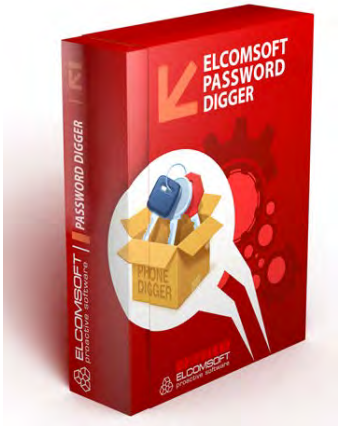
Elcomsoft Password Digger entschlüsselt Mac OS Schlüsselbunde



Moskau, Russland – 16. September 2015 - ElcomSoft Co. Ltd. präsentiert 'Elcomsoft Password Digger', ein digitales Forensik-Tool zum Entschlüsseln von Passwörtern des Mac OS X Schlüsselbunds. Mit diesem Tool kann der gesamte Inhalt aller Schlüsselbunde von Mac OS-Geräten entschlüsselt und exportiert werden. Die Informationen stehen anschließend als unverschlüsselte XML-Datei zur Verfügung. Der Export als "Passwort-Wörterbuch" dient anderen Password Recovery Tools als Datenbasis, um Hinweise auf Syntax und Aufbau der Passwörter zu erhalten.

Über den Max OS X Schlüsselbund

Der Schlüsselbund wurde mit Mac OS 8.6 eingeführt um sensible Daten sicher speichern zu können. Mac OS X benutzt den Schlüsselbund, um sowohl System-Passwörter als auch benutzerspezifische Passwörter zu speichern und zu verwalten. System-Passwörter wie z.B. Passwörter für WLAN sind im System-Schlüsselbund gespeichert, während nutzerspezifische Passwörter von Mac OS X entsprechend im Benutzer-Schlüsselbund abgelegt werden.

Infolge dessen enthält der Benutzer-Schlüsselbund für gewöhnlich hochsensible Authentifizierungs-Informationen wie etwa Passwörter für Webseiten und Accounts (inklusive Apple ID Passwort), Passwörter für VPN, RDP, FTP und SSH, Passwörter für Mail-Konten wie Gmail oder Microsoft Exchange und auch Passwörter für Netzwerk-Freigaben und iWork-Dokumente.

Auch Anwendungen von Drittanbietern können sensible Daten im Schlüsselbund ablegen. So enthält der Schlüsselbund neben den wissentlich hinterlegten Daten oftmals auch Zertifikate, Authentifizierungs-Token und Informationen von anderen Anwendungen. Wichtig ist für Ermittler in diesem Zusammenhang vor allem, die Apple-ID in Erfahrung zu bringen. Sie ermöglicht es, vollständige Backups von iOS-Geräten aus der Apple iCloud zu ziehen. Die Schlüsselbunde sind in den so gewonnen Backups in verschlüsselter Form enthalten.

Zwar sind die im Schlüsselbund gespeicherten Daten sicher verschlüsselt, der Key, mit dem verschlüsselt wird, unterscheidet sich jedoch je nach Schlüsselbund. Für den System-Schlüsselbund wird eine Datei verwendet, die den benötigten Key enthält. Für die Benutzer-Schlüsselbunde werden in der Regel Keys verwendet, die sich aus den Mac OS-Benutzerpasswörtern ableiten lassen.

Um die aus dem Schlüsselbund gewonnenen Daten aufbereitet anzeigen zu lassen, dient Apples eigenes Dienstprogramm 'Keychain Access'. Jedoch ist Keychain Access sehr langsam und unkomfortabel, wenn es für forensische Zwecke benutzt werden soll. Wenn also nicht das Auslesen eines einzelnen Passworts im Vordergrund steht, sondern das systematische Auslesen ganzer Passwort-Datenbanken, ist Keychain Access kaum die erste Wahl. Auch muss bei Keychain Access für jeden Datensatz das Passwort manuell wieder eingegeben werden. Eine entschlüsselte XML-Datei erleichtert in diesem Fall die Arbeit erheblich.

Extrahieren des Max OS X Schlüsselbundes

Der Elcomsoft Password Digger ist geeignet, um alle Daten aus dem System- und dem Benutzer-Schlüsselbund von Mac OS X zu extrahieren. Die gewonnenen Daten werden in einer entschlüsselten XML-Datei ausgegeben. In der entschlüsselten Datei sind danach sämtliche Daten des Schlüsselbundes enthalten, wie beispielsweise die Passwörter im Klartext nebst zugehöriger Website sowie einer Protokollierung von Erstelldaten und Zugriffszeiten dieser Passwörter.

Einmal gewonnen kann diese XML-Datei wiederum in vielen anderen forensischen Tools genutzt werden. Aber auch die manuelle Aufbereitung der Daten durch beispielsweise Microsoft Excel ist problemlos möglich.

Voraussetzungen für den Elcomsoft Password Digger ist ein Windows-PC und die aus Mac OS extrahierten verschlüsselten Rohdaten des Schlüsselbunds. Um Zugriff auf die im Schlüsselbund gespeicherten Daten zu erhalten, werden zudem Authentifizierungs-Informationen benötigt. Im Regelfall ist dies das Mac OS Login oder, falls abweichend, das entsprechende Schlüsselbund-Passwort. Der System-Schlüsselbund wird mittels einer Datei verschlüsselt. Die in der Datei enthaltenen Informationen müssen zunächst vom Gerät extrahiert werden. Bei einem laufenden System sind hierzu Administratorrechte erforderlich.

Erstellung benutzerdefinierter Passwort-Wörterbücher

Brute-Force-Angriffe auf Passwörter sind ohne ein gut recherchiertes Passwort-Wörterbuch wenig Erfolg versprechend. Lässt sich die schiere Zahl möglicher Passwörter nicht drastisch reduzieren, sind auch mit Grafikkarten-Beschleunigung viele Brute-Force-Angriffe viel zu langsam um erfolgreich zu sein. Möchte man beispielsweise Passwörter von neueren MS Office-Dokumenten knacken, so ist eine Passwort-Datenbank unabdingbar. Mit ihr lassen sich bestimmte syntaktische, morphologische oder semantische Gemeinsamkeiten der aus dem Schlüsselbund entwendeten Passwörter ausfindig machen, wodurch die Zahl zu testender Passwörter drastisch gesenkt werden kann.

Genau diese Passwort-Wörterbücher können mit Elcomsoft Password Digger in einem einzigen Klick erstellt werden. Extrahiert wird eine Plain-Text-Passwort-Datei, die ausschließlich Passwörter enthält und es entsprechenden forensischen Tools ermöglicht, die strukturellen Ähnlichkeiten der Passwörter zu nutzen, um intelligente Brute-Force-Attacken zu starten.

Über den Password Digger

Elcomsoft Password Digger ist ein Windows-Programm zum Extrahieren und Entschlüsseln der im Mac OS X Schlüsselbund gespeicherten Informationen. Anschließend werden alle Daten des Schlüsselbunds in eine XML-Datei exportiert, sodass alle Daten aufbereitet und übersichtlich ausgegeben werden können.

Neben der XML-Datei können die Passwörter auf Knopfdruck auch als Passwort-Wörterbuch ausgegeben werden. Die so erstellte Textdatei dient dann als Basis für andere Passwort-Recovery-Tools um hiermit Brute-Force-Angriffe zu beschleunigen. Entschlüsselt werden können System- und Benutzer-Schlüsselbunde.

Preise und Verfügbarkeit

Elcomsoft Password Digger ist ab sofort verfügbar. Für den nordamerikanischen Markt beginnen die Preise bei 199EUR. Die Preise können vor Ort variieren.

Elcomsoft Password Digger läuft mit Windows Vista, Windows 7, 8, 8.1 und Windows 10 oder Windows 2003, 2008 oder 2012 Server und unterstützt allen Versionen des Mac OS Schlüsselbunds, inklusive Mac OS X ‘El Capitan’.

Über ElcomSoft Co. Ltd.

Das Software-Entwicklungshaus ElcomSoft Co. Ltd. wurde 1990 von Alexander Katalov gegründet und befindet sich seither in dessen Besitz. Das in Moskau ansässige Unternehmen hat sich auf proaktive Passwort-Sicherheits-Software für Unternehmen und Privatanwender spezialisiert und vertreibt seine Produkte weltweit. ElcomSoft hat sich zum Ziel gesetzt, mit benutzerfreundlichen Lösungen für die Wiederherstellung von Passwörtern Anwendern den Zugriff auf ihre Daten zu ermöglichen. Des Weiteren gibt die Softwareschmiede Administratoren Sicherheitslösungen an die Hand, mit denen sie unsichere Kennungen in Unternehmens-Netzwerken unter Windows lokalisieren und beseitigen oder EFS-verschlüsselte Dateien retten können.

Regierungen, Behörden, Unternehmen und Privatanwender sind einerseits auf die Sicherheit und andererseits auf die Verfügbarkeit von Daten angewiesen, um Geschäfte abzuwickeln oder tragfähige Entscheidungen treffen zu können. Allerdings sind unsere digitalen Kommunikations-Highways und Aktenschränke zunehmend Sicherheitsrisiken durch Datenspionage und Systemfehler ausgeliefert. So kann eine einzige unsichere Kennung den Schutz eines Unternehmensnetzwerks zunichte machen. Ein unsicheres Passwort in der elektronischen Kommunikation kann das Vertrauen von Geschäftspartnern erheblich beeinträchtigen. Aber auch verloren gegangene Passwörter, beispielsweise für Verträge, können Geschäftsabschlüsse scheitern lassen.