

Oxygen Forensics greift per checkra1n-Jailbreak auf gesperrte iPhones zu

19.02.2020, 13:42 | IT, New Media & Software

Pressemitteilung von: *Oxygen Forensics, Inc.*

Presseagentur: *Prolog Communications GmbH*

Oxygen Forensics hat ein Update seiner All-in-one-Forensik-Lösung Oxygen Forensic Detective Software veröffentlicht.

Version 12.2 des für lizenzierte Strafverfolgungs- und Bundesbehörden nutzbaren Programms bietet neue Funktionen, die die Arbeit für Ermittler erheblich erleichtern. Durch Ausnutzung des checkra1n-Jailbreak etwa kann auf eine größere Anzahl an digitalen Beweisen zugegriffen werden, da nun mobile Endgeräte unterstützt werden, die gesperrt sind, oder für die bisher kein Support durch Oxygen Forensics bestanden hatte.

Das Update für Oxygen Forensics führt zwei neue Methoden ein, die zur Erfassung von Daten auf gesperrten Geräten verwendet werden können. Die erste Methode ermöglicht es Ermittlern, mit verschiedenen Jailbreaks für Apple iOS-Geräte zu arbeiten - einschließlich des neuesten checkra1n-Jailbreaks.

iOS-Extraktion per checkra1n-Jailbreak

Für Geräte, auf denen bereits ein checkra1n-Jailbreak installiert ist, bietet Oxygen Forensic Detective zwei Optionen:

- Wenn das Apple-iOS-Gerät gesperrt ist, kann das Dateisystem eingeschränkt extrahiert werden, jedoch nicht der Schlüsselbund.
- Wenn das Apple iOS-Gerät entsperrt ist, wird das gesamte Dateisystem und der Schlüsselbund extrahiert und geparkt.

Oxygen Forensic Detective 12.2 extrahiert den kompletten Schlüsselbund mit Zertifikat und wichtige Elemente aus den jailbroken Apple-iOS-Geräten. Außerdem werden Apple-GrayKey-Bilder ausgelesen. Die Keys aus der Schlüsselbund-Datei können sogar dazu verwendet werden, sichere Apps zu entschlüsseln - einschließlich Wickr Me und Signal.

Android-Extraktion durch Umgehung der Bildschirmsperre

Mit der zweiten neuen Extraktionsmethode wird die Bildschirmsperre umgangen und eine vollständige Datenextraktion auf Android-Geräten durchgeführt, die auf dem Spreadtrum-Chipsatz basieren. Wenn ein Gerät verschlüsselt und der sichere Start aktiviert ist, bietet Oxygen Forensic Detective eine integrierte Passwort- und Daten-Entschlüsselung per Brute-Force-Angriff.

Eine weitere Methode, die für die Untersuchung von Mobilgeräten relevant sein kann, ist die Möglichkeit, Root-Privilegien auf Android-Geräten zu erlangen. Dies gilt für Android-Geräte, die die Versionen 7, 8 und 9 mit Sicherheitspatch-Level bis einschließlich Oktober 2019 ausführen. Diese Methode ermöglicht den vollen Zugriff auf eine Vielzahl von gängigen Android-Geräten.

Weitere Verbesserungen

Zu den weiteren Verbesserungen, die in Oxygen Forensic Detective 12.2 integriert sind, zählt die Fähigkeit, verfügbare Daten aus Instagram und "Facebook Warrant Returns" zu importieren und zu dekodieren. Außerdem können Ermittler nun Systemdateien auf Windows- und MacOS-Computern erfassen, um so einen Einblick in das Nutzerverhalten zu gewinnen. Diese Dateien umfassen Jumplists, die den Verlauf der letzten Interaktionen des Benutzers mit dem Computer

enthalten. Des Weiteren sind Shellbags und die USBSTOR-Registry enthalten. Mit Ersterem kann der Verlauf der Ordner-Durchsuchung des Benutzers verfolgt werden, mit Zweiterem erhält man Einblick in den Verlauf aller angeschlossenen USB-Geräte.

Die Analyse dieser Dateien ist sowohl für kriminaltechnische als auch für unternehmerische Untersuchungen nützlich - einschließlich der Fälle, in denen Malware-Infektion und Fehlverhalten von Mitarbeitern auftraten.

Die Oxygen Forensic Detective Suite steht Strafverfolgungsbehörden zur Verfügung, die zuvor überprüft und entsprechend lizenziert wurden. Die Suite steht nach entsprechender Prüfung ebenfalls für Privatkunden für Untersuchungen und unternehmensinterne Analysen zur Verfügung.

Pressekontakt:

Prolog Communications GmbH
Herr Achim Heinze
Sendlinger Str. 24
80331 München

fon ..: +49 89 800 77-0
web ..: <http://www.prolog-pr.com>
email : achim.heinze@prolog-pr.com

Portrait

-

News-ID: 1077522 • Views: 798 (Stand: 30.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1077522/Oxygen-Forensics-greift-per-checkra1n-Jailbreak-auf-gesperrte-iPhones-zu.html>