ElcomSoft untersucht iPhone Hardware-Verschlüsselung, bietet erweiterten forensischen Zugang zu geschützten Benutzerdaten

Moskau, Russland – 24. Mai 2011 – ElcomSoft Co. Ltd. ermöglicht einen erweiterten und sofortigen forensischen Zugang zu geschützten Informationen, die in iPhone-Geräten gespeichert werden, und aktualisiert Elcomsoft Phone Password Breaker mit Tools, die auf geschützte Dateisystem-Dumps zugreifen können, die aus iPhone-Geräte extrahiert werden, sogar wenn die Daten durch iOS 4 Hardware-verschlüsselt sind.

iPhone Backups haben viele Informationen über die Nutzung von iPhone-Geräten, aber sie haben nicht alles. Im Hinblick auf den forensischen Aspekt besteht die einzige angemessene Möglichkeit einer Untersuchung darin, den Inhalt des Speicherlaufwerks zu „dumpen“. Ein entschlüsselter Speicherauszug kann mit zertifizierten, fortgeschrittenen Tools wie Guidance EnCase analysiert werden.

Es handelt sich nicht um iPhone Backups

„Dieses Mal geht es nicht um iPhone Backups“, so Vladimir Katalov, Elcomsoft CEO. „Backups, die mit iTunes Software erstellt wurden, enthalten schon viele Daten, aber nicht alles, was in iPhoine-Geräten gespeichert oder gecached wird. Im Gegensatz hatten wir eine Möglichkeit ins Herz von iPhone-Daten-Verschlüsselung einbrechen, indem wir einen kompletten Zugang zu allen Informationen, die in iPhone-Geräten mit iOS 4 gespeichert werden, leisten.“

“Mobile forensische Experten haben ein gutes Kenntnis von der Menge der wertvollen Informationen, die in diesen Geräten gespeichert werden. Vor unserer Entdeckung gab es keine Möglichkeit, um einen kompletten Zugriff auf alle Daten zu bekommen“, setzt er fort. „Wir sind verantwortliche Bürger und wir möchten es nicht, dass diese Technologie in die falschen Händen gerät. So sind wir zu einer festen Entscheidung gekommen, den Zugang zu dieser Fuktionalität zu beschränken und den nur Strafverfolgungsbehörden, forensischen Organisationen, Geheimdiensten und gewissen Regierungsbehörden zu gewähren“.

Hintergrund

Die Benutzer von Apple iPhone-Geräten sammeln eine große Menge von hochsensiblen Informationen, die in ihren Smartphones abgelegt werden. Vergangenheit-Geolocation-Daten, gesehene Google-Karten und Routen, Web-Browsing-Verlauf und Anrufsprotokolle, Bilder, Emails und SMS Nachrichten, einschließlich entfernter Daten, Benutzernamen, Familienamen, Passwörter und fast alles, was auf iPhone eingetippt wird, wird vom Gerät gecached.

Einige von diesen Informationen sind in iPhone-Backups verfügbar, die durch Apple iTunes erstellt werden. Indessen sind die Informationen, die aus Backups extrahiert werden können, natürlicherweise begräntzt.

Die Menge und sensible Natur der Informationen, die in iPhone-Geräten abgelegt werden, forderte einen adäquaten Schutz. Apple führte eine Funktion, so genannte Data Protection, mit der Veröffentlichung von iOS 4 ein. Die neue Systemversion realisierte Hardware-Verschlüßelung in allen Geräten von iPhone 3GS und bestimmte folgende Modelle, einschließlich iPhone 4, iPhone 3GS, der beiden Modellen von iPad und letzten Versionen von iPod Touch. Die Funktion ermöglichte eine effective Chiffrierung von allen Nutzerdaten auf dem Gerät. Wegen der Benutzung von industriestandarden AES-256 Verschlüsselung betrachtete man, dass der Inhalt von iPhone-Geräten einen adäquaten Schutz vor sogar am besten gerüsteten Eindringlingen, einschließlich kriminaltechnische Analytiker und Strafverfolgungsbehörden.

Jedes iPhone-Gerät benutzt eine Kombination von Hardware-abhängigen Verschlüsselungsschlüsseln, sowie Schlüssel zum Entfernen der Daten, die im geschützten Speicher von iPhone verborgen werden. Falls der Schlüssel zum Entfernen der Daten verloren oder gelöscht ist, werden alle iPhone Daten unverfügbar und tatsächlich nutzlos. Aber wenn diese Schlüssel aus dem Gerät extrahiert werden, ist es möglich, eine forensische Untersuchung vom iPhone-Gerät durchzuführen.ElcomSoft veröffentlicht einige technische Informationen in seinem Blog: http://blog.elcomsoft.com/

ElcomSoft Forscher entwickelten ein Toolkit, um alle relevante Verschlüsselung-Schlüssel in iPhone-Geräten mit iOS 4 zu extrahieren und iPhone-Dateisystem-Dumps mit diesen Schlüsseln zu dechiffrieren. Das kann seinerseits einen erweiterten forensischen Zugang zu allen in iPhone-gespeicherten Informationen verschaffen, sogar wenn das Gerät Passcode-geschützt ist.

Diese erweiterte Funktionalität bietet einen Zugriff auf mehr Informationen als in iPhone-Backups. In der Tat glaubt ElcomSoft, dass seine neue Entdeckung einen Zugang zu zu vielen Informationen von der hochsensiblen Natur öffnet. Wegen der Natur der Daten, die zu Analytikern mit dem neuen Toolkit zugänglich werden, beschränkt ElcomSoft Software-Verwendung und den Zugang nur Strafverfolgungsbehörden, forensischen Organisationen, Geheimdiensten, sowie gewissen Regierungsbehörden gewährt.

Über Elcomsoft Phone Password Breaker

Elcomsoft Phone Password Breaker ermöglicht einen forensischen Zugriff auf verschlüsselte Informationen, die in populären Apple und BlackBerry-Geräten gespeichert werden, indem das Tool alle Arten von Daten, einschließlich SMS und Email-Nachrichten, Anrufsprotokolle, Adressbücher und Organizerdaten, Web-browsing Verlauf, Einstellungen von Voice-Mail und E-Mail-Account, dechiffriert.

Das Programm entschlüsselt passwortgeschützte iPhone und BlackBerry-Backups und bietet einen forensischen Zugang zu verschlüsselten iPhone-Dateisystem-Dumps.

Verfügbarkeit und Verteilung

Elcomsoft Phone Password Breaker steht sofort zur Verfügung. Der Zugriff auf die erweiterte Funktionalität der Entschlüsselung von iPhone-Speicher-Dumps ist nur Strafverfolgungsbehörden, forensischen Organisationen und gewissen Regierungsbehörden gewährt.

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). Mehr auf http://www.elcomsoft.de/