Beschrijving Hacking van webshopaccounts; onderdelen voor het barrièremodel

Stap 1: Verkrijgen van accountgegevens

In deze fase is de crimineel op zoek naar alle gegevens van een account om mee in te kunnen loggen bij de webshop. Dit kan direct, door de inloggegevens van het webshopaccount te achterhalen, of indirect door de email te hacken. Dit kan op verschillende manieren. De twee meest voorkomende zijn:

- Phishing (lijkt meer voor te komen bij telecombedrijven dan bij webshops)
- Hergebruik van op het (dark)web aangeboden credentials (lijkt het meeste voor te komen bij webhops; phishing lijkt minder voor te komen)

Overige methoden zijn:

- Brute force
    - Dictionary attack (samengesteld uit resultaten social engineering en meest gebruikte wachtwoorden)

Phishing

Beschrijving

Er worden nog steeds veel phishing-emails verstuurd, en ze worden steeds minder goed van echte mails te onderscheiden. Dit lijkt een veelvoorkomende (meest voorkomende..?) manier te zijn om aan inloggegevens te komen van telecomaccounts, waarbij gebruik wordt gemaakt van phishing middels sites gelijkend op die van de betreffende bedrijven. Bij webshops vindt deze vorm van phishing vrijwel niet meer plaats. Echter worden inloggegevens wel via andere vormen van phishing verkregen. In de aangiften komt soms naar voren dat in eerste instantie de inloggegevens van Marktplaats of Facebook worden gephisht waarna vervolgens email en webshopsaccount worden overgenomen. Phishing gebeurt niet alleen via e-mails maar ook via advertenties.De phishing kan gericht zijn op het verkrijgen van toegang tot de e-mail, rechtstreekse toegang tot het webshopaccount, of het verkrijgen van credentials tot een ander account om vervolgens die credentials uit te proberen bij webshops. Ook kan met behulp van phishing misbruik gemaakt worden van bekende beveiligingslekken waarmee op afstand toegang verkregen wordt tot een computer. De ontvanger van de phishing-email hoeft daarvoor enkel een link te openen die in de e-mail is opgenomen. Het bezoeken van de website leidt vervolgens tot een automatische virusbesmetting door misbruik van een bekend beveiligingslek (drive-by infection).

Faciliterende elementen

- Email met link waar mensen hun gegevens kunnen invoeren. De mail moet “echt” genoeg lijken dat mensen erin trappen en hun gegevens invoeren of de website bezoeken.
- Phishingwebsites, bijvoorbeeld nep-Marktplaats of nep-Facebookwebsites, waar slachtoffers hun gegevens invullen.

Interventies

Veelbelovende interventies:

- Bewustwording creëren bij burgers om phishing te herkennen
    - Actie voor: overheid in combinatie met private partijen. Doel is om bewustwording omtrent phishing te verhogen. Concrete handvatten kunnen bijvoorbeeld van de website www.laatjeniethackmaken.nl verkregen worden.
- Gebruik van een wachtwoordmanager door consumenten stimuleren.

    - Actie voor: overheid. Er kan bijvoorbeeld een campagne worden opgezet om wachtwoordmanagers te promoten en voor de eerste 1000 mensen die zo'n app aanschaffen de aanschafkosten te vergoeden.

Overige interventies:

- Beveiligde emailservers (om te voorkomen dat de server wordt gebruikt om emailadressen te versturen)
    - Actie voor: beveiliging webwinkel en hostingbedrijven.
- Tips bij het aanmaken van een webshopaccount: gebruik hier een uniek wachtwoord/ gebruik hier zeker niet het wachtwoord dat je voor je e-mail gebruikt
    - Actie voor: overheid; voorlichting.
- Spamfilters bij potentiële slachtoffers
    - Actie lastig uitvoerbaar.
- Virusscanners bij potentiële slachtoffers
    - Actie lastig uitvoerbaar.
- Bewustwording creëren bij burgers om updates te installeren
- Achteraf (na het invullen van gegevens via phishing)
    - Waarschuwing/blokkering van server als crimineel probeert in te loggen met de gephishte gegevens, gebruikmakend van een opvallend anders IP-adres / computer dan normaal.
        - Actie voor: beveiliging webwinkel.

Hergebruik van op het (dark)web aangeboden credentials

<u>Beschrijving</u>

Als een account eerder is gehackt, vaak in een grootschalige hack, kunnen deze inloggegevens in grote lijsten worden aangeboden op het dark web. Ongeveer 40% van de mensen hergebruikt hun wachtwoorden op meerdere plekken, waardoor een crimineel hier overal binnen kan komen als slechts één account gehackt is. De lijsten op het dark web kunnen vervolgens worden gekocht door criminelen. Dit lijkt ook te gebeuren bij grote webshops: deze webshops worden zelf niet gehackt, maar via gelekte informatie elders kunnen criminelen alsnog inloggen op klantaccounts. Mogelijke toepassingen zijn het versturen van spam met gehackte emailadressen (komt veel voor, maar niet relevant voor ons gekozen fenomeen) of het proberen in te loggen bij webshops met inloggegevens van deze lijsten.

De scripts om websites/webshops te hacken worden heel algemeen geschreven; ze doorzoeken bijvoorbeeld alle Magento-sites die verouderd zijn. Dit zijn massapogingen om zoveel mogelijk gegevens op het internet buit te maken. De gestolen gegevens gaan vaak naar China en Rusland. Het is niet zeker wat er daarna met de gestolen gegevens gebeurt, maar vroeger (en waarschijnlijk nog steeds) worden emailadressen doorverkocht, voornamelijk om spam te versturen. Dit zou indirect een bron van gegevens kunnen zijn om daarna in te loggen bij webshops (door een Nederlander die deze gegevens opkoopt), maar dit is een gok.

<u>Faciliterende elementen</u>

- Lijsten van datalekken bij websites met klantgegevens. Deze kunnen ook van webshops afkomstig zijn – vaak gaat het dan om kleinere, minder beveiligde webshops die kwetsbaarder zijn voor hackers.

<u>Interventies</u>

Veelbelovende interventies:

- Alle klanten een nieuw wachtwoord laten kiezen, en het liefst ook eisen stellen aan dit nieuwe wachtwoord. Dit zorgt ervoor dat wachtwoorden niet meer kunnen worden hergebruikt, waarmee de rondzwervende lijsten met credentials niet meer automatisch

gebruikt kunnen worden. Het blijft echter gevaarlijk als mensen bijvoorbeeld alleen een “1” achter hun bestaande wachtwoord plaatsen.
    - Actie voor: webshops.

Overige interventies:

- Beter beveiligen inlog- en klantgegevens bij websites/webshops. Bijvoorbeeld door lijsten met gegevens goed beveiligd en versleuteld op te slaan, en beveiligingsupdates te blijven uitvoeren.
    - Actie voor: webshopbouwers (grote bedrijven zoals Mijnwebwinkel, maar vooral ook kleinere bedrijfjes). Webwinkels lijken zich nu niet voldoende bewust van de gevaren, of achten de gevaren niet groot genoeg om de beveiliging te verbeteren.
- Hele omgeving van de webshop beveiligen, van voor tot achter. De betalingen zijn bijvoorbeeld vrijwel altijd goed beveiligd, maar vooral bij kleinere webshops zijn vaak nog zwakke plekken te vinden waar een hacker misbruik van kan maken (bijvoorbeeld email).
    - Actie voor: webshop developer.
- Websites/webshops minder gegevens op laten slaan.
    - Actie voor: IRMA-app, of andere initiatieven hiervoor. Bij IRMA kun je bijvoorbeeld inloggen met een QR-code; zonder wachtwoord, en kun je zelf kiezen welke gegevens je wilt delen met de website. Hiermee geef je niet meer weg dan nodig is.
- Actief informeren
    - Op basis van de aangetroffen gegevens de houders van de e-mailadressen actief informeren dat hun inloggegevens op internet genoemd worden en adviseren het wachtwoord aan te passen en 2-traps verificatie in te stellen.

Brute force

Beschrijving

Dit lijkt de minst gebruikte methode om binnen te dringen in accounts, vooral omdat het teveel tijd en moeite kost. Brute forcing gebeurt dan vooral als een hacker in een specifiek account geïnteresseerd is.

De meeste webshops hebben zich inmiddels tegen brute force-aanvallen beveiligd, bijvoorbeeld door een account te blokkeren vanaf een x aantal inlogpogingen per minuut. Desondanks blijft het op sommige webshops mogelijk om te brute forcen. Hier worden soms speciale lijsten voor gebruikt met veel voorkomende wachtwoorden (dictionary attack). Als het wachtwoord op de lijst staat is de hacker zo binnen.

Faciliterende elementen

- Onbeveiligde website tegen brute force.
- Zo veel mogelijk computerdenkkracht. Echter, met een normale laptop kun je ook al ver komen met zogenaamde “dictionary attacks”, waarin je een lijst met mogelijke wachtwoorden allemaal probeert op de inlogpagina.

Interventies

- Eisen stellen aan wachtwoorden. Vervolgens zouden er ook bepaalde kwaliteitseisen aan de nieuwe wachtwoorden kunnen worden gesteld, bijvoorbeeld minimaal 8 tekens en minimaal 1 leesteken. Met moeilijkere wachtwoorden wordt het lastiger voor hackers om de wachtwoorden te kraken.
    - Actie voor: webshops.
- Beveiliging instellen op website om brute force-aanvallen te blokkeren.
    - Actie voor: hostingbedrijf / webshops

Stap 2: Inloggen

Beschrijving

Het inloggen op het gehackte webshopaccount. Het probleem is hier dat webshops niet kunnen vaststellen dat degene die in probeert te loggen niet de échte klant is, maar een crimineel (identiteitsfraude).

Faciliterende elementen

- Apparaat/device met webbrowser en een internetverbinding. Deze kan afgeschermd zijn door de crimineel, bijvoorbeeld door een VPN, maar dit is lang niet altijd het geval (biedt mogelijkheden bij repressie).

Interventies

Veelbelovende interventies:

- Gebruik maken van een app voor het verifiëren van de digitale identiteit of authenticiteit van de klant. Een voorbeeld kan IRMA zijn, een app die wordt beheerd door de Stichting Privacy by Design en de Radboud universiteit. In de IRMA-app kunnen burgers hun persoonsgegevens laten zetten, afkomstig van een betrouwbare uitgever (bv. een bank of de gemeente). De gegevens worden dan beveiligd en versleuteld opgeslagen in de app. Als een klant dan een bestelling wilt plaatsen bij een webshop, kan de klant via de IRMA-app alle vereiste informatie opgeven bij de webshop, waardoor het risico van identiteitsfraude omlaag gaat. Omdat alle informatie al in de app staat hoeft de klant verder geen gegevens meer handmatig in te vullen; dit levert een snellere check-out op voor de klant. Meer info over IRMA: https://privacybydesign.foundation/irma-uitleg/.
    - Actie voor: webshopeigenaren, om IRMA toe te voegen (verplicht of vrijwillig) als extra controle bij het inloggen en/of bestellen. De projectgroep kan dit promoten als oplossing bij partners en burgers, in samenwerking met de Stichting Privacy by Design en Radboud Universiteit. Er kan worden gekeken of er een pilot kan worden gestart bij een publieke of private partij.
- Frauderegister opzetten met gegevens van fraudeurs, bijvoorbeeld door IP-adres, emailadres, etc. controleren op fraude. Banken hebben wel grote samenwerking op gebied van frauduleuze activiteiten, waar webshops eventueel van kunnen leren. Als deze informatie automatisch (en geanonimiseerd) kan worden gedeeld tussen politie en webshops, zou fraudeurs het inloggen onmogelijk kunnen worden gemaakt. Katvangers kunnen ook op een zwarte lijst worden geplaatst. Sommige pakketjes die gevlagd zijn als frauduleus zouden ook gevolgd kunnen worden tot de aflevering, en dan iemand op heterdaad betrappen. Dit vereist een goede samenwerking tussen politie en webshops.
    - Actie voor: PPS. Politie in samenwerking met webshops en postorderbedrijven.
- Notificatie-email als er wordt ingelogd met een vreemd IP-adres of vanaf een vreemde locatie. Dit doet bijvoorbeeld Google al, en schijnt redelijk goed te werken. Het is geheel vrijblijvend: als de klant de notificatie negeert kan hij alsnog zijn account normaal gebruiken. Er kan worden nagedacht over het beste medium om de notificatie te versturen; indien het emailadres ook gehackt is heeft het sturen van een email geen zin.
    - Actie voor: webshops.

Overige interventies:

- Stopgesprekken voeren met daders. In navolging van de aanpak van de (niet strafrechtelijke) aanpak van katvangers kan de politie stopgesprekken voeren met daders, zeker voor zo ver het jongeren betreft die het begin van hun criminele carrière staan.
    - Actie voor: politie en jongerenwerkers/wijkagenten.
- Two-factor authentication. Dit zorgt ervoor dat een klant op twee verschillende manieren moet bewijzen dat hij/zij zichzelf is: vaak met een wachtwoord en daarna nog een SMS-code. Als een webshop niet een dergelijke beveiliging heeft, is de crimineel meteen binnen als hij/zij de gebruikersnaam en het wachtwoord weet. Met two-factor authentication is dat niet

meer voldoende, en dus kunnen daarmee alle overnames van accounts worden voorkomen, volgens de huidige MO.

- Actie voor: beveiliging van de webshop. Zij zijn de enige die een dergelijke stap kunnen nemen op hun website. Maar momenteel zien veel webshopeigenaren niet de noodzaak om two-factor authentication in te stellen, want (1) ze hebben niet zo veel last van account takeover en (2) ze willen dat hun klanten zo snel mogelijk kunnen betalen, en een extra verificatiestap zit de klant niet op te wachten.
- Eventueel kan de overheid/politie het gebruik van two-factor authentication stimuleren, en burgers van de noodzaak ervoor doordringen. Als het tijd kost is de consument zeer zelden bereid om aan haar eigen beveiliging te denken.

Stap 3: Gegevens aanpassen

Beschrijving

De hacker past de accountgegevens aan. Het gaat dan primair om het afleveradres. Verder ook om zaken als het telefoonnummer, emailadres of wachtwoord.

Faciliterende elementen

- e-mailadres
- (prepaid) telefoonnummer
- katvanger(s)
- kennis van 'typische' adressen, zoals straten met veel senioren of afhaalpunten zonder identificeerplicht

Interventies

Veelbelovende interventie:

- Frauderegister opzetten met gegevens van fraudeurs, bijvoorbeeld door IP-adres, emailadres, etc. controleren op fraude. Banken hebben wel grote samenwerking op gebied van frauduleuze activiteiten. Hier kunnen webshops wat van leren. Katvangers komen ook op zwarte lijst. Sommige pakketjes die gevlagd zijn als frauduleus zouden ook gevolgd kunnen worden tot de aflevering, en dan iemand op heterdaad betrappen. Dit vereist een goede samenwerking tussen politie en webshops.
  - Actie voor: PPS. Politie in samenwerking met webshops en postorderbedrijven.

Overige interventies:

- Two factor authentication als bepaalde gegevens gewijzigd worden, bijvoorbeeld het afleveradres. Dit zou eventueel via IRMA gedaan kunnen worden: bijvoorbeeld als je met de app een QR-code moet scannen om te bevestigen dat jij het bent die de wijziging doorvoert.
- Notificatie per email aan gebruiker als gegevens gewijzigd worden. In het geval van een gewijzigd e-mailadres notificatie per SMS en/of naar het oude e-mailadres
- Monitoring van nieuwe gegevens door webshop; alert zijn op het vaker voorkomen van adressen, telefoonnummers en e-mailadressen tussen aangepaste gegevens van verschillende accounts.
- Bij bovenstaande interventie zouden (grote) webshops ook kunnen samenwerken om sneller frauduleuze e-mailadressen e.d. te herkennen

Stap 4: Bestellen

Beschrijving

De hacker plaatst de bestelling. Vaak gaat het om producten die veel geld waard zijn en makkelijk door te verkopen, bijvoorbeeld elektronica en dure kleren. Deze groep criminelen lijkt zich niet te specialiseren – ze pakken alles aan wat ze kunnen krijgen. Het lijkt erop dat criminelen, wanneer ze eenmaal inloggegevens hebben verkregen, op meerdere webshops proberen in te loggen en

producten te bestellen. Hierbij worden soms ook op het oog willekeurige producten besteld, die niet echt waardevol zijn en niet/nauwelijks door te verkopen. Waarschijnlijk betreft het wel vaak "draagbare" zaken (geen koelkasten of 60 inch TV's).

Faciliterende elementen

- Een webshop met relevante koopwaar voor crimineel.
- Productkennis over welke producten makkelijk zijn door te verkopen.

Interventies

- Tijdelijk blokkeren bestellingen (tot check bij klant) wanneer afleveradres wordt aangepast, wanneer kort daarvoor zowel e-mail als een ander gegeven is aangepast.
    - Actie voor: webshop
- Hogere veiligheidseisen stellen aan bepaalde producten, of vanaf een bepaald bedrag van de bestelling. Dit doen sommige webshops nu al.
    - Actie voor: webshops.
- Continuous Authentication: continu checken, aan de hand van je accountgedragingen. Grote webshops, internationaal en in NL, zijn hiermee bezig, maar staat nog in de kinderschoenen. Er wordt ook gekeken welke browser iemand gebruikt om in te loggen. Als het gedrag afwijkt van normaal kan er worden ingegrepen. Privacy kan een issue zijn met deze methode.
    - Actie voor: grote webshops.
- Bestelgeschiedenis van de klant meenemen in een overweging hoe "normaal" de bestelling is.

Stap 5: Betalen

Beschrijving

Het betalen van de bestelling via het account van het slachtoffer. We zien verschillende manieren van betalen bij frauduleuze bestellingen:

- Achteraf betalen.
- Betalingen met tegoeden van de webshop, gekoppeld aan het account.

Er wordt, voor zover wij weten, minder gebruik gemaakt van gestolen creditcardgegevens een andere aan het account gekoppelde betaalaccounts. Gestolen creditcardgegevens worden meer gebruikt om nieuwe accounts aan te maken. Zelfs de grote webshops hebben slechts een laag percentage "high value accounts", waar de creditcardgegevens van de klant aan gekoppeld zijn.

Faciliterende elementen

- Mogelijkheid achteraf betalen.
- Gekoppelde creditcardgegevens.
- Bestaand tegoed op account.

Interventies

- Maak inloggen bij betaalapplicaties noodzakelijk waar dat nog niet het geval is. Dit zou een zeer groot deel van de fraudegevallen volgens onze MO kunnen stoppen. Zelfs bij achteraf betalen zou het mogelijk zijn om in te loggen op een geverifieerde manier (bijvoorbeeld via IRMA).
    - Actie voor: webshop
- Houd de mogelijkheid voor achteraf betalen, maar voor de helft van het bedrag (is juridische verplichting voor webshops)
    - Actie voor: webshop

Stap 6: Aflevering

De goederen worden afgeleverd door de leverancier en door iemand (een katvanger of medeplichtige van de hacker) afgevangen. We benoemen de volgende zes typen afleveradressen: (1) bestaand adres van klant (zonder wijzigingen), (2) bestaand adres, maar gewijzigd, (3) nepadres (bijvoorbeeld door een extra nummer of nummertoevoeging op te nemen), (4) afhaalpunten met identificeerplicht, (5) afhaalpunt zonder identificeerplicht (6) niet afleveren maar achteroverdrukken door corrupte chauffeurs of overvallen van chauffeurs. We zien dat bij webshops meestal voor afleverpunten wordt gekozen en bij telecomaanbieders meestal voor huisadressen. In het geval van huisadressen gaat het meestal om bestaande gewijzigde adressen (niet van oorspronkelijke klant). Hierbij kan het pakket in sommige gevallen al worden afgevangen voordat het adres bereikt (bijv. in portiekwoningen). Dat het adres van de klant wordt gebruikt zien we vrijwel niet (en lijken meestal fouten te zijn), evenals nepadressen.

Faciliterende elementen:

- gecompromitteerde bezorgers / sorteerders
- vervoer naar locatie
- kopieën van) (fake) ID's
- controle over e-mailverkeer met afhaalcode

Bestaand adres van klant (zonder wijzigingen)

Beschrijving

De crimineel past in dit geval niet de aflevergegevens van de klant aan, maar gebruikt katvangers om de pakketjes af te vangen voor het huis.

Interventies

- Verificatie van identiteit op adres bij afleveren bestelling. Hier zouden postorderbedrijven een rol in kunnen vervullen. De vraag is wel in hoeverre hiervoor geld beschikbaar kan worden gemaakt.
- Afleveren alleen na aanbellen aan deur. Dit is nu al standaard beleid bij postorderbedrijven, maar aangezien de meeste bezorgers per pakketje betaald worden is de verleiding groot om het pakketje al vóór de deur af te geven aan iemand.

Bestaand adres; gewijzigd (niet van oorspronkelijke klant)

Beschrijving

Dit komt op twee manieren voor:

- Naar zichzelf: Crimineel stuurt het pakketje naar een adres van een katvanger, of naar zichzelf, om het op die manier gemakkelijk bezorgd te krijgen.
- Naar een ander: Crimineel stuurt pakketje naar een ander adres, waar het pakketje later wordt opgehaald met een verhaal (bijvoorbeeld dat er een typefout in het adres was gemaakt). Dit komt vaker voor bij adressen waarvan kennelijk bekend is dat er ouderen wonen.

Interventies

- Bewustwording(scampagne) onder ouderen in seniorenflats, aanleunwoningen e.d.
- Extra controle door chauffeur bij tussentijds (dus bij bezorgdienst) aangepaste adressen

Nepadres

Beschrijving

Hier wijzigt de crimineel het afleveradres steeds lichtelijk, bijvoorbeeld door toevoegen van nummertoevoeging, om zogenaamd meerdere adressen te hebben. In de praktijk zal een postbezorger een pakketje voor 68-A vaak gewoon afleveren bij nummer 68 als er geen A is. Op die manier kan een crimineel bijvoorbeeld steeds bij zichzelf thuis laten bezorgen. Ook is het makkelijk

om een pakketje aan te nemen van een verwarde postbezorger die de juiste brievenbus niet kan vinden van nummer 30 terwijl de straat / flat maar 28 huisnummers heeft.
Interventies

- Niet afgeven als er ook sprake is van tussentijds (dus bij bezorgdienst) aangepaste adressen.

Afhaalpunt met identificeerplicht
Beschrijving
Dit betreft de meeste afhaalpunten. Bij PostNL afleverpunten is aangegeven dat ID-bewijzen worden gescand. Het is niet mogelijk om bestellingen af te halen met kopieën van ID-bewijzen.
Interventies

- Erop toezien dat identiteitsbewijzen inderdaad gevraagd worden en dat fraudeurs hier niet onderuit komen.

Afhaalpunt zonder identificeerplicht
Beschrijving
Deze punten zijn kwetsbaar voor katvangers, omdat afhalers zich niet hoeven te identificeren.
Interventies

- Controleren van camerabeelden.
- Deze service niet meer aanbieden

Niet afleveren: achteroverdrukken door chauffeur of overvallen van chauffeur
Beschrijving
Dit is een probleem van postorderbedrijven. De chauffeur krijgt vaak niet veel betaald, en is daarom vatbaar voor het geld dat criminelen hem mogelijk aanbieden, in ruil voor samenwerking. Postorderbedrijven hebben dit probleem op de radar, maar het is nog niet opgelost. Het overvallen van een chauffeur komt veel minder voor nu er minder via rembours wordt betaald.

Interventies

- Beperken reimboursbetalingen
- Monitoren van chauffeurs, bijvoorbeeld door hun afgelegde route bij te houden via een GPS-tracker.

Stap 7: Heling / witwassen

Beschrijving
De gestolen goederen worden verkocht t.b.v. cash, of andere middelen. Hier hebben we weinig zicht op, maar het lijkt erop dat bestelde producten regelmatig via Marktplaats of Used Products worden verkocht. Daar worden soms ook gehackte accounts voor gebruikt, of accounts waaraan een e-mailadres of telefoonnummer is gekoppeld dat ook in de gehackte webshopaccounts wordt gebruikt.

Interventies
Opsporing door politie en OM: De gestolen goederen worden gebruikt en zijn daarmee mogelijk te traceren. Gestolen apparaten worden in veel gevallen gekoppeld aan internet of op een andere manier gekoppeld aan de fabrikant. Dit biedt mogelijkheden om ze te traceren, bijvoorbeeld op basis van serienummer.