ELCOMSOFT
PROACTIVE SOFTWARE

Forensik Software liest Daten und Passwörter aus:

Elcomsoft Phone Breaker 5.0 greift auf iCloud-Daten von iOS 9 Geräten zu

Moskau, Russland – 29.Oktober 2015 - Mit der Präsentation von 'Elcomsoft Phone Breaker 5.0' (EPB) reagiert das russische IT-Forensik-Unternehmen auf die neuesten Entwicklungen aus dem Hause Apple. Eine Unterstützung von iOS 9 ist jedoch nicht die einzige Neuerung, die die aktuelle Version mit sich bringt. Denn Apple änderte auch einiges an der Architektur seiner Cloud-Speicher. Zum einen wurden Verschlüsselungsstandards geändert, für die der EPB angepasst werden musste, zum anderen wurde die iCloud mittlerweile vollständig in iCloudDrive migriert. Hinzu kommt, dass mit iOS 9 auch das Sicherheitssystem 'Rootless' und das ATS-Protokoll eingeführt wurden, wodurch neue Hürden für Ermittler aufgebaut wurden.

Zugriff auf iCloudDrive-Daten und System-Backups

Die zentrale Funktion, das Auslesen von Daten aus iCloud beziehungsweise iCloudDrive, ist ab sofort auch bei iOS 9-Geräten möglich. Wie bei den vorangegangenen Versionen des EPB, stehen dem Ermittler für einen Zugriff auf die Cloud-Daten mehrere Wege offen. Eine Möglichkeit ist es, sich mit Apple ID und Passwort zu legitimieren und sich so die Cloud-Daten herunterzuladen. Auch wenn das nach dem Weg durch die Vordertür klingt, ist es ermittlungstechnisch interessant, da selbst der auf iCloudDrive eingeloggte Apple-Nutzer die mit EPB gewonnenen Backup-Daten nicht einsehen kann.

Insbesondere für stille Ermittlungen relevant ist aber der Zugriff auf iCloudDrive mittels Authentifizierungstoken. Elcomsoft Phone Breaker kann auf Zweitgeräten, wie einem Desktop-Rechner Authentifizierungstoken auslesen, mit denen sich dort bestimmte Programme wie das iCloud Control Panel auf iCloudDrive einloggen können. Legitimiert sich der Ermittler mittels solcher Token gegenüber iCloudDrive, bietet ihm das mehrere Vorteile. Einerseits muss er Apple ID und Passwort nicht mehr in Erfahrung bringen und andererseits kann mit dem Token die Zwei-Faktor-Authentifizierung umgangen werden. Auch ein SMS-Alarm, mit dem Apple Kunden über Zugriff auf Cloud-Daten informiert wird bei Token-Zugriff nicht versandt.

Änderungen bei iCloud, iCloudDrive und iOS

Die bekannteste Neuerung dürfte sein, dass iCloud nun vollständig Teil von iCloudDrive geworden ist. Persönliche Daten in der Cloud wie Dokumente, Bilder, Videos und Musik liegen nun neben App-Daten und den kompletten iOS-Backups nebeneinander auf dem iCloudDrive. Allerdings bedeutet das nicht, dass Apple-Nutzer mit Zugriff auf iCloudDrive nun auch Zugriff auf die Daten haben, die bislang in der iCloud gespeichert waren. Das iCloud Control Panel erlaubt nach wie vor lediglich den Zugriff auf die selbst hochgeladenen Dateien. Backups bleiben unzugänglich. Genau deshalb sind für Ermittler Programme wie Elcomsoft Phone Breaker wichtig, weil es mit Ihnen möglich ist, diese Backups downzuloaden und zu entschlüsseln.

Die zweite große Neuerung ist das ATS-Protokoll (App Transport Security), das von Apple mit iOS9 eingeführt wurde. Traffic Sniffing und Man-in-the-Middle-Angriffe sollen damit ausgeschlossen werden. Gerade für Ermittlungsbehörden ist dies ein herber Rückschlag. War es bislang möglich, mit Hilfe von Dienste-Anbietern und Mobilfunkbetreibern die Aktivitäten des betreffenden Geräts lauschend zu verfolgen, wurde dem nun weitgehend ein Riegel vorgeschoben. Der Zugriff auf ein ständig sich aktualisierendes Online-Backup des Betriebssystems, in dem fast alle relevanten Daten vorgehalten werden, wurde so noch wichtiger.

Rootless verhindert Jailbreaks

Seit iPhone 5S respektive iPad mini Retina sind Jailbreaks nur sehr schwierig zu realisieren. Während die früheren 32 Bit-Geräte noch sehr leicht zu knacken waren, wird dies heute deutlich erschwert. Man mag es als Nutzungseinschränkung oder als Sicherheitsfeature verstehen; Fakt ist, dass spätestens mit Rootless die Möglichkeiten, physisch auf ein iPhone zuzugreifen stark gesunken sind. Online-Zugriffe mittels Login-Informationen oder aber Zugriff auf lokal vorliegende verschlüsselte Backup-Dateien, die mit den richtigen Passwörtern entschlüsselt werden können, bleiben daher vorerst das Mittel der Wahl.

Die iCloud und iCloudDrive - Auslesen unterschiedlicher Daten und Passwörter

Ein Backup aller Daten des iPhone oder iPad in der Cloud bringt dem Nutzer in Hinblick auf Ausfallsicherheit einige Vorteile. Bei Diebstahl oder Defekt können alle Daten lückenlos auf einem neuen Gerät wiederhergestellt werden. Es wundert daher nicht, dass dieses Feature von sehr vielen Nutzern in Anspruch genommen wird. Neuere Versionen von iOS aktivieren diese Form des Backup daher per Default. Aber genau diese umfassende Sammlung von Daten macht das Backup für Ermittler interessant. Nicht nur finden sich Adressbücher und Anrufprotokolle in den Cloud-Daten. Dort liegen auch App-Daten wie Browser-History und nicht zuletzt eine Vielzahl auf dem Gerät gespeicherter Passwörter, die es Ermittlern erlauben, sich im Anschluss Zugriff zu anderen Diensten der betreffenden Person zu verschaffen.

Elcomsoft Phone Breaker - Mehr als nur Zugriff

Gelingt der Zugriff auf die iOS-Backups, ist damit die Arbeit aber noch nicht getan. Als forensisches Werkzeug bietet der EPB vor allem Möglichkeiten aus einmal gewonnen Backups die Daten schnell und übersichtlich auszulesen. Die Struktur der Backups zu verstehen ist nicht einfach; wichtige Daten zu finden für Laien nur schwer möglich. Kommt durch laufende Ermittlungen bedingt dann noch Zeitdruck hinzu, so machen der mitgelieferte Dateiexplorer, übersichtliche Darstellungen von Anrufprotokollen, die Browser-History und Apple-Schlüsselbunde den EPB zu einer vollwertigen Analyse-Software.

Betriebssysteme, Preise und Verfügbarkeit

Der Elcomsoft Phone Breaker 5.0 ist ab sofort in der Windows-Version verfügbar. An der entsprechenden Version für Mac OS wird gearbeitet. Angeboten wird der EPB in drei Versionen: Home, Professional und Forensic. Zugriff auf iCloud-Backups und Login mittels Authentifizierungs-Token gehören zum Leistungsumfang der Forensic Edition. Der Preis für die Forensic Edition beträgt 799,- EUR. Die Windows-Version des Elcomsoft Phone Breaker 5.0 läuft ab Windows Vista bzw. ab Windows 2003. Es ist nicht erforderlich iTunes installiert zu haben. Für die Zugriffe auf iCloud-Backup-Daten wird jedoch die Software 'iCloud for Windows' benötigt.

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/