

VERTROUWELIJK



RAPPORTAGE THREADPHISH



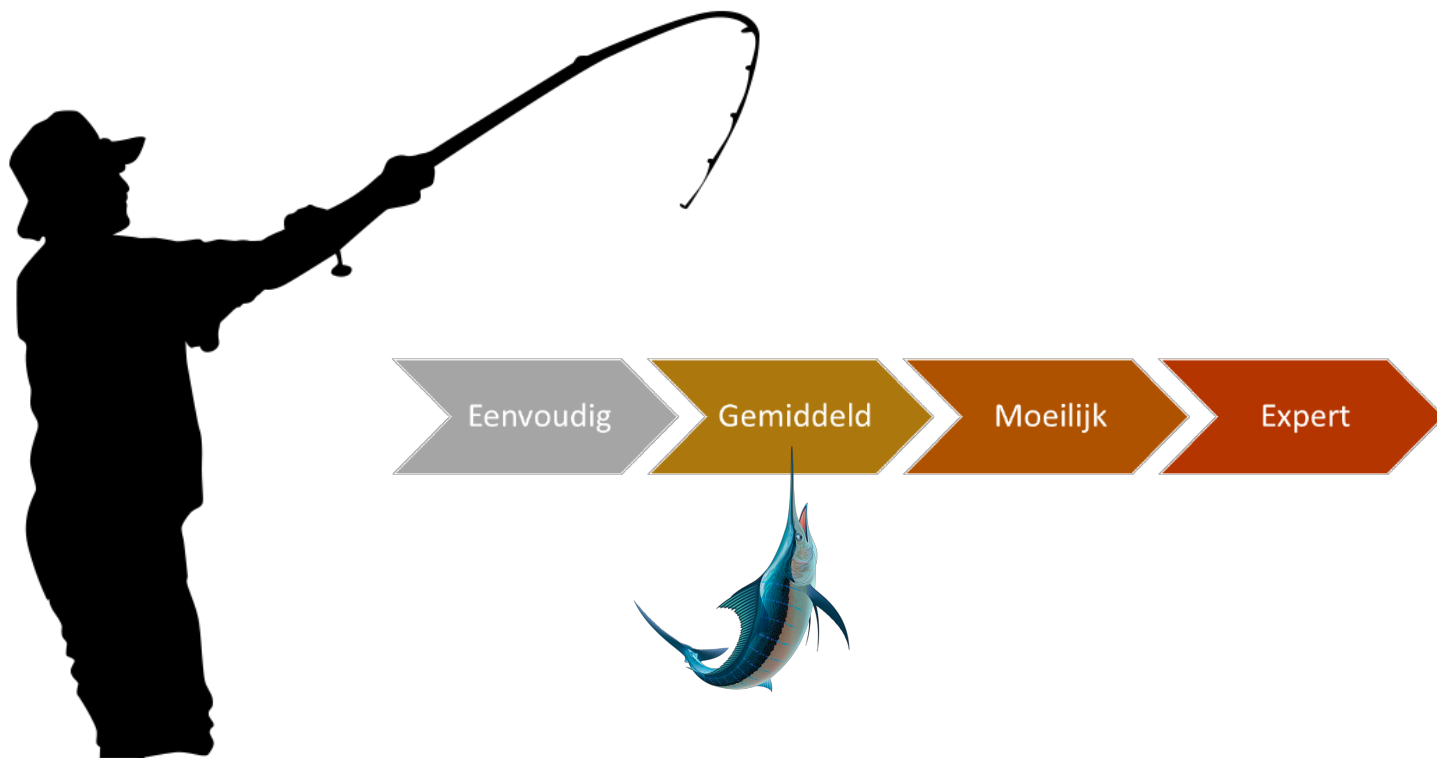
ABONNEMENT INFORMATIE

Naam Organisatie: ThreadStone proefklant
Aantal E-mail adressen: 100
Datum rapportage: 03 maart 2021



De phish

Deze maand is een phishingmail uitgestuurd met de volgende moeilijkheidsgraad:



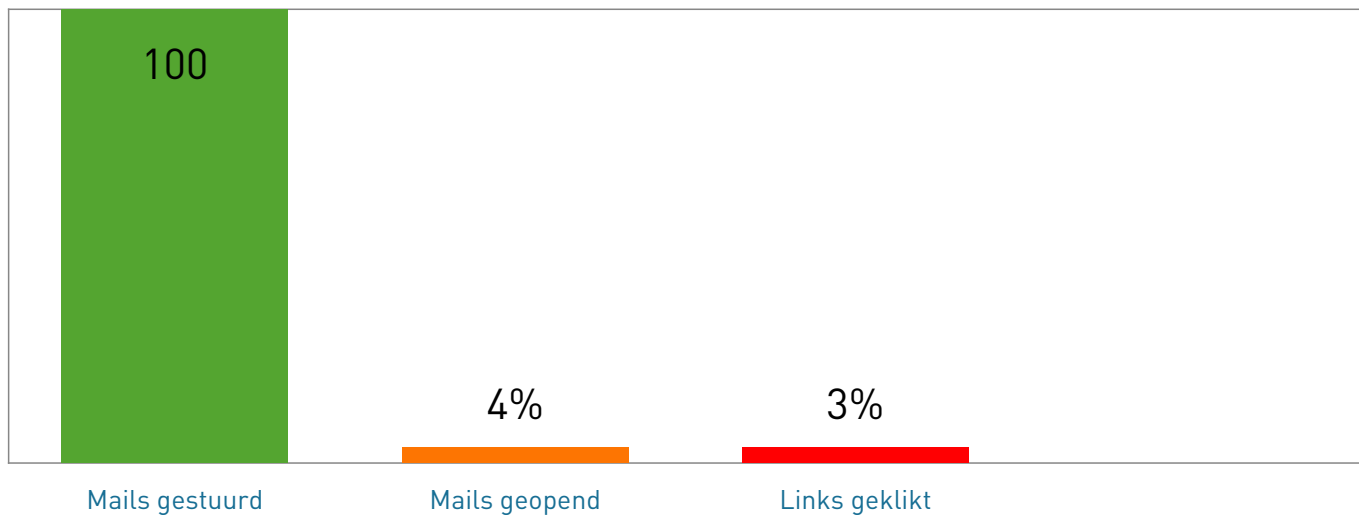
Onderstaande phishing E-mail is verstuurd naar uw medewerkers:



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

- ▶ De mail is gestuurd door een onbekende persoon/organisatie. Je hebt nog niet eerder met deze persoon of organisatie contact gehad.
- ▶ De mail wordt zonder vooraankondiging gestuurd uit naam van Arbodienst24, waarbij wordt aangegeven dat jouw werkgever hier een relatie mee heeft. Dit gebeurt zonder vooraankondiging van jouw werkgever. Als je twijfelt, vraag dan altijd bij je werkgever of dit klopt.
- ▶ De E-mail is verzonden op een tijdstip dat het in Nederland niet gebruikelijk is om E-mails te versturen. Wees extra waakzaam als u mails ontvangt die zijn verstuurd op een tijdstip dat dit voor u niet logisch is!

Uw resultaten




Toelichting

Afgelopen maand zijn er 100 phishing simulatie E-mails verstuurd. Daarvan zijn er bij 4 gebruikers de E-mail geopend. Door 3 gebruikers is op de phishinglink geklikt. Deze gebruikers zijn 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.

 Voor onderstaande E-mail adressen hebben we goed nieuws, zij komen niet voor in de database van Have I Been Pwned:

- DemoAccount50@threadstone.eu
- DemoAccount51@threadstone.eu
- DemoAccount52@threadstone.eu
- DemoAccount53@threadstone.eu
- DemoAccount54@threadstone.eu
- DemoAccount55@threadstone.eu
- DemoAccount56@threadstone.eu
- DemoAccount57@threadstone.eu
- DemoAccount58@threadstone.eu
- DemoAccount59@threadstone.eu
- DemoAccount60@threadstone.eu
- DemoAccount61@threadstone.eu
- DemoAccount62@threadstone.eu
- DemoAccount63@threadstone.eu
- DemoAccount64@threadstone.eu
- DemoAccount65@threadstone.eu
- DemoAccount66@threadstone.eu
- DemoAccount67@threadstone.eu
- DemoAccount68@threadstone.eu
- DemoAccount69@threadstone.eu
- DemoAccount70@threadstone.eu
- DemoAccount71@threadstone.eu
- DemoAccount72@threadstone.eu
- DemoAccount73@threadstone.eu
- DemoAccount74@threadstone.eu
- DemoAccount75@threadstone.eu

- DemoAccount76@threadstone.eu
- DemoAccount77@threadstone.eu
- DemoAccount78@threadstone.eu
- DemoAccount79@threadstone.eu
- DemoAccount80@threadstone.eu
- DemoAccount81@threadstone.eu
- DemoAccount82@threadstone.eu
- DemoAccount83@threadstone.eu
- DemoAccount84@threadstone.eu
- DemoAccount85@threadstone.eu
- DemoAccount86@threadstone.eu
- DemoAccount87@threadstone.eu
- DemoAccount88@threadstone.eu
- DemoAccount89@threadstone.eu
- DemoAccount90@threadstone.eu
- DemoAccount91@threadstone.eu
- DemoAccount92@threadstone.eu
- DemoAccount93@threadstone.eu
- DemoAccount94@threadstone.eu
- DemoAccount95@threadstone.eu
- DemoAccount96@threadstone.eu
- DemoAccount97@threadstone.eu
- DemoAccount98@threadstone.eu
- DemoAccount99@threadstone.eu
- DemoAccount100@threadstone.eu
- Info@threadstone.eu
- support@threadstone.eu
- sales@threadstone.eu
- marketing@threadstone.eu
- portal@threadstone.eu
- DemoAccount8@threadstone.eu
- DemoAccount9@threadstone.eu

- DemoAccount10@threadstone.eu
- DemoAccount11@threadstone.eu
- DemoAccount12@threadstone.eu
- DemoAccount13@threadstone.eu
- DemoAccount14@threadstone.eu
- DemoAccount15@threadstone.eu
- DemoAccount16@threadstone.eu
- DemoAccount17@threadstone.eu
- DemoAccount18@threadstone.eu
- DemoAccount19@threadstone.eu
- DemoAccount20@threadstone.eu
- DemoAccount21@threadstone.eu
- DemoAccount22@threadstone.eu
- DemoAccount23@threadstone.eu
- DemoAccount24@threadstone.eu
- DemoAccount25@threadstone.eu
- DemoAccount26@threadstone.eu
- DemoAccount27@threadstone.eu
- DemoAccount28@threadstone.eu
- DemoAccount29@threadstone.eu
- DemoAccount30@threadstone.eu
- DemoAccount31@threadstone.eu
- DemoAccount32@threadstone.eu
- DemoAccount33@threadstone.eu
- DemoAccount34@threadstone.eu
- DemoAccount35@threadstone.eu
- DemoAccount36@threadstone.eu
- DemoAccount37@threadstone.eu
- DemoAccount38@threadstone.eu
- DemoAccount39@threadstone.eu
- DemoAccount40@threadstone.eu
- DemoAccount41@threadstone.eu

- DemoAccount42@threadstone.eu
- DemoAccount43@threadstone.eu
- DemoAccount44@threadstone.eu
- DemoAccount45@threadstone.eu
- DemoAccount46@threadstone.eu
- DemoAccount47@threadstone.eu
- DemoAccount48@threadstone.eu
- DemoAccount49@threadstone.eu

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

Inbreuken op: info@overheid.nl

River City Media Spam List - In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.



Gaat over: E-mailadressen, IP addresses, Namen, Physical addresses

Inbreuken op: info@overheid.nl

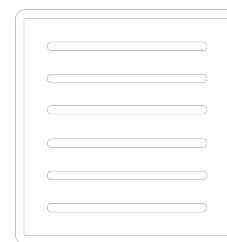
Verifications.io - In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.



Gaat over: Dates of birth, E-mailadressen, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

Inbreuken op: info@mijnbedrijf.nl

Exploit.In - In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

**Gaat over: E-mailadressen, Wachtwoorden**

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.