ElcomSoft aktualisiert iOS Forensic Toolkit mit Unterstützung von iOS 5 und schnellerer Aufnahmezeit

Moskau, Russland – der 1. November 2011 – ElcomSoft Co. Ltd. aktualisiert iOS Forensic Toolkit und fügt iOS 5 zur Liste von unterstützten Systemen hinzu. Mit Unterstützung von iOS 5 kann Elcomsoft iOS Forensic Toolkit die Code-Sperre wiederherstellen und/oder eine Analyse der physikalischen Übernahme von Apple-Geräten mit iOS 3.x, 4.x und 5 durchführen. Darüber hinaus wurde die Geschwindigkeit der physischen Aufnahme 2 bis 2,5-mal verbessert. Mit mehr als doppelte Geschwindigkeit der Übernahme der früheren Versionen kann das aktualisierte Elcomsoft iOS Forensic Toolkit ein 16-Gb iPhone 4 in etwa 20 Minuten erwerben, oder eine 32-GB-Version in 40 Minuten.

Mit dem nahezu sofortigen forensischen Zugang zu verschlüsselten Informationen, die in den neuesten iPhone- und iPad-Geräten gespeichert sind, ermöglicht Elcomsoft iOS Forensic Toolkit einen Zugriff auf geschützte Dateisystem-Dumps, die aus unterstützte Apple-Geräte extrahiert sind, auch wenn die ursprüngliche Code-Sperre unbekannt ist.

Forensische Analyse der iOS 5-Geräte

Mit der Veröffentlichung von iOS 5 hat Apple einige kleinere Verbesserungen und einige wichtige Änderungen an Daten-Verschlüsselung gemacht. *"Es gab keinen Durchbruch im iOS Security-Modell"*, sagt Andrey Belenko, ElcomSofts führender Entwickler. *"Die Änderungen an der Architektur sind eher eine Weiterentwicklung des bestehenden Modells. Allerdings begrüßen wir diese Veränderungen, weil sie eine bessere Sicherheit für den Endanwender aufweisen. Insbesondere ist die Zahl der Keychain-Elemente, die ohne Passkey entschlüsselt werden können, jetzt weniger als es früher war. Code-Sperre ist eine der Markenzeichen des Sicherheitsmodells von Apple, und sie erweitern die Nutzung davon, um mehr Daten als je zuvor zu umfassen. "*

Während die meisten Verschlüsselungsalgorithmen nur ein wenig optimiert sind, hat Apple eine signifikante Änderung an Sicherheitseinstellungen über den Schutz von Kezchain gemacht und den Verschlüsselungs-algorithmus von Keychain komplett ersetzt. Darüber hinaus hat Apple Escrow Keybag nutzlos für forensische Spezialisten gemacht, weil Escrow Keybag auch mit der Code-Sperre geschützt ist. Offenbar verlässt sich der Schutz sensibler Informationen von iOS 5-Geräten stärker auf Code-Sperre als in früheren Versionen.

"Ich liebe Herausforderungen", sagt Dmitry Sklyarov, ElcomSofts führender Kryptoanalyse-Spezialist. *"Die neue Systemversion präsentiert einen perfekten Fall. Als wir gerade erst begannen, wussten wir gar nicht, ob wir eine Chance haben, es zu knacken. Es gibt komplett neue Verschlüsselungs-Algorithmen, veränderter Schlüsselbund-Schutz, neue Datenstrukturen... die Liste geht weiter und weiter. Wir hatten das meiste davon in Zeiten von iOS 4 gemacht, aber das neue System präsentierte einige unerwartete Herausforderungen. "*

Keychains enthalten erhebliche Mengen von Informationen, die sehr wertvoll für forensische Ermittler sind. Zu diesen Informationen gehören gespeicherte Logins und Passwörter für Websites, Wi-Fi-Zugangs-Passwörter, E-Mail- und Anwendungs-Passwörter und vieles mehr. Im Lichte der neuen Verschlüsselung, die zur Schutz von Keychain verwendet wird, ist Elcomsoft iOS Forensic Toolkit das erste kommerziell erhältliches Produkt, das eine komplette Unterstützung zur Wiederherstellung von Keychain-Informationen der iOS 5-Geräte anbietet.

Die Wiederherstellung der meisten Objekte von Keychain erfordert die Kenntnis der ursprünglichen Code-Sperre. Elcomsoft iOS Forensic Toolkit kann die ursprünglichen Code-Sperre wiederherstellen, indem es einen Brute-Force-Angriff durchführt. Mit dem Klartext-Passwort kann Elcomsoft iOS Forensic Toolkit alle Artikel entschlüsseln, die in Keychain gespeichert sind.

www.elcomsoft.com
© 2011 ElcomSoft Co. Ltd.

Hintergrund

Forensische Experten sind sich sehr wohl von der Menge der wertvollen Informationen bewusst, die in Apple iOS-Geräten, wie z.B. iPhone, gespeichert sind. iPhone-Benutzer sammeln große Mengen von hochsensiblen Informationen in ihren Smartphones. Neben den offensichtlichen Angaben wie Bilder, E-Mail- und SMS-Nachrichten speichern iPhone-Geräte erweiterte Nutzungsinformationen wie Geolocation-Daten, angesehene Google-Karten und Routen, Web-Browsing-Verlauf und Anruflisten, Login-Informationen (Benutzernamen und Passwörter), und fast alles was im iPhone eingegeben wurde.

Einige, aber nicht alle diese Informationen werden in iPhone-Backups gespeichert, wenn sie mit Apple iTunes produziert sind. Aber die Menge der Informationen, die von Telefon-Backups extrahiert werden kann, ist natürlich begrenzt.

Die Methode der physischen Akquisition verwendet den gedumpten Inhalt des physischen Geräts, um eine umfassende Analyse der Benutzer- und Systemdaten, die im Gerät gespeichert sind, durchzuführen. Physische Übernahme der Daten gewährleistet einen vollen Zugriff auf alle in diesen Geräten gespeicherten Daten und bietet forensischen Spezialisten einige wichtige Vorteile, die in iPhone-Backups nicht verfügbar sind. Vor Elcomsoft iOS Forensic Toolkit wardiue Entschlüsselung der verschlüsselten Dump-Daten einfach unmöglich, mit oder ohne Code-Sperre. Die neueste Version von Elcomsoft iOS Forensic Toolkit macht eine solche Übernahme möglich in etwa 20 Minuten für ein 16-Gb iPhone bis 40 Minuten für eine 32-GB-Version.

Über Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit ermöglicht einen forensischen Zugriff auf verschlüsselte Daten, die in populären Apple-Geräten mit iOS 3.x, 4.x, und iOS 5 gespeichert sind. Durch die Durchführung einer Analyse der physischen Aufnahme der Daten bietet das Toolkit einen sofortigen Zugriff auf alle geschützten Informationen, einschließlich SMS und E-Mail-Nachrichten, Anruflisten, Kontakte und Organizer-Daten, Web-Browsing-Verlauf, Voicemail und E-Mail-Konten und Einstellungen, gespeicherter Logins und Passwörter, Geolocation-Daten und der ursprünglichen Code-Sperre im Klartext. Das Tool kann auch eine logische Aufnahme der Daten von iOS-Geräten durchführen oder einen forensischen Zugriff auf verschlüsselte iOS Dateisystem-Dumps versorgen.

Verfügbarkeit und Verteilung

Elcomsoft iOS Forensic Toolkit steht sofort zur Verfügung. Das neue Toolkit ist nur Strafverfolgungsbehörden, forensischen Organisationen und Regierungsbehörden gewährt. Lizenzpreise sind auf Anfrage erhältlich; entsprechende Ermäßigungen erhalten alle bestehenden Kunden.

Über ElcomSoft Co. Ltd.

ElcomSoft Co.Ltd. hat sich zum Ziel gesetzt, Unternehmen und Privatanwendern zuverlässige Applikationen zur Validierung und Rettung von Passwörtern an die Hand zu geben. Seit der Unternehmensgründung 1990 hat sich ElcomSoft einen weltweiten Kundenstamm geschaffen. So wird die Software in den meisten der Fortune 500 Unternehmen, in vielen militärischen Einrichtungen sowie von Regierungen und führenden Wirtschaftsprüfern und Steuerberatern eingesetzt. ElcomSoft ist Mitglied der Russian Cryptology Association (RCA), des Computer Security Institute, der Association of Shareware Professionals (ASP) und ist Microsoft Gold Certified Partner (Independent Software Vendor Partner, ISV) und Intel Premier Elite Partner. Mehr auf http://www.elcomsoft.de/

Elcomsoft iOS Forensic Toolkit unterstützt Windows (2000, XP, Vista, Windows 7, Server 2003 und Server 2008 Server) und MacOS X (10.6 'Snow Leopard' und 10.7 'Lion)', und ist Strafverfolgungsbehörden und Regierungsbehörden gewährt. Mehr auf *http://ios5.elcomsoft.com/*

www.elcomsoft.com
© 2011 ElcomSoft Co. Ltd.