Mit Elcomsoft Phone Breaker Passwort-Container auslesen

Moskau, Russland – 11. August 2015 - Das IT-Security-Unternehmen Elcomsoft präsentiert die neue Version 4.10 seiner forensischen Software Elcomsoft Phone Breaker (EPB). Sie gestattet als erstes forensisches Programm überhaupt die in BlackBerrys Passwort-Container 'Password Keeper' gespeicherten Passwörter im Klartext auszulesen. Hierzu sind keine zeitintensiven Brute-Force-Attacken nötig, vielmehr kann der Zugang durch den Escrow-Key direkt ausgelesen werden. Ebenfalls neu ist ein Support für Passwörter, die in einem Password-Container von 1Password gespeichert sind. Der Zugriff hier erfolgt jedoch klassisch über eine automatisierte Brute-Force-Attacke auf das Master-Passwort.

BlackBerry Password Keeper direkt auslesen

Wie fast alle großen Smartphone-Hersteller bietet auch BlackBerry bei seinen Geräten die Möglichkeit Passwörter auf dem Gerät lokal zu speichern. Einmal authentifiziert ist der Nutzer daraufhin vom lästigen Eingeben der Passwörter befreit. In der neuen Version BlackBerry 10 erfolgt der Zugriff auf die Passwort-Datenbank jedoch nicht mehr über ein Master-Passwort, sondern über einen sogenannten Escrow-Key. Dieser auf dem Gerät hinterlegte Key enthält alle nötigen Informationen, um den Passwort-Container freizuschalten. Dies macht der Escrow-Key jedoch nur dann, wenn er von einer autorisierten Quelle den Befehl dazu erhält. Elcomsoft gelang es in der neuen Version die Informationen, die im Escrow-Key zur Authentifizierung gespeichert sind auszulesen und sich somit direkten Zugriff auf die Passwort-Datenbank zu verschaffen. Es geht also nicht darum, dass die Software dem Escrow-Key einen legitimen Zugriff glaubhaft macht. Vielmehr bedient sich der EPB direkt beim Escrow-Key und liest die Informationen aus diesem aus, mit denen der Key selbst die Datenbank entschlüsseln würde.

Bevor jedoch die Daten aus dem Escrow-Key und damit aus der Passwort-Datenbank ausgelesen werden können, ist es erforderlich, sich zunächst Zugriff auf die Daten des jeweiligen Geräts zu verschaffen. Dies kann einerseits klassisch über den physikalischen Zugriff auf die Hardware durch Ermittlungsbehörden erfolgen oder aber man verschafft sich Zugriff auf oftmals online hinterlegte Backups der Daten. Diese Backups sind für gewöhnlich ebenfalls verschlüsselt, kann aber mit Hilfe des EPB entschlüsselt werden.

Brute-Force-Attacken auf 1Password

Ein weiterer sehr beliebter Passwort-Container ist 1Password. Im Gegensatz zu BlackBerrys Password Keeper ist er plattformunabhängig und existiert in Versionen für Mac OS X, Windows, Android und iOS. Dies bietet Ermittlern den Vorteil, dass die verschlüsselte Datenbank in der Regel nicht nur lokal auf einem Gerät oder in verschlüsselten Backups (iTunes) enthalten ist, sondern dass Nutzer von 1Password dazu neigen, die Passwort-Datenbank regelmäßig über Cloud-Services wie Dropbox oder iCloud zu synchronisieren. In Ermittlungen können mit einem legitimierten Zugriff auf Cloud-Daten Passwörter zugänglich gemacht werden, für die kein physischer Zugriff auf die Hardware erforderlich ist. Zwar gibt es bei 1Password keine bekannte Backdoor um an die Passwörter im Klartext zu gelangen, jedoch können mit dem EPB 4.10 intelligente Brute-Force-Attacken gestartet werden, mit denen das Masterpasswort ausfindig gemacht werden kann.

Maximum Performance mit Nvidia

Weitere Neuerungen umfassen vor allem Performance-Steigerung bei Brute-Force-Attacken mit Hilfe von NVidia-Grafikkarten. Durchschnittlich konnte die Leistung um rund **15 bis 50 Prozent** gesteigert werden und entspricht nun dem theoretischen Maximum, das NVidia-Grafikkarten bei Brute-Force-Attacken leisten können. Möglich wurde dies nicht zuletzt durch eine direkte Zusammenarbeit mit Entwicklern von NVidia.

Einfaches Auslesen von iCloud Authentifizierungs-Token

Eines der gefragtesten Features von EPB unter Ermittlungsbehörden ist der Zugriff auf Daten der iCloud ohne vorher die Apple ID oder das Passwort in Erfahrung gebracht zu haben. Möglich ist dies, da von den Nutzern meist über Zweitgeräte wie das Notebook auf dieselbe iCloud zugegriffen wird. Das Notebook wiederum legitimiert sich gegenüber der iCloud in der Regel aber durch einen auf dem Gerät hinterlegten Authentifizierungs-Token. EPB bot daher auch in früheren Versionen die Möglichkeit mit extra Tools und ein wenig Geschick diese Token auszulesen. In der neuen Version 4.10 ist dieser Prozess ganz erheblich optimiert worden. Direkt über die Bedienoberfläche kann auf Knopfdruck von einem entsprechenden Gerät das Authentifizierungs-Token ausgelesen und sogleich verwendet werden.

Preise und Verfügbarkeit

Der Elcomsoft Phone Breaker ist in den Versionen Home, Professional und Forensic verfügbar. Das komplette Auslesen von Online-Backups auf einen Computer ist nur in der Professional- und Forensic-Version möglich. Der Zugriff mittels Sicherheitstoken ist auf die Forensic-Version beschränkt. Die Preise liegen bei 79,- EUR für die Home-, 199,- EUR für die Professional und 799,- EUR für die Forensic-Version. Elcomsoft Phone Breaker läuft auf Windows 7 und aufwärts. Für die Benutzung muss keinerlei Software von Apple oder BlackBerry installiert werden.

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/