Komplettlösung zum Dekodieren verschlüsselter Laufwerke

Moskau, Russland – 31. Januar, 2018 - ElcomSoft veröffentlicht ein wichtiges Update für Elcomsoft Forensic Disk Decryptor, ein forensisches Tool zum Extrahieren von Informationen aus verschlüsselten Volumes. Die neue Version macht das Toolkit zu einer All-in-one-Lösung für den Zugriff auf verschlüsselte Volumes von FileVault 2, PGP, BitLocker und TrueCrypt. Das aktualisierte Toolkit ermöglicht ab sofort das Mounten oder Entschlüsseln verschlüsselter Volumes mithilfe von Klartext-Passwörtern, Escrow-Schlüsseln oder kryptografischen Schlüsseln, die aus dem Speicher des Computers extrahiert wurden. Darüber hinaus wird jetzt ein neues von Microsoft signiertes Zero-Level-Memory-Dumping-Tool mit dem Toolkit ausgeliefert, mit dem Experten die Daten aus dem Arbeitsspeicher darstellen können.

"Elcomsoft Forensic Disk Decryptor bietet Echtzeitzugriff auf Informationen, die in verschlüsselten Containern gespeichert sind. Durch die Unterstützung aller wichtigen Verschlüsselungsprodukte für die gesamte Festplatte und die Bereitstellung von Zero-Footprint-Funktionen stellt das Tool ein äußerst wertvolles Werkzeug für digitale, forensische Untersuchungen dar", sagt ***Vladimir Katalov,*** *CEO von ElcomSoft.*

Im Rahmen einer strafrechtlich relevanten Untersuchung ist das Tool äußerst hilfreich. Insbesondere, wenn ein Computer in einem eingeschalteten Zustand vorgefunden wird. Während die vollständige Entschlüsselung, abhängig von der Größe des Datenträgers und der Datenmenge, Stunden dauern kann, stellt der Elcomsoft Forensic Disk Decryptor Daten in Echtzeit bereit und bietet sofortigen Zugriff auf wichtige Beweise. Als letzter Ausweg besteht die Möglichkeit, den Passwort-Hash aus dem verschlüsselten Volume zu extrahieren, um das Passwort mithilfe von Elcomsoft Distributed Password Recovery wiederherzustellen. Hierzu führt das Tool einen Angriff auf ein lokales Netzwerk aus.

Integrierte Lösung für den Zugriff auf verschlüsselte Volumes

In früheren Versionen war das Toolkit in seinen Funktionen auf das Mounten oder Entschlüsseln von Volumes mit binären, kryptografischen Schlüsseln beschränkt, die aus dem Speicherabbild oder der Ruhezustandsdatei des Computers extrahiert wurden. Elcomsoft Forensic Disk Decryptor 2.0 bietet ab sofort die Möglichkeit, verschlüsselte Volumes zu mounten oder eine vollständige Entschlüsselung für die Offline-Analyse durchzuführen, indem Klartext-Passwörter, Escrow- oder Wiederherstellungsschlüssel sowie die aus dem Speicherabbild des Computers extrahierten Binärschlüssel verwendet werden. FileVault 2-Wiederherstellungsschlüssel können mit Elcomsoft Phone Breaker aus der iCloud extrahiert werden, während BitLocker-Wiederherstellungsschlüssel in der Active Directory oder im Microsoft-Konto des Benutzers zur Verfügung stehen.

Eingebautes Kernel Level Memory Dumping-Tool

Elcomsoft Forensic Disk Decryptor ist in der Lage, das Speicherbild des Computers zu scannen, um nach kryptografischen Schlüsseln zu suchen, die für den Zugriff auf verschlüsselten Containern gespeicherten Daten verwendet werden. Durch das Extrahieren und Verwenden dieser Schlüssel kann das Tool den Inhalt des Volumes entschlüsseln, ohne dass ein langwieriger Angriff auf das ursprüngliche Klartext-Passwort nötig ist.

Elcomsoft Forensic Disk Decryptor wird in Version 2.0 mit einem Forensic-Speicher-Imaging-Tool ausgeliefert, um ein möglichst vollständiges Speicherabbild aus dem Arbeitsspeicher zu erhalten. Der RAM-Imaging-Treiber von ElcomSoft arbeitet im Kernel-Modus und trägt eine digitale Signatur von Microsoft, wodurch der Treiber vollständig kompatibel zu allen 32-Bit- und 64-Bit-Versionen von Windows 7 bis zum neuesten Windows 10 Fall Creators-Update ist.

Automatische Erkennung von verschlüsselten Volumes und Verschlüsselungs-einstellungen

Mit dem neuesten Update von Elcomsoft Forensic Disk Decryptor ist eine vollautomatische Erkennung von verschlüsselten Volumes und Verschlüsselungs-Einstellungen, einschließlich TrueCrypt, möglich. Experten müssen hierzu nur den Pfad zum verschlüsselten Container oder Disk-Image angeben, und Elcomsoft Forensic Disk Decryptor zeigt und erkennt verschlüsselte Volumes und Details sowie die jeweiligen Verschlüsselungsalgorithmen an.

EnCase .E01-Untersützung und Installation auf USB-Flash-Laufwerken

Elcomsoft Forensic Disk Decryptor 2.0 unterstützt ab sofort EnCase-Images im branchenüblichen ".E01"-Format sowie verschlüsselte DMG-Images. Darüber hinaus kann Elcomsoft Forensic Disk Decryptor dazu verwendet werden, um eine portable Installation auf einem USB-Flash-Laufwerk zu erstellen. Mithilfe der portablen Version kann der Speicher des zu untersuchenden Computers abgebildet oder verschlüsselte Volumes gemountet und entschlüsselt werden.

Kompatibilität

Elcomsoft Forensic Disk Decryptor läuft auf allen 32-Bit und 64-Bit Editionen von Windows 7, 8, 8.1 und 10 sowie den entsprechenden Windows Server Versionen. Das Tool unterstützt alle älteren und aktuellen Versionen von BitLocker, PGP und TrueCrypt (sowie dessen Nachfolger) einschließlich BitLocker-to-Go und PGP Whole Disk Encryption bis einschließlich des aktualisierten BitLocker mit XTS-AES. Verschlüsselte Volumes und eine vollständige Festplatten-Verschlüsselung werden für PGP und TrueCrypt unterstützt.

Preise und Verfügbarkeit

Elcomsoft Forensic Disk Decryptor ist ab sofort für 599 Euro verfügbar, wobei ein Einführungsrabatt von 30 Prozent bis Ende Februar 2018 besteht.

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/