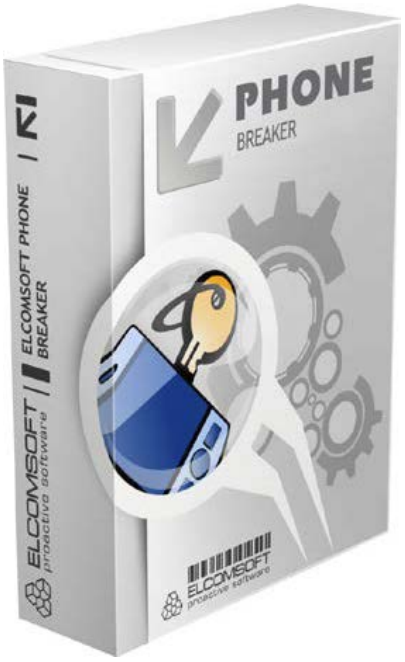
Elcomsoft Phone Breaker entschlüsselt iCloud Drive und Apple Schlüsselbunde



Moskau, Russland - 12. März 2015 - In der neuesten Version rüstet Elcomsoft den Elcomsoft Phone Breaker (EPB) mit dem angekündigten Support für iCloud Drive nach. Mit dem gleichen Update kann mit dem EPB auch der Apple Schlüsselbund dechiffriert werden, der per iCloud Backup gesichert wurde. Voraussetzung hierfür ist, dass die sogenannte 'securityd' bekannt ist. Mit den beiden Erweiterungen macht Elcomsoft als Hersteller forensischer Decryption-Tools einen weiteren Schritt in Richtung kompletter iCloud-Transparenz für Ermittler. Weitere Updates für Windows Mobile und Blackberry-Devices sind in Planung.

Ein neues Feature macht sich gleich beim Aufrufen des Backups bemerkbar. Backup-Eigenschaften und -Kennwerte können ausgelesen werden, Dateistrukturen eingesehen und zugehörige Daten wie IMEI, ICCID etc. abgerufen werden, bevor das ganze Backup geladen und geöffnet wird.

iCloud Drive - die einst sichere Weiterentwicklung von Apple iCloud

Bereits die Vorgängerversion des Elcomsoft Phone Breaker erlaubte Ermittlern den Zugriff auf die iCloud, in der automatische Backups und einige App-Informationen gespeichert waren. Mit dem Upgrade auf iOS 8 können Apple-User auch das fortgeschrittene Cloud-System iCloud Drive nutzen, das als Online-Speicher in Konkurrenz zu großen Cloud-Providern wie Dropbox, Google Drive und Microsoft OneDrive steht. Mittels iCloud Drive kann der Nutzer beliebige Dateien speichern; auch der Umfang automatisch in der Cloud abgelegter Daten hat sich erhöht.

Die neue Version des EPB schließt damit eine Lücke im forensischen Cloud-Zugriff. Bislang konnte lediglich mit verschiedenen Tools ein Zugriff auf Daten gewährt werden, die via Mac Finder oder Windows Explorer zu iCloud Drive hochgeladen wurden, vorausgesetzt Apple ID und Password waren bekannt. Zugriffe auf Backups und Systemdaten, die über Explorer nicht ausgelesen werden konnten, blieben verborgen.

Um an Apple ID und zugehöriges Password zu gelangen, bietet EPB Möglichkeiten, gespeicherte Authentifizierungs-Tokens auszulesen. Diese Tokens können sich auch auf Zweitgeräten befinden, etwa dem Rechner, mit dem am Arbeitsplatz auf die Cloud zugegriffen wurde, und dienen alternative zu Apple ID und Password dazu, sich gegenüber den Apple-Servern zu legitimieren. Ein Programm, dass das Auslesen solcher Tokens bei Apple-Geräten gestattet, ist das 'Elcomsoft iOS Forensic Toolkit (EIFT). Nähere Informationen hierzu finden sich unter www.elcomsoft.de/eift.html

Geplant war seitens Elcomsoft, dass ein umfassender Zugriff auf den neuen Speicher direkt mit dessen Einführung erfolgen sollte. Jedoch stellte die Entwicklung den Spezialisten für forensische Software vor unerwartete Schwierigkeiten. Nur auf die bislang noch weit verbreiteten iCloud-Accounts, die nicht auf iCloud Drive umgestellt wurden, konnte mit den Vorgängerversionen vollumfassend zugegriffen werden. Mit der neuen Version des Elcomsoft Phone Breaker wird die Funktionalität auf alle Arten von Apple Cloud-Storages erweitert.

Zu den im iCloud Drive gespeicherten Informationen gehören neben vom User selbst abgelegten Files auch iWork-Dokumente, von Apps abgelegte Daten wie Spielstände, WhatsApp, Gespräche und Password-Speicher (archivierte Schlüsselbunde) sowie Systemdateien, etwa personalisierte Wörterbücher.

Zugriff auf Apple Schlüsselbunde via iCloud-Backup

In sogenannten Schlüsselbunden organisiert und speichert Apple Zugangsdaten, Logins, Passwörter und Zertifikate, die Apps oder das Betriebssystem brauchen um sich zu legitimieren. Auf Schlüsselbunde, die iOS automatisch in iCloud-Backups speichert, kann mit EPB zugegriffen werden und mit Hilfe der sogenannten 'securityd' können diese entschlüsselt werden. Gemeint ist hiermit nicht der iCloud-Schlüsselbund, sondern klassischerweise hardwareseitig gespeicherte Schlüsselbunde, die nur als Backup in der iCloud oder auf iCloud Drive liegen und nur abgerufen werden, wenn sie wiederhergestellt werden müssen. Zum Auslesen des securityd kann ebenfalls das Elcomsoft iOS Forensic Toolkit genutzt werden.

Interessanterweise ist der 'securityd'-Schlüssel hardwareseitig für ein Gerät festgelegt und wird nicht einmal durch ein Factory Reset geändert. Wurde er für ein Gerät einmal entschlüsselt, steht er Ermittlern über die gesamte Lebensdauer damit zur Verfügung.

Preise und Verfügbarkeit

Der Elcomsoft Phone Breaker ist in den Versionen Home, Professional und Forensic verfügbar. Das komplette Auslesen von Online-Backups auf einen Computer ist nur in der Professional- und Forensic-Version möglich. Der Zugriff mittels Sicherheitstoken ist auf die Forensic-Version beschränkt. Die Preise liegen bei 79,- EUR für die Home-, 199,- EUR für die Professional und 799,- EUR für die Forensic-Version. Elcomsoft Phone Breaker läuft auf Windows 7 und aufwärts. Für die Benutzung muss keinerlei Software von Apple oder BlackBerry installiert werden. Developer Program.

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/