03 jan 2023 -11:00

13 miljoen kliks naar verdachte websites vermeden in 2022

Dankzij de samenwerking met de bevolking werden in 2022 maar liefst 13 miljoen kliks naar verdachte websites vermeden. Dat zijn ongeveer 25 waarschuwingen naar internetgebruikers per minuut.

Het *Belgium Anti-Phishing Shield* (BAPS) is een systeem van het Centrum voor Cybersecurity België (CCB) dat internetgebruikers waarschuwt voor onveilige websites.

Het CCB rekent al ettelijke jaren op de medewerking van de hele bevolking om verdachte berichten te melden. Elke dag ontvangen wij duizenden verdachte e-mails. In 2021 werden er 4.500.000 berichten doorgestuurd naar verdacht@safeonweb.be. In 2022 groeit dit aantal nog steeds: we hebben meer dan 5,5 miljoen berichten ontvangen en konden we 1,5 miljoen verdachte URL's detecteren. Dat betekent dat we dagelijks gemiddeld 15.000 berichten verwerken.

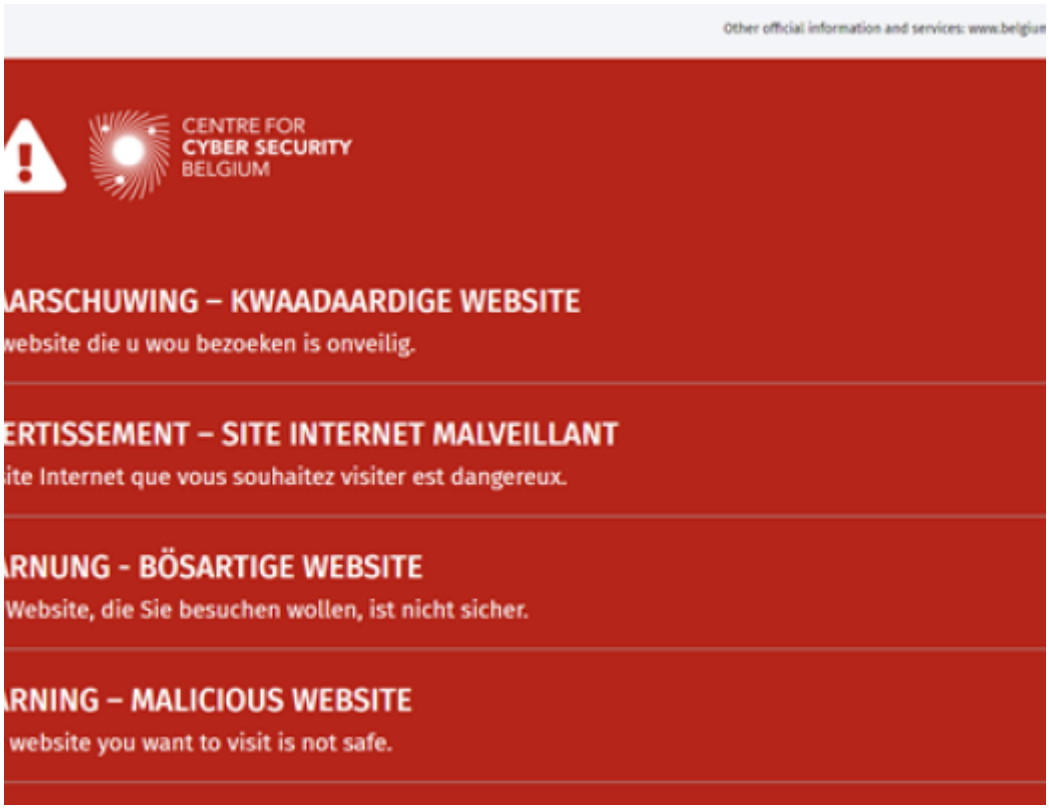
De verdachte URL's uit deze e-mails sturen we door naar Google SafeBrowsing en Microsoft SmartScreen. Browsers maken van deze info gebruik om bezoekers te waarschuwen voor kwaadaardige websites. Omdat wij geen controle hebben over de snelheid waarmee Google en Microsoft de links blokkeren, heeft het CCB samen met de internetaanbieders Belnet, Proximus, Telenet en Orange met succes een eigen systeem en procedure ontwikkeld om de internetgebruiker in real time te waarschuwen, het zogenaamde Belgium Anti-Phishing Shield (BAPS).

Het Centrum voor Cybersecurity België vraagt om verdachte berichten steeds door te sturen naar verdacht@safeonweb.be. Hoe sneller het bericht behandeld kan worden en hoe minder slachtoffers er vallen. Iemand die minder oplettend is en zou klikken op een verdachte link, komt op een waarschuwingspagina terecht. BAPS is enkel mogelijk dank zij het doorsturen van deze verdachte berichten door de bevolking.

Je kan ook afbeeldingen van een vals sms'je bezorgen en berichten met QR-codes doorsturen. Onze technologie kan URL's in afbeeldingen en QR codes detecteren.

> "Dit is een mooi voorbeeld van constructieve samenwerking tussen de bevolking en de overheid en is uniek in Europa. Het toont aan dat ons land met beperkte middelen toch heel veel kan bereiken. Door samen de strijd aan te gaan tegen de cybercriminaliteit zullen we die de komende jaren stevig kunnen terugdringen.
>
> Er is nog veel werk aan de winkel, maar we mogen niet opgeven."

Miguel De Bruycker
Directeur Centrum voor Cybersecurity België



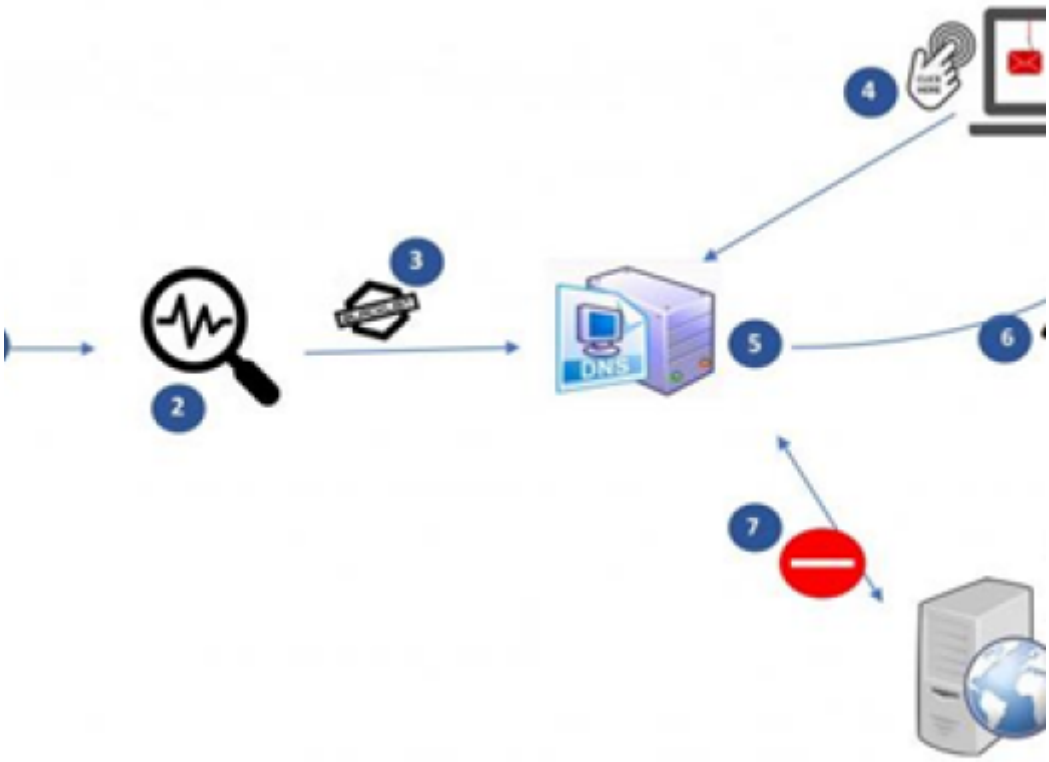
Wat is het Belgium Anti-Phishing Shield of ook BAPS?

Het Belgium Anti-Phishing Shield (BAPS) waarschuwt de bevolking op basis van de kwaadaardige links die het CCB ontvangt op verdacht@safeonweb.be. BAPS werd in 2021 getest en progressief gelanceerd.

Wanneer een gebruiker in België op een link klikt, wordt de vraag om zijn internet pagina op te halen naar zijn internetaanbieder (ISP) gestuurd. Dankzij BAPS vergelijkt de server van de internetaanbieder het aangevraagde internetdomein (website) met een lijst van volledig kwaadaardige domeinen. Als de aangevraagde URL op deze lijst voorkomt, zal de server van de internetaanbieder de gebruiker doorverwijzen naar een waarschuwingspagina.

Waar komt die lijst van kwaadaardige websites vandaan?

De lijst van kwaadaardige websites kunnen wij opstellen dankzij de duizenden verdachte berichten die mensen ons dagelijks doorsturen via verdacht@safeonweb.be. De internetdomeinen die voorkomen in deze berichten worden automatisch geëvalueerd en heel snel naar de internetaanbieders doorgestuurd, hoe sneller hoe effectiever. Dank zij een grondige evaluatie wordt efficiënt vermeden dat een echte website per vergissing op de lijst terecht komen en BAPS is exclusief tegen phishing. Pas als ze gemarkeerd zijn als volledig 'gevaarlijk' dan komen ze op de lijst terecht.



Hoe werkt BAPS?

- Het CCB ontvangt informatie over mogelijke kwaadaardige websites onder meer via verdacht@safeonweb.be;
- Er gebeurt een analyse van mogelijk kwaadaardige websites en deze worden opgenomen in een lijst;
- De lijst met kwaadaardige websites wordt doorgestuurd naar de internetaanbieders;
- Een internetgebruiker klikt op kwaadaardige URL;
- De internetaanbieder vergelijkt het DNS-verzoek met de lijst van kwaadaardige websites (domeinen);
- Als dit naar een kwaadaardige website leidt, dan wordt de internetgebruiker 'omgeleid' naar een

waarschuwingspagina;

- De internetgebruiker bezoekt de kwaadaardige website niet.

Contactpersonen voor de pers

Michele Rignanese (Persverantwoordelijke CCB, NL/FR): 0477 38 87 50, michele.rignanese@ccb.belgium.be)

Over het Centrum voor Cybersecurity België

Het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cyberveiligheid in België. Het CCB superviseert, coördineert en waakt over de toepassing van de Belgische cyberveiligheidsstrategie. Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, aanbieders van essentiële diensten en de bevolking zich gepast beschermen. www.ccb.belgium.be

Centrum voor Cyber Security België
Wetstraat 18
1000 Brussel
België
http://www.ccb.belgium.be

Michele Rignanese
Woordvoerder FR
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be

Katrien Eggers
Woordvoerder NL
+32 485 76 53 36
katrien.eggers@cert.be