07 jan 2021 -10:22

Berichten naar verdacht@safeonweb.be bijna verdubbeld in 2020

Afgelopen jaar stuurde de internetgebruiker maar liefst 3 225 234 berichten door naar het e-mailadres verdacht@safeonweb.be. Dat betekent dagelijks meer dan 8800 berichten, wat bijna een verdubbeling is tegenover 2019. Toen stuurden jullie ons 1 700 000 berichten door.

Wat doen wij met deze 3 miljoen berichten?

Het is bedroevend dat cybercriminelen steeds meer berichten versturen met de bedoeling de internetgebruiker in de val te lokken. Deze berichten komen per e-mail, maar ook via tekstberichten of social media. De berichten die jullie doorsturen naar verdacht@safeonweb.be lezen we natuurlijk niet allemaal. We laten ze geautomatiseerd analyseren.

De links en de bijlages worden eerst gedetecteerd. Uit 3 miljoen berichten die we ontvangen, halen we wel 8.545.658 links, waarvan 667.356 frauduleuze (phishing, valse webshops, oplichting…) . Deze verdachte links geven we door aan Google Safebrowsing en Microsoft Smartscreen die een waarschuwing publiceren. Als iemand deze webpagina's wil bezoeken dan krijgt die een rood scherm met een duidelijke boodschap: Opgepast, de webpagina die je wil bezoeken is gevaarlijk. In deze berichten konden we daarnaast 26109 bijlages detecteren waarvan er 4370 een virus bevatten.

Speelde de coronacrisis een rol?

Cybercriminelen leken extra actief tijdens deze coronacrisis. We kunnen niet bevestigen of er effectief meer phishingberichten verstuurd werden tijdens deze periode. We weten alleen zeker dat mensen deze berichten vaker naar ons doorstuurden. In 45195 berichten vinden we een trefwoord terug dat met Corona gerelateerd was. Dit is uiteindelijk een minderheid. We zagen vooral traditionele phishingberichten steeds weer terugkeren:

- Berichten die van een pakjesdienst afkomstig lijken te komen en je vragen om eerst verzendkosten te betalen.
- Berichten die van banken lijken te komen en je aanmoedigen om een nieuwe kaart aan te vragen of je rekening te deblokkeren.
- Berichten die van een overheidsinstelling lijkten te komen en je een premie of tegemoetkoming beloven.
- Berichten die van diensten zoals Dropbox, PayPal, Microsoft lijken te komen.
- Berichten met een link naar de actualiteit: mondmaskers, feestdagen, een beloofde premie.

Wanneer is een bericht verdacht?

Er zijn verschillende zaken die je aandacht moeten trekken, maar eerst en vooral: gebruik je gezond verstand. Heb je er niet onmiddellijk vertrouwen in, dan is het waarschijnlijk vals.

- Een bericht dat te mooi is om waar te zijn? Kijk maar beter uit.
- Moet je snel reageren, of anders… Wees maar zeker dat iemand je in de val wil lokken.

- Komt het bericht onverwachts of van een onbekende? Ga eerst op zoek naar meer info voor je ingaat op een aanbod of vraag. Waarschijnlijk is het vals.
- Bekijk nauwkeurig de afzender en de URL van de link… Zien die er ongewoon uit? Niek klikken en niet antwoorden.
- Moet je je bankgegevens doorgeven? Of andere belangrijke info? Rood alarm! Informeer je eerst via een andere weg voordat je deze info doorgeeft en je bankrekening geplunderd wordt.

Leer valse berichten herkennen.

Wat kan ik doen?

Stuur een verdacht bericht onmiddellijk door naar verdacht@safeonweb.be. Hoe sneller wij het bericht behandelen en hoe minder slachtoffers er vallen. Je kan ons nu ook afbeeldingen van een vals bericht bezorgen. Onze technologie kan nu URL's in afbeeldingen detecteren. Wij moedigen iedereen aan om elk bericht zeer kritisch te bekijken alvorens het te openen en om 2 keer na te denken voor je op een link of een bijlage klikt.

"De 3 miljoen verdachte berichten zorgen ervoor dat we op de hoogte zijn van de nieuwste trends op vlak van phishing. In 2020 zagen we Corona gerelateerde berichten opduiken. Dit is niet te verbazen. Cybercriminelen maken altijd gebruik van actuele onderwerpen om de aandacht te trekken. Hierdoor wordt de 'klik-kans' groter.
Het detectiesysteem waarmee we bepalen of een website al dan niet frauduleus is, wordt voortdurend aangepast en verbeterd. Sinds vorig jaar bestaat de mogelijkheid om screenshots te analyseren. Dit geeft de burger de kans om heel eenvoudig smishing berichten door te geven."

Rosie De Vleeschauwer
projectverantwoordelijke Centrum voor Cybersecurity België

Centrum voor Cyber Security België
Wetstraat 16
1000 Brussel
België
http://www.ccb.belgium.be

Katrien - Eggers
Communicatieverantwoordelijke
+32 485 76 53 36
katrien.eggers@cert.be

Andries Bomans
Communicatieverantwoordelijke
+32 471 66 00 06
andries.bomans@ccb.belgium.be