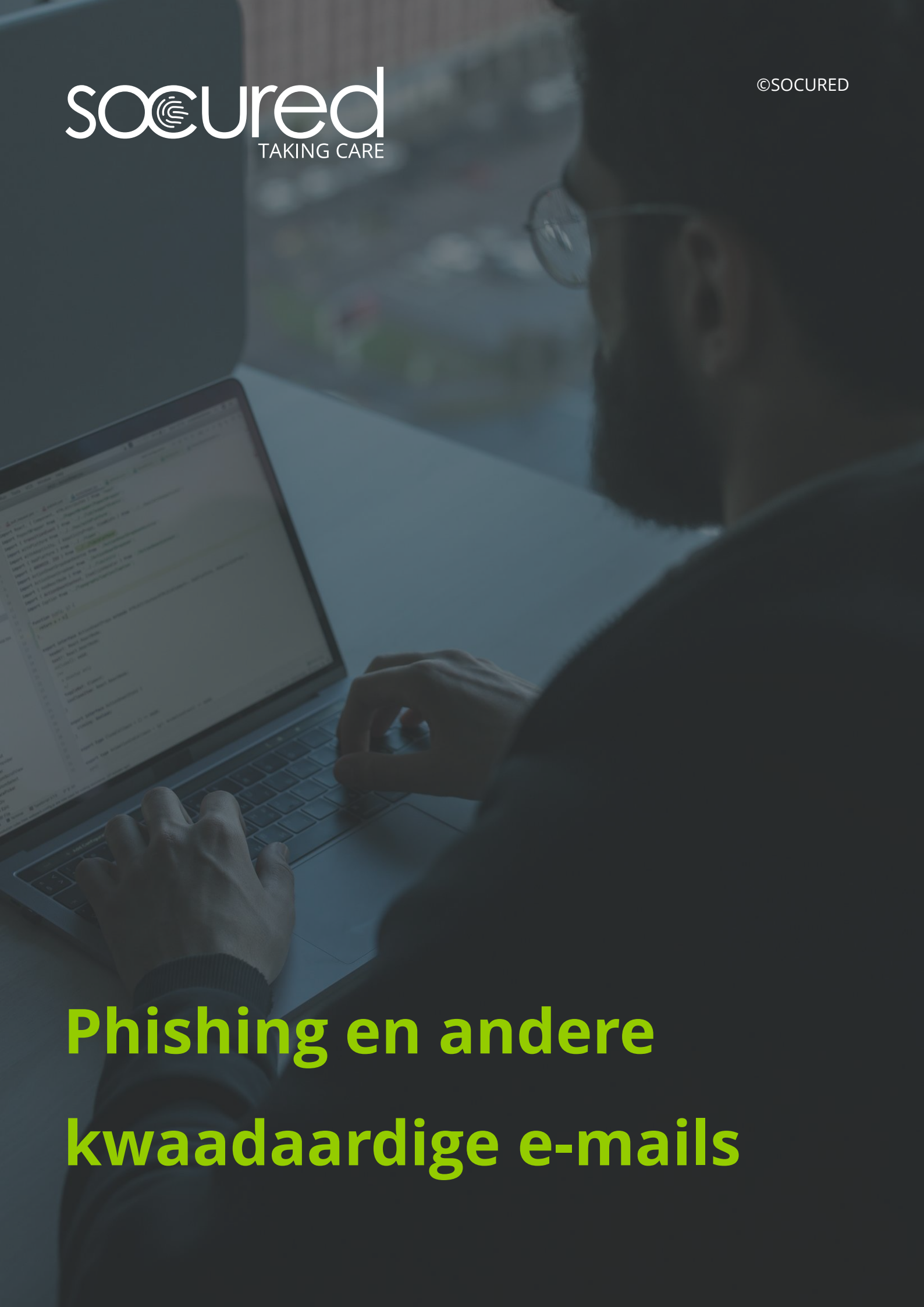


Phishing en andere kwaadaardige e-mails

Phishing en andere kwaadaardige e-mails

WAT IS PHISHING?

Phishing is in onze bedreigingssignalen het meest voorkomende soort kwaadaardige e-mail. Deze e-mails zijn ontworpen om iemand over te halen gevoelige informatie, zoals gebruikersnamen en wachtwoorden, met een aanvaller te delen. Hiervoor schrijven aanvallers e-mails met verschillende thema's, zoals productiviteitstools, een wachtwoord opnieuw instellen of een andere urgente melding om een gebruiker te verleiden op een link te klikken. De phishingwebpagina's die bij deze aanvallen worden gebruikt, kunnen gebruikmaken van kwaadaardige domeinen, zoals domeinen die door de aanvaller worden gekocht en beheerd, of besmette domeinen, waarbij de aanvaller misbruik maakt van een kwetsbaarheid in een legitieme website om schadelijke content te hosten.

De phishingpagina's kopiëren vaak bekende legitieme inlogpagina's, zoals voor Office 365 of Google, om gebruikers inloggegevens in te laten vullen. Zodra de gebruiker dit heeft gedaan, wordt hij vaak naar een legitieme website doorgestuurd, zoals de echte inlogpagina voor Office 365. Zo weet de gebruiker niet dat de gegevens zijn gestolen. Ondertussen worden de ingevoerde inloggegevens opgeslagen of verstuurd naar de aanvaller voor later misbruik of verkoop. Aanvallers proberen met phishing ook toestemmingen te verkrijgen. Dan sturen ze gebruikers links die de aanvaller, als erop wordt geklikt, toegang en toestemmingen voor applicaties geven, zoals via het OAuth 2.0-protocol. Zo kunnen gebruikers aanvallers onbewust toestemming geven voor applicaties waarmee de aanvallers toegang tot een schat aan gevoelige informatie hebben.

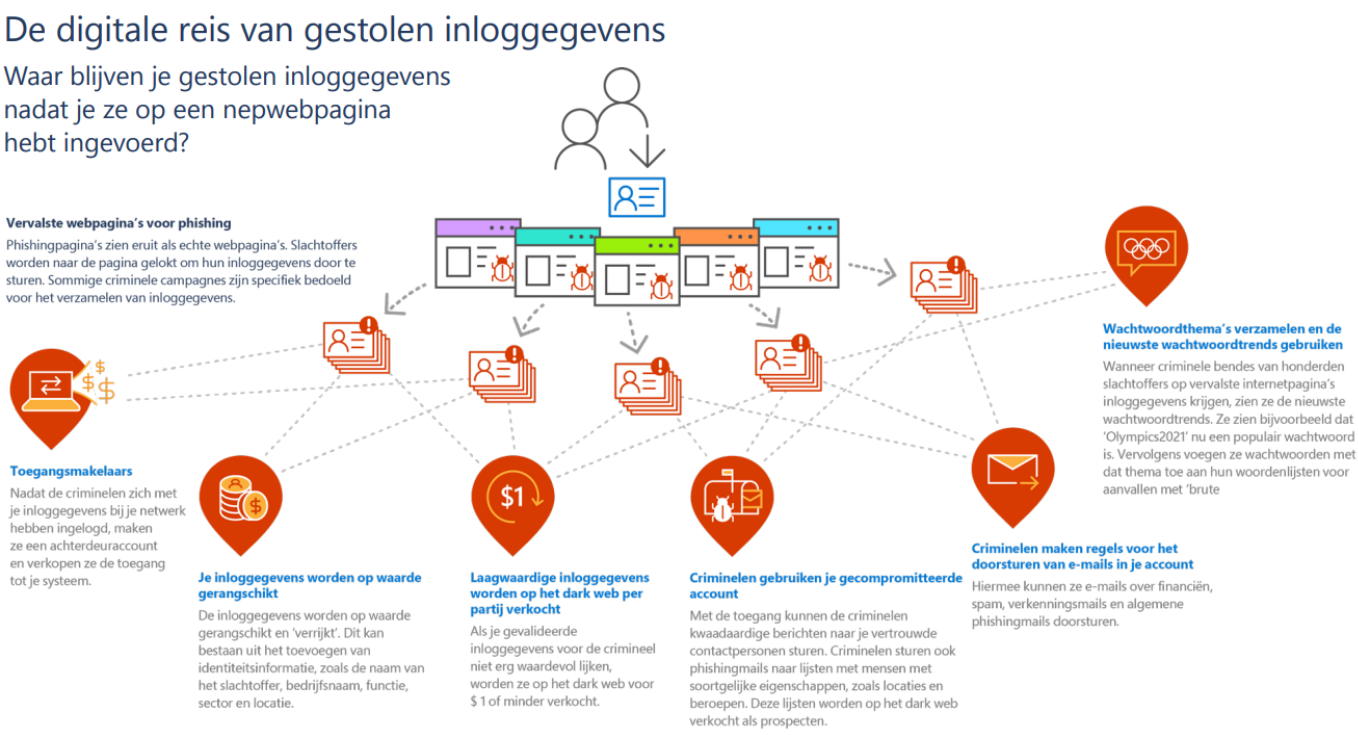
BEDREIGING VOOR IDENTITEITEN

In het IC3-rapport van de FBI uit 20209 werd phishing genoemd als het door slachtoffers meest genoemde soort misdaad. Het aantal meldingen is ten opzichte van het voorgaande jaar verdubbeld. Phishing vormt een aanzienlijke bedreiging voor zowel bedrijven als personen, en phishing naar inloggegevens werd vorig jaar bij veel van de meest schadelijke aanvallen gebruikt. Uit onze onderzoeken naar online netwerken van georganiseerde misdaad betrokken bij het compromitteren van zakelijke e-mails zagen we een sterke diversificatie van manieren om inloggegevens te verkrijgen, controleren en misbruiken, wat de toegenomen dreiging kan verklaren.

Criminelen gebruiken meer automatiserings- en inkooptools om de waarde van hun criminele activiteiten te vergroten. Inloggegevens van nietsvermoedende slachtoffers kunnen worden verkregen via phishingwebsites die zich voordoen als een groot aantal online diensten, of via logboeken op besmette apparaten waarin wordt bijgehouden wat er wordt getypt, zodat kan worden geraden welke gelekte inloggegevens voor andere online diensten worden hergebruikt. Voor elk paar inloggegevens zijn er diensten die informatie over de bijbehorende identiteit verrijken met details zoals de naam, het bedrijf waar hij of zij werkt, functie, anciënniteit binnen het bedrijf en in welke sector het bedrijf actief is.

Met deze informatie kan de identiteit worden gebruikt om zakelijke e-mails te onderscheppen, spam te verzenden, gevoelige informatie te verzamelen of phishingwebsites voor gerelateerde online accounts te hosten. Zelfs nadat een aanval heeft plaatsgevonden, kunnen accounts opnieuw worden verkocht nadat geautomatiseerde systemen hebben gecontroleerd of ze bruikbaar blijven. Een ander gevaar is impersonatie, zoals bij aanvallen op zakelijke e-mails waarbij een partij in een financiële transactie wordt geïmiteerd om betalingen naar een niet-geautoriseerde ontvanger om te leiden. Uit ons onderzoek bleek dat criminelen aan financiën gerelateerde berichten volgen om te zien wie er kan worden geïmiteerd. Vervolgens registreren ze nepdomeinen (bijvoorbeeld waarbij een teken is vervangen door een gelijkend ander teken), zodat ze het e-mailadres van het slachtoffer kunnen imiteren. In dit geval zorgt de diefstal van inloggegevens van één persoon dat iemand anders het slachtoffer wordt.

“Criminelen gebruiken meer automatiserings- en inkooptools om de waarde van hun criminele activiteiten te vergroten.”

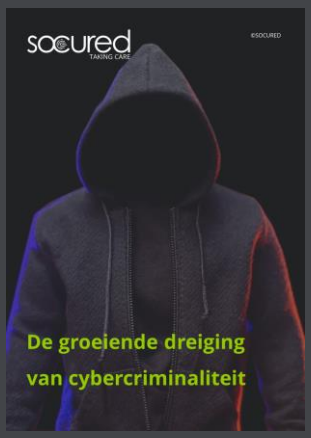


AANVALLEN OP ZAKELIJKE E-MAILS

Hoewel aanvallen op zakelijke e-mails niet het grootste volume uitmaken, heeft dit type aanval wel de grootste financiële gevolgen. Bij deze aanvallen doet de crimineel zich voor als een legitieme zakenpartner. Daarvoor gebruikt hij een gecompromitteerd e-mailadres, een gelijkend domein dat hij heeft geregistreerd of een gratis e-maildienst zoals Hotmail of Gmail, waarmee hij e-mails stuurt om ontvangers over te halen tot een financiële transactie, het geven van gevoelige informatie, of het verstrekken van middelen zoals cadeaubonnen aan de aanvaller. Het afgelopen jaar zag Microsoft vooral deze oplichting met cadeaubonnen. Bij deze trucs maken aanvallers meestal een groot aantal gratis e-mailaccounts aan, waarbij ze de weergavenaam aan het doelwit aanpassen. Soms registreren aanvallers hun eigen domeinen voor deze aanvallen of maken ze voor specifieke doelwitten gratis e-mailaccounts aan. Vervolgens doen ze zich voor als iemand waar de ontvanger mee samenwerkt (vaak hun baas of een directeur van hun bedrijf) en vragen ze de ontvanger om cadeaubonnen te kopen (vaak met bedrijfsgeld). Vaal wordt in deze e-mails gesuggereerd dat de afzender de cadeaubon als verjaardagscadeau voor een familielid of beloning voor werknemers nodig heeft. Meestal wordt de ontvanger gevraagd om de gekochte digitale cadeaukaarten naar de aanvaller te sturen, maar we zien ook dat aanvallers de ontvanger vragen om fysieke cadeaubonnen te kopen en een foto van de codes achterop de kaarten te sturen, zodat de aanvaller ze online kan doorverkopen of voor cryptovaluta kan ruilen.

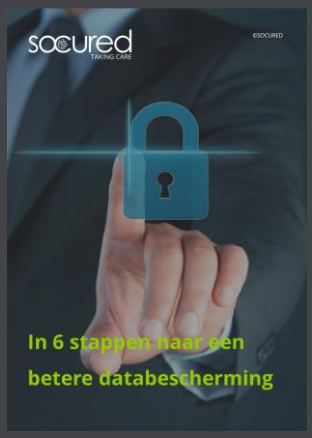
Een veel geavanceerdere en financieel schadelijker soort aanval op zakelijke e-mail is fraude met overschrijvingen. Hierbij proberen criminelen zich tussen verwachte financiële transacties te nestelen, en vragen ze de ontvanger om de rekeninggegevens voor een uitgaande overschrijving aan te passen. De criminelen doen zich voor als de beoogde ontvanger van het geld, waardoor het voor het slachtoffer niet ongewoon lijkt. Zodra het slachtoffer het geld naar de nieuwe rekening heeft overgemaakt, wordt het door de criminelen opgenomen, waarna het moeilijk op te sporen is. Bedrijven kunnen dit soort oplichting helpen voorkomen met financieel beleid dat het controleren van veranderende rekeningen verplicht. Voordat financieel medewerkers rekeningnummers op basis van e-mails veranderen, moeten ze dit controleren via een andere weg dan e-mail, bijvoorbeeld door de ontvanger op een bekend en vertrouwd telefoonnummer te bellen. Bovendien kunnen beveiligingsfuncties tegen impersonatie in e-mailbeveiligingsproducten helpen voorkomen dat aanvallers dit soort oplichting met succes kunnen uitvoeren.

MEER LEZEN?



De groeiende dreiging van cybercriminaliteit

Download



In 6 stappen naar een betere databescherming

Download

BEDANKT VOOR HET LEZEN VAN DEZE WHITEPAPER. HEEFT U NOG VRAGEN OVER HET ONDERWERP?

Neem dan gerust contact met ons op via info@socured.nl of 020 708 55 65.

Socured
Klokkenbergweg 50A
1101 AP AMSTERDAM-ZO
Tel.: 020 708 55 65
info@socured.nl
www.socured.nl

Onderdeel van Socia

Over Socured

Socured is gevestigd in Amsterdam en is onderdeel van Socia. Socia helpt al meer dan 15 jaar haar klanten op het gebied van IT en heeft inmiddels een mooie voetafdruk achtergelaten bij veel bedrijven in Nederland als het gaat om IT-diensten.