



Beveiliging 360: jaarlijks trendrapport

Mobiele apparaten



Voorwoord

In verschillende sectoren en voor verschillende use cases, van retail tot de gezondheidszorg, zoeken bedrijfsleiders innovatieve manieren met mobiele apparaten (zoals smartphones en tablets) om mensen anders te laten werken en om resultaten voor de organisatie te optimaliseren. Veel werknemers in verschillende sectoren werken vrijwel alleen nog maar met mobiele apparaten. En bij de moderne werkplek gaat het erom werknemers in staat te stellen overal en altijd verbinding te maken via het apparaat van hun voorkeur.

Een van de belangrijkste factoren die mobiel werken bevorderde, was de acceptatie van mobiliteit als werkpleksservice. Het zijn niet langer apparaten voor erbij, ze zijn steeds vaker het belangrijkste middel voor werknemers om toegang te krijgen tot de resources die ze nodig hebben om hun werk te doen. Nu mobiliteit geen onbekende op de werkplek meer is, wordt de steeds verdergaande integratie ervan in belangrijke workflows duidelijker dan ooit tevoren. De werkplek van vandaag vereist niet alleen uitstekende digitale ervaringen, maar ook **veilige** digitale ervaringen die de productiviteit van werknemers maximaliseren, ongeacht waar ze werken.

– Josh Stein,
VP Product Management

Inleiding

Het Jamf-rapport Beveiliging 360 is de weerslag van een analyse van incidenten bij klanten, onderzoek naar bedreigingen en gebeurtenissen in de sector van het afgelopen jaar. Dit rapport verkent het mobiele bedreigingslandschap om de risico's waarmee organisaties te maken hebben in de schijnwerpers te zetten.

We evalueren de verschillende aanvalsvectoren die actief worden ingezet om gebruikers te misleiden, mobiele apparaten te compromitteren en organisaties te infiltreren. Aangezien deze aanvallen zich niet beperken tot kwetsbaarheden in apparaten, omvat onze analyse ook riskante apps, webbedreigingen en meer.

Naast een analyse van deze trends in bedreigingen bevat het rapport een perspectief van de CISO van Jamf om de inzichten te verschaffen die beveiligingsleiders gebruiken bij de bescherming van hun mobiele vloot op gebruikers-, apparaat-, applicatie- en netwerkniveau.

Onderzoeksmethode

Om de werkelijke impact van de beveiligingstrends die in dit rapport worden geïdentificeerd te begrijpen en te kwantificeren, hebben we onderzoek gedaan met een steekproefgroep van 1,4 miljoen apparaten die door Jamf worden beschermd. We deden onze analyse in het eerste kwartaal van 2025, en daarbij keken we naar de voorafgaande 12 maanden en bestreken we in totaal 90 landen en meerdere platforms, meer specifiek iOS, iPadOS en Android-apparaten.



De in dit onderzoek geanalyseerde metadata zijn afkomstig van geaggregeerde logbestanden die geen tot personen of organisaties te herleiden informatie bevatten: zo was de privacy beschermd en waren de hoogste normen bij het verzamelen en verwerken van gegevens gewaarborgd.

Doel van het onderzoek

Met deze analyse willen we organisaties en gebruikers inzicht geven in de nieuwe trends op het gebied van cyberbeveiliging en laten zien welke stappen organisaties en gebruikers kunnen nemen om de risico's te beperken. Bovendien geven we bevindingen van het bijzonder impactvolle onderzoek door Jamf Threat Labs, zoals ontdekte bedreigingen en kwetsbaarheden. Door ons publiek te informeren over wat er allemaal is, hopen we eventuele mythes te ontkrachten en te laten zien hoe je beveiligingen kunt implementeren om je gebruikers en gegevens te beschermen. Organisaties kunnen onder meer de volgende, meest gebruikelijke best practices implementeren:

- Telkens meteen nieuwe updates van het besturingssysteem installeren
- Gebruikers 'opvoeden' en trainen
- Toepassingen doorlichten
- Meervoudige authenticatie instellen
- Zorgen voor zero-trust beveiligingskaders
- Basisrichtlijnen voor compliance vaststellen en beheren
- Beleid voor aanvaardbaar gebruik van bedrijfsgegevens implementeren

We hebben onze analyse en ons rapport ingedeeld in vier risicocategorieën die volgens ons de hoogste prioriteit hebben voor organisaties wereldwijd:

I. Phishing via mobiel

II. Kwetsbaarhedenbeheer

III. Applicatierisico

IV. Malware en spyware



De statistieken in dit artikel zijn gebaseerd op **Apple- en Android-apparaten**.

De analyse in dit rapport is gebaseerd op Jamfs kennis over bedreigingen, een brede verzameling inzichten afgeleid van origineel bedreigingsonderzoek, reële gebruiksgegevens, nieuwsanalyses en datafeeds. Deze kennis over bedreigingen is tot stand gekomen door onderzoek door de Jamf Threat Labs- en Data Science-teams die apparaten, apps en netwerkverkeer controleren op risico's, bedreigingen en zero-day kwetsbaarheden.



We hebben ook een Beveiliging 360-rapport speciaal voor **Mac-apparaten**: dat kun je [hier](#) vinden.

Belangrijkste trends voor mobiel

I. Phishing blijft bedrijven uitdagen

Phishing blijft een van de meest voorkomende aanvalstechnieken van bedreigingsactoren, en heeft nog altijd evenveel invloed binnen het bedreigingslandschap. In september 2024 **publiceerde Apple een blogpost** met tips voor iOS-gebruikers om "om fraudepogingen te vermijden en ... wat je moet doen als je verdachte e-mails, telefoontjes of andere berichten ontvangt". Hoe veilig een platform of besturingssysteem ook is, social engineering-technieken, zoals phishing, zijn ontworpen om bedrijfsgegevens te infiltreren, en beginnen bij het minst veilige deel van het apparaat: de gebruiker.

II. Eén enkele kwetsbaarheid kan aanvallers toegang geven tot het hele systeem

Het is een gegeven: er zitten kwetsbaarheden in de software (zowel besturingssystemen als applicaties) die we dagelijks gebruiken. In **de speciale publicatie 800-124rd van het NIST** (National Institute of Standards and Technology in Amerika) staat: "In typische software komen fouten en kwetsbaarheden voor met een geschatte frequentie van ~25 fouten per 1000 regels code." De lijst Common vulnerabilities and exposures (CVE, bekende kwetsbaarheden en blootstellingen) in de National Vulnerability Database (NVD) biedt het publiek inzicht in de CVE's die er rondzwerven. Deze updates zijn van essentieel belang, maar ze moeten wel worden toegepast voordat ze nuttig kunnen zijn voor de organisatie.

Apple en Google geven belangrijke informatie wanneer een kwetsbaarheid is ontdekt, en laten weten in welke update van het besturingssysteem de kwetsbaarheid is verholpen. Eerder dit jaar bracht Apple bijvoorbeeld iOS 18.3.2 uit naar aanleiding van **CVE-2025-24201**: bij deze kwetsbaarheid kon kwaadaardige webcontent uit de sandbox voor webcontent breken. **Google gaf het Android-beveiligingsbulletin uit**, waarin 43 beveiligingsproblemen worden behandeld, waaronder twee kritieke 'zero-day'-problemen.

III. Apps introduceren risico's, ook in veilige platforms

Sinds hun introductie beschermen de App Store van Apple en de Play Store van Google zowel gebruikers als organisaties. Apple-gebruikers worden beschermd wanneer ze apps uit de App Store downloaden en gebruiken omdat Apple "**elke app scant op malware en andere software die van invloed kan zijn op de veiligheid, beveiliging en privacy van gebruikers**". Voor Android-gebruikers is er Google Play Protect van de Google Play Store. Maar dat houdt bedreigingsactoren niet tegen. In de afgelopen vijf jaar heeft Apple meer dan 9 miljard dollar aan mogelijk frauduleuze transacties voorkomen. **De Verordening digitale markten (DMA) van de Europese Unie** staat de oprichting van alternatieve app-marktplaatsen toe en verplicht 'poortwachters' om hun ommuurde ruimten open te stellen. Apps die gedistribueerd worden via alternatieve appstores volgen niet dezelfde richtlijnen als de App Store-apps van Apple, waardoor er mogelijk risico's ontstaan voor de beveiliging, privacy en veiligheid van gebruikers. Bijvoorbeeld social engineering (bijv. phishing), ransomware en spyware voor consumenten worden beschreven als risico's die kunnen worden geïntroduceerd voor gebruikers die apps downloaden of alternatieve betalingssystemen gebruiken buiten de Apple App Store om.

Voor Android-apparaten **waarschuwde Google eerder dit jaar voor een nieuwe trojan** die was ontdekt "bij aanvallen op meer dan 750 legitieme bank- en winkelapps". En nu werden de twee meest gebruikte appstores gedwongen om gebruikers toe te staan om apps te sideloaden in de EU, waarmee het aanvalsoppervlak voor bedreigingsactoren werd geopend.

IV. Gerichte aanvallen brengen mobiele apparaten in gevaar

Mobiele apparaten bieden ons de flexibiliteit om te werken waar we dat willen of moeten; vaak zijn spraakmakende gebruikers afhankelijk van hun mobiele apparaten om overal ter wereld zaken te doen. **Maar juist spraakmakende gebruikers zijn vaak het meest geliefde doelwit** vanwege de gegevens die op hun apparaten staan, zoals intellectueel eigendom en financiële gegevens. Aanvallers verwachten met spraakmakende personen met goede connecties de hoogst mogelijke opbrengst van hun chantagelannen te realiseren.

In de afgelopen twaalf maanden ontdekten we dat:



25%

van de organisaties is getroffen door een social engineering-aanval



1 op de 10

gebruikers klikte op een schadelijke phishinglink

I. Mobiel phishing

Phishing is momenteel een van de meest voorkomende en schadelijke bedreigingen voor organisaties. Volgens het Cybersecurity & Infrastructure Security Agency van de Amerikaanse overheid begint "meer dan 90% van de succesvolle cyberaanvallen **met een phishingmail**".

Phishing komt via verschillende kanalen op mobiele apparaten: niet alleen meer via e-mail, maar ook via sms-berichten (smishing genoemd), sociale media of links naar nepwebsites.

Maar waarom hebben aanvallers met phishing zoveel meer succes op mobiele apparaten?

Ten eerste is het belangrijk om te begrijpen dat **wereldwijd meer dan 62% van de bekeken webpagina's** op mobiele apparaten zijn bekeken. Dit betekent dat mobiele apparaten een groter deel van het internetverkeer uitmaken, waardoor bedreigingsactoren een grotere groep potentiële doelwitten hebben om kwetsbaarheden op te sporen.

Mobiele apparaten zijn bovendien compacte apparaten met kleinere schermen. Daar is ook deels hun populariteit aan te danken: door hun formaat kunnen gebruikers ze overal mee naartoe nemen. Bovendien stellen ze organisaties in staat om workflows met mobiele apparaten te implementeren, zoals in:

- Detailhandel (verkooppunt of voorraad)
- Gezondheidszorg (verpleegfondes of aan het bed van de patiënt)
- Productie (instructies voor operator/machine)
- Luchtvaart (electronic flight bags of apparaten onder de vleugel)

Maar deze voordelen zorgen er ook voor dat gebruikers makkelijk afgeleid zijn bij kwaadaardige phishingaanvallen. De perceptie dat mobiele apparaten inherent veilig zijn, blijft bestaan, maar zoals we hebben beschreven is er maar één link nodig om een apparaat te compromitteren.

De twintig merken die het meest worden gebruikt in phishingcampagnes

Met mobiele apparaten kunnen organisaties nieuwe workflows implementeren, het contact met klanten stroomlijnen en de gebruikerservaring verbeteren. Velen van ons werken tegenwoordig met een mobiel apparaat, of dat nu een van de vele apparaten is die je gebruikt of het belangrijkste toegangspunt. De mobiel is onze verbinding met alles om ons heen, zowel op het werk als thuis. Aanvallers weten dit en maken er gebruik van voor hun kwaadaardige activiteiten.

In ons onderzoek ontdekten we dat bepaalde populaire merken worden gebruikt bij social engineering-aanvallen om de goedgelovigheid van eindgebruikers op mobiele apparaten uit te buiten. We hebben deze merken onderverdeeld in **vier categorieën** die het meest worden gebruikt om het vertrouwen van eindgebruikers misbruiken:

Er zijn talloze redenen om mobiele apparaten te gebruiken (zoals toegang krijgen tot e-mails op het werk, een huishoudelijk artikel bestellen, bankieren) en dat maakt dat bedreigingsactoren vaak via dit soort veelvoorkomende, vaak noodzakelijke, scenario's proberen toegang te krijgen tot gegevens. In de onderstaande tabel zie je de twintig merken die het meest werden gebruikt in social engineering, uitgesplitst in deze vier categorieën.

1.	2.	3.	4.
Entertainment	Business	Nutsbedrijven	Privé
Netflix Bet365 Steam	Outlook Office365 Allegro InterActive Corp Tencent	United States Postal Service Gazprom AT&T Inc Orange S.A. DHL BT Group	Amazon.com Inc Telegram Facebook, Inc Chase WhatsApp Yahoo, Inc.

Vanwege hun populariteit, aanzien en impact op zowel bedrijven als individuele personen worden deze merken vaak door bedreigingsactoren gebruikt in social engineering-aanvallen. Door hun reputatie als een betrouwbaar bedrijf zijn gebruikers eerder geneigd om in te gaan op kwaadaardige content vermomd als legitieme communicatie.

Deze lijst toont slechts de top twintig van getroffen merken van het afgelopen jaar, en is verre van volledig. Aanvallers passen zich voortdurend aan en welke merken ze nabootsen, kan op elk moment veranderen. Uiteindelijk onderstreept dit hoe aanvallers het vertrouwen dat deze merken in de loop der jaren hebben opgebouwd, misbruiken om gebruikers te misleiden en uit te buiten.

In de moderne wereld lopen onze persoonlijke gegevens voortdurend gevaar. Nu er steeds meer mobiele apparaten worden gebruikt voor werk en privé, wordt het bereik van de aanvaller steeds groter. Aanvallers zetten geavanceerdere tactieken in en maken gebruik van realistische interfaces, gebruikerservaringen en authentieke communicatiestijlen om nietsvermoedende slachtoffers in hun val te lokken. Maar organisaties kunnen voorzorgsmaatregelen (zoals voortdurende training van medewerkers en tools om bedreigingen te voorkomen) treffen om hun gebruikers en gegevens te beschermen.



Jamf identificeerde in onze onderzoeksperiode van **12 maanden** ongeveer **10 miljoen phishing-aanvallen** op onze steekproefgroep van **1,4 miljoen apparaten**.

Daarnaast ontdekten we dat **1,5-2%** van deze aanvallen regelmatig werd geclassificeerd als '**zero day**', wat betekent dat de aanvallers gloednieuwe, nooit eerder vertoonde bestemmingen gebruikten om gebruikers te verleiden op kwaadaardige koppelingen te klikken.

Het identificeren en verifiëren van 'zero-day' phishingaanvallen helpt organisaties om gebruikers te beschermen tegen gloednieuwe en nog niet ontdekte phishingsites

Het perspectief van een CISO

- **Introduceer een robuust trainingsprogramma:**
dit is een integraal onderdeel van ons succes. We voeren geavanceerde phishingcampagnes uit, geven training in gamevorm, bieden eenmalige trainingen voor gebruikers die daarom vragen en stellen gebruikers in staat om phishingmails te melden, terwijl ze het hele jaar door naadloos een bevestiging van en feedback op hun meldingen ontvangen. Dit is voor ons niet een training die je jaarlijks kunt afvinken.
- **Blijf op de hoogte van nieuwe trends en tactieken:**
dit lijkt misschien een open deur, maar aanvallers zullen altijd misbruik maken van kansen en vaak is dat iets nieuws, baanbrekends of controversieels dat in het nieuws is. Je moet je training en blokkeringstactieken aanpassen om die situaties aan te pakken. Dit kan enige onrust veroorzaken onder gebruikers, maar blijf transparant. De training is bedoeld om ze voor te bereiden op een potentiële slechte actor die geen rekening houdt met hun gevoelens wanneer ze schade toebrengen en die vaak juist op zoek is naar een emotionele reactie om een slachtoffer te verwarren en te slim af te zijn.
- **Zorg voor een gelaagde aanpak:**
er is niet één complete oplossing of tool om te voorkomen dat je slachtoffer wordt van een gerichte phishingcampagne. Zorg dat je vanuit meerdere kanten gedekt bent. Blokkeer kwaadaardige domeinen. Zorg voor MFA. Gebruik een zero-trust methodologie. Schakel regels voor onmogelijke snelheden in. Misschien is het niet genoeg om een of twee van deze methoden toe te passen, maar het afdwingen van meerdere beveiligingslagen is de beste manier om te voorkomen dat ook jij slachtoffer wordt van een phishingaanval.

II. Kwetsbaarhedenbeheer

Een kwetsbaarheid is een zwak punt of fout in een systeem, applicatie of protocol dat kan worden uitgebuit door aanvallers om de veiligheid, integriteit en/of beschikbaarheid van de betreffende systemen, applicaties of protocollen in gevaar te brengen. **Apple** en **Google** bieden een lijst met bekende kwetsbaarheden die hun besturingssystemen troffen. Maar dit betekent wel dat deze kwetsbaarheden bestaan zolang Apple of Google er geen update of beveiligingspatch voor hebben uitgebracht. Van 1 januari 2024 tot 1 april 2025 heeft Apple **29 beveiligingsupdates** vastgelegd met bijbehorende CVE's voor grote en kleine iOS-versies. En in diezelfde periode legde Android **39 systeemkwetsbaarheden** met bijbehorende CVE's vast in het Android Security Bulletin.

Apple en Google brengen standalone beveiligingspatches uit tussen software-updates door, respectievelijk via **Rapid Security Responses** en **Android Security Patches**. Het voordeel van deze patches? Het zijn snelle updates, wat betekent dat organisaties updates automatisch kunnen installeren zonder te hoeven wachten op grotere updates.



Nieuwe **cyberbedreigingen** zijn creatief en complex en zowel consumenten als bedrijven moeten alert zijn met het updaten van hun apparaten. En ze moeten niet alleen het apparaat updaten, ze moeten ook controleren of de **updateauthenticatie** is.

Jamf Threat Labs heeft zich onlangs verdiept in een specifiek aspect tijdens een aanvalsreeks: volharding. Hun onderzoek toonde aan hoe "tegenstanders de iOS-instellingeninterface konden misbruiken en konden knoeien met de instellingen voor systeemupdates, compleet met prompts en meldingen die aangeven dat er een update van iOS beschikbaar is".



Laten we eens wat dieper ingaan op een aantal opmerkelijke kwetsbaarheden van recente Apple-releases (dit rapport is geschreven in april 2025):



Apple CVE-oplossing	Datum	Kwetsbaarheidsscore	Impact
iOS 18.4.1 en iPadOS 18.4.1	April 2025	CVE-2025-31200 CVSS - Score: 7,5 Ernst: Hoog	CoreAudio
iOS 18.4 en iPadOS 18.4	April 2025	CVE-2025-30430 CVSS - Score: 9,8 Ernst: Kritiek	Authenticatieservices
iOS 18.3 en iPadOS 18.3	Januari 2025	CVE-2025-24085 CVSS - score: 7,8 Ernst: Hoog	CoreMedia
iOS 18.3 en iPadOS 18.3	Januari 2025	CVE-2025-24154 CVSS - Score: 9,1 Ernst: Kritiek	WebContentFilter



Bijgewerkte AOSP*-versies	Datum	Kwetsbaarheidsscore	Impact
13, 14, 15	April 2025	CVE-2025-26416 Ernst: kritiek	Escalatie van privileges
15	Maart 2025	CVE-2025-22403 Ernst: kritiek	Uitvoering van code op afstand
15	Februari 2025	CVE-2025-0096 Ernst: Hoog	Escalatie van privileges
12, 12L, 13, 14, 15	Januari 2025	CVE-2024-43771 Ernst: kritiek	Uitvoering van code op afstand

*Android Open Source Project

De kwetsbaarheden, allemaal geregistreerd op de website van Apple en Android, laten zien dat bij het bouwen van software kwetsbaarheden kunnen optreden. Voor beveiligingsprofessionals is het belangrijk dat ze deze kwetsbaarheden kunnen bekijken en er actie op kunnen ondernemen om je gegevens veilig te houden.

Een van de beste manieren om dat te doen is door steeds de recentste besturingssystemen te installeren, en de juiste tools te gebruiken om die updates uit te rollen.

Handhaaf een goede beveiligingshouding met de recentste besturingssysteemversie

De beste manier voor bedrijven om kwetsbaarheden te beperken en te zorgen dat hun organisatie compliant is, is door de apparaten steeds te voorzien van het recentste besturingssysteem. Zoals je op de vorige pagina zag, bieden zowel Apple als Android regelmatig updates voor besturingssystemen met bekende kwetsbaarheden.

Een gebruikelijke manier waarop organisaties hun besturingssysteem (en de zakelijke apps die hun werknemers dagelijks gebruiken) bijwerken, is met een oplossing voor het beheer van mobiele apparaten (MDM). MDM biedt ook uitgebreide inventarisatierapporten voor het OS dat op elk beheerd apparaat is geïnstalleerd. Maar vaak zijn er in organisaties allerlei apparaten in omloop voor verschillende doeleinden, waarop verschillende apps voor verschillende gebruikers worden uitgevoerd. Het is moeilijk (en vaak niet haalbaar, zoals het testen van apps voordat ze worden uitgerold) om ervoor te zorgen dat elk apparaat in een vloot het meest recente besturingssysteem heeft.

In de afgelopen twaalf maanden:



Had

32%

van de organisaties minstens één apparaat met kritieke (en herstelbare) kwetsbaarheden in gebruik



Draaide

55,1%

van de mobiele apparaten die op het werk worden gebruikt op een kwetsbaar OS



Organisaties bleken mobiele apparaten te gebruiken zonder de nieuwste beveiligingspatches. Uit onze gegevens bleek dat **4,8%** van alle Android-apparaten met kwetsbaarheden werden gebruikt om toegang te krijgen tot bedrijfsbronnen.

Door mobiliteit kunnen we werken zoals we willen. Van het aannemen van een zakelijk telefoontje in de auto tot het uitbreiden van workflows voor eerstelijnsmedewerkers die direct contact met de klant hebben, mobiele apparaten bieden toegang tot alles wat mogelijk is op het werk. Maar net als elk computerapparaat is het systeem kwetsbaar voor bedreigingsactoren. Organisaties kunnen stappen nemen om bedreigingen op hun mobiele apparaten te beperken met tools die een balans bieden tussen gebruiksvriendelijkheid en veiligheid, training van medewerkers en inzicht in de meest voorkomende bedreigingen van dit moment.

Het perspectief van een CISO

- **Houd zicht op de kwetsbaarheden binnen je organisatie:** zoveel mogelijk inzicht krijgen in de kwetsbaarheden op de apparaten van je eindgebruikers of in je infrastructuur is een goed uitgangspunt. Je kunt met die gegevens beginnen om specifieke informatie over footprint, potentiële risico's, impactradius en dergelijke van de app te analyseren. Dit is een uitstekende manier om op basis van gegevens de prioriteit van de verschillende kwetsbaarheden te bepalen.
- **Introduceer een solide patchprogramma:** om terug te komen op MDM: voor een gezonde en veilige omgeving is het van het grootste belang dat je een tool hebt die ervoor zorgt dat je steeds de nieuwste of ondersteunde N-X versies van software of het OS hebt geïnstalleerd. Als je dit doet met weinig tot geen impact op eindgebruikers, wordt het alleen maar gemakkelijker om samen te werken en het bedrijf meer mogelijkheden te bieden
- **Implementeer een op risico's gebaseerde toegangs aanpak:** als er in je omgeving apparaten zijn die niet aan je voorwaarden voldoen en die toegang proberen te krijgen tot resources van je bedrijf, moet je die toegang beperken totdat de eindgebruiker de maatregelen kan treffen om dat apparaat zo makkelijk mogelijk weer te laten voldoen aan de voorwaarden.

III. Apprisico

Eind november 2024 publiceerde het Cybersecurity Agency van de Amerikaanse overheid **een rapport over de meest routinematig uitgebuite kwetsbaarheden in 2023** (dit is de nieuwste versie van het rapport). Het rapport gaat dieper in op de belangrijkste vijftien kwetsbaarheden en geeft meer informatie over wat aanvallers met die kwetsbaarheden kunnen doen. De kwetsbaarheden doen zich voor in besturingssystemen op verschillende computerplatforms en in applicaties die studenten en medewerkers van organisaties dagelijks gebruiken. Zoals in het rapport staat: "Kwaadwillende cyberactoren maakten in 2023 meer gebruik van zero-day kwetsbaarheden om enterprisenetwerken te compromitteren dan in 2022, waardoor ze acties konden uitvoeren tegen doelen met een hoge prioriteit." Het Cybersecurity Agency geeft verder aan wat ontwikkelaars en eindgebruikersorganisaties kunnen doen om kwetsbaarheden te beperken. Voor eindgebruikersorganisaties noemt het rapport:

- Software, OS, apps en firmware *tijdig* bijwerken
- Routinematig een geautomatiseerde asset-discovery laten uitvoeren
- Een robuust patchbeheerproces implementeren
- Veilige basisconfiguraties vastleggen
- Regelmatige beveiligde systeemback-ups uitvoeren
- Ervoor zorgen dat het responsplan voor cyberbeveiligingsincidenten steeds geactualiseerd wordt

Wat maakt een app 'riskant'? Enkele van de belangrijkste kenmerken van riskante apps zijn:

- Afwijkende kenmerken
- Kwaadaardige codepatronen
- Gevaarlijke machtigingen
- Riskant dynamisch gedrag
- Verdachte ontwikkelaarsprofielen

Door inzicht te krijgen in appversies, eventuele lekkende apps en dergelijke kunnen organisaties hun aanvallers voor blijven: klaar om onmiddellijk het risico te onderzoeken en in te grijpen.

Het is belangrijk voor bedrijven om inzicht te hebben in de volledige status van hun applicaties. Enkele van de belangrijkste gegevens waar organisaties op moeten letten om riskante apps te identificeren en op te lossen zijn:

- Aantal gebruikers die een verouderde app hebben geïnstalleerd
- Aantal gebruikers met een specifieke appversie
- Lijst van apps met gaten in coderingsimplementaties, waardoor gevoelige gegevens kunnen lekken naar onbeveiligde netwerken
- Apps die bepaalde toestemmingen vragen om toegang te krijgen tot gegevens op andere delen van het apparaat



Een nadere blik op een reële kwetsbaarheid die Transparency, Consent and Control (TCC) omzeilt

In de besturingssystemen van Apple biedt het TCC-mechanisme een cruciaal beveiligingsframework: het vraagt gebruikers om verzoeken van afzonderlijke apps om toegang te krijgen tot gevoelige gegevens, zoals foto's, contacten en locatiegegevens, toe te staan of te weigeren. Een TCC bypass-kwetsbaarheid treedt op wanneer deze controle faalt, waardoor een applicatie toegang kan krijgen tot privégegevens zonder toestemming of medeweten van de gebruiker. Dit betekent dat aanvallers ongeautoriseerde toegang kunnen krijgen tot bestanden en mappen, statusgegevens, de microfoon en/of de camera zonder gebruikers te waarschuwen.

Jamf Threat Labs ontdekte CVE-2024-44131, een TCC bypass-kwetsbaarheid die File Provider op iOS-apparaten treft. Apple reageerde snel op deze ontdekking met een patch in iOS 18.0. CVE's, zoals CVE-2024-44131, zijn belangrijke herinneringen aan de noodzaak om organisatorische apparaten up-to-date te houden.

App Store-bescherming en fraudepogingen

Eerder in dit rapport werd al vermeld dat Apple in de afgelopen vijf jaar voor meer dan 9 miljard dollar aan frauduleuze transacties heeft voorkomen. Alleen al in 2024 blokkeerde het bedrijf meer dan 2 miljard dollar aan frauduleuze transacties. En verder heeft Apple in 2024:

- Meer dan 146.000 accounts van ontwikkelaars beëindigd vanwege mogelijke fraude
- Nog eens 139.000 inschrijvingen van ontwikkelaars afgewezen
- Meer dan 43.000 ingediende apps afgewezen omdat ze verborgen of niet-beschreven functies bevatten
- Meer dan 320.000 ingediende apps afgewezen die een kopie van andere apps of spam bleken te zijn of gebruikers op een andere manier misleidden
- Meer dan 10.000 illegale apps op illegale verkooppunten gedetecteerd en geblokkeerd

De App Store wordt over het algemeen beschouwd als de veiligste, meest gebruiksvriendelijke en meest privacyvriendelijke manier om apps te downloaden. De App Store voor iOS gebruikt sandboxing, vraagt de gebruiker om toestemming en laat alleen ondertekende code op het apparaat draaien. Maar zoals de gegevens laten zien, blijven slechte actoren en potentiële fraude bestaan. De toewijding van Apple om te zorgen dat de App Store een veilige, vertrouwde plek voor applicaties blijft, beschermt gebruikers en ontwikkelaars al sinds de introductie van de App Store in 2008. Maar 'sideloaded apps', apps uit appstores van derden, zoals AltStore, hebben niet dezelfde bescherming.

Het perspectief van een CISO

Effectieve mobiele beveiliging vereist een gelaagde aanpak. Ook wanneer je de nieuwste hardware van een betrouwbare leverancier hebt, met het meest recente besturingssysteem zijn je organisatie en je meest gevoelige bedrijfsmiddelen nog niet 100% beschermd tegen aantasting. Goede beveiligingspraktijken moeten zich uitstrekken tot elk laag van je technologiestapel, en hier vallen ook applicaties onder.

- **Introduceer een doorlichtingsprogramma voor de gevoelige mobiele apps van je organisatie:**
begin met de meest kritieke apps en controleer routinematig of overal alleen de nieuwste, veilige versies worden uitgevoerd. Als je het applicatieprogramma uitbreidt, moet je elke applicatie die in je enterprise-appstore terechtkomt, doorlichten.
- **Ontwikkel beleid dat aangeeft dat apparaten niet meer aan de voorwaarden voldoen** wanneer er ongewenste applicaties op zijn geïnstalleerd en voorkom dat deze risicovolle apparaten toegang krijgen tot je SaaS-applicaties, kritieke datacenters of externe workloads zolang de riskante apps niet zijn bijgewerkt of verwijderd.
- **Neem de beveiliging van mobiele apps op in trainingsprogramma's**, zodat gebruikers een deel van de oplossing kunnen worden door waar nodig updates uit te voeren op apparaten die ze de hele werkdag of werkweek bij zich hebben.
- **Als je organisatie geen alternatieve marktplaatsen voor apps vereist**, stel dan beleid op om te voorkomen dat gebruikers naar alternatieve winkels gaan op apparaten van het werk. Voorkom bovendien het apps via sideloading worden geïnstalleerd, zodat je zeker weet dat er alleen apps van officiële bronnen op het apparaat worden gebruikt.

Het Jamf Threat Labs team publiceerde een demonstratie van hoe een sideloaded app voor social media foto's kan volgen en uploaden naar een server van de aanvaller. Deze applicatie was 'aangepast, maar volledig functioneel'. Het team biedt een aantal duidelijke beveiligingen om de veiligheid te vergroten, namelijk:

- Het rapport over privacy van apps inschakelen en regelmatig controleren
- Selectief zijn met rechten voor apps
- Geen gevoelige informatie opslaan

Alleen apps van betrouwbare bronnen (zoals de App Store) downloaden

Zowel native applicaties als in de cloud gehoste webapplicaties kunnen risico's met zich mee brengen. Cloudapplicaties staan meer bloot aan risico's omdat ze een groter aanvalsoppervlak hebben. Maar met de juiste zichtbaarheid, controle en mogelijkheden om in te grijpen kunnen organisaties risicovolle applicaties op het werk beperken.

IV. Gerichte aanvallen en geavanceerde spyware

Sinds 2021 heeft Apple meldingen van bedreigingen gestuurd naar gebruikers in meer dan 150 landen. Deze meldingen informeren en helpen gebruikers, meestal personen die in de aandacht staan, zoals journalisten, politici of diplomaten, die het doelwit zijn van spyware-aanvallen die in opdracht worden uitgevoerd. En eind april 2025 meldde Apple dat het "deze week meldingen [heeft gestuurd] naar verschillende mensen die volgens het bedrijf het doelwit waren van spyware van een overheid". Maar niet alleen Apple wordt getroffen. Deze aanvallen zijn gericht op alle soorten besturingssystemen en apps.

Volgens The Citizen Lab was er "spyware geladen in WhatsApp en in andere apps op hun [Android]-apparaten"

Malware en spyware, zoals waarvoor Apple meldingen stuurde, behoren tot de meest geavanceerde bedreigingen waarmee organisaties en personen tegenwoordig worden geconfronteerd. Maar er zijn manieren om alle gebruikers, op elk niveau van je organisatie, te beschermen tegen deze geavanceerde bedreigingen.

Apple biedt adviezen voor gebruikers om zichzelf te beschermen tegen malware, waarvan we er al een groot aantal hebben behandeld in dit artikel. Apple adviseert gebruikers met name om:

- Apparaten bij te werken naar de nieuwste software, want deze bevat de nieuwste beveiligingsreparaties
- Apparaten te beschermen met een toegangscode
- Authenticatie met twee factoren en een sterk wachtwoord voor je Apple-account te gebruiken
- Apps te installeren vanuit de App Store
- Online sterke en unieke wachtwoorden te gebruiken
- Niet op links of bijlagen van onbekende afzenders te klikken



Jamf Threat Labs: een apparaat compromitteren zonder medeweten van het slachtoffer

Jamf Threat Labs demonstreerde hoe een apparaat zonder beschermende beveiligingssoftware werd gecompromitteerd zonder dat het slachtoffer het in de gaten had. In de demo kon je zien hoe een aanvaller toegang kon krijgen tot e-mail, zakelijke berichten, authenticatie met twee factoren en meer persoonlijke gegevens. Het team liet vervolgens zien hoe organisaties organisatorische en persoonlijke gegevens kunnen beschermen:

1.

Dwing veilige configuraties af om compliance te handhaven op zowel apparaten van het bedrijf als BYOD-apparaten

2.

Maak bedreigingspreventie en -bewaking met gerichte acties mogelijk, waarbij de privacy van de eindgebruiker behouden blijft

3.

Dwing apparaatversleuteling af op alle beheerde apparaten

Het perspectief van een CISO

Malware is niet zo wijdverbreid op mobiele apparaten als op andere primaire computerapparaten. Maar wanneer malware wordt ontdekt, blijken er vaak zeer geavanceerde technieken te zijn gebruikt en wordt met de malware op individuele personen gemikt.

- **Word niet laks** en ga er niet vanuit dat mobiele malware nooit jouw organisatie zal raken. Apple stuurde vorig jaar nog berichten over een spywareaanval naar gebruikers in ongeveer 100 landen.
- **Stel op zijn minst een leidinggevende voor mobiele beveiliging aan** en geef deze de opdracht om regelmatig te rapporteren over de status van de mobiele implementatie van je organisatie. Catalogiseer incidenten van gestolen telefoons, gerichte phishing, prestatieverslechtingen en al het andere dat wijst op afwijkend gedrag. Als je het helemaal goed wilt doen, creëer je een telemetriestroom vanuit je apparaatbeheer- en beveiligingstools en neem je die gegevens op in je Security Operations Center. Behandel mobiele apparaten als elk ander eindpunt.
- **Verzamel waar mogelijk gegevens over mobiele systemen en kijk of je signalen ziet van 'zero-day'-aanvallen.** De benodigde expertise hiervoor is mogelijk intern aanwezig of kun je uitbesteden. Enterpriseorganisaties met speciale beveiligingsanalisten moeten investeren in de ontwikkeling van expertise op het gebied van mobiel forensisch onderzoek binnen de teams.



Belangrijkste leerpunten:

Mobiele phishing is een van de meest voorkomende manieren waarop aanvallers toegang krijgen tot gevoelige informatie. Organisaties die een trainingsprogramma kunnen implementeren, trends en tactieken kunnen bijhouden (inclusief het aanpassen van trainingen) en een gelaagde benadering van beveiliging hebben, bieden bescherming vanaf verschillende kanten.

Kwetsbaarheden komen voor in allerlei soorten software. Een goede beveiligingshygiëne beperkt de risico's die kwetsbaarheden kunnen veroorzaken. Door besturingssystemen regelmatig bij te werken en onnodige besturingselementen (bijv. appstores van derden) uit te schakelen kunnen organisaties blijven voldoen aan interne richtlijnen en externe frameworks.

Onjuist beheer en gebruik van apps brengt risico's met zich mee. Het is niet altijd de app zelf, het kunnen ook apps zijn die verbinding maken met een kwaadaardig netwerk. Met een eigen appstore van de enterprise en door applicaties voortdurend door te lichten (vooral persoonlijke en aangepaste apps) kunnen organisaties kwetsbare applicaties beter bewaken, herstellen en patchen.

APT's en spyware-aanvallen komen steeds vaker voor. Deze bedreigingen (vaak afkomstig van natiestaten of speciale groepen) treffen organisaties over de hele wereld en zijn vaak gericht op in het oog springende personen met gevoelige gegevens op hun apparaat. Door een defense-in-depth beveiligingsstrategie te bieden en mobiele apparaten te behandelen als elk ander apparaat, kunnen organisaties zorgen voor beschermende maatregelen van hun ecosysteem van mobiele apparaten en gegevens waarmee apparaten verbinding maken.

Stel een beleid voor aanvaardbaar gebruik op en dwing dit af voor apparaten die eigendom van het bedrijf zijn en waarvoor een afdwingbaar beleid voor aanvaardbaar gebruik nodig is, die verbinding maken met werkresources of die moeten voldoen aan het beleid van de organisatie. Op BYOD-apparaten zijn extra privacychecks nodig, zoals de [privacybescherming die Apple biedt](#) voor apparaten.

