Pressemitteilung von SentinelOne vom 09. Juli 2020

SentinelOne veröffentlicht kostenloses Entschlüsselungs-Tool für „EvilQuest“-Ransomware zum Schutz von MacOS-Umgebungen

Entschlüsselungs-Programm ermöglicht macOS-Benutzern ein Rollback ihrer Daten, um Lösegeldzahlungen zu vermeiden

München, 09. Juli 2020 - SentinelOne <https://www.sentinelone.com/>, das Unternehmen mit der führenden autonomen Cybersicherheitsplattform, veröffentlicht einen Ransomware-Entschlüsseler, der macOS-Benutzern ein Rollback der neuen „EvilQuest/ThiefQuest"-Ransomware ermöglicht. Der von der SentinelOne-Forschungsabteilung SentinelLabs entwickelte Dekryptor ist ein weiterer Beweis für die Führungsrolle von SentinelOne bei der Sicherung von macOS-Umgebungen. In dem Bestreben, die macOS-Gemeinschaft zu unterstützen und Ransomware-Opfern dabei zu helfen, Dateien ohne Lösegeldzahlungen zurückzuerhalten, veröffentlicht SentinelOne das Tool auf GitHub <https://github.com/Sentinel-One/foss/tree/master/s1-evilquest-decryptor>. SentinelOne blockiert die EvilQuest-Ransomware in Maschinengeschwindigkeit bei jedem seiner 4.000 Kunden – wie in diesem Video <https://assets.sentinelone.com/evilquest/436134590> gezeigt wird.

„Cyberkriminelle sind sehr darauf erpicht und geschickt darin, jede Gelegenheit zu nutzen, um einen Benutzer oder ein Unternehmen mit Ransomware zu infizieren, unabhängig vom Betriebssystem der jeweiligen Organisation", sagte Migo Kedem, Senior Director, SentinelLabs. „Die Herausforderung für macOS-Benutzer besteht darin, dass die meisten Sicherheitsanbieter macOS vernachlässigen und unterdurchschnittliche und ineffektive Produkte liefern, die der heutigen Bedrohungslandschaft nicht gewachsen sind. SentinelOne hat strategisch in den Aufbau der marktführenden macOS-Sicherheitslösung investiert, und wir freuen uns, dieses Tool jedem macOS-Benutzer zur Verfügung stellen zu können, um die EvilQuest-Ransomware abzuwehren.”

Die EvilQuest-Ransomware weist verschiedene Verhaltensweisen auf dem Gerät des Opfers auf, einschließlich Dateiverschlüsselung, Datenexfiltration und Keylogging. Forschungsergebnisse von SentinelLabs deuten jedoch darauf hin, dass EvilQuest nichts mit der Verschlüsselung mit öffentlichen Schlüsseln zu tun hat und stattdessen oft eine Tabelle verwendet, die normalerweise mit der Blockchiffre RC2 assoziiert wird. Da das SentinelLabs-Team davon wusste, war es dem Forscherteam möglich, die Verschlüsselungsroutine von EvilQuest zu durchbrechen, Dateien zu entsperren und die Angriffskette zu unterbrechen.

Weitere technische Einzelheiten zur EvilQuest-Ransomware finden Sie auf dem SentinelOne-Blog unter folgendem Link: https://www.sentinelone.com/blog/evilquest-a-new-macos-malware-rolls-ransomware-spyware-and-data-theft-into-one/.

Über SentinelOne

SentinelOne bietet autonomen Endpunktschutz durch einen einzigen Agenten, der Angriffe über alle wichtigen Vektoren hinweg erfolgreich verhindert, erkennt und darauf reagiert. Die Singularity-Plattform wurde für eine extrem einfache Bedienung entwickelt und spart Kunden Zeit, indem sie KI zur automatischen Beseitigung von Bedrohungen in Echtzeit sowohl für standortbasierte als auch für Cloud-Umgebungen einsetzt. Sie ist die einzige Lösung, die direkt vom Endpunkt aus eine vollständige Transparenz über Netzwerke hinweg bietet. Wenn Sie mehr erfahren möchten, besuchen Sie www.sentinelone.com/de oder folgen Sie uns bei @SentinelOne, auf LinkedIn oder Facebook.

Kontakt

Kafka Kommunikation GmbH & Co.
Dr. Bastian Hallbauer-Beutler
Lukas Reck
Kafka Kommunikation
089 74 74 70 580
sentinelone@kafka-kommunikation.de