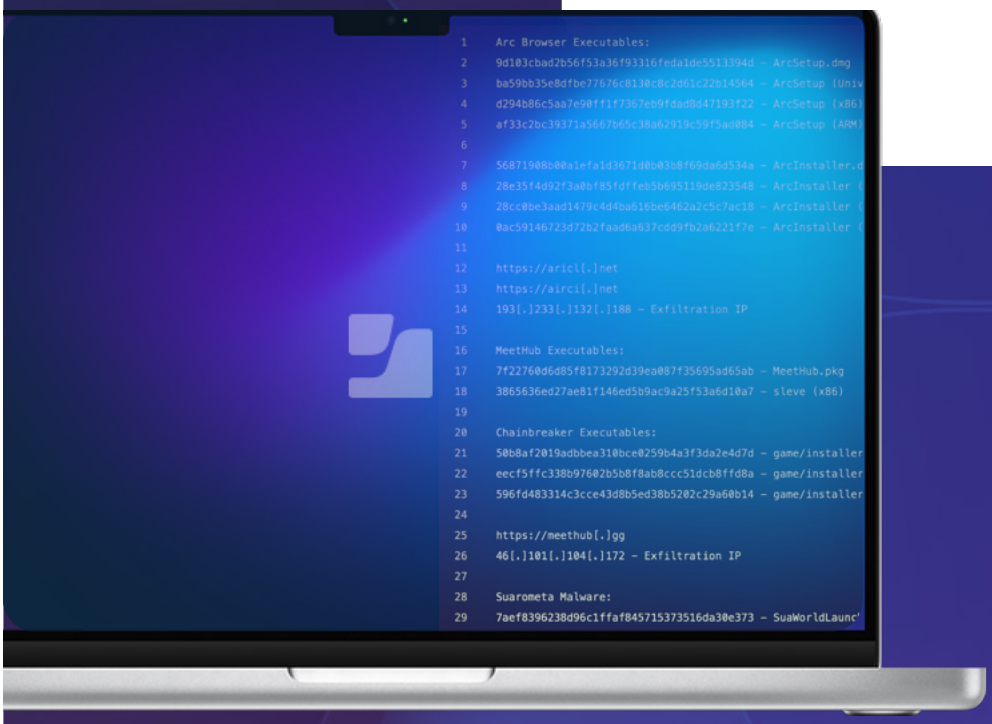
jamf

Sicherheit 360:

Jährlicher Trendbericht für Macs



Einleitung

Wir lieben den Mac. Es ist der erste Rechner, für den wir Software entwickelt haben, und er ist nach wie vor der Computer, für die sich so viele von uns begeistern. (Wir sind **offizieller Mitwirkender am macOS Security Compliance Project.**) Im Laufe unserer Geschichte haben wir beobachtet, wie Mac zu einem **immer wichtigeren Bestandteil der Arbeitsumgebung geworden ist.** Was als Rechner für Kreative und Führungskräfte begann, wird immer mehr zu einem festen Bestandteil des täglichen Betriebs für Ingenieure und andere Personen. Durch die fortlaufende Integration bei der Arbeit wird sie jedoch zu einer immer größeren Angriffsfläche für Cyberkriminelle.

Die Bedrohungslandschaft für Macs ist vielfältiger denn je, und es gibt immer mehr kreative Wege, Macs zu kompromittieren. Im Rahmen unserer Mission, „Unternehmen mit Apple zum Erfolg zu verhelfen“, untersuchen wir die Bedrohungslage für Mac Geräte genauer, um unsere Kunden und die Apple Community insgesamt besser betreuen zu können.

- **Jaron Bradley,**
Director, Jamf Threat Labs

Einführung

Der Bericht „Sicherheit 360“ von Jamf basiert auf der Analyse realer Kundenvorfälle, Bedrohungsanalysen und Branchenereignissen des vergangenen Jahres. Dieser Bericht konzentriert sich auf die Untersuchung der Bedrohungslage für Macs, um die Risiken, denen Unternehmen ausgesetzt sind, zu beleuchten.

Wir bieten eine Bewertung der verschiedenen Angriffsvektoren (wie Malware, Schwachstellen und Social Engineering), die aktiv eingesetzt werden, um Benutzer:innen auszutricksen, Geräte zu kompromittieren und Organisationen zu infiltrieren. Die Analyse umfasst Themen wie Schwachstellen von Geräten, Bedrohungen aus dem Internet, Malware und mehr.

Neben der Analyse dieser Bedrohungstrends enthält der Bericht auch eine Stellungnahme des CISO von Jamf, um Führungskräften, die ihre Macs auf Nutzer-, Geräte-, Anwendungs- und Netzwerkebene schützen wollen, einen umfassenden Einblick zu geben.

Methodik der Forschung

Um die tatsächlichen Auswirkungen der in diesem Bericht identifizierten Sicherheitstrends zu verstehen und zu quantifizieren, haben wir eine Stichprobe von 1,4 Millionen Geräten untersucht, die durch Jamf geschützt sind. Unsere Analyse wurde im ersten Quartal 2025 durchgeführt, wobei wir den vorangegangenen 12-Monats-Zeitraum erneut untersuchten und weltweit 90 Länder einbezogen haben.

Zum Schutz der Privatsphäre und zur Wahrung höchster Sicherheitsstandards bei der Datenerfassung und -verarbeitung stammen die in unserer Untersuchung analysierten Metadaten aus zusammengefassten Protokollen, die keine personenbezogenen oder organisationsidentifizierenden Informationen enthalten.

Zweck der Forschung

Mit dieser Analyse wollen wir Organisationen und Benutzer:innen in die Lage versetzen, die aktuellen Trends im Bereich der Cybersicherheit besser zu verstehen, und aufzeigen, wie Organisationen und Benutzer:innen Maßnahmen zur Risikominderung ergreifen können. Er bietet außerdem eine Übersicht über die wichtigsten Untersuchungen von Jamf Threat Labs, einschließlich Malware und Schwachstellen.

Es gibt mehrere Maßnahmen, die jeder ergreifen kann, um den Mac sicherer zu machen. Laden Sie zum Beispiel nur Software von Quellen herunter, denen Sie vertrauen. Aber es gibt noch weitere Best Practices, die jedes Unternehmen implementieren kann:

- Kontinuierliche und zeitnahe Betriebssystem-Updates
- Nutzerschulung und -ausbildung
- Antragsprüfung
- Multi-Faktor-Authentifizierung
- Zero-Trust-Sicherheitsrahmenwerke
- Richtlinien zur akzeptablen Nutzung von Unternehmensdaten
- Implementierung von Apple-optimierten Workflows für verschiedene Anwendungsfälle

Während einige dieser Anforderungen für alle Organisationen gelten, gibt es andere Sicherheitsanforderungen für Geräte, die unternehmensspezifisch sind. So müssen Organisationen in einer regulierten Industrie möglicherweise Benchmarks oder Frameworks (wie CIS Benchmarks oder HIPAA) einhalten.

Dieses Jahr haben wir unsere Analyse in drei Risikokategorien unterteilt, die unserer Meinung nach für Organisationen auf der ganzen Welt die höchste Priorität haben:

I. Anwendungsrisiken und Malware

II. Schwachstellenverwaltung

III. Social Engineering

Wir haben auch einen Sicherheit 360-Bericht, der sich auf **Mobilgeräte** konzentriert und den Sie **hier** finden können.

Die Analyse in diesem Bericht stützt sich auf die Threat Intelligence von Jamf, eine umfassende Sammlung von Erkenntnissen, die aus originärer Bedrohungsforschung, realen Nutzungsmetriken sowie Nachrichtenanalysen und Datenfeeds gewonnen werden. Die Threat Intelligence von Jamf basiert auf manuellen Recherchen der Jamf Threat Labs und Data Science-Teams, die Geräte, Apps und den Netzwerkverkehr auf Risiken, Bedrohungen und Zero-Day-Schwachstellen überwachen.

Wichtige Trends für Macs im Unternehmen

Malware birgt Risiken - selbst auf sicheren Plattformen.

Apple entwickelt seine **Plattformen mit dem Schwerpunkt auf Sicherheit**. Es geht nicht nur um die Plattformen selbst, sondern auch darum, wie Apple seinen Nutzer:innen die Sicherheit vermittelt. Auf der **Website der Apple Plattform** gibt es zum Beispiel eine Seite, die Apple Nutzer:innen über den Schutz gegen Malware in macOS informiert. Die verschiedenen Technologien von Apple (wie App Store, XProtect oder Gatekeeper) schützen vor bösartigen Apps in verschiedenen Phasen des Lebenszyklus einer App.

Bei Mac-Geräten am Arbeitsplatz ist die Sicherheit ein Balanceakt: Zum einen müssen den Nutzer:innen die Apps zur Verfügung gestellt werden, die sie für optimale Arbeit benötigen, zum anderen muss der Zugriff auf Apps, die Risiken bergen können, verhindert werden. Apps für den Mac gibt es in allen Formen und Größen, wie native Mac Apps, Web-Apps und hybride Apps, die von Entwickler:innen für eine Vielzahl von Anwendungsfällen erstellt und entworfen werden. **Viele der gängigsten Apps für den Mac** stammen jedoch nicht aus dem Mac App Store, sondern werden direkt von den Entwickler:innen als Paket angeboten. Darüber hinaus können die Nutzer:innen Apps von jeder Website herunterladen, zu der sie Zugang haben.

II. Durch eine einzige Schwachstelle können sich Cyberkriminelle systemweiten Zugang verschaffen

Es stimmt, dass Schwachstellen in der Software (sowohl OS als auch Apps) auftreten, die wir täglich nutzen.

Das Nationale Institut für Normen und Technologie sagt dazu: „Bei typischer Software treten Fehler und Schwachstellen mit einer geschätzten Häufigkeit von ~25 Fehlern pro 1000 Codezeilen auf.“ Allgemeine Schwachstellen und Gefährdungen (CVE), die in der National Vulnerability Database (NVD) veröffentlicht werden, stehen der Öffentlichkeit zur Verfügung:

- Ein besseres Verständnis von CVEs
- Das betroffene Produkt oder der betroffene Anbieter
- Eine Beschreibung der Bedrohungen

In der Zeit zwischen der Entdeckung einer Schwachstelle und dem Patch kann Schaden angerichtet werden. Wenn ein Patch zur Verfügung gestellt wird, muss er noch auf den betroffenen Geräten installiert werden. Sicherheitstools, die Aufschluss darüber geben, welche Schwachstellen vorhanden und besonders kritisch sind, helfen IT- und InfoSec-Teams, die wichtigsten Patches zu priorisieren und ihre Prozesse zu verbessern.

Social Engineering kompromittiert weiterhin Nutzer:innen

Social Engineering ist ebenso wie Phishing nach wie vor eine der häufigsten Angriffstechniken von Angreifer:innen, und sein Einfluss auf die Bedrohungslandschaft ist nach wie vor ungebrochen. Im September 2024 **veröffentlichte Apple einen Blog-Beitrag** mit einer Anleitung für Nutzer:innen, um „Betrug zu vermeiden und zu erfahren, was zu tun ist, wenn Sie verdächtige E-Mails, Telefonanrufe oder andere Nachrichten erhalten“. Die Angreifer:innen werden immer kreativer in ihren Techniken und geben sich als Recruiter:innen, Familienmitglieder, vertrauenswürdige Brands und vieles mehr aus. Unabhängig davon, wie sicher eine Plattform oder ein Betriebssystem auch sein mag, Social-Engineering-Techniken zielen darauf ab, Unternehmensdaten zu infiltrieren, indem sie beim unsichersten Teil des Geräts ansetzen: dem Nutzer.

Teil 1: Malware, die sich auf Mac fokussiert

Mit diesem Bericht möchten wir ein Verständnis für Mac Malware vermitteln, einschließlich der Arten, die wir gesehen haben, wie sie sich jeweils auf Organisationen auswirken und mit welcher Häufigkeit. Aufgrund der zunehmenden Verbreitung des Macs am Arbeitsplatz und dem Zugang zu kritischen Apps über die Plattform werden Nutzer:innen im gesamten Unternehmen zum Ziel von Angriffen.

Die Malware-Abwehr von Apple ist in drei Ebenen gegliedert:

1. **Verhinderung des Starts oder der Ausführungs von Malware**
2. **Blockierung der Malware auf den Systemen der Kunden**
3. **Entfernung von Malware, die ausgeführt wurde**

Die Technologien von Apple - App Store, GateKeeper, XProtect und Notarisierung - bieten den Nutzer:innen native Möglichkeiten, um Bedrohungen zu entschärfen. XProtect ist zum Beispiel ein integriertes Antivirenprogramm. Und wenn Malware entdeckt wird, kann Apple auf verschiedene Weise reagieren, etwa durch den Entzug einer Entwickler-ID.

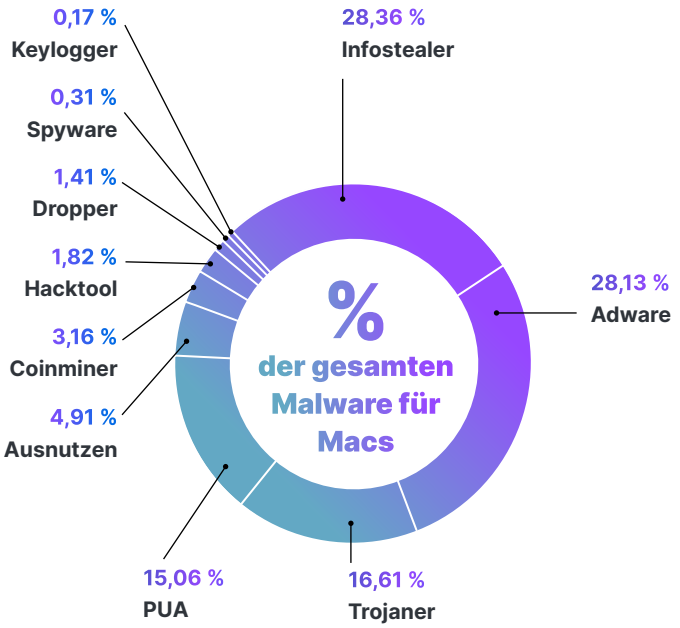
macOS ist trotz seiner starken, integrierten Systemsicherheitsmechanismen nicht immun gegen Malware. **Im März dieses Jahres** arbeiteten die Teams von Jamf Threat Labs und Data Science gemeinsam an einem Artikel, um über den Mythos „Malware auf Macs“ zu diskutieren, neue Malware mit bekannter Malware zu vergleichen und macOS Malware-Vektoren mit Titan - einem von Jamf Threat Labs entwickelten 3D-Visualisierungstool - darzustellen. Titan hilft dabei, mehr Hintergrundinfos zu liefern und verwandte Malware-Muster zu identifizieren. Die identifizierten Malware-Familien zeigen „die ständig wachsende Zahl neuer, maßgeschneiderter Malware“ für macOS. Was bedeutet das? Mac-Malware existiert, es gibt verwandte Malware-Familien und sie wird zunehmend von Bedrohungsakteuren eingesetzt.

Dieses Jahrentdeckte Jamf Threat Labs eine Malware, die vermutlich mit der Demokratischen Volksrepublik Korea (DVRK) in Verbindung steht und **in eine auf Flutter basierende App eingebettet** ist. Die Verwendung von Apps, die mit Flutter zur plattformübergreifenden Unterstützung entwickelt wurden, ist zwar nicht ungewöhnlich, aber dieser Angriff ist insofern bemerkenswert, als das es das erste Mal ist, dass das Jamf Threat Labs-Team beobachtet hat, dass dieses Framework für Angriffe auf macOS-Geräte eingesetzt wurde. Das Team analysiert die Malware, ihre Varianten in Python und Golang und erklärt, warum die „Malware wahrscheinlich auf eine stärkere Instrumentalisierung hin getestet wird“. Außerdem ist die unbeabsichtigte Undurchsichtigkeit zu beachten, die Flutter auf den von den Nutzer:innen seines Frameworks geschriebenen Code anwendet.

Malware-Familien für Macs

Im Folgenden finden Sie eine vollständige Aufschlüsselung der untersuchten und gezählten neuen Mac Malware-Instanzen aus dem Jahr 2024, basierend auf unseren Erkenntnissen:

Was sagen uns diese Daten? Ein Vergleich mit dem letztjährigen Bericht über Malware zeigt einige Übereinstimmungen: Adware, Trojaner, PUA (potenziell unerwünschte Anwendungen) und Exploits (Anwendungen, von denen bekannt ist, dass sie einen Exploit missbrauchen) stehen nach wie vor ganz oben auf der Liste der Malware-Kategorien. (Im letzten Jahr hatten Trojaner mit 17 % die größte Anzahl an Familien, dieses Jahr sind es mit 16,6 % etwas weniger.) Den ersten Platz belegen dieses Jahr Infostealer. Tatsächlich verzeichneten Infostealer einen Anstieg von 28,08 % gegenüber der Gesamtzahl der untersuchten Malware.



Die Präsenz von Infostealern stimmt mit den Untersuchungen von Jamf Threat Labs aus dem letzten Jahr überein, wobei macOS-Umgebungen ständig von diesem Malware-Typ angegriffen werden. Interessant an diesen Taktiken ist, dass Angreifer:innen nicht nur Infostealer einsetzen, um sich Zugang zu den gewünschten Daten zu verschaffen, sondern auch eine andere, bereits in diesem Bericht erwähnte Strategie anwenden: Social Engineering. Dies zeigt uns, dass Bedrohungsakteure eine Kombination von Angriffstechniken verwenden, um ihre Opfer auszutricksen. Für Mitarbeiter:innen oder Organisationen in hochrangigen Industrien - wie der Kryptoranche - ist es wichtig, sowohl in Bezug auf Schulungen als auch auf Sicherheitstools wachsam zu bleiben. Angriffe geschehen nicht zufällig, sondern sind geplant.

Untersuchungder Verwendung von PyInstallers zum Einsatz von Infostealern auf macOS

Im April 2025 entdeckteJamf Threat Labs neue, bisher unentdeckte macOS-Infostealer-Samples, die Python-Code mithilfe von PyInstaller in Mach-O-Executables bündeln. (Jamf Threat Labs entdeckte drei unentdeckte Stealer auf VirusTotal).

PyInstaller ist ein legitimes Open-Source-Tool, mit dem Entwickler:innen Python-Skripte in eigenständige Binärdateien verpacken können. Angreifer:innen nutzen nun dieselbe Technik, um bösartige Payloads auszuliefern, die sich unter macOS problemlos ausführen lassen. Das Team überprüfte mehrere wichtige Funktionen, um die wahre Natur der Malware zu bestätigen - einen Infostealer. Zu den wichtigsten Funktionen gehören:

- Versucht, Anmeldeinformationen von Nutzer:innen abzufangen, indem er trügerische Passwortaufforderungen auslöst
- Führt beliebige Applescript-Payloads vom Server des Angreifers aus
- Extrahiert gespeicherte Anmeldeinformationen und sensible Informationen direkt aus dem macOS-Schlüsselbund
- Durchsucht das Dateisystem nach bekannten Kryptowährungs-Wallets, um private Schlüssel zu extrahieren und Krypto-Assets zu stehlen

Da Infostealer in der macOS-Bedrohungslandschaft immer häufiger vorkommen, werden Bedrohungsakteure weiterhin nach neuen Wegen suchen, um sie zu verbreiten. Es gibt jedoch Maßnahmen, die Organisationen ergreifen können, um sich vor der oben beschriebenen Malware zu schützen. Zum Beispiel:

- Verwenden Sie nur Apps, die von Apple und identifizierten Entwickler:innen signiert wurden.
- Nutzen Sie Brand-Osascript-Eingabeaufforderungen, die für legitime IT-Prozesse verwendet werden, und schulen Sie die Belegschaft, damit sie vor der Eingabe ihrer Anmeldedaten das Branding überprüfen.

Malware, auf die man achten sollte

Poolrat

Poolrat, eine macOS-Backdoor, die für ihre Beteiligung an der Kompromittierung der 3CX-Lieferkette berüchtigt ist, ermöglicht es Cyberkriminellen, wichtige Systemdaten zu sammeln und Befehle gleichzeitig mit Dateioperationen auszuführen. Eine schlankere Version von Poolrat, genannt Pondrat, wurde kürzlich entdeckt.

Pondrat

Pondrat, eine Backdoor, die Ähnlichkeiten mit AppleJeus und Poolrat aufweist, wurde über bösartige PyPi-Pakete verbreitet. Nach der Installation stellt Pondrat Verbindungen zu Command-and-Control-Servern (C2) her, um das Hoch- und Herunterladen von Dateien zu erleichtern, den Betrieb für eine bestimmte Dauer anzuhalten und beliebige Befehle auszuführen.

NotLockBit

Golang-basierte Ransomware, die sich als eine Variante der berüchtigten LockBit Ransomware tarnt. Die Ransomware verwendet einen eingebetteten, öffentlichen Schlüssel, um eine Liste fest codierter Dateiendungen aufzulisten und zu verschlüsseln. Die neuesten Varianten von NotLockBit exfiltrieren Daten in einen vom Angreifer kontrollierten S3-Bucket und verwenden Osascript, um das Hintergrundbild des Desktops zu ändern (LockBit 2.0). Es wird vermutet, dass NotLockBit noch aktiv weiterentwickelt wird.

ThiefBucket

Thiefbucket, eine Malware-Familie, die mit der nordkoreanischen Lazarus-Gruppe in Verbindung steht, greift die Opfer mit anspruchsvollen Social Engineering-Kampagnen an. Es wurde als Payload der zweiten Stufe eingstuft, die durch eine getarnte Codierungsaufgabe übermittelt wurde. Die Hintertür weist mehrere Funktionen auf, vor allem die automatisierte Infostealer-Funktionalität. Zu den weiteren Fähigkeiten gehören: - Persistenzmechanismen - Prozessbeendigung - Dateilöschung - Herunter-/Hochladen von Dateien - Selbstlöschung - Ausführen von Shell-Befehlen - Schnelle Dateisuche über Spotlight - Kommunikation mit Command-and-Control-Servern

HZ Rat

HZ Rat, eine macOS-Backdoor, zielte ursprünglich auf Windows-Nutzer:innen ab, hat sich aber inzwischen weiterentwickelt, um macOS-Nutzer:innen über getarnte legitime Software-Installer anzugreifen. Nach der Installation stellt HZ Rat Verbindungen zu Command-and-Control-Servern (C2) her, die es Angreifern ermöglichen, Befehle auszuführen, Dateien zu stehlen und sensible Informationen wie Benutzernamen, E-Mails, Telefonnummern und andere persönliche Informationen aus WeChat und DingTalk zu extrahieren.

BansheeStealer

Der auf Telegram beworbene Atomic Stealer arbeitet als Malware-as-a-Service mit einer Web-Schnittstelle für Angreifer:innen. Er ist auf Informationsdiebstahl spezialisiert und kann eine Reihe sensibler Daten exfiltrieren, z. B. Kontopasswörter, Browserdaten, Sitzungscookies und Kryptowährungs-Wallets. Wie andere Infostealer missbraucht auch Banshee AppleScript-Dialogfunktionen, um Nutzer:innen zur Eingabe ihrer Anmeldeinformationen zu verleiten. Sobald die Nutzer:innen ihr Passwort eingegeben haben, stiehlt er weitere sensible Daten aus dem macOS Schlüsselbund. Banshee setzt verschiedene Umgehungstechniken ein, darunter Anti-VM- und Anti-Debugging-Maßnahmen, um die Analyse zu vereiteln, sowie die Erkennung russischsprachiger Systeme.

InvisibleFerret

InvisibleFerret ist ein auf Python basierender Trojaner, der von Malware verwendet wurde, die in getarnte Apps eingebettet ist. Insbesondere wurde es vom BeaverTail InfoStealer (von einigen der DVRK zugeschrieben) als Implantat der zweiten Stufe eingesetzt. Das bösartige Python-Skript ist plattformübergreifend und ermöglicht den Angreifer:innen, Daten auszuspähen, die Zwischenablage zu kopieren und Befehle aus der Ferne auszuführen. Er ist auch in der Lage, die Software AnyDesk zu installieren, wenn eine zusätzliche Steuerung aus der Ferne gewünscht wird.

BeaverTail

BeaverTail ist ein InfoStealer, der als legitime App getarnt wurde, bevor er über Social Engineering-Kampagnen an die Opfer geschickt wurde. Ähnlich wie andere InfoStealer entnimmt es wertvolle Daten aus dem Schlüsselbund, den Browser-Cookies, Krypto-Wallets usw. der Opfer und lädt sie auf einen von den Angreifer:innen kontrollierten Server hoch. Er ist auch in der Lage, zusätzliche Payloads aus der Ferne auf dem System des Opfers auszuführen, z. B. die InvisibleFerret-Backdoor. Sie wird von einigen der DVRK zugeschrieben.

PoseidonStealer

Der auf Telegram beworbene Poseidon Stealer (ein Konkurrent von Atomic Stealer) arbeitet als Malware-as-a-Service mit einer Web-Schnittstelle für Angreifer:innen. Er ist auf Informationsdiebstahl spezialisiert und kann eine Reihe sensibler Daten exfiltrieren, z. B. Kontopasswörter, Browserdaten, Sitzungscookies und Kryptowährungs-Wallets. Atomic missbraucht insbesondere AppleScript Dialogfunktionen, um Nutzer:innen zur Eingabe ihrer Anmeldedaten zu verleiten. Sobald die Nutzer:innen ihr Passwort eingegeben haben, stiehlt er weitere sensible Daten aus dem macOS Schlüsselbund. Die Malware wird unter dem Deckmantel legitimer Apps verbreitet und über Malvertising in Google Ads beworben.

Kuiper

Kuiper ist eine Ransomware-as-a-Service (RaaS), die in Go entwickelt wurde und von einem Nutzer namens Robinhood in Untergrundforen beworben wurde. Es verwendet eine Kombination aus RSA, ChaCha20 (Dateien kleiner als 600 Megabyte) und AES (Dateien größer als 600 Megabyte) zur Verschlüsselung von Dateien. Während sich die meisten Funktionen der Malware auf Windows konzentrieren, generiert die macOS-Variante einen zufälligen Schlüssel und einen zufälligen Initialisierungsvektor (IV) unter Verwendung von `/dev/urandom`, entschlüsselt eine Lösegeldforderung, verschlüsselt das Ziel rekursiv (unter Anhängen einer `.kuiper`-Erweiterung), entfernt den Schlüssel und den IV aus dem Speicher und startet das System neu.

Häufig eingesetzte Malware für Macs

Ein detaillierterer Blick auf neue Mac Malware, die in Kundenumgebungen beobachtet wurde, zeigt, dass die folgenden Malware-Familien unter den Top 10 rangieren:

Familienname	Kategorie	Prozentsatz
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	Trojaner	**3.07**
Macinformer	PUA	**2.33**
Pirrit	Adware	**2.33**

Diese Zahlen zeigen, dass zwar viele Arten von Malware, wie beispielsweise Infostealer, zahlenmäßig stark zunehmen, Adware und potenziell unerwünschte Anwendungen (PUA) jedoch weiterhin die von Nutzer:innen am häufigsten heruntergeladenen und installierten Anwendungen sind. Dieser Trend ist auf allen OS Plattformen zu beobachten, da Adware eine große Reichweite hat und die Infostealer gezielter vorgehen.

Jamf Threat Labs hat einen Blog über **Infostealer veröffentlicht, die es auf Einzelpersonen in der Kryptobranche abgesehen haben**. Was ist das Ziel der Angreifer:innen? Sammeln von Anmeldeinformationen mit Daten aus verschiedenen Krypto-Wallets. Das Team verfolgte zwei Angriffe, bei denen Infostealer in die Systeme der Opfer eingedrungen sind:

1. Durch gesponserte Google-Anzeigen: Die Suche nach „Arc Browser" führte Nutzer:innen zu einer bösartigen Website, wenn sie auf eine Google-Anzeige klickten.
2. Über virtuelle Meetings: Wenn sie Kontakt aufnehmen, um etwas zu besprechen (z. B. ein Vorstellungsgespräch), fordern Angreifer:innen die Verwendung von Meethub an, um ein Meeting zu vereinbaren.

In beiden Fällen wurden die Nutzer:innen aufgefordert, die App unter Umgehung von Gatekeeper herunterzuladen und ihr macOS-Anmeldepasswort einzugeben.

Die von uns untersuchten Malware-Familien und die von uns angeführten Beispiele zeigen, dass grundlegende Sicherheitsprinzipien erforderlich sind, wie z. B.:

- Abrufen von Apps aus legitimen Quellen
- Anwendung eines Überprüfungsverfahrens (entweder durch vertrauenswürdige Drittanbieter wie den Mac App Store oder durch einen Anbieter für die Geräteverwaltung)
- Ausführen aktueller Sicherheits-Software

Aus der Perspektive des CISO

- **Führen Sie eine speziell entwickelte, auf Mac fokussierte EDR Lösung ein:** Wir sehen oft, dass Software einen Windows-first-Ansatz verfolgt und Apple Geräte im Unternehmen nur nachrangig behandelt. Diese Zeiten sind längst vorbei, insbesondere was die Sicherheit betrifft. Wir müssen uns auf Sicherheitsprodukte konzentrieren, die von Grund auf für Apple Produkte entwickelt werden, da die Bedrohungslandschaft reift.
- **Implementieren Sie eine robuste MDM-Lösung:** Die Verwaltung von Geräten ist entscheidend für deren Sicherheit. Angesichts der vielen Freiheiten, die Nutzer:innen haben, und des Zugangs, den sie möglicherweise haben, ist ein robustes Framework zur Verwaltung von Geräten und Nutzer:innen auf diesen Geräten von entscheidender Bedeutung, um potenzielle Malware-Ausbrüche zu stoppen, bevor sie entstehen.
- **Implementierung starker Kommunikationsstrategien:** Von der Zusammenarbeit zwischen Sicherheit und IT, über Schulungen, Sensibilisierung der Endnutzer:innen bis hin zu Memos für die Geschäftsführung. Eine effektive Kommunikation Ihres Programms, der verwendeten Sicherheitstools und Ihrer aktuellen Strategien hilft allen Beteiligten, sich auf ein gemeinsames Ziel zu konzentrieren.

Verwaltung von Schwachstellen

Schwachstellen sind nicht gleich Schwachstellen. Sie variieren im Schweregrad, und den meisten ist ein Score zugewiesen. **Apple** stellt eine Liste der gepatchten Sicherheitsschwachstellen bereit, die macOS betreffen, sowie das Betriebssystem, das die Schwachstelle behebt. So veröffentlichte Apple im Jahr 2024 macOS 15.1.1 als Reaktion auf **CVE-2024-44308** und **CVE-2024-44309**, bei denen bösartig gestaltete Webinhalte möglicherweise aus der Sandbox für Webinhalte ausbrechen können. Dieser CVE hatte einen hohen Schweregrad. Apple veröffentlicht aber auch Sicherheitsupdates für CVEs mit niedrigen Scores. Was bedeutet das? Prioritäten setzen ist wichtig. Wenn IT- und Sicherheitsteams einen vollständigen Überblick über die Schwachstellen in ihren Geräten, einschließlich Systemen und Apps, haben, können sie die dringendsten Probleme zuerst angehen.

Apple verfügt über eine speziellere Version von Sicherheitsaktualisierungen, die sogenannten „Schnellen Sicherheitsreaktionen“, die **wichtige Sicherheitsverbesserungen** zwischen den Software-Aktualisierungen liefern. Warum sind diese Patches von Vorteil? Es handelt sich um leichte Updates, d. h. Organisationen können Updates automatisch anwenden, ohne dass interne Systeme beschädigt werden. Zum Beispiel dokumentierte Apple zwischen Juni 2024 und April 2025 **20 Sicherheitsupdates** mit CVEs in Verbindung mit Haupt- und Nebenversionen von macOS.

Ein eingehender Blick auf eine reale Schwachstelle Umgehung von Transparenz, Zustimmung und Kontrolle (TCC)

In den Apple Betriebssystemen dient Transparency, Consent and Control (TCC) als entscheidendes Security Framework, das die Nutzer:innen dazu auffordert, den Zugang zu sensiblen Daten wie Mikrofon, Webcam und Festplattenzugriff durch einzelne Apps zuzulassen oder abzulehnen. Eine TCC-Umgehungsschwachstelle tritt auf, wenn diese Kontrolle versagt, sodass eine Anwendung ohne die Zustimmung oder das Wissen der Nutzer:innen auf private Informationen zugreifen kann. Das bedeutet, dass die Angreifer:innen unbefugten Zugang zu Dateien und Ordnern, Gesundheitsdaten, dem Mikrofon oder der Kamera und mehr erhalten können, ohne dass Nutzer:innen gewarnt werden.

Jamf Threat Labs hat **CVE-2024-44131 gefunden, eine TCC-Bypass-Schwachstelle**, die File Provider auf iOS Geräten betrifft. Apple reagierte schnell auf diese Entdeckung mit einem Patch in macOS 15. CVEs, wie CVE-2024-4413, verstärken die Notwendigkeit für Organisationen, über Tools zu verfügen, die unerwartete Verhaltensweisen erkennen und blockieren können. Durch die proaktive Überwachung des Verhaltens von Apps und die Verhinderung des unbefugten Zugangs zu Daten sind Organisationen immer einen Schritt voraus, bevor Schwachstellen behoben werden können.

Werfen wir einen genaueren Blick auf einige bemerkenswerte Schwachstellen aus den jüngsten Veröffentlichungen von Apple (dieser Bericht wurde im April 2025 verfasst):

Behebung von CVEs bei Apple	Datum	Einstufung der Schwachstellen	Auswirkungen
macOS Sequoia 15.4.1	April 2025	CVE-2025-31200 CVSS – Score: 7.5 | Schweregrad: hoch	CoreAudio
macOS Sequoia 15.4	März 2025	CVE-2025-24234 CVSS – Score: 7,8 | Schweregrad: hoch	AccountPolicy
macOS Sequoia 15.4	März 2025	CVE-2025-24180 CVSS – Score: 8.1 | Schweregrad: hoch	Authentifizierungsdienste
macOS Sequoia 15.3	Januar 2025	CVE-2025-24085 CVSS – Score: 7,8 | Schweregrad: Hoch	CoreMedia

Wie bereits erwähnt, treten bei der Erstellung von Software Schwachstellen auf (etwa 25 Fehler pro 1000 Codezeilen). Für Sicherheitsexperten ist es wichtig, dass sie diese Schwachstellen erkennen und Maßnahmen ergreifen können, um die Daten zu schützen. Es ist nicht immer möglich, Betriebssysteme auf dem neuesten Stand zu halten (z. B. zum Testen von Apps/Agenten), aber Organisationen müssen auf dem Laufenden bleiben und geschützt werden.

Es geht um mehr als nur um Schwachstellen in einem Betriebssystem. Ende November 2024 veröffentlichte die Agentur für Cybersicherheit **einen Bericht über die am häufigsten ausgenutzten Schwachstellen im Jahr 2023**. (Dies ist die neueste Version des Berichts.) Der Bericht geht näher auf die 15 wichtigsten Schwachstellen ein - einschließlich der CVE und der Frage, was die Angreifer:innen mit jeder Schwachstelle anrichten können. Die Schwachstellen befinden sich in Betriebssystemen auf verschiedenen Computer-Plattformen und in Anwendungen, die die Mitarbeiter:innen und Schüler:innen einer Organisation täglich nutzen. In dem Bericht heißt es: „Böswillige Cyberkriminelle nutzten im Jahr 2023 mehr Zero-Day-Schwachstellen aus, um Unternehmensnetzwerke zu kompromittieren, als im Jahr 2022, wodurch sie Angriffe auf Ziele mit hoher Priorität durchführen konnten.“ Die Agentur für Cybersicherheit beschreibt zudem, was Entwickler:innen und Nutzer:innen tun können, um Schwachstellen zu entschärfen. Für Endbenutzerorganisationen nennt der Bericht:

- Zeitnahe Aktualisierung von Software, OS, Apps und Firmware
- Routinemäßige Durchführung einer automatischen Bestandsermittlung
- Implementierung eines robusten Patch-Management-Prozesses
- Dokumentation sicherer Basiskonfigurationen
- Regelmäßige Durchführung sicherer System-Backups
- Erstellung eines aktualisierten Plans zur Reaktion auf Cybersicherheitsvorfälle

Wie oben dargestellt, stellt Apple routinemäßig Updates für OS mit bekannten Schwachstellen bereit. Wir erwähnen es immer wieder, denn das Aktualisieren von Software ist sehr wichtig. Eine gängige Methode für Unternehmen, das OS (und die Apps, die ihre Mitarbeiter:innen täglich nutzen) zu aktualisieren, ist eine Mobile Device Management (MDM)-Lösung. Es gibt jedoch noch weitere Ebenen der Cyberverteidigung. Pläne zur Reaktion auf Vorfälle, das Sammeln und Analysieren von Telemetriedaten oder interne Verfahren zum Patchen sind alles Beispiele dafür, wie sich Organisationen besser schützen können. Durch die Durchführung der oben genannten Maßnahmen werden außerdem zusätzliche Ebenen der Cyberabwehr genutzt, beispielsweise die Identifizierung von Software-Schwachstellen oder die Aufdeckung von Risiken, die möglicherweise in Endpunkten durch Bedrohungssuche-Workflows schlummern. All diese Maßnahmen wirken zusammen, um Unternehmen bei der Risikominimierung zu unterstützen.

Jamf Threat Labs hat eine Gatekeeper-Schwachstelle in macOSentdeckt, die mit CVE-2023-41067 gekennzeichnet wurde. Diese Schwachstelle betraf Launch Services, die zur Ausführung einer nicht signierten und nicht autorisierten App führen können, ohne dass den Nutzer:innen entsprechende Sicherheitsabfragen angezeigt werden. Gatekeeper ist die erste Verteidigungslinie, die sicherstellt, dass aus dem Internet heruntergeladene Apps blockiert werden, wenn sie nicht mit einer gültigen Entwickler-ID signiert sind. Auch wenn dieses CVE von Apple schnell gepatcht wurde, zeigt es, dass Schwachstellen in jedem System auftreten können. Mit den richtigen Kontrollen und Schulungen lassen sich Risiken durch Schwachstellen wie die von Jamf Threat Labs in Gatekeeper entdeckte verringern.

In den vergangenen zwölf Monaten haben wir Folgendes festgestellt:

32%

derOrganisationen betreiben mindestens ein Gerät mit kritischen (und patchbaren) Schwachstellen

Aus der Perspektive des CISO

- **Sorgen Sie für Sichtbarkeit der Schwachstellen in Ihrer gesamten Organisation:** Ein guter Ausgangspunkt ist es, sich einen Überblick über die Schwachstellen auf Ihren Geräten oder in Ihrer Infrastruktur zu verschaffen. Sie können mit diesen Daten beginnen, um den Fußabdruck einer bestimmten Anwendung, potenzielle Risiken, den Wirkungsradius usw. zu analysieren. Auf diese Weise können Sie Ihre Schwachstellen auf der Grundlage von Daten nach Prioritäten ordnen.
- **Führen Sie ein solides Patching-Programm ein:** Um auf den Punkt MDM zurückzukommen: Ein Tool, das sicherstellt, dass Sie mit den neuesten oder unterstützten N -X-Versionen von Software oder OS Schritt halten können, ist für eine stabile und sichere Umgebung von größter Bedeutung. Wenn dies mit geringen oder gar keinen Auswirkungen auf die Endbenutzer:innen geschieht, ist es einfacher, Partnerschaften einzugehen und das Unternehmen zu unterstützen.
- **Implementieren Sie einen risikobasierten Zugangsansatz:** Wenn nicht konforme Geräte versuchen, auf Unternehmensressourcen zuzugreifen, sollten Sie diesen Zugang blockieren, bis die Nutzer:innen entsprechende Maßnahmen ergreifen, um das Gerät mit möglichst geringem Aufwand wieder konform zu machen.

Teil 3: Social Engineering

Social Engineering ist die Praxis, bei der die Angreifer:innen Personen manipulieren und dazu bringen, sensible Daten oder Anmeldeinformationen zur Verfügung zu stellen. Laut dem **Bericht „Global Cybersecurity Outlook 2025“** des Weltwirtschaftsforums „waren 42 % der Unternehmen im vergangenen Jahr Opfer eines erfolgreichen Social-Engineering-Angriffs“.

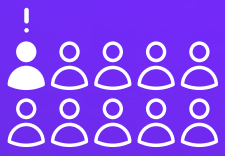
Phishing ist eine der häufigsten und schädlichsten Bedrohungen, denen Organisationen heute ausgesetzt sind. Während Phishing auf Mobilgeräten (wegen der kleinen Bildschirmgröße, der Mobilität und der Verwendung an anderen Standorten) häufiger vorkommt, sind Macs (und alle Desktops oder PCs) ein attraktives Angriffsziel für Bedrohungsakteure. Schließlich werden Macs immer noch von dem schwächsten Glied in der Cybersicherheitskette verwendet - demn Nutzer:innen

Da die Angriffe immer kreativer und realistischer werden, sind unsere persönlichen und beruflichen Daten ständig in Gefahr. Mit der zunehmenden Verbreitung von Mac Geräten am Arbeitsplatz wird die Angriffsfläche immer größer. Die Angreifer:innen wenden immer raffiniertere Taktiken an und nutzen realistische Benutzeroberflächen, Nutzererfahrungen und authentische Kommunikationsstile, um ahnungslose Opfer in ihre Falle zu locken. Es gibt jedoch Schutzmaßnahmen (z. B. kontinuierliche Mitarbeiterschulungen und Tools zur Bedrohungsprävention), die Unternehmen einsetzen können, um ihre Nutzer:innen und Daten zu schützen.

In den vergangenen zwölf Monaten haben wir Folgendes festgestellt:

25 %

der Organisationen waren von einem Social Engineering Angriff betroffen



1 von 10

Nutzer:innen hat auf einen bösartigen Phishing-Link geklickt

Jamf Threat Labs veröffentlichte einen Artikel über **die laufenden Nachforschungen des FBI über die** Erlangung von finanziellen Gewinnen durch die DVRK mit illegalen Mitteln, insbesondere in der Kryptobranche. Das Team verzeichnete einen konkreten Angriff, bei dem jemand auf LinkedIn von einer Person kontaktiert wurde, die behauptete, ein Recruiter im HR-Team eines Technologieunternehmens zu sein. Die Angreifer:innen senden dem Nutzer eine gezippte Programmieraufgabe (ein üblicher Schritt in einem modernen Bewerbungsverfahren eines Entwicklers), um sich ein Bild von seinen Fähigkeiten zu machen. Sobald der Nutzer diese anklickt, wird die Malware (in diesem Fall ein Infostealer) gestartet. Schulungen für Mitarbeiter:innen zur Nutzung Sozialer Medien und zum Herunterladen von Software sind nach wie vor ein wichtiges Thema für alle Organisationen.

Die 20 häufigsten Marken, die in Phishing-Kampagnen verwendet werden

Bei unseren Nachforschungen haben wir festgestellt, dass bestimmte Marken mit einem hohen Bekanntheitsgrad häufig für Phishing-Angriffe genutzt werden, vielleicht weil sie bekannt und vertrauenswürdig sind. Wir haben diese Marken in vier Kategorien eingeteilt:

1. Unterhaltung	2. Business	3. Dienstprogramme	4. Privat
Netflix	Outlook	United States Postal Service (US-Postdienst)	Amazon.com Inc
Bet365	Office365	Gazprom	Telegram
Steam	Allegro	AT&T Inc	Facebook, Inc
	InterActive Corp	Orange S.A.	Chase
	Tencent	DHL	WhatsApp
		BT Group	Yahoo, Inc.

Die unterschiedlichen Gründe für die Nutzung des Macs - Bewerbung auf eine Stelle, Download einer App oder Arbeit in einer bestimmten Industrie wie der Kryptoindustrie - haben dazu geführt, dass Bedrohungsakteure diese häufigen, oft notwendigen Anwendungsfälle ausnutzen, um Zugang zu Daten zu erhalten. In der obigen Tabelle sind die zwanzig wichtigsten Websites aufgeführt, die für Phishing-Angriffe verwendet wurden, basierend auf diesen vier Kategorien.

Diese Marken werden aufgrund ihrer Beliebtheit, ihres Ansehens und ihres Einflusses auf Unternehmen und Privatpersonen gleichermaßen von böswilligen Akteuren genutzt, die versuchen, Nutzer:innen mit Social Engineering-Angriffen zu kompromittieren. Sie sind unwissende Beteiligte in einem immer anspruchsvolleren Spiel. Es sei auch darauf hingewiesen, dass diese Liste nicht alle von Bedrohungsakteuren verwendeten Marken umfasst. Dies sind die Top-20-Marken des vergangenen Jahres, aber das kann sich nächstes Jahr, nächsten Monat oder nächste Woche ändern, aber es gibt Aufschluss darüber, wie Angreifer denken. Dies sind die Top 20 Marken des vergangenen Jahres, aber das kann sich im nächsten Jahr, Monat oder Woche ändern. Dennoch gibt es Aufschluss darüber, wie Angreifer:oinnen denken. Mit der Zunahme der Hybridarbeit und der Arbeit aus der Ferne versuchen Cyberkriminelle, neue Wege zu finden, um jemanden dazu zu bringen, auf einen Link zu klicken.

In der moderen Welt sind unsere personenbezogenen Daten ständig gefährdet. Mit der zunehmenden Verbreitung von Macs am Arbeitsplatz wird die Angriffsfläche immer größer. Die Angreifer:innen wenden immer raffiniertere Taktiken an und nutzen realistische Benutzeroberflächen, Nutzererfahrungen und authentische Kommunikationsstile, um ahnungslose Opfer in ihre Falle zu locken. Es gibt jedoch Schutzmaßnahmen (z. B. kontinuierliche Mitarbeiterschulungen und Tools zur Bedrohungsprävention), die Unternehmen einsetzen können, um ihre Nutzer:innen und Daten zu schützen.

Jamf hat in einem **Zeitraum von 12 Monaten** etwa **10 Millionen Phishing-Angriffe** identifiziert, wobei 1,4 Millionen Geräte unserer Stichprobe betroffen waren. Darüber hinaus haben wir festgestellt, dass **1,5 bis 2 %** dieser Angriffe regelmäßig als Zero-Day-Angriffe eingestuft werden, was bedeutet, dass die Angreifer:innen neue Domains für Phishing-Angriffe einrichten, die in den gängigen Datenbanken noch nicht als bösartig erkannt oder identifiziert worden sind. Das Erkennen und Überprüfen von Zero-Day Phishing-Angriffen hilft Organisationen, Nutzer:innen davor zu schützen, Opfer von brandneuen und unentdeckten Phishing-Seiten zu werden.

Aus der Perspektive des CISO

- **Einführung eines umfangreichen Schulungsprogramms:** Das war entscheidend für unseren Erfolg. Wir führen anspruchsvolle Phishing-Kampagnen und spielerische Schulungen durch, bieten einmalige Schulungen für Nutzer:innen an, die diese anfordern, und geben unseren Nutzer:innen die Möglichkeit, Phishing-E-Mails zu melden und gleichzeitig das ganze Jahr über Bestätigungen und Feedback zu ihren Einsendungen zu erhalten. Für uns ist dies nicht nur eine einmal im Jahr stattfindende Schulung, die dann „abgehakt" ist.
- **Bleiben Sie über neue Trends und Taktiken auf dem Laufenden:** Dies mag offensichtlich erscheinen, aber Cyberkriminelle nutzen immer alles aus, was sie können, und dazu gehört oft etwas Neues, Bahnbrechendes oder Kontroverses in den Nachrichten. Sie müssen Ihr Training und Ihre Blocking-Taktiken anpassen, um diese Herausforderungen zu meistern. Dies kann bei den Nutzer:innen zu einer gewissen Verunsicherung führen, aber Transparenz ist entscheidend. Die Schulung soll sie auf potenzielle Kriminelle vorbereiten, die keine Rücksicht auf ihre Gefühle nehmen, wenn sie Schaden anrichten, und oft sogar versuchen, eine emotionale Reaktion hervorzurufen, um das Opfer zu verwirren und zu überlisten.
- **Verfolgen Sie einen mehrschichtigen Ansatz:** Es gibt keine Einzellösung oder ein einziges Tool, um zu verhindern, dass Sie Opfer einer gezielten Phishing-Kampagne werden. Stellen Sie sicher, dass Sie aus mehreren Gesichtspunkten abgesichert sind. Blockieren Sie bösartige Domains. Implementieren Sie MFA. Nutzen Sie Zero-Trust. Aktivieren Sie die Regeln für unmögliche Geschwindigkeiten usw. Aktivieren Sie die Regeln für unmögliche Geschwindigkeiten.

Die wichtigsten Erkenntnisse

Malware für Macs ist auf dem Vormarsch. Es gibt jedoch Maßnahmen, die Organisationen ergreifen können, um die Risiken von macOS Malware zu mindern. Das Sammeln und Analysieren von Telemetriedaten hilft beispielsweise bei der Identifizierung und Berichterstattung über Malware. Bedrohungsakteure suchen kontinuierlich nach neuen Wegen, um Nutzer:innen und Systeme zu kompromittieren. Doch mit den richtigen Tools können Organisationen die Auswirkungen bösartiger Software verringern.

Die Implementierung einer angemessenen Sicherheitshygiene mindert die Risiken. Die regelmäßige Aktualisierung von Betriebssystemen und die Deaktivierung unnötiger Steuerelemente (z. B. App-Stores von Drittanbietern) helfen Unternehmen dabei, interne Richtlinien und externe Rahmenbedingungen einzuhalten. Durch die Einrichtung eines App-Stores für Unternehmen und die kontinuierliche Überprüfung von Apps (insbesondere für private und benutzerdefinierte Apps) können Organisationen anfällige Anwendungen besser überwachen, beheben und patchen.

Social Engineering ist eine der häufigsten Methoden, um sich Zugang zu vertraulichen Informationen zu verschaffen. Über 90 % der Cyberangriffe gehen auf Phishing zurück. Phishing gibt es in allen Formen und Größen - nicht nur per E-Mail. Es ist wichtig, einen Schutz für das gesamte Gerät (Browser und Apps) zu implementieren, damit die Nutzer:innen und die Organisation sicher bleiben.

jamf

Kontaktieren Sie uns, um mehr über die Bedrohungen für Macs zu erfahren. Oder Sie wenden sich an Ihren bevorzugten Partner.