



Beveiliging 360: jaarlijks trendrapport

Mac

```
1 Arc Browser Executables:
2 9d103cbad2b56f53a36f93316feda1de5513394d - ArcSetup.dmg
3 ba59bb35e8dfbe77676c8130c8c2d61c22b14564 - ArcSetup (Univ
4 d294b86c5a57e90ff1f7367eb9fdad8d47193f22 - ArcSetup (x86)
5 af33c2bc39373a5607b0c38a62919c59f5ad884 - ArcSetup (ARM)
6
7 5687190b00a1efald3671d0b03b8f69da6d534a - ArcInstaller.d
8 28c35f4d92f3a0b185f0ffeb5b695119de823548 - ArcInstaller
9 28cc0be3aad1479c4d4ba618be6462a2c5c7ac18 - ArcInstaller
10 0ac59146723d72b2faad8a637cd9fb2a6221f7e - ArcInstaller
11
12 https://arcll.inet
13 https://arcll.inet
14 193[.]233[.]132[.]108 - Exfiltration IP
15
16 Meethub Executables:
17 7f22760d6d85f8173292d39ea087f35695ad65ab - Meethub.pkg
18 3865636ed27ae81f146ed509ac9a25f53a6d10a7 - sleeve (x86)
19
20 Chainbreaker Executables:
21 50b8af2019adbbea310bce0259b4a3f3da2e4d7d - game/installer
22 eecf5ffc338b97602b5b8f8ab8ccc51dcb8ffdb8a - game/installer
23 596fd483314c3cce43d8b5ed38b5202c29a60b14 - game/installer
24
25 https://meethub[.]gg
26 46[.]101[.]104[.]172 - Exfiltration IP
27
28 Suarometa Malware:
29 7aef8396238d96c1ffa845715373516da30e373 - SuaWorldLaunc'
```

Voorwoord

Jamf houdt van de Mac. Het is de eerste machine waarvoor we software ontwikkelden en nog steeds ligt deze machine velen van ons heel na aan het hart. (We zijn **officieel betrokken bij het macOS Security Compliance Project**.) Tijdens onze bestaansgeschiedenis hebben we de Mac een **steeds grotere rol zien innemen in de werkomgeving**. Wat begon als een machine voor creatieve beroepen en leidinggevenden, raakt steeds meer ingeburgerd in de dagelijkse werkzaamheden voor technici en andere beroepsgroepen. Maar met de steeds verdere integratie van de Mac in de werkomgeving, wordt die ook steeds interessanter voor bedreigingsactoren.

Het bedreigingslandschap voor Mac is gevarieerder dan ooit, met allerlei creatieve manieren om Macs te compromitteren. Vanuit onze missie om 'organisaties te helpen slagen met Apple' gaan we dieper in op het bedreigingslandschap voor Mac-apparaten ten behoeve van onze klanten en de Apple-gemeenschap in het algemeen.

- Jaron Bradley,
Directeur, Jamf Threat Labs

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. Het rapport verkent het Mac-landschap om de risico's waarmee organisaties te maken hebben in de schijnwerpers te zetten.

We evalueren de verschillende aanvalsvectoren (zoals malware, kwetsbaarheden en social engineering) die actief worden ingezet om gebruikers te misleiden, apparaten te compromitteren en organisaties te infiltreren. De analyse omvat onderwerpen als kwetsbaarheden van apparaten, webbedreigingen en malware.

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 Mac 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.



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 veiligheidsnormen 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 malware en kwetsbaarheden.

Iedereen kan verschillende acties ondernemen om de beveiliging van zijn Mac te verbeteren. Download bijvoorbeeld alleen software van bronnen die je vertrouwt. Maar er zijn ook andere best practices die elke organisatie kan implementeren:

- Telkens meteen nieuwe updates van het besturingssysteem installeren
- Gebruikers 'opvoeden' en trainen
- Toepassingen doorlichten
- Meervoudige authenticatie instellen
- Zorgen voor zero-trust beveiligingskaders
- Beleid voor aanvaardbaar gebruik van bedrijfsgegevens
- De Apple-best workflows implementeren in verschillende use cases



Sommige van deze practices zijn het absolute minimum voor iedere organisatie, maar daarnaast zijn er meer organisatiespecifieke vereisten voor apparaatbeveiliging. Organisaties in een gereguleerde sector moeten bijvoorbeeld voldoen aan sectorbenchmarks of bepaalde kaders (zoals CIS-benchmarks of HIPAA).

Dit jaar hebben we onze analyse ingedeeld in drie risicocategorieën die volgens ons de hoogste prioriteit hebben voor organisaties wereldwijd:

I. Applicatierisico en malware

II. Kwetsbaarhedenbeheer

III. Social engineering



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

Een groot deel van 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.

Belangrijkste trends voor Mac in enterprises

Malware introduceert risico's, ook in veilige platforms

Apple ontwerpt zijn **platforms met beveiliging als uitgangspunt**.

Het gaat hierbij niet alleen om de platforms zelf, maar ook om de manier waarop Apple over beveiliging communiceert met zijn gebruikers. De **Apple Platform Security-site** bevat bijvoorbeeld een pagina met informatie voor Apple-gebruikers over bescherming tegen malware in macOS. De verschillende technologieën van Apple (zoals de App Store, XProtect of Gatekeeper) bieden een gelaagde bescherming tegen kwaadaardige apps in verschillende fasen van de levenscyclus van een app.

Voor Mac-apparaten op het werk is beveiliging een evenwichtsoefening: gebruikers moeten de apps krijgen die ze nodig hebben om hun werk goed te kunnen doen, maar mogen geen toegang hebben tot applicaties die mogelijk risico's met zich mee brengen. Er zijn Mac-apps in alle soorten en maten, zoals native Mac-apps, webapps en hybride apps, die door ontwikkelaars zijn gemaakt en ontworpen voor uiteenlopende gebruikssituaties. **Veel van de momenteel meest gebruikte zakelijke apps voor de Mac** komen echter niet uit de Mac App Store, maar worden rechtstreeks door de ontwikkelaar geleverd. Bovendien kunnen gebruikers apps downloaden van elke site waartoe ze toegang hebben.

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.

Het National Institute of Standards and Technology in Amerika

stelt: "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 bekende kwetsbaarheden
- De getroffen producten of leveranciers
- Een beschrijving van bedreigingen

Tussen het moment dat een kwetsbaarheid wordt ontdekt en het moment dat die wordt gepatcht, kan er schade worden aangericht. Als er een patch beschikbaar is, kan het namelijk nog even duren voordat die is geïnstalleerd op de desbetreffende apparaten. Beveiligingstools die bijvoorbeeld laten zien welke kwetsbaarheden er zijn en welke het meest kritiek zijn, helpen IT- en InfoSec-teams om prioriteit te geven aan de meest urgente patches en hun processen te verbeteren.

Social engineering blijft gebruikers in gevaar brengen

Social engineering blijft, net als phishing, 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 gebruikers om "om fraudepogingen te vermijden en ... wat je moet doen als je verdachte e-mails, telefoontjes of andere berichten ontvangt". Aanvallers worden steeds creatiever in hun technieken en doen zich voor als recruiters, familieleden, vertrouwde merken en meer. Hoe veilig een platform of besturingssysteem ook is, social engineering-technieken zijn ontworpen om bedrijfsgegevens te infiltreren, en beginnen bij het minst veilige deel van het apparaat: de gebruiker.



Deel 1: op Mac gerichte malware

Met dit rapport willen we meer inzicht geven in Mac-malware, zoals welke soorten we hebben gezien, wat de gevolgen ervan voor organisaties zijn en hoe vaak ze optreden. Naarmate het gebruik van Macs op de werkplek toeneemt en meer essentiële applicaties via het platform gebruikt worden, zullen meer gebruikers in de organisatie het doelwit worden.

De verdediging van Apple tegen malware bestaat uit drie lagen:

1. **Introductie of uitvoering van malware voorkomen**
2. **Voorkomen dat malware wordt uitgevoerd op systemen van klanten**
3. **Systemen herstellen nadat malware is uitgevoerd**

Technologieën van Apple (App Store, GateKeeper, XProtect en Notarization) bieden gebruikers verschillende native manieren om bedreigingen te beperken. XProtect is bijvoorbeeld een ingebouwde antivirusapp. En wanneer malware wordt ontdekt, kan Apple op verschillende manieren reageren, bijvoorbeeld door een ontwikkelaars-ID intrekken.

Maar macOS is, ondanks zijn sterke, ingebouwde beveiligingsmechanismen, niet immuun voor malware. **In maart van dit jaar** werkten de Jamf Threat Labs- en Data Science-teams samen aan een artikel over de Mac-malwaremythe, over inzicht in nieuwe malware met bekende malware en over macOS-malwarevectoren met Titan, een 3D-visualisatietool ontwikkeld door Jamf Threat Labs. Titan geeft context en identificeert verwante malware-samples. De malwarefamilies die zo aan het licht kwamen, laten "het voortdurend groeiende aantal soorten malware op maat" voor macOS zien. Waarom? Mac-malware bestaat, er zijn verwante families van malware en het wordt steeds vaker gebruikt door bedreigingsactoren.

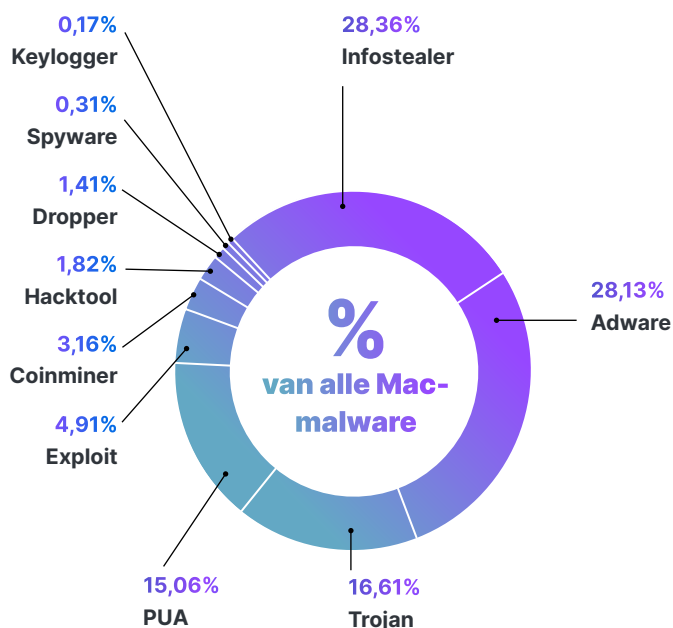


Dit jaar ontdekte Jamf Threat Labs malware die vermoedelijk gelinkt was aan de Democratische Volksrepubliek Korea (DPRK) **en was ingebed in een op Flutter gebaseerde applicatie**. Dat applicaties die zijn ontwikkeld met Flutter worden gebruikt voor platformoverschrijdende ondersteuning is niet ongewoon. Wat deze aanval echter opmerkelijk maakt, is dat het de eerste keer is dat het Jamf Threat Labs-team zag dat dit framework werd gebruikt om macOS-apparaten aan te vallen. Het team ontleedt de malware, zijn varianten in Python en Golang en onderzoekt waarom de "malware waarschijnlijk aan het testen is voor een breder gebruik als wapen". Ook viel de onbedoelde onduidelijkheid op die Flutter toepast op code geschreven door gebruikers van zijn framework.

Mac-malwarefamilies

Hieronder zie je een volledig overzicht van nieuwe Mac-malwaregevallen die in 2024 zijn onderzocht, op basis van onze bevindingen:

Wat vertellen deze gegevens ons? In vergelijking met het malwarerapport van vorig jaar zien we een aantal overeenkomsten: adware, trojans, PUA (potentieel ongewenste toepassingen) en exploits (applicaties waarvan bekend is dat ze misbruik maken van een exploit) staan nog steeds bovenaan de lijst van malwarecategorieën. (Vorig jaar hadden trojans met 17% het grootste aantal families, dit jaar met 16,6% iets minder.) De topospositie gaat dit jaar naar infostealers. Infostealers gaven een toename van maar liefst 28,08% van de totale hoeveelheid onderzochte malware te zien.



De aanwezigheid van infostealers is in lijn met het onderzoek dat Jamf Threat Labs het afgelopen jaar heeft gedaan, waarbij macOS-omgevingen constant werden aangevallen door dit soort malware. Interessant aan deze tactieken is niet alleen dat beide aanvallers infostealers gebruiken om toegang te krijgen tot de gegevens die ze willen hebben, maar dat ze ook een andere strategie toepassen die eerder in dit rapport is genoemd: social engineering. Hieruit blijkt dat bedreigingsactoren een combinatie van aanvalsprincipes gebruiken om hun slachtoffers te misleiden. Voor werknemers of organisaties in high-profile sectoren, zoals crypto, is het belangrijk om waakzaam te blijven, zowel wat betreft training als wat betreft beveiligingstools. Aanvallen doen zich niet zomaar voor, ze worden bewust ontwikkeld.



Onderzoek naar het gebruik van PyInstallers om infostealers te implementeren op macOS

In april 2025 ontdekte Jamf Threat Labs nieuwe onbekende infostealer-samples voor macOS die Python-code bundelen in Mach-O executables met behulp van PyInstaller (Jamf Threat Labs ontdekte drie onbekende stealers op VirusTotal).

PyInstaller is een legitieme, open-sourcetool waarmee ontwikkelaars Python-scripts kunnen verpakken in zelfstandige binaries. Aanvallers maken nu gebruik van dezelfde techniek om kwaadaardige payloads te leveren die probleemloos worden uitgevoerd op macOS. Het team bekeek verschillende basisfuncties om de ware aard van de malware te bevestigen: een infostealer. Enkele van deze basisfuncties zijn:

- Probeert gebruikersgegevens te verzamelen door misleidende wachtwoordprompts te activeren
- Voert willekeurige applescript-payloads uit vanaf een server van de aanvaller
- Haalt opgeslagen gegevens en gevoelige informatie rechtstreeks uit de macOS-sleutelhanger
- Scant het bestandssysteem op bekende cryptowallets om privésleutels te exfiltreren en crypto-assets te stelen

Omdat infostealers steeds vaker voorkomen in het macOS-dreigingslandschap, zullen bedreigingsactoren blijven zoeken naar nieuwe manieren om ze te verspreiden. Organisaties kunnen echter diverse praktische stappen nemen om zichzelf te beschermen tegen de hierboven beschreven malware. Bijvoorbeeld:

- Beperk de uitvoering van software tot apps die zijn ondertekend door Apple en geïdentificeerde ontwikkelaars.
- Brandmerk osascript-prompts die worden gebruikt voor legitieme IT-processen en train personeel om het merk te bevestigen voordat ze hun gegevens invoeren.

Malware om in de gaten te houden

Poolrat

Poolrat, een macOS-backdoor die berucht is vanwege zijn betrokkenheid bij de supply chain-aanval op 3CX-software, stelt aanvallers in staat om cruciale systeemgegevens te verzamelen en opdrachten gelijktijdig met bestandsbewerkingen uit te voeren. Onlangs is een lichtere versie van Poolrat, Pondrat, ontdekt.

Pondrat

Pondrat, een backdoor die overeenkomsten vertoont met zowel AppleJeus als Poolrat, werd verspreid via kwaadaardige PyPi-pakketten. Na installatie maakt Pondrat verbinding met command-and-control-servers (C2) om bestanden makkelijker te uploaden en downloaden, processen voor een bepaalde duur te pauzeren en willekeurige commando's uit te voeren.

NotLockBit

Op Golang gebaseerde ransomware die zich voordoeft als een variant van de beruchte LockBit-ransomware. Sinds de eerste proefversie gebruikt deze ransomware een ingesloten publieke sleutel om een lijst met hard-gecodeerde extensies op te sommen en te versleutelen. De meest recente varianten van NotLockBit exfiltreren gegevens naar een door de aanvallers beheerde S3-bucket en wijzigen de bureaubladachtergrond met osascript (LockBit 2.0). NotLockBit wordt vermoedelijk actief ontwikkeld.

ThiefBucket

Thiefbucket is een malwarefamilie gelinkt aan de Noord-Koreaanse Lazarus Group en richt zich op slachtoffers via geraffineerde social engineering-campagnes. Het is waargenomen als een tweede fase-payload, afgeleverd via een vermomde codeerchallenge. Deze backdoor kan verschillende acties uitvoeren, waarvan de geautomatiseerde infostealer-functionaliteit het opvallendst is. Enkele andere mogelijke acties zijn:

- Volhardingsmechanismen - Processen beëindigen - Bestanden verwijderen - Bestanden downloaden/uploaden - Zichzelf verwijderen - Shellcommando's uitvoeren - Snel bestanden zoeken via Spotlight - Communicatie met command-and-control-servers

HZ Rat

HZ Rat, een macOS-backdoor, was in eerste instantie gericht op Windows-gebruikers, maar richt zich inmiddels ook op macOS-gebruikers via vermomde legitieme software-installatieprogramma's. Na installatie maakt HZ Rat verbinding met command-and-control-servers (C2) zodat aanvallers commando's kunnen uitvoeren, bestanden kunnen stelen en gevoelige informatie zoals gebruikersnamen, e-mails, telefoonnummers en andere persoonlijke gegevens uit WeChat en DingTalk kunnen halen.

BansheeStealer

Banshee Stealer wordt aangeprezen op Telegram en werkt als een Malware-as-a-Service met een webinterface voor aanvallers. Deze malware is gespecialiseerd in het stelen van informatie en kan allerlei gevoelige gegevens exfiltreren, zoals accountwachtwoorden, browsergegevens, sessiecookies en cryptowallets. Net als andere infostealers maakt Banshee misbruik van AppleScript-dialogfuncties om gebruikers te misleiden zodat ze hun inloggegevens opgeven. Zodra de gebruiker zijn wachtwoord heeft ingevoerd, steelt de malware aanvullende gevoelige gegevens uit de macOS-sleutelhanger. Banshee maakt gebruik van verschillende ontwijkstechnieken, waaronder anti-VM- en anti-debuggingmaatregelen om analyses te dwarsbomen, en detectie van Russischtalige systemen.

InvisibleFerret

InvisibleFerret is een op Python gebaseerde trojan die wordt gebruikt door malware geïntegreerd in vermomde applicaties. Wat het meest opvalt, is dat het door de BeaverTail InfoStealer (door sommigen toegeschreven aan de DPRK) was afgegeven als een tweede-fase implantaat. Het kwaadaardige Python-script is platformonafhankelijk en stelt de aanvaller in staat om verkenningen uit te voeren, gegevens te exfiltreren, het klembord te kopiëren en commando's op afstand uit te voeren. Het kan ook de AnyDesk-software installeren als extra controle op afstand gewenst is.

BeaverTail

De infostealer BeaverTail is vermomd als een legitieme applicatie aangetroffen en vervolgens via social engineering-campagnes naar slachtoffers werd gestuurd. Net als andere infostealers haalt het waardevolle gegevens uit de sleutelhanger, browsercookies, cryptowallets enz. van het slachtoffer en uploadt het die naar een server waarover de aanvaller de controle heeft. Het kan ook op afstand extra payloads uitvoeren op het systeem van het slachtoffer, zoals de InvisibleFerret-backdoor. Het wordt door sommigen toegeschreven aan de DPRK.

PoseidonStealer

Poseidon Stealer (een concurrent van Atomic Stealer) wordt aangeprezen op Telegram en werkt als een Malware-as-a-Service met een webinterface voor aanvallers. Deze malware is gespecialiseerd in het stelen van informatie en kan allerlei gevoelige gegevens exfiltreren, zoals accountwachtwoorden, browsergegevens, sessiecookies en cryptowallets. Net als Atomic maakt Poseidon misbruik van AppleScript-dialoogfuncties om gebruikers te misleiden zodat ze hun gegevens opgeven. Zodra de gebruiker zijn wachtwoord heeft ingevoerd, steelt de malware aanvullende gevoelige gegevens uit de macOS-sleutelhanger. De malware wordt vermomd als een legitieme applicatie verspreid en wordt gepromoot via malvertising op Google Ads.

Kuiper

Kuiper is een Ransomware-as-a-Service (RaaS) ontwikkeld in Go, waarmee werd geadverteerd op ondergrondse forums door een gebruiker met de naam Robinhood. De ransomware gebruikt een combinatie van RSA, ChaCha20 (bestanden kleiner dan 600 megabytes) en AES (bestanden groter dan 600 megabytes) voor het versleutelen van bestanden. De functionaliteit van deze malware is voornamelijk gericht op Windows, maar de macOS-variant genereert een willekeurige sleutel en een willekeurige initialisatievector (IV) met behulp van `/dev/urandom`, decodeert een losgeldbrief, versleutelt het doel recursief (door een `.kuiper` extensie toe te voegen), verwijdert de sleutel en IV uit het geheugen en start het systeem opnieuw op.

Waargenomen Mac-malware

Wanneer we meer in detail kijken naar de Mac-malware die we hebben waargenomen in klantomgevingen, zien we de volgende malwarefamilies in de top 10:

Familienaam	Categorie	Percentage	
Genieo	Adware	13,63	
Imobie	PUA	10,96	
Multiverze	Adware	9,44	
Mackeeper	PUA	7,19	
Tnt	PUA	6,07	
Jailbreak	PUA	5,74	
Ccleanmac	Adware	4,33	
Puagent	Trojan	3,07	
Macinforme	PUA	2,33	
Pirrit	Adware	2,33	

Deze cijfers laten zien dat veel soorten malware, zoals infostealers, weliswaar sterk in aantal toenemen, maar dat adware en potentieel ongewenste toepassingen (PUA) nog steeds het meest gedownload en geïnstalleerd worden. Dit is een vrij algemene trend die op alle OS-platforms te zien is, gezien het brede bereik van adware en de meer gerichte aard van infostealers.



Ja mf Threat Labs publiceerde een blog over **infostealers die zich richten op individuen in de cryptosector**. Het doel van de aanvallers? Inloggegevens verzamelen met gegevens van verschillende cryptowallets. Het team volgde twee aanvallen waarbij infostealers op de systemen van het slachtoffer terechtkwamen:

1.

Via gesponsorde Google-advertenties: gebruikers die zochten naar "Arc Browser" kwamen op een schadelijke site wanneer ze op een Google-advertentie klikten.

2.

Via virtuele vergaderingen: wanneer gebruikers contact opnemen om een kans te bespreken (zoals een sollicitatiegesprek), vragen aanvallers om Meethub te gebruiken om een gesprek te plannen.

In beide gevallen werden gebruikers gevraagd om de applicatie te downloaden buiten Gatekeeper om en om hun macOS-inlogwachtwoord in te voeren.

De malwarefamilies die we hebben bestudeerd en de voorbeelden die we geven, laten zien hoe belangrijk basisbeveiligingsprincipes zijn, zoals:

- Applicaties alleen downloaden van legitieme bronnen
- Een doorlichtingsproces toepassen (via vertrouwde derde partijen zoals de Mac App Store of van een leverancier van apparaatbeheer)
- De recentste beveiligingssoftware gebruiken



Het perspectief van een CISO

- **Introduceer een speciaal voor Mac ontworpen edr-oplossing:** we zien vaak dat software in eerste instantie op Windows gericht is en dat er daarna ook nog wat voor Apple aan wordt toegevoegd. Maar dat kan niet meer, vooral wat veiligheid betreft. Met de verdere ontwikkeling van het bedreigingslandschap moeten we ons richten op beveiligingsproducten die van de grond af aan zijn ontwikkeld voor Apple-producten.
- **Implementeer een robuuste MDM-oplossing:** goed apparaatbeheer is cruciaal voor de beveiliging van je apparaten. Gezien de hoeveelheid vrijheid en de mogelijke toegang die gebruikers hebben, is een robuust framework om apparaten en gebruikers op die apparaten te beheren van het grootste belang om potentiële malware-uitbraken te stoppen voordat ze beginnen.
- **Zorg voor sterke communicatiestrategieën:** van samenwerking tussen beveiliging en IT, uitbreiding van beveiligingsmerken en trainingsprogramma's tot bewustmaking van eindgebruikers en memo's voor leidinggevend. Effectieve communicatie over je beveiligingsprogramma, de tools die je gebruikt en je huidige strategieën maakt het makkelijker om iedereen op één lijn te brengen en te zorgen dat iedereen zich richt op een gemeenschappelijk doel.

Kwetsbaarhedenbeheer

Niet alle kwetsbaarheden zijn gelijk. Ze variëren in ernst en aan de meeste is een score toegekend. **Apple** heeft een lijst met gepatchte beveiligingslekken die gevolgen hadden voor macOS en het besturingssysteem waarmee het beveiligingslek is verholpen. In 2024 bracht Apple bijvoorbeeld macOS 15.1.1 uit naar aanleiding van **CVE-2024-44308** en **CVE-2024-44309**: bij deze kwetsbaarheden kon kwaadaardige webcontent uit de sandbox voor webcontent breken. Deze CVE had een hoge ernstscore. Maar Apple brengt ook beveiligingsupdates uit voor CVE's met lage scores. Waarom? Het is belangrijk om prioriteiten te stellen. Als IT- en beveiligingsteams een volledig overzicht hebben van de kwetsbaarheden in hun apparaten, inclusief systemen en applicaties, kunnen ze de meest urgente problemen naar behoren aanpakken.

Apple heeft ook een meer gespecialiseerde versie van beveiligingsupdates, de zogenaamde Rapid Security Responses, die **belangrijke verbeteringen in de beveiliging** bieden tussen grotere software-updates door. Het voordeel van deze patches? Het zijn weinig ingrijpende updates, wat betekent dat organisaties de updates automatisch kunnen installeren zonder interne systemen te verstoren. Tussen juni 2024 en april 2025 heeft Apple bijvoorbeeld **twintig beveiligingsupdates** vastgelegd met CVE's die verband houden met grote en kleine versies van macOS.

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

In de besturingssystemen van Apple biedt het Transparency, Consent and Control (TCC)-mechanisme een cruciaal beveiligingsframework: het vraagt gebruikers om verzoeken van afzonderlijke apps om toegang te krijgen tot gevoelige gegevens, zoals microfoon, webcam en volledige schijftoegang, toe te staan of te weigeren. Een TCC bypass-kwetsbaarheid treedt op wanneer deze controle faalt, zodat een applicatie toegang kan krijgen tot privégegevens zonder toestemming of medeweten van de gebruiker. Dit betekent dat aanvallers ongeautoriseerde toegang kunnen krijgen tot bijvoorbeeld 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 Mac-apparaten treft. Apple reageerde snel op deze ontdekking met een patch in macOS 15. CVE's als CVE-2024-44131 versterken de noodzaak voor organisaties om tools te hebben die onverwacht gedrag kunnen detecteren en blokkeren. Door proactief app-gedrag te monitoren en ongeautoriseerde toegang tot gegevens te voorkomen kunnen organisaties aanvallers een stap voor blijven tot de kwetsbaarheden zijn aangepakt.

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

Apple CVE-oplossing	Datum	Kwetsbaarheidsscore	Impact
macOS Sequoia 15.4.1	April 2025	CVE-2025-31200 CVSS – Score: 7,5 Ernst: Hoog	CoreAudio
macOS Sequoia 15.4	Maart 2025	CVE-2025-24234 CVSS – Score: 7,8 Ernst: Hoog	AccountPolicy
macOS Sequoia 15.4	Maart 2025	CVE-2025-24180 CVSS – Score: 8,1 Ernst: Hoog	Authenticatieservices
macOS Sequoia 15.3	Januari 2025	CVE-2025-24085 CVSS – Score: 7,8 Ernst: Hoog	CoreMedia

Zoals gezegd, is het een gegeven dat er bij het bouwen van software kwetsbaarheden ontstaan (gemiddeld 25 fouten per 1000 regels code). Voor beveiligingsprofessionals is het belangrijk dat ze deze kwetsbaarheden kunnen bekijken en er actie op kunnen ondernemen om gegevens veilig te houden. Het is niet altijd mogelijk om besturingssystemen up-to-date te houden (bijvoorbeeld om applicaties/agenten te testen), maar organisaties moeten zich bewust blijven en beschermd worden.

Het gaat om meer dan alleen kwetsbaarheden in een besturingssysteem. Eind november 2024 publiceerde het Cybersecurity Agency van de Amerikaanse overheid [een rapport over de meest routinematig uitgebuide kwetsbaarheden in 2023](#) (dit is de nieuwste versie van het rapport). Het rapport gaat dieper in op de belangrijkste vijftien kwetsbaarheden, zoals de CVE, en op wat bedreigingsactoren 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
- Regelmatig beveiligde systeemback-ups maken
- Ervoor zorgen dat het responsplan voor cyberbeveiligingsincidenten steeds geactualiseerd wordt

Zoals hierboven aangegeven, biedt Apple routinematig updates voor besturingssystemen met bekende kwetsbaarheden. We blijven erop hameren: het is essentieel om software bij te werken. De meest 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. Er zijn echter nog andere lagen voor cyberbeveiliging. Organisaties kunnen aanvullende stappen voor blijven met bijvoorbeeld incidentresponsplannen, door telemetrie te verzamelen en te analyseren of met interne patchingprocessen. Hiermee worden ook extra cyberbeveiligingslagen ontsloten, zoals de identificatie van kwetsbaarheidsniveaus van software of het blootleggen van risico's die mogelijk sluimeren binnen eindpunten door middel van threat hunting-workflows: al deze lagen werken ook samen om organisaties te helpen risico's te beperken.



Jamf Threat Labs ontdekte een kwetsbaarheid in Gatekeeper in macOS, waaraan code CVE-2023-41067 is toegewezen. Deze kwetsbaarheid betrof Launch Services en kon ertoe leiden dat een niet-ondertekende en niet-geauthenticeerde applicatie wordt uitgevoerd zonder dat de juiste beveiligingsmeldingen aan de gebruiker worden weergegeven. Gatekeeper is de eerste verdedigingslinie die ervoor moet zorgen dat applicaties die van het internet worden gedownload, worden geblokkeerd als ze niet zijn ondertekend met een geldige ontwikkelaars-ID. Hoewel deze CVE snel door Apple werd gepatcht, laat het zien dat kwetsbaarheden in elk systeem kunnen voorkomen. Met de juiste controles en training kunnen risico's door kwetsbaarheden zoals die Jamf Threat Labs heeft gevonden in Gatekeeper, worden beperkt.

In de afgelopen twaalf maanden ontdekten we dat:



32%

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

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 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 bedrijfsresources, 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.

Deel 3: Social engineering

Bij social engineering manipuleren en misleiden aanvallers personen met de bedoeling om hen zover te krijgen dat ze gevoelige gegevens of toegangsgegevens verstrekken. Volgens het [Global Cybersecurity Outlook 2025-rapport](#) van het World Economic Forum heeft "42% van de organisaties het afgelopen jaar te maken gehad met een succesvolle social engineering-aanval".

Phishing, een vorm van social engineering, is momenteel een van de meest voorkomende en schadelijke bedreigingen voor organisaties. Hoewel phishing vaker voorkomt op mobiele apparaten (vanwege hun kleine scherm, draagbaarheid en het gebruik op locaties buiten kantoor), zijn Macs (en alle desktops of pc's) een aantrekkelijk doelwit voor bedreigingsactoren. Macs worden immers nog steeds gebruikt door de meest kwetsbare schakel in de cyberbeveiligingsketen: de eindgebruiker.

Nu aanvallen steeds creatiever en realistischer worden, lopen onze persoonlijke en werkgegevens voortdurend gevaar. En doordat in bedrijven steeds meer met Mac-apparaten wordt gewerkt, wordt het aanvalsoppervlak 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.

In de afgelopen twaalf maanden ontdekten we dat:



25%

van de organisaties is getroffen door een social engineering-aanval



1 op de 10

gebruikers op een kwaadaardige phishinglink klikte



Jamf Threat Labs publiceerde een artikel over [het lopende onderzoek van de FBI naar financieel voordeel voor de DPRK](#) met illegale middelen, en dan met name in de cryptosector. Het team noemt een specifieke aanval "waarbij een gebruiker werd benaderd op LinkedIn door een persoon die beweerde een recruiter te zijn in het HR-team van een techbedrijf". De aanvallers sturen de gebruiker een gezippte coderingstest (niet-ongebruikelijk voor een moderne ontwikkelaarsfunctie) om inzicht te krijgen in diens vaardigheden. Wanneer de gebruiker op het bestand klikt, wordt de malware (in dit geval een infostealer) gestart. Het trainen van werknemers in het omgaan met sociale media en het downloaden van software blijft een belangrijk punt voor alle organisaties.

De twintig merken die het meest worden gebruikt in phishingcampagnes

In ons onderzoek ontdekten we dat bepaalde bekende merken vaak worden gebruikt in phishingaanvallen, misschien juist vanwege hun herkenbare en vertrouwde namen. We hebben deze merken onderverdeeld in vier categorieën:

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

Er zijn veel verschillende redenen om een Mac te gebruiken (solliciteren, een app downloaden of werk in een specifieke sector, zoals crypto) en dat maakt dat bedreigingsactoren vaak via dit soort veelvoorkomende, vaak noodzakelijke, use-cases proberen toegang te krijgen tot gegevens. In de bovenstaande tabel zie je de twintig sites die het meest werden gebruikt in phishingaanvallen, op basis van deze vier categorieën.

Deze merken worden vanwege hun populariteit, aanzien en impact op zowel bedrijven als individuele personen gebruikt door kwaadwillende actoren die proberen gebruikers te compromitteren via social engineering-aanvallen. Ze zijn de ongewilde spelers in een steeds geraffineerder spel. Besef wel dat dit niet een volledige lijst is van alle merken die worden gebruikt door bedreigingsactoren. Dit zijn de twintig meest misbruikte merken van het afgelopen jaar, en dit kan over een jaar, maand of week

anders zijn. Het werpt wel een licht op hoe aanvallers denken. Ze gebruiken het vertrouwen dat merken in de loop der jaren bij hun klanten hebben opgebouwd om gebruikers uit te buiten. Met de toename van hybride en extern werk proberen aanvallers nieuwe manieren uit om iemand te laten klikken.

In de moderne wereld lopen onze persoonlijke gegevens voortdurend gevaar. Nu Mac steeds gebruikelijker wordt op het werk, wordt het aanvalsoppervlak 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 werden geclassificeerd als 'zero day', wat betekent dat de aanvallers nieuwe domeinen lanceren voor phishingaanvallen die nog niet zijn gedetecteerd of geïdentificeerd als kwaadaardig in de gemeenschappelijke databases. Het identificeren en verifiëren van 'zero-day' phishingaanvallen helpt organisaties om gebruikers te beschermen tegen gloednieuwe en nog niet ontdekte phishing sites

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. Pas je training en je blokkeringtactieken aan die situaties aan. 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 methode. Schakel regels voor onmogelijke snelheden in enz. 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.

Belangrijkste leerpunten:

Mac-malware rukt op. Maar er zijn stappen die organisaties kunnen nemen om de risico's van macOS-malware te beperken. Het verzamelen en analyseren van telemetrie helpt bijvoorbeeld bij het identificeren van en rapporteren over malware. Bedreigingsactoren blijven zoeken naar nieuwe manieren om gebruikers en systemen te compromitteren. Maar met de juiste hulpmiddelen kunnen organisaties de impact van kwaadaardige software beperken.

Een goede beveiligingshygiëne beperkt de risico's. Door besturingssystemen regelmatig bij te werken en onnodige besturings-elementen (bijv. appstores van derden) uit te schakelen kunnen organisaties blijven voldoen aan interne richtlijnen en externe frameworks. 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.

Social engineering is een van de meest voorkomende manieren waarop aanvallers toegang krijgen tot gevoelige informatie. Meer dan 90% van de cyberaanvallen begint met phishing. Phishing is er in alle soorten en maten - niet alleen als e-mail. Het is belangrijk om bescherming te implementeren op het hele apparaat (browsers en apps) om gebruikers en organisaties veilig te houden.



Neem contact met ons op voor meer informatie over het bedreigingslandschap van de Mac. Of neem contact op met de reseller van jouw keuze.