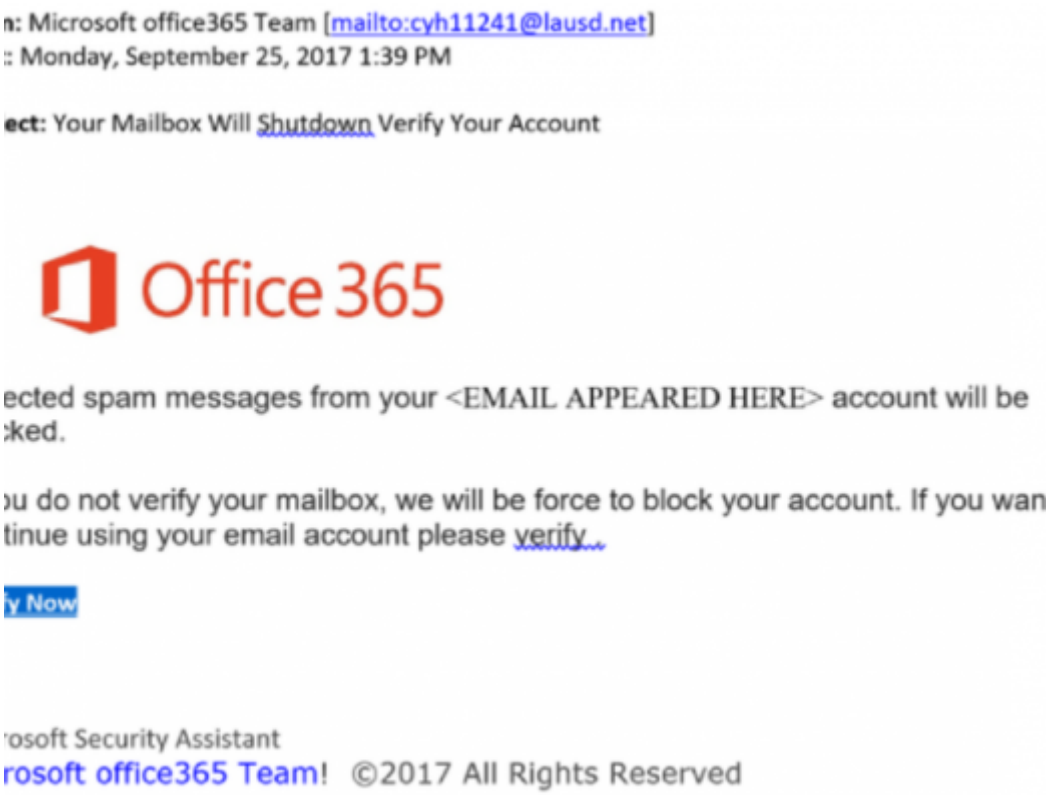
04 feb 2021 -08:00

Cybercriminelen misbruiken mailboxen van Belgische bedrijven om wachtwoorden te stelen

De COVID-19 pandemie lijkt het uitgelezen moment voor cybercriminelen om hun slag te slaan. Verschillende cybersecuritypartners melden ons aanvallen die gericht zijn op Belgische bedrijven. Een schatting maken van het aantal slachtoffers is moeilijk omdat er altijd een grote onderrapportage is. Mensen geven niet graag toe dat ze slachtoffer werden en bedrijven vrezen voor imagoschade.



Hoe gaan de cybercriminelen te werk?

De oplichters maken de loginpagina's van populaire platformen zoals Microsoft Office 365, PayPal en andere onlinediensten minutieus na. Vervolgens sturen ze een phishingbericht met een link of een bijlage naar hun slachtoffers met een smoes om hen te laten inloggen zoals *'Your mailbox will shutdown. Verify your account'*. De nietsvermoedende gebruiker voert zijn of haar logingegevens in op de nagemaakte website en geeft ze daarbij onbewust weg aan de criminelen.

"Met dit soort aanvallen kunnen de cybercriminelen via de contacten van het slachtoffer opnieuw andere gebruikers en bedrijven besmetten. Zo kunnen veel bedrijven in korte tijd slachtoffer worden."

Phédra Clouner
Vice-directrice van het CCB

Hoe kan je je beschermen tegen het hacken van login gegevens?

- Wees voorzichtig als je een bericht krijgt van een platform waarbij je wordt gevraagd om je wachtwoord in te voeren.
- Controleer het e-mailadres van de afzender en de URL van de link waar je moet op klikken. Zien die er ongewoon uit, dan gaat het waarschijnlijk om phishing.
- Wat kan je beter doen? Open je browser en voer zelf de juiste URL in, bv. https://www.office.com/ https://www.paypal.com/

"Phishing kan zeer ernstige gevolgen hebben. De beste verdediging bestaat eruit om alert te zijn en te weten waar je op moet letten. Wees bijvoorbeeld heel voorzichtig bij berichten die een dringende oproep doen of mails waarin spellingfouten staan. Voor meer tips raden we aan om een kijkje te nemen op onze website."

Bart Asnot
Security expert bij Microsoft BeLux

Hoe kan je opmerken dat je slachtoffer bent van deze aanval?

- Er worden e-mails in jouw naam verstuurd vanuit jouw mailbox, maar jij hebt dit zelf niet gedaan.
- Enkele weken later kan het gebeuren dat je meer phishingberichten krijgt dan gewoonlijk, omdat je gegevens mogelijk op het internet verspreid werden en door cybercriminelen hergebruikt worden.

Wat kan je doen als je slachtoffer bent geworden?

- Verander onmiddellijk je wachtwoord (op elke account waar je dit wachtwoord gebruikt);
- Waarschuw je contacten;
- Activeer tweestapsverificatie (Stel Microsoft 365 aanmelding in voor multi-factor authenticatie - Office Support);
- Een automatisch antwoord is misschien geactiveerd door de cybercriminelen. Verwijder het;
- Er kan een regel ingesteld zijn die je e-mails doorstuurt naar een interne archiefmap of een extern e-mail adres. Verwijder deze regel;
- Controleer de informatie die beschikbaar is via deze mailbox. Sommige gevoelige of vertrouwelijke informatie kan gecompromitteerd zijn. Het is beter om hiervan op de hoogte te zijn.

Als je een phishingbericht krijgt, stuur het dan onmiddellijk naar verdacht@safeonweb.be. Wij laten de links blokkeren zodat minder oplettende internetgebruikers geen slachtoffer kunnen worden.

Meer informatie:

- https://www.safeonweb.be
- https://anchor.fm/fraudeur-hacker-en-jij (Podcast)
- https://www.microsoft.com/security/blog/2019/10/16/top-6-email-security-best-practices-to-protect-against-phishing-attacks-and-business-email-compromise/

Contactpersonen voor de pers

- Andries Bomans (Persverantwoordelijke CCB, NL/FR) : 0471 66 00 06, andries.bomans@ccb.belgium.be
- Katrien Eggers (Persverantwoordelijke CCB, NL/FR) : 0485 765 336, katrien.eggers@cert.be
- Cathy Suykens (Persverantwoordelijke Cyber Security Coalition), NL/FR : 0499 71 84 96, cathy.suykens@cybersecuritycoalition.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

Over de Cyber Security Coalition vzw

De Cyber Security Coalition heeft als missie de Belgische cyberveiligheid weerbaarder te maken door een sterk ecosysteem voor cyberbeveiliging op nationaal niveau uit te bouwen. Dit is mogelijk door de vaardigheden en expertise van de academische wereld, bedrijven en de overheid samen te brengen in een op vertrouwen gebaseerd platform dat zich focust op het bevorderen van informatie-uitwisseling, operationele samenwerking, het formuleren van aanbevelingen voor efficiëntere beleidslijnen en richtlijnen, en tenslotte het uitvoeren van gezamenlijke bewustmakingscampagnes voor burgers en organisaties. Meer dan 500 vertegenwoordigers van onze 102 lid organisaties nemen deel aan onze activiteiten en dragen zo bij aan onze missie. www.cybersecuritycoalition.be

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

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

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