

ElcomSoft Phone Breaker 7.0 – das erste Tool, das auf Informationen im iCloud-Schlüsselbund zugreifen kann



Moskau, Russland – 22. August 2017 - ElcomSoft aktualisiert [Elcomsoft Phone Breaker \(EPB\)](#), das forensische Erfassungstool des Unternehmens. Die Version 7.0 ist ab sofort in der Lage, Passwörter aus dem Cloud-Speicher von Apple, dem iCloud-Schlüsselbund, zu extrahieren und zu entschlüsseln. Damit ist Elcomsoft Phone Breaker 7.0 die erste forensische Lösung, die Zugriff auf Passwörter und andere sensible Informationen im iCloud-Schlüsselbund erlangen kann.

*"Es war lange Zeit unmöglich, auf Informationen im iCloud-Schlüsselbund zuzugreifen", sagt **Vladimir Katalov**, CEO von ElcomSoft. "Passwörter aus dem Schlüsselbund auslesen zu können, ist deshalb eine große Herausforderung. Der iCloud-Schlüsselbund ist ein komplexer und extrem sicherer Online-Passwortspeicher beziehungsweise Speicher-Synchronisationssystem. Ein Tool entwickelt zu haben, das sich in den iCloud-Schlüsselbund hacken kann, ist eine große Leistung."*

Hintergrund

iOS und macOS implementieren einen systemweiten geschützten Speicher für sensible Informationen wie Web-Logins und Passwörter, Kreditkartendaten, WLAN-Kennwörter usw. Diese Elemente werden im Systemschlüsselbund gespeichert. Bei iOS-Geräten kann der Schlüsselbund in lokalen oder Cloud-Backups gespeichert und bei Bedarf wiederhergestellt werden.

Der forensische Zugang zum iOS-Schlüsselbund erweist sich aufgrund mehrerer Verschlüsselungsstufen als sehr schwierig. Der in einer iCloud-Sicherung gespeicherte Schlüsselbund ist mit einem hardwarebasierten Encryption Key sicher verschlüsselt und kann nur auf dem Gerät wiederhergestellt werden, von dem es gespeichert wurde. Der forensische Zugriff auf hardwareverschlüsselte Schlüsselbunde ist außer bei wenigen Ausnahmen (ältere Geräte, Jailbreak) unmöglich. Für die Extraktion des Schlüsselbundes kann eine passwortgeschützte lokale Sicherung verwendet werden – wenn jedoch die Sicherung mit einem langen, unbekanntem Passwort geschützt ist, kann ein Brute-Force-Angriff erhebliche Zeit in Anspruch nehmen und im schlimmsten Fall fruchtlos sein.

Zusätzlich zu lokalen Schlüsselbunden bietet Apple auch einen Cloud-Passwortspeicher beziehungsweise -Synchronisationssystem, den iCloud-Schlüsselbund. Dabei handelt es sich um ein Feature, das die Passwörter des Benutzers über mehrere Geräte hinweg synchronisiert. Dieser Dienst bietet einen sicheren Speicher-, Authentifizierungs- und Synchronisationsmechanismus, sodass neu registrierte Geräte Zugriff auf Schlüsselbund-Elemente von bereits verwendeten Geräten des Benutzers erhalten können. Der iCloud-Schlüsselbund wird von mehreren Verschlüsselungsstufen geschützt, unter anderem durch branchenübliche Verschlüsselungstechnologien, aber auch durch

Zugriffsbeschränkungen der Vertrauenskette. Dieses System ist so sicher, dass bis jetzt der Zugang Dritter zum iCloud-Schlüsselbund unmöglich war.

Die neue Version von Elcomsoft Phone Breaker

[Elcomsoft Phone Breaker 7.0](#) ist das erste Tool, das auf die im iCloud-Schlüsselbund gespeicherten Informationen zugreifen kann. Die Daten werden direkt aus dem iCloud-Konto des Benutzers ausgelesen. Um auf den iCloud-Schlüsselbund zugreifen zu können, sind das Apple ID-Login und das dazugehörige Passwort des Benutzer erforderlich. Wenn die Zwei-Faktor-Authentifizierung im Benutzerkonto aktiviert wurde, ist der Zugriff auf ein vertrauenswürdigenes Gerät notwendig zusammen mit dem Geräte-Passcode (bei Geräten mit iOS) oder dem Systempasswort (bei einem Mac) des Geräts, das bereits mit dem iCloud-Schlüsselbund registriert wurde. Wenn die Zwei-Faktor-Authentifizierung deaktiviert ist, müssen Experten eine Benachrichtigungsaufforderung auf einem der vertrauenswürdigen Geräte bestätigen und den iCloud Security Code des Benutzers eingeben.

Durch die Extraktion der gespeicherten Passwörter eines Benutzers aus dem iCloud-Schlüsselbund können sich Experten in die Online-Konten des Nutzers einloggen, auf seine Konten in sozialen Netzwerken zugreifen und Chats, Nachrichten und Posts extrahieren. Darüber hinaus eignen sich gespeicherte Passwörter ausgezeichnet für den Aufbau von benutzerdefinierten Wörterbüchern für gezielte Brute-Force-Angriffe auf verschlüsselte Container, Archive und Dokumente des Nutzers.

Preise und Verfügbarkeit

[Elcomsoft Phone Breaker 7.0](#) ist sowohl für Windows als auch für macOS verfügbar. Erhältlich sind die Versionen Home, Professional und Forensic. Zugriff auf die iCloud ist nur in den Professional- und Forensic-Editionen verfügbar, während der Passwort-freie iCloud-Zugang sowie die Möglichkeit, beliebige Informationen aus der iCloud und vom iCloud Drive herunterzuladen, nur in der Forensic-Edition verfügbar sind. Elcomsoft Phone Breaker Pro ist für 199 EUR zuzüglich Mehrwertsteuer erhältlich, während die Forensic-Edition, die Over-the-Air-Zugriff auf iCloud-Daten und Unterstützung für binäre Authentifizierungs-Token bietet, für 799 EUR zuzüglich Mehrwertsteuer erworben werden kann. Die Home-Edition ist für 79 EUR zuzüglich Mehrwertsteuer verfügbar. Lokale Preise können variieren.

Systemanforderungen

[Elcomsoft Phone Breaker](#) läuft unter Windows 7, 8, 8.1 und Windows 10 sowie den Server-Betriebssystemen Windows 2008, 2012 und 2016. Die Mac-Version läuft unter Mac OS X 10.7 und neuer. Elcomsoft Phone Breaker funktioniert ohne die Installation von iTunes oder BlackBerry Link.

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/>