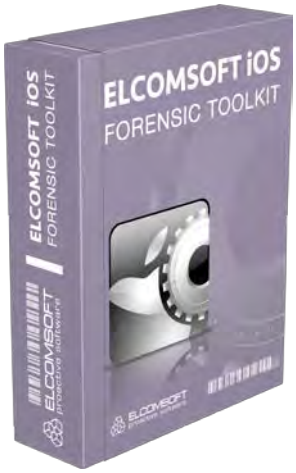
Elcomsoft iOS Forensic Toolkit: Erste Software für physischen Zugriff auf iOS 9 und 64-bit-Geräte



Moskau, Russland – 18. November 2015 - Nach dem 'Elcomsoft Phone Breaker 5.0' (EPB) und dem 'Elcomsoft Phone Viewer 2.0' (EPV) stellt Elcomsoft nun auch das 'Elcomsoft iOS Forensic Toolkit 2.0' (EIFT) vor. Stein des Anstoßes war bei allen drei Programmen das neue Betriebssystem iOS 9, welches massive Änderungen für IT-Forensiker mit sich brachte. Während der EPB darauf spezialisiert ist, sich Zugriff auf die Hardware und auf die Cloud zu verschaffen, ist der EPV, wie der Name schon sagt, ein Viewer, mit dem alle gewonnen Daten aufbereitet und angezeigt werden können. Das EIFT ist da eher etwas für IT-Ingenieure. Es greift nicht auf Cloud-Daten zu, sondern ist für das Auslesen der vorliegenden Hardware gedacht, auf die ein Jailbreak bereits installiert wurde.

Den Hardware-Speicher des iPhones bitweise auslesen

Als erste und einzige Software kann das EIFT 2.0 auf die Speicher aller iOS-Systeme physisch zugreifen. Sowohl das neueste Betriebssystem iOS 9, als auch die neueste 64-bit-Hardware wie das iPhone 6S können vollständig ausgelesen werden. Voraussetzung dafür ist ein installierter Jailbreak und das Entsperren der Codesperre. Die einzige Ausnahme ist folglich iOS 9.1, da hier aktuell noch kein Jailbreak bekannt geworden ist.

Das EIFT ist also weniger für Ermittler gedacht, die die Sicherheitssperren des Nutzers überlisten wollen, sondern eher für Detektive, die auf dem Gerät nach Daten suchen, die sich weder über die Benutzeroberfläche von iOS noch mit anderer Apple-Software anzeigen lassen. Nutzer wissen daher oft nicht, welche Daten auf dem Gerät hinterlegt sind und Ermittlern im Ernstfall zur Verfügung stehen. Zu ihnen zählen beispielsweise alle gespeicherten Passwörter aus den Apple Schlüsselbunden, Browser-Historys, Chroniken und Log-Files, App-Daten, wie etwa Skype oder WhatsApp und sogar das Passwort zur zugehörigen Apple ID.

Beim Zugriff auf 32-bit- und 64-bit-Architektur gibt es technisch einige Unterschiede zu beachten. So wird bei 32-bit-Geräten wirklich bitweise der Hardware-Speicher des betreffenden Geräts ausgelesen, wohingegen bei 64-bit-Geräten ein UNIX TAR-Archiv des Dateisystems extrahiert wird. Bis auf das Auslesen der im Apple Schlüsselbund gespeicherten Passwörter sind beide Verfahren vom Ergebnis her gleich. Aber genau bei den im Apple Schlüsselbund gespeicherten Passwörtern gibt es einen wichtigen Unterschied. Ein Zugriff auf ein 32-bit-Gerät liefert alle Passwörter des Apple Schlüsselbund im Klartext, ein Zugriff auf ein 64-bit-Gerät gibt den Apple Schlüsselbund nur in verschlüsselter Form aus.

Daten auslesen trotz iOS-Codesperre

Lange Zeit galt Apples Codesperre als sichere Barriere gegen unbefugten Zugriff. Denn Apples iOS-Codesperre ist im Vergleich zu Androids Bildschirmsperre deutlich zentraler für das Sicherheitskonzept des Smartphones. Die Codesperre verhindert nicht nur den unbefugten Zugriff auf ein Live-System sondern dient gleichzeitig auch als Key für die Verschlüsselung des Geräts. Apple betont daher gern und oft, dass ein mit Codesperre geschütztes Gerät absolut sicher und unangreifbar ist. Es wurde schließlich nicht nur der Zugriff gesperrt, sondern mit aktivierter Bildschirmsperre sind automatisch auch alle Daten verschlüsselt worden.

Dies stimmt aber so nicht ganz, denn damit ein iPhone wesentliche Prozesse auch im Standby-Modus ausführen kann, muss es auf bestimmte Daten trotz Bildschirmsperre zugreifen können. Andernfalls könnten mit aktiver Codesperre nicht einmal eingehende Anrufe registriert werden.

Genau diese Schwachstelle macht sich das EIFT 2.0 zu Nutze. Bei vorhandenem Jailbreak können einem iOS-Gerät mit aktiver Codesperre sehr wohl jene Daten entnommen werden, auf die das Gerät im gesperrten Zustand selbst zugreifen muss. Dazu zählen nicht nur eingehende Anrufe und Nachrichten, sondern auch bestimmte Log-Files und SQLite WAL Dateien. Selbst ein paar Geoinformationen, die bei der Anmeldung an Funkmasten protokolliert werden, können bei aktiver Codesperre mittels logischem Zugriff ausgelesen werden. Welche App-Daten gewonnen werden können ist weitgehend davon abhängig, ob die jeweilige App auch bei bestehender Codesperre Aufgaben ausführt. Ein gesperrtes Gerät kann beispielsweise keine WhatsApp-Nachrichten empfangen, wohl aber Facebook-Nachrichten. Ergo kann auf letztere auch bei bestehender Codesperre zugegriffen werden.

Eine genaue Erklärung der informatischen Grundlagen, der rechtlichen Bewertung und eine Übersicht über die so zugänglichen Daten findet sich im Blog von Elcomsoft:
http://blog.elcomsoft.com/2015/11/extracting-data-from-locked-iphones/

Ältere iPhones gänzlich ungeschützt

Auch wenn die Marktanteile älterer Modelle naturgemäß sinken, sind alte iPhones und iPads für Ermittler durchaus von Bedeutung. Kaum jemand macht sich die Mühe, beim Wechsel zu einem neueren Modell alle Daten von seinem Vorgängermodell zu entfernen. Für Ermittler sind Altgeräte daher eine oft nur schlecht geschützte Fundgrube, die viele nach wie vor gültige Passwörter und Kontaktadressen verrät. Alle iPhones bis zum iPhone 4 können nämlich uneingeschränkt physisch ausgelesen werden. Erst danach wird es schwieriger. Mit einem Jailbreak können auch alle neueren Modelle und Betriebssysteme ausgelesen werden.

Preise und Verfügbarkeit

Das 'Elcomsoft iOS Forensic Toolkit 2.0' ist ab sofort erhältlich. Die angebotene Version ist sowohl für Windows XP und neuere Versionen als auch für Mac OS X ab 10.6 (Snow Leopard) geeignet. Angeboten wird das Elcomsoft iOS Forensic Toolkit in der Forensic Version für 1.499 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/