

Extrahierte Benachrichtigungen aus iOS-Geräten - wertvolle Einblicke für Forensiker



Moskau, Russland – 2. März 2017 - ElcomSoft aktualisiert [Elcomsoft Phone Viewer \(EPV\)](#), ein einfach zu bedienendes forensisches Tool für den schnellen Zugriff auf Informationen, die aus lokalen und mobilen Cloud-Backups extrahiert werden. In der neuen Version können ungelesene Gerätebenachrichtigungen aus iOS-Sicherungen angezeigt werden, die sogar einige Jahre zurückreichen können. In einem Fall konnte ElcomSoft nicht weniger als 1.200 Meldungen aus dem Jahr 2012 extrahieren.

Entwickler von Betriebssystemen können genau entscheiden, welche Daten in einem Backup gespeichert werden sollen. Bei den meisten Instant Messenger-Anwendungen werden daher weder Konversationen noch einzelne Nachrichten jemals in der Cloud oder in lokalen Backups gespeichert. Auch heruntergeladene E-Mails werden nicht in einer Sicherung aufbewahrt. Die Extraktion von Nachrichten ist also nur über die physische Erfassung mit Jailbreak möglich, der nicht immer vorhanden ist. Das Extrahieren von iOS-Benachrichtigungen kann demnach wertvolle Einblicke in die Kommunikation und die täglichen Aktivitäten des Benutzers liefern.

Elcomsoft Phone Viewer 3.30 zeigt iOS-Benachrichtigungen an

Die meisten iOS-Apps benutzen Push-Benachrichtigungen, um zeitsensible, textbasierte Informationen an den Benutzer zu liefern. Sie werden von Anwendungen wie E-Mail-Clients, Instant Messenger, Zwei-Faktor-Authentifizierungs-Apps sowie Reise-Anwendungen für die Buchung von Flugtickets, Hotels oder Taxis verwendet.

Die App Uber beispielsweise, genau wie viele lokale Taxi-Dienste auch, verwendet solche Benachrichtigungen, um den Nutzer über die Ankunft des Taxis zu informieren, oft mit der genauen Zeit- und Ortsangabe und manchmal sogar mit dem Kennzeichen des Autos. Auch Banken versenden mittlerweile Informationen in Echtzeit über Kreditgeschäfte und Kontoaktualisierungen in Form von Push-Benachrichtigungen anstatt von SMS-Nachrichten.

Es ist nicht ungewöhnlich, dass Banking-Apps Sign-In-Bestätigungscodes über die Benachrichtigungsfunktion an den Kunden schicken. Shopping-Apps beispielsweise von Amazon übermitteln mithilfe von Push-Benachrichtigungen Informationen über den Lieferstatus von Sendungen. Google Trips, Booking und Expedia Apps zeigen bevorstehende Reiseereignisse an, während Skype, Facebook, Twitter, LinkedIn, Pinterest und viele andere

Anwendungen Push-Benachrichtigungen über aktuelle Aktivitäten wie Kommentare, Likes, Freundschaftsanfragen oder Retweets versenden.

Solche flüchtige Echtzeit-Informationen werden häufig von Ermittlern übersehen, obwohl sie bei Untersuchungen eine bedeutende Rolle spielen können. Doch wenn iOS-Benachrichtigungen vom Benutzer nicht gelesen oder gelöscht werden, werden sie automatisch in lokalen und Cloud-Backups gespeichert. Sobald sie gesichert sind, können Benachrichtigungen in der Cloud oder in neu erstellten lokalen Backups für Jahre aufbewahrt werden. Bei der Untersuchung eines besonders alten Kontos konnten Forscher von ElcomSoft nicht weniger als 1.200 Benachrichtigungen aus dem Zeitraum von 2012 bis 2017 auslesen.

*"Benachrichtigungen sind ein wesentlicher Bestandteil von mobilen Betriebssystemen und können große Mengen an hochsensiblen Informationen enthalten", sagt **Vladimir Katalov**, CEO von ElcomSoft. "Sie werden von Instant Messaging-Anwendungen, E-Mail-Clients, Online-Banking Apps, Shopping- und Sendungsverfolgungs-Anwendungen, Buchungs- und Taxi-Apps verwendet. Ungelesene Benachrichtigungen werden automatisch in der iCloud und in lokalen Backups gespeichert und können mit Elcomsoft Phone Viewer 3.30 angezeigt werden. Diese Daten sind für Ermittler von besonderer Wichtigkeit, da sie an keiner anderen Stelle mehr gespeichert sind und nur auf diese Art eingesehen werden können."*

[Elcomsoft Phone Viewer 3.30](#) kann Benachrichtigungen in iOS-Backups automatisch identifizieren und zeigt ihren vollständigen Inhalt zusammen mit Metadaten (Datum, Uhrzeit, App-Paketname) an.

Preise und Verfügbarkeit

[Elcomsoft Phone Viewer 3.30](#) ist ab sofort verfügbar. Die Standardedition ist für 79 EUR zuzüglich Mehrwertsteuer erhältlich. Lokale Preise können variieren.

Systemanforderungen

Elcomsoft Phone Viewer <https://www.elcomsoft.de/epv.html> ist für Windows PC und Mac verfügbar. Die Software läuft sowohl auf 32-Bit- als auch 64-Bit-Versionen von Windows 7, 8, 8.1 und 10 sowie auf den Server-Betriebssystemen Windows 2008, 2012 und 2016 und unterstützt MacOS 10.8 und neuer. EPV funktioniert ohne die Installation von iTunes oder BlackBerry Desktop Software.

Über die ElcomSoft Co. Ltd.

Die im Jahr 1990 gegründete [ElcomSoft Co. Ltd.](#) entwickelt dem neuesten Stand der Technik entsprechende forensische Computer-Tools, bietet kriminaltechnisches Computer-Training und Beratungsdienstleistungen für Computerbeweismaterial. Seit 1997 hat ElcomSoft Unternehmen, Rechtsschutzbehörden, Militär und Geheimdiensten Unterstützung gewährt. ElcomSoft-Tools werden von den meisten der Fortune 500-Unternehmen, einer Vielzahl militärischer Einheiten überall auf der Welt, ausländischen Regierungen und allen großen Wirtschaftsprüfungsgesellschaften genutzt. ElcomSoft ist Microsoft Certified Partner und Intel Software Partner. Für weitere Informationen besuchen Sie bitte unsere Website: <http://www.elcomsoft.de/>