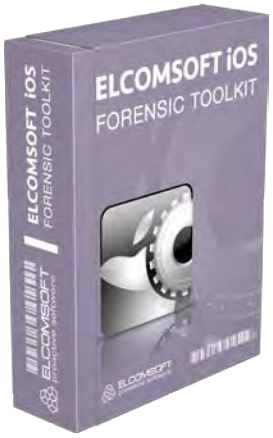
Elcomsoft iOS Forensic Toolkit mit logischem und physischem Zugriff auf iPhones und iPads



Moskau, Russland – der 11. August 2016 - ElcomSoft aktualisiert sein iOS Forensic Toolkit (EIFT). In der neuen Version wird der physische Zugriff durch das Tool auf die meisten modernen Geräte mit iOS 9.2 bis 9.3.3 ermöglicht. Eine zusätzliche Erneuerung ist die Option zum logischen Zugriff auf Geräte, wobei die Entschlüsselung der Codesperre nun nicht mehr erforderlich ist.

Die neue Version bietet logischen Zugriff für alle Generationen von iPhone, iPad, iPad Pro und iPod Touch, unabhängig davon, ob es sich um eine iOS- oder eine Jailbreak-Version handelt. Im Gegensatz zum Zugriff über Apple iTunes ermöglicht EIFT die Nutzung von Lockdown-Dateien (Pairing Records) auf iOS-Geräten, ohne die Codesperre oder die Touch ID zur Entsperrung verwenden zu müssen. Mithilfe der Erweiterung des Toolkits durch den logischen Zugriff zusätzlich zum physischen strebt ElcomSoft eine forensische All-in-One-Erfassungslösung für das breiteste Spektrum an iOS-Geräten an. Das Toolkit ist dabei sowohl für Windows als auch für Mac OS X verfügbar.

Darüber hinaus unterstützt Version 2.1 den physischen Zugriff auf Apple-Geräte, auf denen iOS 9.3.3 mit dem neu veröffentlichten Pangu Jailbreak für 64-Bit-Geräte ausgeführt wird. Außerdem bietet die neue Version die Möglichkeit, Informationen aus allen Arten von iOS-Geräten zu extrahieren, unabhängig davon, ob es sich dabei um eine iOS- oder Jailbreak-Version handelt, selbst wenn sie mit einem unbekannten Passwort geschützt sind.

"*Beim iOS Forensic Toolkit ging es bis jetzt ausschließlich um den physischen Zugriff", sagt **Vladimir Katalov**, CEO von ElcomSoft. "Wir waren die ersten, die Zugriff auf das iPhone 4s, 5 und 5c ermöglicht hatten. Wir schafften als erster den physischen Zugriff auf 64-Bit-Geräte, aber bis jetzt hatten wir nicht die Möglichkeit, auf Geräte ohne Jailbreak zuzugreifen. Wenn Sie ein iPhone oder iPad ohne Jailbreak haben, können wir jetzt seinen Inhalt in ein iTunes-ähnliches Backup laden, ohne tatsächlich iTunes zu benutzen, und das manchmal sogar ohne dass eine Codesperre hinderlich wäre."*

Der logische Zugriffsprozess erfordert, dass das Gerät zumindest einmal nach dem Kaltstart freigeschaltet wird. Die Ermittler werden das Gerät mithilfe der Codesperre, der Touch ID oder des nicht abgelaufenen Pairing Record (Lockdown-Datei) entsperren, die sie vom Computer des Benutzers gesammelt hatten.

*"Wir hatten schon seit Monaten keinen Jailbreak", sagt **Andy Malyshev**, CTO von ElcomSoft. "Wir konnten bei iOS 9.2 oder 9.3 ohne Jailbreak nichts machen. Der neue Pangu Jailbreak erlaubt uns, die Entwicklung fortzusetzen und den physischen Zugriff für die neuesten Versionen von iOS zu ermöglichen."*

Logischer Zugriff: Funktioniert bei allen iOS-Geräten

Der logische Zugriff ist eine einfachere und sichere Zugriffsmethode im Vergleich zum physischen Zugriff. Dabei wird ein iTunes-ähnliches Backup von den Informationen erzeugt, die auf dem Gerät gespeichert sind. Während durch die logische Methode weniger Informationen als durch die physische gewonnen werden, wird Experten empfohlen, ein logisches Backup des Gerätes zu erstellen, bevor sie weitere invasive Erfassungstechniken anwenden. Die neue Version von EIFT bietet nun die Option, logischen Zugriff auf iOS-Geräte zu erhalten. Das funktioniert auf allen Geräten mit iOS 4 oder höher, unabhängig davon, ob es sich um eine Hardware- oder Jailbreak-Version handelt. Allerdings muss das Gerät mindestens einmal nach dem Kaltstart entriegelt werden, andernfalls kann der Backup-Dienst nicht gestartet werden.

Experten müssen das Gerät mit Codesperre oder Touch ID entsperren oder eine nicht abgelaufene Lockdown-Datei (iTunes Pairing Record) vom Computer des Benutzers benutzen. Lockdown-Dateien sind Pairing Records, die auf Computern erstellt werden, die mit dem betroffenen iOS-Gerät verbunden sind. Lockdown-Dateien werden erzeugt, damit der Benutzer nicht jedes Mal sein iOS-Gerät manuell entsperren muss, wenn es mit iTunes synchronisiert. Wenn ein Computer zusammen mit einem iOS-Gerät beschlagnahmt wurde, kann es ausreichen, erfolgreich Informationen von einem gesperrten iOS-Gerät zu erhalten.

Wenn das Gerät konfiguriert ist, um passwortgeschützte Backups zu erzeugen, müssen Experten Elcomsoft Phone Breaker benutzen, um das Kennwort zu ermitteln und die Verschlüsselung zu entfernen. Apple iTunes wird nicht benötigt, um ein Backup zu erzeugen.

Logische Backups, die von EIFT erzeugt werden, können mit Elcomsoft Phone Viewer oder mit Forensik-Tools von Drittanbietern analysiert werden. Wenn ein verschlüsseltes Backup mit einem unbekannten Passwort erstellt wurde, kann man Elcomsoft Phone Breaker verwenden, um das Passwort zu ermitteln und das Backup zu entschlüsseln. Wenn kein Passwort für das Backup festgelegt ist, wird das Tool das System automatisch mit einem temporären Passwort ausstatten, um Schlüsselbunde entschlüsseln zu können (das Passwort wird nach dem Zugriff zurückgesetzt).

Physischer Zugriff: iOS 9.3.3-Support mit neuem Pangu Jailbreak

Apple-Nutzer sind schnell, wenn es darum geht, neueste Technologien zu übernehmen. Laut Apple verwenden rund 86 % der Nutzer iOS 9 auf kompatiblen Geräten. In den letzten 4 Monaten gab es zu keiner Version von iOS neuer als iOS 9.1 ein Jailbreak. Das Pangu Team gab kürzlich ein öffentliches Jailbreak für iOS 9.2 bis 9.3.3 frei und ermöglichte so Ermittlern, Apple-Geräte mit den letzten Versionen von Apple iOS zu entschlüsseln und so physischen Zugriff auf sie zu erhalten. Eine Anleitung für die Installation des neuen Pangu Jailbreak ist unter http://en.pangu.io/help.html verfügbar.

Physischer Zugriff ist die umfassendste Erfassungsmethode, die für iOS-Geräte verfügbar ist. Es ist die einzige Methode, die vollen Zugriff auf alle verschlüsselten Informationen ermöglicht, die in Apples sicherem Speicher, dem Schlüsselbund (nur für 32-Bit-Geräte), gesammelt sind. Dazu gehören Passwörter von Webseiten und Anwendungen einschließlich des Passworts für das Apple-ID-Konto des Benutzers. E-Mail-Nachrichten und Anhänge, Log-Dateien und Historien sowie bestimmte Anwendungsdaten sind nur über physischen oder erweiterten logischen Zugriff verfügbar.

Preise und Verfügbarkeit

EIFT 2.1 ist ab sofort verfügbar und ab 1.495 EUR erhältlich. Sowohl die Windows- als auch die Mac OS X-Version ist bei einer Lizenz enthalten. Bestehende Kunden können je nach Ablauf ihrer Lizenz kostenlose oder ermäßigte Upgrades erhalten.

EIFT ist auch als ein Teil von Elcomsoft Mobile Forensic Bundle (2.995 EUR zuzüglich Mehrwertsteuer) erhältlich. Elcomsoft Mobile Forensic Bundle führt alle Elcomsoft Tools für die logische, physische und Cloud-Forensik zusammen.

Kompatibilität

Es stehen Windows und Mac OS X-Versionen von EIFT zur Verfügung. Die Unterstützung des physischen Zugriffs für die verschiedenen iOS-Geräte variiert je nach Sperrzustand, Jailbreak-Zustand und der Version von iOS, die installiert ist. Uneingeschränkter Zugriff ist für sehr alte Geräte (iPhone 4 und älter) gewährleistet. Der Zugriff auf iPhone 4s bis 5c und dem iPad mini kann nur dann erfolgen, wenn ein Jailbreak zur Verfügung steht. Physischer Zugriff auf 64-Bit-Geräte wird für das iPhone 5s bis 6s (und ihre Plus-Versionen), das iPad mini 2 bis 4 und die 64-Bit-Versionen von Full-Size-iPads unterstützt. Der 64-Bit-Erfassungsprozess kann den Schlüsselbund auslesen, aber nicht entschlüsseln.

Logischer Zugriff ist auf alle iOS-Geräte möglich, unabhängig vom Jailbreak-Status, wenn das Gerät mit Codesperre, Touch ID oder Pairing Record (Lockdown-Datei) freigeschaltet wird. EIFT produziert iTunes-ähnliche Backups und erfordert nicht, dass iTunes von Apple installiert wird, um den logischen Zugriff durchzuführen.

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/