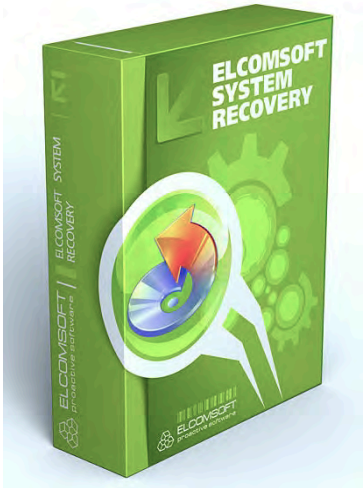
Windows 10 im Visier

Elcomsoft System Recovery und Elcomsoft Forensic Disk Decryptor knacken Windows 10 und Microsoft-Konto



Moskau – 18. März 2016 - Umfassende Updates für 'Elcomsoft System Recovery' und 'Elcomsoft Forensic Disk Decryptor' versetzen Ermittler und Behörden in die Lage viele Geheimnisse und geschützte Informationen aus Windows 10 und den cloudbasierten Microsoft-Konten auszulesen.

Elcomsoft System Recovery (ESR) ist eine Software, die auf die Passwörter von Windows-Konten abzielt. Möglich ist sowohl der Zugriff auf Windows-Konten ohne das Passwort zu kennen als auch der Zugriff auf den Hashwert des Passworts für Offline-Brute-Force-Attacken. ESR kann ebenfalls eingesetzt werden, um die seit Windows 10 forcierten Cloud-basierten "Microsoft-Konten", ehemals Windows Live ID, zu knacken. Mit einem Klartext Microsoft-Konto-Passwort stehen Ermittlern dann auch die Daten aller übrigen Microsoft-Dienste wie Hotmail, Skype und OneDrive offen.

Windows-Passwort kein Hindernis für ESR

Da sich Nutzer seit Windows 10 mit dem cloudbasierten Microsoft-Konto einloggen, erfolgt die Authentifizierung nun online. Dies führt aber mitnichten dazu, dass die Möglichkeiten des klassischen Passwort-Auslesens nun nicht mehr existieren. Um auch beim Microsoft-Konto an die Passwörter zu gelangen startet der ESR ein als Bootimage beigefügtes WinPE (Windows Preinstallation Environment). Dieses muss sich dann wie eine Windows 10 Installation ebenfalls online authentifizieren um Zugriff auf ein Windows 10-Konto zu erhalten, jedoch macht es sich zu Nutze, dass auch Windows 10 für Verbindungsabbrüche die Passwort-Hashes lokal gespeichert hat. Die WinPE-Umgebung kann nun das lokal gecachte Passwort einfach resetten und das Benutzerkonto auf offline umstellen, so dass Ermittler auch ohne bekanntes Passwort auf lokale Windowskonten zugreifen können.

WinPE mit zahlreichen Extras

Das WinPE-Image wurde für den komfortablen Zugriff auf die Windows-Konten erheblich erweitert und angepasst, so dass es wenig mit der von Windows-Installationen bekannten Benutzeroberfläche gemeinsam hat. Die WinPE von ESR unterstützt eine große Bandbreite moderner Hardware und was noch wichtiger sein dürfte, sie verfügt über einen großen Fundus administrativer Tools, mit denen das frisch geknackte Windows-Konto untersucht werden kann. Dazu gehören Möglichkeiten die Ablaufdaten von Passwörtern zu deaktivieren, administrative Rechte neu zu setzen, und Daten wie etwa Hashes aus System- und SAM-Dateien oder dem Active Directory auszulesen.

Mit ausgelesenen Passwörtern von Microsoft-Konten Zugriff auf Skype, Hotmail und OneDrive erhalten

Das Auslesen des Passwort-Hashwertes des Microsoft-Kontos ist von besonderem Interesse, denn so können statt der reinen Online-Authentifizierung unbeschränkte Offline-Brute-Force-Attacken gegen das Microsoft-Konto-Passwort gefahren werden. Mit dem Passwort im Klartext steht Ermittlern dann noch weit mehr offen, als nur das Windows-Konto. Ähnlich wie Ermittlern mit Zugriff auf ein einziges Google-Konto die Daten verschiedener Google-Dienste wie YouTube, GoogleMail und Google+ offenstehen, kann mit dem Zugriff auf ein Microsoft-Konto auch auf Microsoft-Dienste wie Skype, Hotmail oder OneDrive zugegriffen werden. Das Microsoft-Konto-Passwort im Klartext ist dann auch die Eintrittskarte um an alle Daten zu gelangen, die in den Microsoft Cloud-Services gespeichert wurden. Selbst Zugriff auf Windows Phone, Windows 10 Mobile Backup, synchronisierte Browser-Verläufe, Lesezeichen und Autofill-Informationen, unter denen sich auch weitere Passwörter befinden können, sind abrufbar.

Elcomsoft Forensic Disk Decryptor (EFDD) zielt auf verschlüsselte Laufwerke ab. Während ESR bereits ausreicht um EFS-verschlüsselte Windows-Volumes zu durchsuchen, können mit dem EFDD in der neuesten Version auch Informationen aus Volumes ausgelesen werden, die mit BitLocker, PGP oder TrueCrypt verschlüsselt wurden. Unterstützt wird BitLocker unter Windows 8, 8.1 und 10. Die Verschlüsselung wird dabei im eigentlichen Sinn nicht geknackt, sondern mit Hilfe temporärer Dateien auf dem betroffenen PC umgangen. Speicherabbilder wie sie beispielsweise für den Ruhemodus erstellt werden, sind dabei die bevorzugte Fundquelle für die Security-Token, die der EFDD nutzt um auf das verschlüsselte Volume zu entschlüsseln. Wichtig ist dabei nur, dass das System zum Zeitpunkt des Speicherabbilds auf das verschlüsselte Laufwerk Zugriff hatte. War das der Fall, kann der EFDD automatisch die benötigen Token auslesen und einsetzen.

Der EFDD unterstützt auch die neueste Version BitLocker 1511, die auf XTS-AES setzt und erst mit Windows 10 eingeführt wurde. Sie kann optional aktiviert werden, da sie nicht abwärtskompatibel zu früheren Windows-Versionen ist.

Preise und Verfügbarkeit

Sowohl Elcomsoft System Recovery (ESR) als auch Elcomsoft Forensic Disk Decrypter (EFDD) sind verfügbar für Windows XP und neuer, sowie für die entsprechenden Windows Server Versionen. Beide Produkte kosten je 299,- EUR zzgl. MwSt.

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/