ElcomSoft bringt frischen Wind in die iOS-Forensik, unterstützt Physische Akquisition für iOS 7-Geräte

Moskau, Russland – 30. Januar 2014 - ElcomSoft Co. Ltd. präsentiert die neueste Fassung des iOS Forensic Toolkit, jetzt mit Unterstützung Physischer Akquisition für iOS 7-Geräte mit Jailbreak. Physische Akquisition ist somit für Apple iOS 7-Geräte verfügbar, inklusive iPhone 4S, 5 und 5C, iPad 2. bis 4. Generation, iPad Mini, iPod Touch 5. Generation - entweder ohne Passcode-Schutz oder mit installiertem Jailbreak.

Da mehr als 83% aller iOS-Geräte derzeit unter iOS 7 laufen, eröffnet ElcomSoft der Mobilforensik-Industrie neue Perspektiven. Elcomsoft iOS Forensic Toolkit ist nach wie vor die einzige kommerziell verfügbare Forensik-Lösung, die eine Physische Akquisition von iPhone 4S, iPad 2 und neuerer Hardware durchführen kann.

Physische Akquisition erlaubt es, Informationen aus der Keychain auszulesen, Apples geschütztem Speicherbereich. In vielen Fällen enthält die erweiterte iOS 7-Keychain die ursprünglichen Passwörter von Apple ID-Konten. Hierdurch ist es Ermittlern möglich, auf in der iCloud gespeicherte Daten ebenso wie mittels des Mein iPhone suchen-Dienstes der Apple iCloud in Echtzeit auf die Geolocation-Koordinaten des jeweiligen Anwenders zuzugreifen.

Derzeit ist die Physische Akquisition der neusten iOS 7-Geräte nur möglich, wenn eine der folgenden Aussagen zutrifft:

- Es ist kein Passcode-Schutz eingerichtet
- Der Ermittler kennt den Passcode
- Der Anwender hat einen Jailbreak durchgeführt

"*Apple-Anwender sind schnell, wenn es um Upgrades geht*", weiß Vladimir Katalov, CEO bei ElcomSoft. "*Die neuste iOS-Fassung, iOS 7, ist bereits auf etwa 83% der kompatiblen Geräte installiert. Wir sind stolz, die ersten Anbieter einer Anwendung zu sein, die unseren Kunden Zugriff auf wertvolle Daten gestattet, die in diesen Geräten gespeichert sind*."

Hintergrund

Im Moment sind acht iPhone-Modelle, sieben iPad-Modelle sowie fünf iPod Touch-Generationen erhältlich. Mit mehr als 700 Millionen iOS-Geräten, von denen 83% iOS 7 einsetzen, ermöglicht das Update des iOS Forensic Toolkit Datenzugriff auf 580 Millionen Geräte.

iOS 7 Physische Akquisition

Physische Akquisition ist für Kunden im forensischen und strafrechtlichen Bereich seit geraumer Zeit die Methode der Wahl, um auf Daten in iOS-Geräten zuzugreifen. Physische Akquisition gestattet es Ermittlern, ein vollständiges, bitgenaues Abbild eines Gerätes in Echtzeit anzufertigen, inklusive geheimer Gerätedaten und nicht zugewiesener Datenblöcke, die gelöschte Daten und zerstörte Beweise enthalten können. Physische Akquisition ruft erheblich mehr Informationen von den Geräten ab als jede andere Methode, also z.B. logische Akquisition oder Backup-Analyse, inklusive der Daten in Apples geschütztem Speicher, der Keychain.

Zudem arbeitet Physische Akquisition auf der Basis einen festen Zeitrahmens, der garantiert, dass der gesamte Geräteinhalt zeitgerecht vorliegt. Der für die Akquisition erforderliche Zeitraum ist modellabhängig und wird zudem von der Menge der auf dem Gerät gespeicherten Daten beeinflusst. Die Akquisitionszeit eines iPhone 5 mit 32 GB Speicher liegt z.B. bei 25 Minuten, während für ein iPhone 4 mit 32 GB durch seinen langsameren Controller etwa 40 Minuten nötig sind.

Durch die Veröffentlichung des iPhone 4S mit verbesserter Sicherheit wurde die Physische Akquisition unmöglich - es sei denn, man war ElcomSoft-Kunde. Das Elcomsoft iOS Forensic Toolkit war das erste und bleibt das einzige kommerziell verfügbare Produkt, das eine Physische Akquisition der neusten Apple-Hardware mit den aktuellen Versionen von iOS - bis hinauf zu und inklusive Version 7 - durchführen kann.

Auf iOS 7-Geräten mit Jailbreak kann iOS Forensic Toolkit den Original-Passcode per Brute Force- oder Dictionary-Angriff knacken. Die Geschwindigkeit der Passcode-Suche auf einem iPhone 5 oder 5C mit Jailbreak beträgt etwa 15,5 Passcodes/Sekunde, wodurch iOS Forensic Toolkit normale vierstellige Passcodes in etwa 10 Minuten findet.

Vorzüge der Physischen Akquisition

Physische Akquisition bietet gegenüber anderen Methoden zahlreiche Vorzüge. Fester Zeitrahmen und garantierte Datenlieferung sind nur zwei davon. Die folgenden Informationen lassen sich ausschließlich über die physische Methode auslesen:

1. Im Cache befindliche (heruntergeladene) Mails, unabhängig von der Art des Email-Kontos. Gecachete Mails sind in Off- oder Online-Backups nicht enthalten.
2. Geolocation-Daten. iTunes und iCloud-Backups enthalten nur sehr rudimentäre Geolocation-Daten. Physische Akquisition extrahiert umfassende Informationen, inklusive häufiger Orte sowie Geolocation-Daten, die von allen Apple- und Drittanbieter-Apps sowie Systemdiensten angefordert wurden. Geolocation-Daten werden bei vielen Gelegenheiten angefordert und gespeichert, z.B. bei der Nutzung von Karten, der Kalibrierung des Kompasses, für das Werbetracking, auf der Suche nach Mobil- und WiFi-Netzwerken etc. Daraus ergibt sich, dass die umfassende Extraktion von Geolocation-Daten per Physischer Akquisition eine präzise Rekonstruktion der Aufenthaltsorte des Telefonbenutzers in jeder einzelnen Minute ermöglicht.
3. Systemlogs und Absturzlogs, die zeigen, welche Apps liefen oder installiert waren.
4. Cache-Daten von Anwendungen, wie z.B. Webseiten und Adressen, sowie viele weitere Arten von Daten sind nur über die Physische Akquisition verfügbar. Zieht man in Betracht, dass viele iOS-Anwendungen das Internet nutzen, können die im Cache befindlichen Daten, die durch Physische Akquisition verfügbar sind, äußerst umfangreich sein.

Erweiterte Keychain-Akquisition

Mit iOS 7 kamen einige Änderungen an Format und Inhalten von Apples geschütztem Speicher, der Keychain. Bei iOS 7-Geräten kann es vorkommen, dass ein unter einer bestimmten Apple-ID registriertes Gerät in seinem Cache

eine Kopie der iCloud-Keychain für sein Apple-Konto enthält - abhängig davon, ob der Benutzer dies gestattet hat. Wenn ja, eröffnen diese Daten Forensik-Experten völlig neue Perspektiven, da sie hierdurch Zugang zu auf anderen Geräten unter derselben Apple-ID gespeicherten Passwörtern sowie Kreditkarteninformationen haben.

iCloud-Zugriff als Bonus

iOS 7 speichert mehr Daten in der Keychain als alle seine Vorgänger. Dies kann dazu führen, dass Ermittler, die Physische Akquisition anwenden, unter gewissen Umständen - und unter anderem - die Login-Daten der Apple-iCloud erhalten. Wenn dies so ist, können die Forensiker Daten aus der Apple iCloud herunterladen und z.B. Online-Backups aller in dem jeweiligen Konto registrierten Geräte erhalten. Ein separat erhältliches Produkt, Elcomsoft Phone Password Breaker, führt Downloads aus der iCloud durch. Zudem ist es möglich, mittels des Mein iPhone suchen-Dienstes der Apple iCloud in Echtzeit auf die Geolocation-Koordinaten der in diesem Konto registrierten Geräte zuzugreifen.

Kompatibilität

Elcomsoft iOS Forensic Toolkit ist für Windows und Mac OS X verfügbar. Die Durchführung einer Physischen Akquisition ist je nach Gerät von Sperrzustand, Jailbreak-Zustand und der installierten Version von iOS abhängig.

Die Anwendung kann Physische Akquisitionen folgender iOS-Geräte unabhängig von Sperrung, Jailbreak und iOS-Version durchführen:

- Legacy iPhone-Modelle bis einschließlich iPhone 4, alle GSM- & CDMA-Modelle
- Das Original-iPad
- iPod Touch Generationen 1 bis einschließlich 3

Physische Akquisitionen können auf den folgenden Modellen durchgeführt werden, wenn sie unter iOS 5 laufen, allen Versionen von iOS 6 oder iOS 7 mit Jailbreak, oder wenn der Ermittler einen Jailbreak installieren kann:

- iPhone 4S, 5 und 5C
- iPad 2, 3 und 4
- iPad Mini
- iPod Touch 4. und 5. Generation

Die Unterstützung für iPhone 5S, iPad Air und iPad Mini mit Retina-Display wird derzeit entwickelt.
Von iOS 7-Geräten ohne Jailbreak und mit unbekanntem Passcode ist derzeit keine Physische Akquisition möglich.

Über Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit macht den forensischen Zugriff auf verschlüsselte Daten möglich, die in populären Apple-Geräten mit iOS 3 bis 7 gespeichert sind. Durch die Physische Akquisition eines Gerätes bietet die Anwendung sofortigen Zugriff auf alle geschützten Informationen, z.B. SMS- und Email-Nachrichten, Anruflisten, Kontakte und Organizer-Daten, Browserverlauf, Voicemail- und Email-Konten und -Einstellungen, gespeicherte Logins und Passwörter, Geolocation-Daten, das Original-Passwort von iTunes im Klartext, Unterhaltungen auf verschiedenen sozialen Netzwerken wie Facebook, sowie alle anwendungsspezifischen Daten im Gerät. Die Anwendung kann ebenfalls eine logische Datensammlung auf iOS-Geräten durchführen, oder für forensischen Zugriff auf verschlüsselte iOS-Dateisystem-Dumps sorgen.

Über ElcomSoft Co. Ltd.

ElcomSoft Co. Ltd. wurde in 1990 gegründet und ist heute industrieweit anerkannter Experte der Computer- und Mobilfunk-Forensik. Zum Angebot gehören Software, Training und Beratungsdienstleistungen für Strafverfolgung, Forensik, Finanz- und Geheimdienste. ElcomSoft Co. Ltd. hat zahlreiche Kryptographie-Techniken entwickelt und patentieren lassen und übertrifft regelmäßig die Erwartungen durch das Aufstellen stets neuer Industrie-Leistungsrekorde. ElcomSoft ist Microsoft Gold Independent Software Vendor, Intel Software Premier Elite Partner, Mitglied des Russischen Verbands für Kryptologie (RCA) und des Instituts für Computersicherheit.