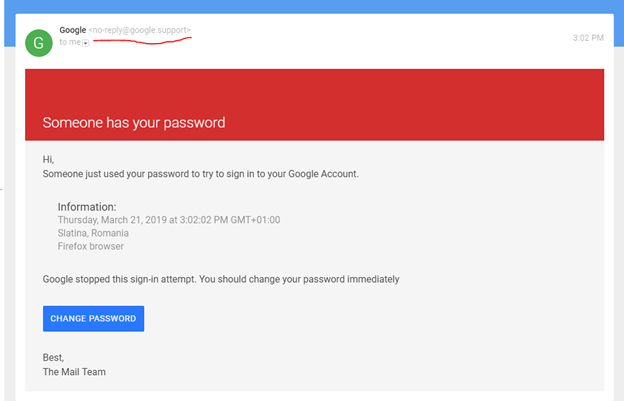


Dit is geen phishing mail, alle links zijn van dropbox.



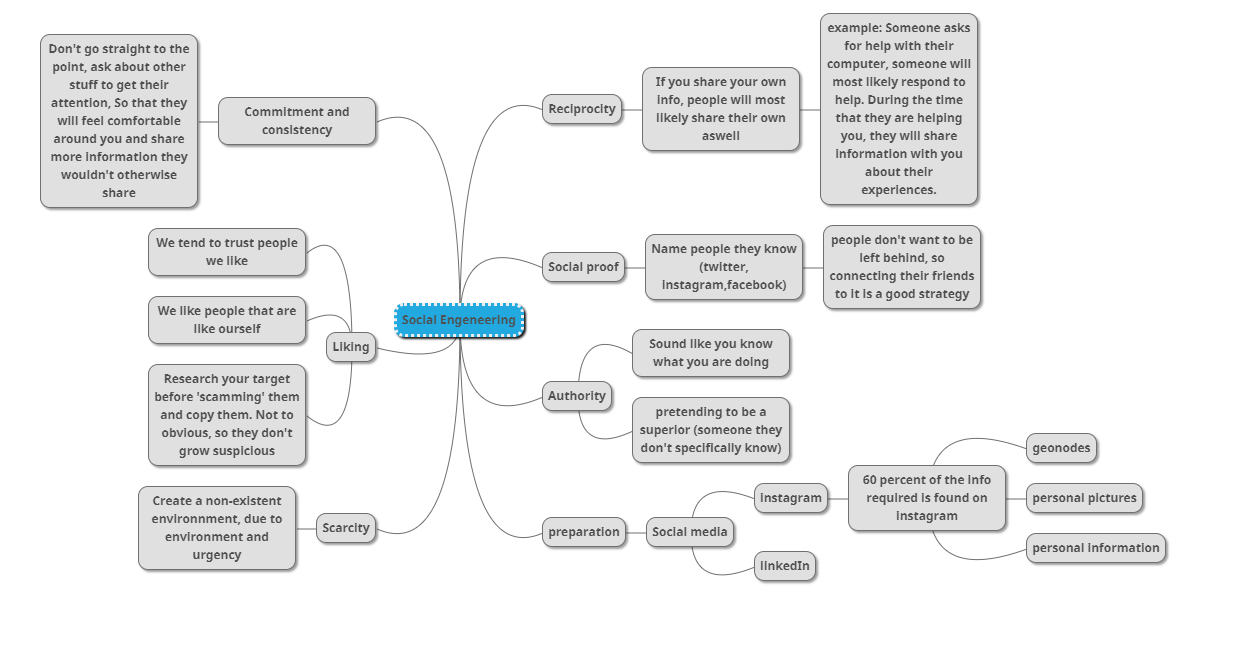
De PDF bevat waarschijnlijk een virus.





Mailadres eindigt op .support, de link verwijst naar, opnieuw een goed leesbare foto ervan, een kopie van google.com met een adres achter naar een phishing site.

**3.9: Social Engineering**



Example 1:

So jess, the one calling and pretending to be the victim’s wife, called the provider company whilst spoofing the victim’s number. She created a sense of urgency by having baby crying sounds playing and telling fake personal information. She asked if she could add their daughter to the account, to provoke the provider into saying she isn’t in there either. From here she uses a fake social security number and the victim’s girlfriend’s name, to create herself a new account. She even gets the support as far as changing the main password.

**Social proof:**

she had the victim’s name and spoofed his phone number.

**Liking:**

She was really kind and not pressuring and the baby in the back caused for understanding. She also told some fake personal info to get the support to like her.

**Authority:**

She convinces the support that she cant receive the code via text, cause she is currently calling. However, this is not true, but she said it in such a way that she convinced support.

**Urgency:**

She created an outside force pressing on her. ‘Her husband had to do this today, while she had a baby crying’ This makes us think that she is being pressured and make us help her quicker.

Social engineering chain:

1. Gathering information (social media)

2. Looking for exploitable apps

3. Call as authorization to confirm the exploitable app.

4. Tailor malware to avoid detection and plant it

How to defend against social engineering?

1. Be politely paranoid

2. Train staff to face clients

3. Use real world 2FA

4. 2FA

**HUMANS ARE YOUR FIRST LINE OF DEFENSE**

**3.10: Common Scams**

Man in the middle scams → phishing

Man in the middle scams zijn een vorm van phishing, specifieker is het een vorm van spear phishing omdat het meestal gericht is naar 1 persoon of bedrijf.

Warrant call → phishing

De Warrant call scam is ook een vorm van phishing, specifieker is het een vorm van Vishing, dit is omdat het meestal via telefoon is.

Begging with a purpose → social engineering

Begging with a purpose is social engineering omdat het inspeeld op het medeleven/emoties van de andere persoon.

**3.11**

Eerste deel van dit virus zoekt bestanden in de directory, als er 1 of meerdere bestanden aanwezig zijn, open dit bestand.

Daarna wordt er een kopie van dit virus gemaakt in het lokale geheugen.  
Het opgeslagen virus bestand van de temp wordt dan in het geopende bestand geplaatst, bestand wordt gesloten na dit proces.  
Herhaal dit proces met alle bestanden, wanneer alle bestanden geïnfecteerd zijn, wordt alles afgesloten.

Tijdsraming

|  |  |  |  |
| --- | --- | --- | --- |
| Naam | Opdracht | Tijd | Totaal |
| Igor | 3.7, 3.11 | 30 min, 1 uur | 1.30 uur |
| Vicky | 3.7, 3.11, opmaak, nakijken | 30 min, 1 uur, 15 min, 15 min | 2 uur |
| Bram | 3.9, nakijken | 1 uur, 15 min | 1 uur |
| Vincent | 3.10 | 30 min | 30 min |

Doorsturen documenten: Vicky