Unverzichtbarer Leitfaden für Antivirus für Mac in der Hochschulbildung

jamf

Der Zustand von Malware für Apple-Geräte ist zu einem größeren Thema geworden, da das Apple-Ökosystem im Hochschulbereich immer mehr Fuß fasst.

Insgesamt betrachtet steht Apple gut da, obwohl Bedrohungen auf allen Computer-Plattformen im Anstieg sind. Apple hat sich besonders darauf konzentriert Malware-spezifische Erkennungen in dem nativen Apple Security Framework auszubauen.

Schwerwiegende Bedrohungen, die als Malware eingestuft werden – wie Rootkits und Ransomware – haben sich im Vergleich zu den Vorjahren verringert. Viele der größeren Frameworks der Botnets sind im vergangenen Jahr stark zurückgegangen, trotz einiger Angriffe, die Schlagzeilen machten. Wahrscheinlich geht das auf eine Veränderung der Verwendung von Geräten zurück, sowie darauf, wo diese verwendet werden. Die globale Gesundheitskrise ist der wichtigste Katalysator für diesen Wandel von unternehmenseigenen Netzwerkumgebungen, auf die Millionen von Benutzern täglich vor Ort zugreifen, zum Modell der Telearbeit, das so viele Unternehmen als Reaktion darauf eingeführt haben.

Mit anderen Worten: Die Sicherheitslandschaft hat sich drastisch verändert. Deshalb passen Malware-Autoren und Hacker sich an diese Änderungen an, indem sie den Bereich und die Größe der Malware-Tools in ihrem Arsenal ändern. Durch die gleichzeitige Nutzung mehrerer Bedrohungstypen erhöhen Angreifer die Komplexität, während eine zunehmende Automatisierung den Angriff auf weitere Ziele ermöglicht auf die Benutzer vertrauen.

Dieses E-Book enthält Folgendes:

- Definition von Mac-fokussierten Antivirus-Programmen (AV)
- Malware-Bedrohungen, die zunehmend auf Mac Nutzer ausgerichtet sind
- Trends die für die Sicherung privater Daten wichtig sind
- Jamf Schutz für Mac Geräte

Mac fokussierte Antiviren

Antivirus (AV) ist eine Grundvoraussetzung für die meisten institutionellen Geräte, um eine Basissicherheit zu gewährleisten. Apple bietet einen grundlegenden Virenschutz in macOS mit XProtect, Gatekeeper und MRT. Diese Tools werden jedoch nur sporadisch aktualisiert, und den Unternehmen fehlt der Überblick über ihre Aktionen. Institutionen benötigen ausgefeilte Antiviren-Funktionen, um Mac-Malware zu verhindern und unter Quarantäne zu stellen, die weit über das hinausgehen, was Windows-fokussierte Lösungen unter macOS leisten können.

Und sie sollten nicht warten, bis Malware, Adware oder andere unerwünschte Softwareprobleme auftreten.

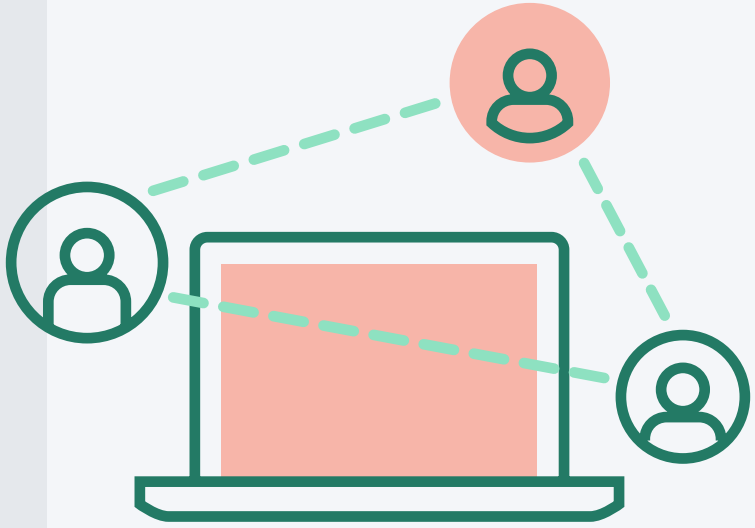
Sie müssen AV implementieren, das Mac-spezifische Angriffe effektiv identifiziert und behebt, ohne wertvolle Ressourcen für die Suche nach Bedrohungen für Windows auf einem Mac auszugeben. Effektive, effiziente und umfassende Mac AV-Funktionen sind für die Sicherheit und die Benutzerfreundlichkeit von Geräten unerlässlich.

Eine sich ändernde Bedrohungslandschaft

Im Brennpunkt steht eine starke Zunahme der Phishing-Kampagnen, die mit der Krise verbunden sind, indem sie die Ängste und Bedenken von Individuen ausnutzen. In Verbindung mit diesem Anstieg ist ein Schwerpunkt sogenannter 'threat actors', die stark zugenommen haben, die Sammlung von Informationen.

Ausspionieren online

Adware, Spyware und ein relativ neues Phänomen, Stalkerware, sind alle Arten von Malware, die Daten über Computerbenutzer entdecken und stehlen sollen. Stalkerware wird auch als Online-Spionage bezeichnet, das es in Echtzeit alle Arten von personenbezogenen Daten ausnutzt.



Beispiele wie die Übertragung von GPS-Koordinaten, die Decodierung von Nachrichten und die Überwachung und Aufzeichnung von Telefongesprächen sind nur einige der vielen Verstöße gegen den Datenschutz – laut einem Bericht von Kaspersky Labs.

Es ist Schach, nicht Dame

Bei der Überprüfung dieser Informationen sollte man bedenken, dass Hacker oft langfristig planen, was bedeutet, dass die Angriffe so lange dauern können, wie das eben nötig ist. Sie sind nicht darauf begrenzt, ein Stück Malware in ein Gerät einzuschleusen, sondern versuchen oft, mehrmals Zugriff zu erhalten und existierende Schwachstellen zu nutzen. So haben sie Zeit, ihre Angriffsstrategie oder -tools zu ändern, so viele Informationen zu sammeln, wie sie möchten, und schließlich der Malware die Möglichkeit zu geben, sich tiefer in die betroffenen Systeme einzunisten.

Das ist zyklisch, und jede Facette hat direkt **Auswirkungen** auf die nächste und **verstärkt** sie.

Zustand der Antivirus-Software für den Mac

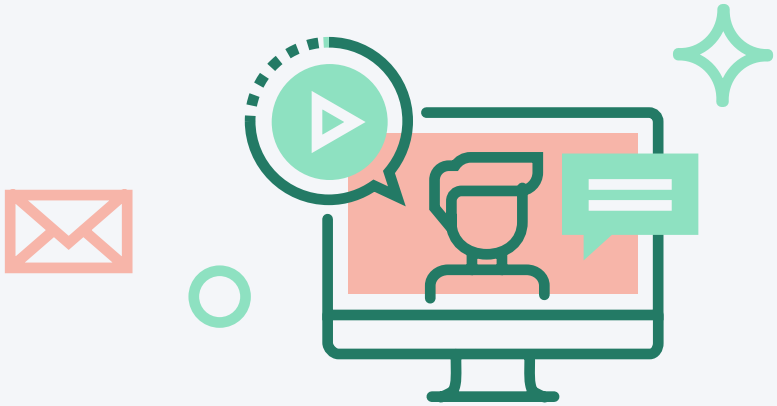
Die gute Nachricht für Mac Nutzer ist, dass insgesamt die Zahl der Malware-Erkennungen auf Mac Geräten im Jahr 2020 um über 38 % gefallen ist, laut einem Bericht von Malwarebytes Labs (State of Malware Report 2021).

Leider wird der Bildungssektor oft als einer der unsichersten eingestuft. Das bedeutet, dass die Universitäten ihre Sicherheitsstrategie und ihren Sicherheitsstatus ständig weiterentwickeln müssen, da sie sonst Gefahr laufen, immer neuen Bedrohungen ausgesetzt zu sein.

Mehrere Faktoren wirken sich auf diesen Wandel aus, von denen die drei wichtigsten sind:

- Anhaltendes Markt- und Mac-Wachstum von Apple im höheren Bildungsbereich
- Benutzer, die sich für Apple-Geräte im Rahmen von Programmen entscheiden, die von Studenten/Fakultäten gewählt werden, oder in Laboren, die MacBook anbieten
- Die globale Verlagerung hin zum Lernen aus der Ferne hat die Trennlinie, die früher zwischen dem Campus und dem Zuhause verlief, erweitert.

Holen Sie die Partyhüte noch nicht raus



Auch wenn Konsumenten dieser Reduzierung als Grund zum Jubel betrachten, zeigen Telemetrie-Daten aus verschiedenen Quellen, dass Geräte im Privatbereich immer noch von PUPs (potentiell unerwünschte Programme) befallen werden, wobei Adware am häufigsten ist.

Für Privatanwender von Mac-Produkten stellen PUPs und Adware jedoch einen Versuch dar, die persönlichen Daten des Anwenders ins Visier zu nehmen, oder eine Vorbereitung auf etwas viel Schlimmeres, wenn bösartige Werbung geschaltet wird, private Daten verfolgt werden oder eine zweifelhafte Anwendung heruntergeladen wird, die behauptet, den Mac zu reinigen.

Kombinerbare Malware

Ein seltsames Ergebnis, das wohl nur die Spitze des Eisbergs darstellt, betrifft neuartige Methoden zur Implementierung von Ransomware in Angriffen. Während die letzte bekannte neue Ransomware, die auf Macs abzielte, vor mehreren Jahren entdeckt wurde, brachte 2020 EvilQuest an die Spitze (auch als ThiefQuest bezeichnet). Diese Malware weist alle Merkmale von Ransomware auf, mit Ausnahme der Verschlüsselungswarnungen und der Aufforderung zur Zahlung für die Entschlüsselung von Dateien, die lediglich als Vorwand dienen, um ihre wahre Absicht zu verschleiern: **den anhaltenden und gezielten Diebstahl von persönlichen und geschäftlichen Daten.**

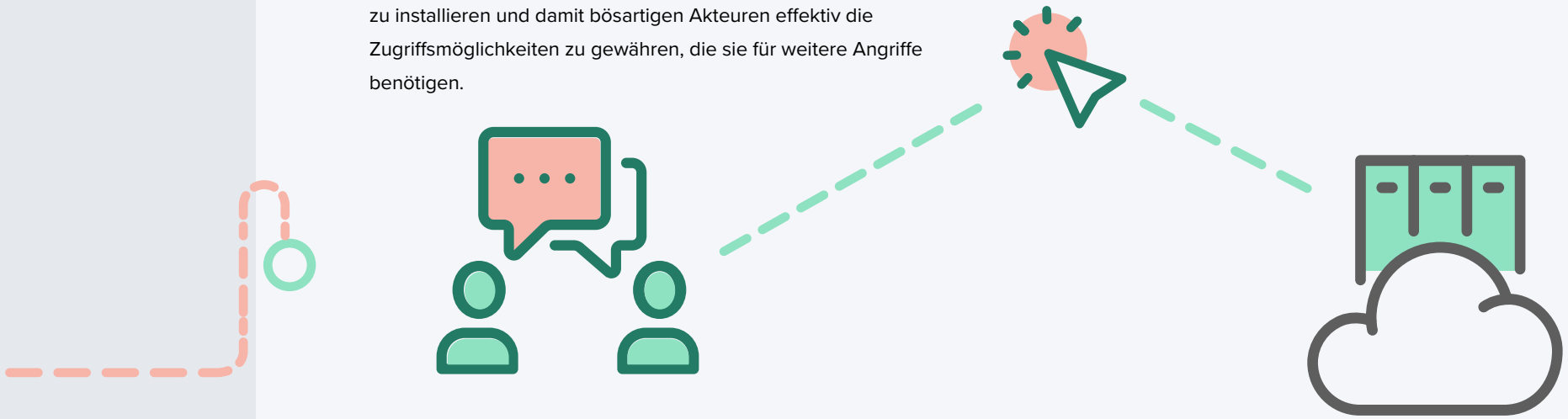
Malware wie diese kann sich im Laufe der Zeit weiterentwickeln — genau wie normale Software — und zusätzliche Funktionen enthalten, die mehr Schaden anrichten, während sie sich gleichzeitig immer besser tarnen, um der Entdeckung zu entgehen. Sie kann sich sogar aktualisieren, um sich weiterzuentwickeln, nachdem sie ein Gerät infiziert hat. EvilQuest dürfte auch in Zukunft eine Rolle spielen, da es sich laufend verändern wird.

Selbst alte Hunde *können* noch neue Tricks lernen

Diese momentan nur lästige Malware, die an Adware erinnert, entwickelt sich ebenfalls. Angesichts der Tatsache, dass die neueren macOS Versionen die App-Signaturen prüfen, bevor Apps starten können, haben manche Malware-Entwickler sich sehr bemüht, unkonventionelle Wege zu gehen, um die wertvollen Daten auf Ihrem System zu erbeuten und die Anzeigen zu monetarisieren, die Sie beim Surfen im Internet sehen.

Ein Beispiel für diese Art von Angriff wäre die Duplizierung der Safari App selbst und deren Modifizierung durch die Installation nicht autorisierter Erweiterungen zur Verfolgung von Benutzern. Oder die Verwendung von Konfigurationsprofilen – die auch von IT-Administratoren verwendet werden, um Geräteeinstellungen zu verwalten – um Benutzer zu überlisten, sie auf ihren Geräten zu installieren und damit bösartigen Akteuren effektiv die Zugriffsmöglichkeiten zu gewähren, die sie für weitere Angriffe benötigen.

Auch wenn Adware als weniger gefährlich gilt, ist sie die häufigste Malware auf macOS und zeigt auch die modernste Form der Innovation in Bezug auf die Infektion von Systemen – ganz abgesehen von der zunehmend häufigen Fähigkeit, weitere Malware-Payloads aus der Ferne zu übertragen – was beweist, dass Adware ein kritisches Zerstörungspotenzial erreichen könnte.



Arbeiten Sie intelligenter, statt mehr

Leider gibt es keine Universallösung für die derzeitige Eskalierung von Bedrohungen Eine der wichtigsten Erkenntnisse ist, dass Bedrohungen nicht alle aus derselben Richtung kommen. Hacker variieren ihre Taktik zunehmend und konzentrieren sich auf Geräte und Services, die die besten Ergebnisse erzielen. Zudem zeigen die Daten, dass die Angriffe keinesfalls aufhören.

Was bedeutet das für alle, die sich privat und bei der Arbeit auf Computer verlassen? Einfach gesagt müssen die Sicherheitsmaßnahmen alle Bedrohungen abwehren, umleiten, verhindern oder beheben, die auftauchen. Wachsamkeit ist ein wichtiger Teil der Sicherheit, ganz gleich, ob man Benutzer trainiert, häufige Bedrohungen wie Phishing-Versuche zu erkennen, oder sie dazu bringt, keine unbekannte Software zu installieren.

Auch die IT-Abteilung muss die Wachsamkeit in ihren Workflow einbeziehen, um den Sicherheitsstatus der Organisation ständig zu stärken und zu unterstützen. Die Nutzung von Software zur Lokalisierung von Bedrohungen auf der Grundlage bekannter Signaturen oder Heuristiken, die Verhaltensanalysen durchführt, um unbekannte Bedrohungen zu erkennen, bevor sie passieren, hilft der IT-Abteilung dabei, nicht nur zu sehen, woher die Bedrohungen für ihre Organisation kommen, sondern auch wie man sich am besten gegen sie schützt.

Wichtig sind dabei schnelle Reaktionen und Automatisierung, um rasch auf entdeckte Bedrohungen zu reagieren und gleichzeitig die notwendigen Maßnahmen zur Behebung der Probleme durchzuführen. Beide helfen dabei, die Angriffsfläche zu minimieren und das Risiko effizienter zu verwalten, während sie gleichzeitig der gestaffelten Abwehr eine weitere Ebene hinzufügen.

Schließlich benutzen wir Macs, um etwas zu erledigen – nicht, um durch Tausende Zeilen von Code nach Fehlern zu suchen, bevor wir eine App starten. In diesen Momenten erinnern wir uns daran, dass Apple sich bemüht, die Benutzererfahrung außergewöhnlich einfach machen und etwas Außergewöhnliches erschaffen will. Warum sollte Sicherheitssoftware nicht auch diesen Richtlinien folgen?

Jamf Integration + Support

Jamf Protect verhindert Malware und behebt schädliches Verhalten durch signaturbasierte Erkennung und Verhaltensanalysen auf dem Mac Mit einem granularen Top-Down-Einblick in die Geräte können IT-Abteilungen erkennen, was die Geräteleistung aus der Sicherheitsperspektive beeinträchtigt. Zudem werden in Kombination mit Jamf Pro die zentralisierte Patch-Verwaltung und Behebung ermöglicht, um eine Lösung für fast alle auftretenden Probleme zu ermöglichen. Schließlich vervollständigt die Kombination von Jamf Pro und Jamf Protect mit Jamf Connect dieses hochsichere Dreiergespann, indem sie ein Identitätsmanagement ermöglicht, bei dem Ihr Mac über cloudbasierte Identitätsdienste für den Geräte- und Ressourcenzugriff an institutionelle Ressourcen gebunden wird - so werden die Daten der Benutzer gesichert, indem ihre Geräte durchgängig geschützt werden.

Eine gestaffelte Abwehr, die die integrierten Tools von Apple umfasst und durch die kombinierte Leistung von Jamf erweitert, hilft Ihnen dabei, eine effektive Mac Sicherheit zu gewährleisten, die sich nahtlos in die Endbenutzererfahrung integriert, während sie dennoch alle relevanten Einblicke und Analysen über Geräte bietet. Diese abgestufte Strategie ermöglicht es der IT-Abteilung, die besten Entscheidungen zu treffen, wenn es um den Schutz der Geräte und die Sicherung der Benutzerdaten geht.

Jamf –der Standard im Apple Enterprise Management– bietet die Produkte und Lösungen an, die Ihnen bei der Umsetzung der besten Sicherheitsstratgie für Ihre Organisation und Ihre Benutzer helfen.

Überzeugen Sie sich selbst von unseren Leistungen.

Stellen Sie AV- und Endpunktschutz auf die Probe.

Wenn Sie bereit sind, Ihre Mac-Flotte vor eskalierenden Sicherheitsbedrohungen und bekannter Malware in freier Wildbahn zu schützen und bösartiges Verhalten zu beheben, fordern Sie eine kostenlose Testversion an oder wenden Sie sich an Ihren bevorzugten Apple-Fachhändler.

jamf

Weitere Informationen über Jamf Protect und Mac Endgeräteschutz finden Sie auf jamf.com/de

Testversion anfordern

Oder wenden Sie sich an Ihren bevorzugten Partner für Apple Hardware.