München, 07. April 2020

Aktueller Kommentar von SentinelOne: „Wie AppleScript für den Angriff auf MacOS genutzt wird“

von Matthias Canisius, Regional Director CE & EE bei SentinelOne

Anwendungen und Skripte für MacOS werden in aller Regel als sicher angesehen, denn die wenigsten Unternehmen verfügen über viele Mac-Rechner und setzen flächendeckend eher auf Windows-Systeme. Statista <https://de.statista.com/statistik/daten/studie/157902/umfrage/marktanteil-der-genutzten-betriebssysteme-weltweit-seit-2009/> weist für Windows OS im Januar 2020 einen Marktanteil von 78 Prozent aus. Dennoch nutzen Cyberkriminelle auch immer wieder Mac-Systeme und Anwendungen, um ihre Malware einzuschleusen oder ihre Aktivitäten zu verstecken. Eine Möglichkeit dafür bietet AppleScript. Dabei handelt es sich um eine alte MacOS-Technologie, die schon 8 oder 9 Jahre älter ist als MacOS 10, sie wird auch als „PowerShell des MacOS“ bezeichnet. Überraschenderweise wird sie oft von Angreifern verwendet, obwohl sie kaum auf dem Radar von Sicherheitsverantwortlichen auftaucht.

Die Sicherheitsforscher von SentinelOne <https://www.sentinelone.com/blog/how-offensive-actors-use-applescript-for-attacking-macos/> untersuchten nicht zuletzt aus diesem Grund eine Reihe von aktuellen Angriffen. Dazu zählt ein kürzlich entdeckter Browser-Hijacker für Safari, der sich in den Browser installiert einen versteckten LaunchAgent, der über ein Shell-Skript AppleScript lädt, kompiliert und ausführt. Andere Angriffe verwenden das Skript, um jede andere Art von Skript auszuführen, einschließlich Python-Skripts. Oder sie nutzen es, um sich und ihre Aktivitäten einfach darin zu verstecken.

Viele Sicherheitsverantwortliche haben AppleScript wenig Aufmerksamkeit zukommen lassen, weil die Entwicklung von Skripten schwierig ist. Der Grund dafür ist die (Apple)Script Editor.app die nur wenige Funktionen hat, die Entwickler normalerweise erwarten und brauchen. Es gibt keinen Debugger, keine Variablen-Introspektion, keine Code-Schnipsel oder effektive Code-Vervollständigung, um nur einige fehlende Funktionen zu nennen.

Angreifer nutzen AppleScript, weil es für die Automatisierung und die Kommunikation zwischen den Anwendungen entwickelt wurde. Normale Nutzer sollen die Möglichkeit bekommen, um sich wiederholende Aufgaben zu verketten und diese ohne weitere Nutzerinteraktion auszuführen. Sie können beispielsweise Mail.app automatisch ein Skript auslösen lassen, wenn es eine E-Mail von einem bestimmten Absender oder mit einem bestimmten Schlüsselwort in der Betreffzeile oder im Inhalt erhält, beliebige Details aus der E-Mail extrahieren und dann eine Datenbank in Excel oder Numbers mit den gewünschten Informationen füllen, die on-the-fly formatiert und sortiert werden, sobald die Daten eingehen. Und wie sich herausstellt, ist die Automatisierung der Kommunikation zwischen den Anwendungen und die Umgehung der Benutzerinteraktion ein gefundenes Fressen für die Malware-Entwickler.

Angreifer haben trotz der schwierigen und aufwendigen Handhabung AppleScript immer wieder genutzt und sie werden es auch zukünftig nutzen. Dank der systemeigenen Anbindung an Objective C und die leistungsfähigen Cocoa-Frameworks, der Vielfalt der Ausführungsmethoden und der Verfügbarkeit einer hervorragenden, frei nutzbaren IDE ist AppleScript zu einem leistungsfähigen, vielseitigen und einfach zu entwickelnden Werkzeug geworden. Cyberkriminelle werden immer versuchen, die Dinge auszunutzen, die die Verteidiger ignorieren. Das Skript wurde bisher von der Security Community ignoriert und es ist an der Zeit, es sich genauer anzuschauen.

Kontakt
Kafka Kommunikation GmbH & Co.
Dr. Bastian Hallbauer-Beutler
Lukas Reck
Kafka Kommunikation, Tel. 089 74 74 70 580, E-Mail: sentinelone@kafka-kommunikation.de

Kafka Kommunikation GmbH & Co KG, Auf der Eierwiese 1, 82031 Grünwald, Tel. +49 (0) 89

74747058-0, Fax + 49 (0) 89 74747058-20