

VERTROUWELIJK



RAPPORTAGE THREADPHISH



ABONNEMENT INFORMATIE

Domein:

Aantal E-mail adressen:

1

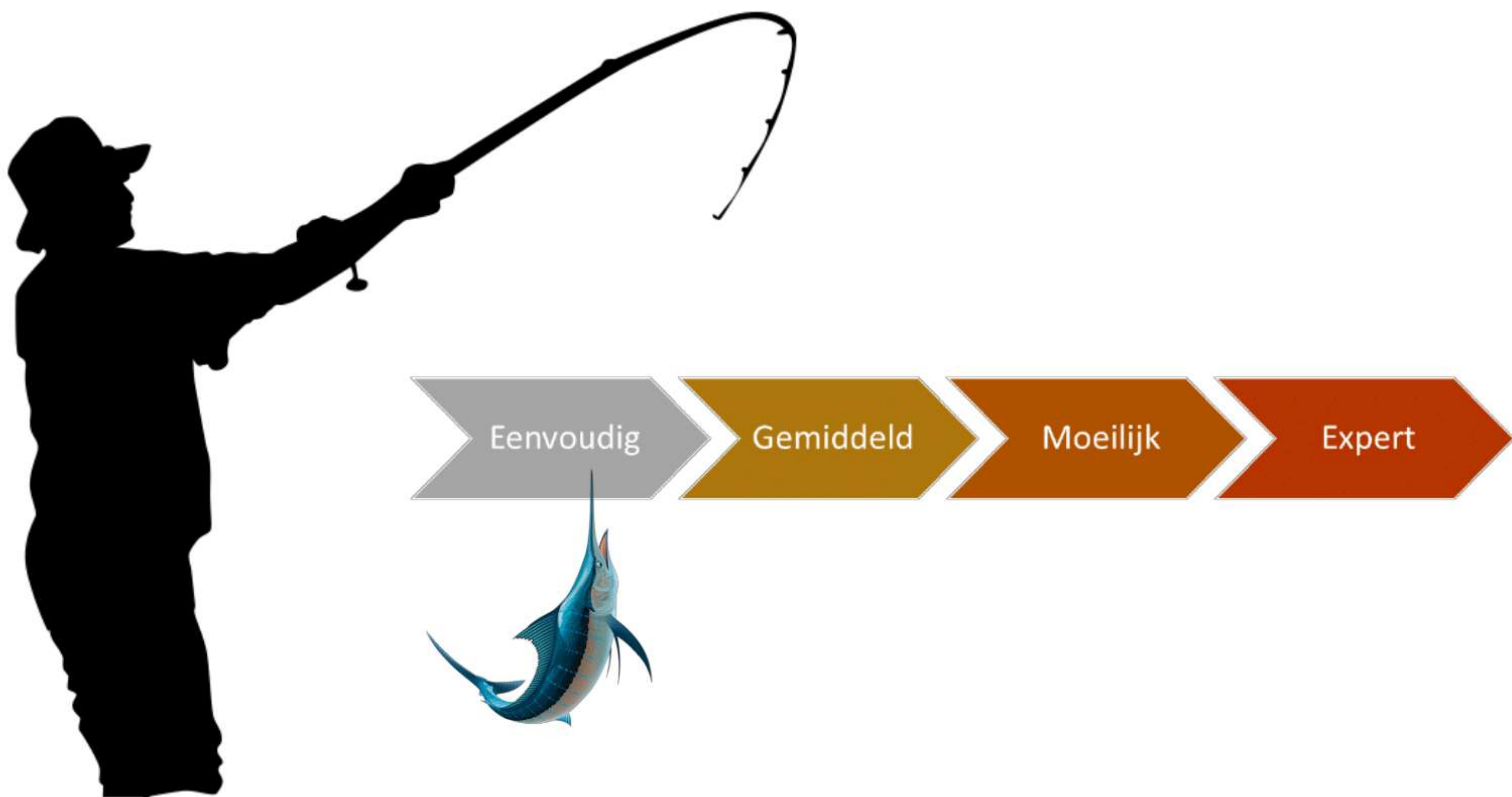
Datum rapportage:

07 januari 2020

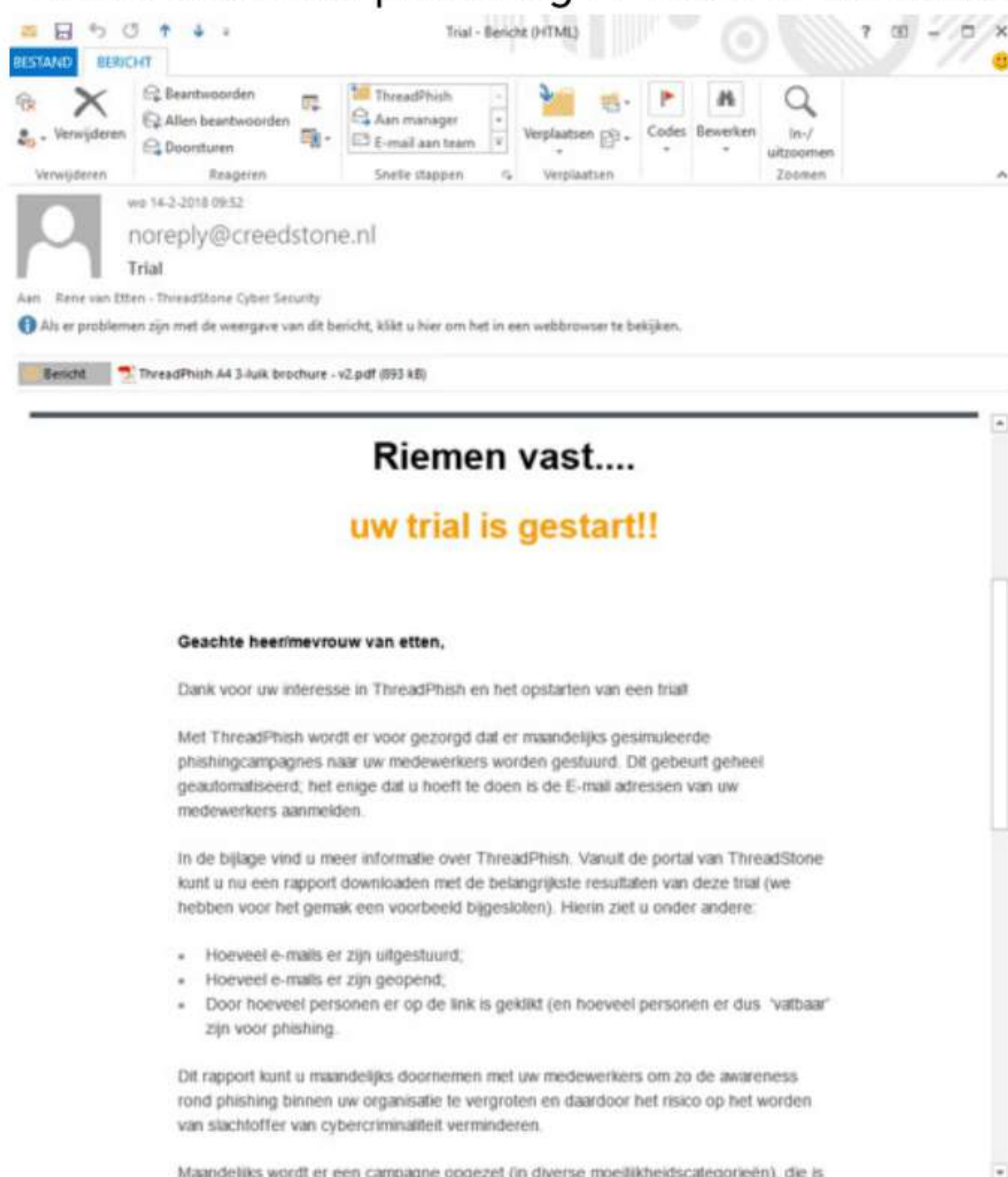


De phish

Deze maand is een phishingmail uitgestuurd met de volgende moeilijkheidsgraad:



Onderstaande phishing E-mail is verstuurd naar uw medewerkers:



Waaraan had u kunnen herkennen dat dit een phishing e-mail betreft?

- ▶ U heeft nog niet eerder gecommuniceerd met deze persoon en/of organisatie.
- ▶ De afzender gebruikt een domein dat veel lijkt op <www.threadstone.nl>, maar het is een ander <www.creedstone.nl>!
- ▶ In de E-mail zijn geen verkorte links opgenomen, bijvoorbeeld <http://bit.ly/1FEbbAJ> of <http://tinyurl.com/ohpkk2z>. Achter deze links kunnen eenvoudig phishing aanvallen schuil gaan.

Uw resultaten



Toelichting

Afgelopen maand is er 1 phishing simulatie E-mail verstuurd. Door 1 gebruiker is op de phishinglink geklikt. Deze gebruiker is vatbaar voor phishing.

Controle Have I been Pwned

Wij controleren de E-mail adressen die een phishing mail hebben ontvangen in de database van Have I Been Pwned. In deze database worden E-mail adressen bijgehouden die in het verleden zijn voorgekomen bij grotere hacks, datalekken etc. Voor meer informatie over Have I Been Pwned verwijzen we naar <https://haveibeenpwned.com> waar u ook direct andere (privé) E-mail adressen kunt controleren.

 **Let op! Onderstaande E-mail adressen komen voor in de database van Have I Been Pwned:**

Inbreuken op:

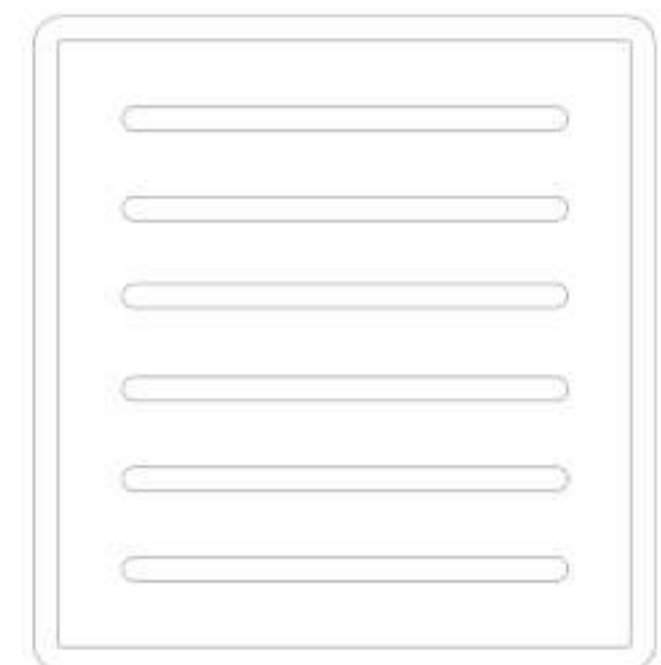
APOLLO

Apollo - In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.

Gaat over: E-mailadressen, Medewerkers, Geografische locaties, Functietitels, Namen, Telefoonnummers, Aanwinsten, Social media-profielen

Inbreuken op:

Data Enrichment Exposure From PDL Customer - In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.



Gaat over: E-mailadressen, Medewerkers, Geografische locaties, Functietitels, Namen, Telefoonnummers, Social media-profielen

Inbreuken op:

You've Been Scraped - In October and November 2018, security researcher Bob Diachenko identified several unprotected MongoDB instances believed to be hosted by a data aggregator. Containing a total of over 66M records, the owner of the data couldn't be identified but it is believed to have been scraped from LinkedIn hence the title "You've Been Scraped". The exposed records included names, both work and personal email addresses, job titles and links to the individuals' LinkedIn profiles.



Gaat over: E-mailadressen, Medewerkers, Geografische locaties, Functietitels, Namen, Social media-profielen

Ons advies

Spreek de resultaten van de test door met uw team/medewerkers. Door periodiek aandacht te geven aan dit phishing zullen uw medewerkers meer waakzaam worden en daarmee uw organisatie meer behoeden tegen cybercriminaliteit. Overigens maken we niet bekend wélke gebruikers op de phishingmails hebben geklikt. Het doel van de campagnes is om het algemene bewustzijn binnen de organisatie te vergroten; niet om individuen aan te wijzen die wel of niet geklikt hebben.

Have I been Pwned

Indien er E-mail adressen in de database van Have I been Powned voorkomen, dan adviseren we om de gebruikers van deze E-mail adressen hun wachtwoorden te laten wijzigen. Zeker als de gebruiker het wachtwoord ook op andere websites, applicaties of systemen gebruiken. Hackers die de beschikking hebben over de databestanden die Have I Been Powned gebruiken (maar dan inclusief wachtwoorden) zullen proberen om met de buitgemaakte gebruikersnaam en wachtwoord combinaties - veelal volledig geautomatiseerd - in te loggen op andere systemen, omdat ze weten dat veel gebruikers slechts één gebruikersnaam en wachtwoord gebruiken voor verschillende systemen.