ELCOMSOFT
PROACTIVE SOFTWARE

Elcomsoft Phone Breaker 6.0 entschlüsselt FileVault 2 und unterstützt die iCloud Fotomediathek

Moskau, Russland – der 25. August 2016 - ElcomSoft aktualisiert Elcomsoft Phone Breaker (EPB), das mobile Forensik-Tool des Unternehmens für logischen und Over-the-Air-Zugriff auf mobile Geräte. In der neuen Version wird das Entschlüsseln von FileVault 2-Volumes durch die Ermittlung des Recovery Key aus der iCloud unterstützt. Darüber hinaus können mit EPB 6.0 bestehende und kürzlich gelöschte Fotos und Medien-Dateien aus der iCloud Fotomediathek heruntergeladen werden. Weitere Aktualisierungen betreffen den Keychain Explorer des Tools und seine Fähigkeit, Online-Authentifizierungs-Daten für aufeinander folgende Anmeldungen in iCloud, Windows Phone und BlackBerry 10 zu cachen.

*"In dieser Version zielen wir auf zwei weitere Bereiche der iCloud ab", sagt **Vladimir Katalov**, CEO von ElcomSoft. "Durch die Ermittlung des Recovery Key von FileVault 2 können wir Daten entschlüsseln, die in Mac OS X FileVault 2 Containern gespeichert sind. Der Zugang zur iCloud Fotomediathek ermöglicht uns, bestehende Medien herunterzuladen und Dateien wiederher-zustellen, die vor mehr als 30 Tagen gelöscht wurden und auf den Geräten oder auf iCloud.com nicht mehr im 'Zuletzt gelöscht'-Ordner erscheinen."*

Um auf die iCloud beziehungsweise auf die iCloud Fotomediathek zugreifen zu können, muss die korrekte Apple ID mit dem dazugehörigen Passwort oder das nicht abgelaufene iCloud Authentifi-zierungs-Token verwendet werden. Zugang zum zweiten Authentifizierungsfaktor ist erforderlich, wenn die zweistufige oder die Zwei-Faktor-Authentifizierung für ein Apple-Konto eingerichtet wurde, es sei denn die Authentifizierung erfolgt mit einem binären Token. Zugriff auf iCloud und auf die iCloud Fotomediathek ist in den Professional und Forensic Versionen enthalten. Unterstützung für die Zwei-Faktor-Authentifizierung und binäre Authentifizierungs-Token ist nur in der Forensic Version enthalten.

Entschlüsselung von FileVault 2-Volumes

FileVault 2 ist eine vollständige Festplatten-Verschlüsselung, die in Apples Mac OS X verwendet wird. Sie schützt das gesamte Startvolume mit einer sicheren XTS-AES 256-Verschlüsselung. FileVault 2-Volumes können mit dem Passwort eines jeden Kontos entriegelt werden. Wenn der Benutzer das Passwort seines Accounts vergisst oder wenn das verschlüsselte Volume auf einen anderen Computer verschoben wird, kann FileVault 2 mit einem Wiederherstellungs-Schlüssel (Recovery Key) entriegelt werden.

Dieser wird erstellt, sobald der Benutzer FileVault 2 auf seiner Festplatte einrichtet. Der Schlüssel wird angezeigt und kann gespeichert oder ausgedruckt werden. Wenn der Benutzer sich mit seiner Apple ID anmeldet, kann der Recovery Key im iCloud-Konto des Benutzers gespeichert werden. Sollte der Benutzer sein Passwort vergessen, kann das System den Recovery Key automatisch verwenden, um das verschlüsselte Volume zu entsperren.

Apple stellt keine Möglichkeit für den Benutzer zur Verfügung, den Recovery Key von FileVault 2 in der iCloud anzuzeigen oder ihn zu extrahieren. In der neuen Version kann EPB den Recovery Key aus dem iCloud-Konto des Benutzers auslesen und ihn verwenden, um verschlüsselte Disk-Images zu entschlüsseln. Gültige Authentifizierungs- (Apple ID und Passwort oder iCloud Authentifizierungs-Token) sowie Volume-Identifikations-Daten, die aus dem Disk-Image (verschlüsselt durch FileVault) ausgelesen werden, werden benötigt, um den Schlüssel zu ermitteln. Sobald der Recovery Key erfolgreich ermittelt wurde, kann der Benutzer eine vollständige Entschlüsselung für Offline-Analysen durchführen.

Herunterladen der iCloud Fotomediathek

Die Einführung von Apple iCloud im Jahre 2011 ermöglichte iPhone- und iPad-Nutzern, den Inhalt ihrer Geräte in die Cloud hochzuladen und sie wiederherzustellen. Damals wurden Fotos und Videos, die mit einem iOS-Gerät erstellt wurden, in die Hauptsicherung mit einbezogen und konnten nicht einfach heruntergeladen werden. Die einzige Möglichkeit, Zugriff auf diese Medien-Dateien zu erlangen, war die vollständige Wiederherstellung der Sicherung auf einem neuen Apple-Gerät.

In iOS 8.1 und OS X Yosemite (10.10) führte Apple einen neuen Dienst zum Speichern und Teilen von Fotos und Videos ein. Die iCloud Fotomediathek speichert und synchronisiert mithilfe des Cloud-Service Medien-Dateien zwischen mehreren Geräten. Wenn die iCloud Fotomediathek verwendet wird, werden diese nicht länger in iOS iCloud-Backups gespeichert.

Die iCloud Fotomediathek teilt sich verfügbaren Speicherplatz mit der Apple iCloud, beim Zugriff auf die Mediathek wird jedoch ein separater Satz von APIs verwendet. Die Möglichkeit, auf iCloud-Backups zuzugreifen beziehungsweise gespeicherte Dateien aus dem iCloud Drive herunterzuladen, bedeutet demnach nicht automatisch, dass man Zugriff auf Medien-Dateien hat, die in der iCloud Fotomediathek gespeichert sind.

In dieser Version kann Elcomsoft Phone Breaker Fotos und Videos aus der iCloud Fotomediathek herunterladen und Medien-Dateien auslesen, die vor mehr als 30 Tagen gelöscht wurden. Dadurch wird Zugang zu mehr Beweismaterial ermöglicht als beim Extrahieren des "Zuletzt gelöscht"-Albums.

Experten können den kürzlich aktualisierten Elcomsoft Phone Viewer 2.30 verwenden, um Bilder aus der iCloud Fotomediathek anzeigen zu lassen. Elcomsoft Phone Viewer ist ein einfach zu bedienendes Forensik-Tool, das lokale Backups und Backups aus der Cloud unterstützt. Die neueste Version kann Fotos und Metadaten aus der iCloud Fotomediathek anzeigen.

Neuer Viewer für Schlüsselbunde

Elcomsoft Phone Breaker 6.0 erhält einen neuen Look für seinen Schlüsselbund Viewer. Die neue Version erleichtert den Zugriff auf Browser-Passwörter, Authentifizierungs-Token (einschließlich der für iCloud-Backups und -Dateien), gespeicherte Kreditkartendaten und WLAN-Passwörter, die mit dem iCloud-Schlüsselbund synchronisiert wurden. Der neue Viewer versucht automatisch, das Kennwort für die Apple ID und/oder das Authentifizierungs-Token des Benutzers zu ermitteln, indem er Browser-Passwörter beziehungsweise iTunes- und App Store-Einstellungen analysiert. Passwörter zu E-Mail-Konten sowie zu sozialen Netzwerken, Gaming-Portalen und Instant Messaging-Anwendungen können ebenfalls angezeigt werden.

Schlüsselbund-Daten können aus Passwort-geschützten iTunes-Backups ausgelesen werden. Das Passwort muss bekannt sein oder mit EPB ermittelt werden.

Preise und Verfügbarkeit

Elcomsoft Phone Breaker 6.0 ist ab sofort für Windows und Mac OS X erhältlich. Es stehen die Versionen Home, Professional und Forensic zur Verfügung. Zugriff auf die iCloud ist nur in den Professional und Forensic Versionen möglich, während der Passwort-freie Zugang zur iCloud sowie die Möglichkeit, Informationen aus der iCloud und vom iCloud Drive herunterzuladen, nur in der Forensic Version zur Verfügung steht. Elcomsoft Phone Breaker Pro ist für 199 EUR zuzüglich Mehrwertsteuer erhältlich, während die Forensic Version, 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 Version ist für 79 EUR inklusive Mehrwertsteuer verfügbar. Lokale Preise können variieren.

Systemanforderungen

Elcomsoft Phone Breaker 6.0 unterstützt Windows Vista, Windows 7, 8, 8.1 und Windows 10 sowie die Server-Betriebssysteme Windows 2003, 2008 und 2012. Die Mac-Version unterstützt Mac OS X 10.7.x und neuer. Elcomsoft Phone Breaker kann ohne Installierung von Apple iTunes oder BlackBerry Link benutzt werden. Um iOS-Backups und Dateien aus der iCloud herunterladen zu können, muss die iCloud für Windows installiert werden.

Über ElcomSoft

Das im Jahr 1990 gegründete Unternehmen ElcomSoft 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.