ELCOMSOFT
PROACTIVE SOFTWARE

ElcomSoft Analysierte 17 Sichere Passwort Managers für Smartphones, fand keine Sicherheit

Moskau, Russland – 16. März 2012 - ElcomSoft Co. Ltd analysierte 17 populäre Kennwortverwaltung-Applikationen für Apple iOS und BlackBerry-Plattformen, darunter kostenlose und kommerziell erhältliche Tools, und entdeckte, dass keine einzelne Kennwortverwaltung ein behauptetes Schutzniveau anbietet. Keine der Kennwortverwaltungen außer einer Applakation verwendet iOS oder BlackBerry bestehende Sicherheitsmodelle, indem sie sich ausschließlich auf ihre eigene Implementierung der Datenverschlüsselung verlassen. ElcomSofts Forschung zeigt, dass diese Implementierungen kein angemessenes Schutznevau gewährleisten, so dass ein Angreifer die verschlüsselten Informationen in weniger als einem Tag erholen kann, wenn das vom Benutzer wählbare Master-Kennwort 10 bis 14 Ziffern lang ist.

Schließlich, speichern 7 von 17 Produkten die Kennwörter der Benutzer unverschlüsselt order so schlecht verschlüsselt, dass sie sofort wiederhergestellt werden können. "*Es ist nicht genug, ein richtiger Verschlüsselungsalgorithmus zu benutzen*", sagt Andrey Balanko, ElcomSoft Chief Security Researcher. "*Es reicht nur ein schwaches Glied, um das gesamte Sicherheitsmodell zu ruinieren. Einige der Tools hätte eine bessere Chance, unsere Sicherheitstest zu bestehen, wenn sie etwa 10.000 bis 20.000-mal sicherer in Bezug auf ihre Passwort-Recovery-Geschwindigkeit waren. Einige andere Programme sind überhaupt hoffnungslos und sollte unter allen Umständen vermieden werden*."

"*Unsere Forschungen beweisen einmal mehr, dass die IT-Sicherheit mehr als nur Programmierkenntnisse erfordert*", kommentiert Dmitry Sklyarov, IT Security Analyst von ElcomSoft. "*Mit Open-Source-Krypto-Bibliotheken kann jeder Mensch eine Kennwortverwaltung schreiben und behaupten, dass sein Produkt einen sicheren Schutz anbietet – was nicht wirklich der Fall ist. Ein gutes Sicherheitsmodell soll das gesamte System berücksichtigen, einschließlich der Nutzer selbst - und nicht nur die Stärke des Verschlüsselungsalgorithmus allein*".

Hintergrund

Passwörter sollten lang und komplex sein. Das gleiche Passwort sollte nicht für verschiedene Dienste verwendet werden, egal wie komplex das Kennwort ist. Diese Anforderungen sind aktuell und werden oft in der Sicherheits-Politik des Unternehmens gefordert. Allerdings stellen diese Anforderungen eine Herausforderung, Dutzende von komplexen Passwörtern sich zu merken, was ein durchschnittlicher Mensch nicht sehr gut kann.

Passwortverwaltungen oder Passwort-Management-Applikationen sind Anwendungen, die Speicherung und Verwaltung der Passwörter auf mobilen Plattformen wie Apple iOS und BlackBerry erleichtern. Passwortverwaltungen dienen zur Bequemlichkeit und bieten eine zentrale Speicherung und einen schnellen Zugriff auf alle Benutzer-Passwörter und einzelne sensible Informationen wie Kreditkarten-Daten. Typischerweise wird der Zugriff auf Benutzer-Passwörter mit einem einzigen Master-Passwort geschützt.

www.elcomsoft.de
© 2012 ElcomSoft Co. Ltd.

Microsoft Partner
Gold Independent Software Vendor (ISV)

intel Software Partner

Idealerweise sollen Kennwortverwaltungen einen kryptographisch starken Schutz sensibler Informationen anbieten, der schwer zu durchbrechen ist. Sie sollen das Sicherheitsmodell jeder Plattform benutzen und ein Extraschutznevau obendrauf aufbauen, um die empfindlichsten Bits der Informationen zu schützen. Tatsächlich behaupten die meisten Passwortverwaltungen, vor allem diejenigen die von BlackBerry selbst vorgesehen sind, ein hohes Sicherheitsnevau dank der Verwendung von Industriestandard-Verschlüsselungsalgorithmen wie AES-256 oder Blowfish.

Da die Anwendungen mit sensiblen Daten anvertraut sind, stellen sich die Fragen darüber, wie sicher sie wirklich sind. Bei der Untersuchung von Kennwortverwaltungen wurde es festgestellt, ob sie die vorgesehenen Security-Mechanismen von mobile OS verwenden und ob sie ein zusätzliches Sicherheitsnevau dazu hinzufügen, durch die Durchführung einer eingehenden Analyse von 17 populären Kennwortverwaltungen.

Die Untersuchung

Beide Plattformen, die analysiert werden, BlackBerry und Apple iOS, haben umfassende eingebaute Datensicherheit-Mechanismen. Das genaue Sicherheitsnevau variiert je nachdem, welche Version von Apple iOS verwendet wird oder wie BlackBerry-Nutzer die Verschlüsselung der Speicherkarte behandelt. Aber im Allgemeinen ist das Niveau des Schutzes von dem jeweiligen Plattform ausreichend, wenn die Benutzer allgemeinene Vorsichtsmaßnahmen befolgen.

Das gleiche kann über die meisten von ElcomSoft analysierten Passwortverwaltungen leider nicht gesagt werden. Nur eine Passwortverwaltung-Applikation für iOS-Plattform, DataVault Password Manager, speichert Passwörter in der sicheren iOS-verschlüsselten Keychain. Dieses Schutznevau ist gut genug für sich, allerdings versorgt diese Applikation wenig Extraschutz über iOS standardmäßigen Ebenen. Ohne näher auf die komplexe Mathematik einzugehen (was in der ursprünglichen Whitepaper verfügbar ist), können die Daten von 10 aus 17 Kennwortverwaltungen an einem Tag gewonnen werden - garantiert, wenn das benutzerdefinierte Master-Passwort 10 bis 14 Ziffern lang ist, je nach Anwendung. Was ist mit den anderen sieben Passwortverwaltungen? Passwörter, die in ihnen gespeichert sind, können sofort wiederhergestellt werden, weil die Passwörter entweder unverschlüsselt gespeichert werden, oder mit einem festen Passwort verschlüsselt sind, oder Kryptographie überhaupt missbraucht wird.

Interessanterweise bieten BlackBerry Password Keeper und Wallet 1.0 und 1.2 sehr wenig Schutz über BlackBerry-Gerät-Passwort. Sobald das Gerät-Passwort bekannt ist, wird es relativ leicht, ein Master-Passwort/wörter für BlackBerry Wallet and Password Keeper zurückzugewinnen.

Empfehlungen

Mehrere Passwortverwaltungen auf dem Markt bieten keine ausreichende Sicherheit. ElcomSoft empfehlt den Benutzer sich auf die beworbenen Sicherheit nicht zu verlassen, sondern iOS oder BlackBerry eingebaute Sicherheits-Features zu benutzen.

Um die Daten sicher zu speichern, sollen Apple-Benutzer einen Passcode und ein wirklich komplexes Backup-Passwort einrichten. Das entsperrte Gerät soll an den unvertrauenswürdigen Computern nicht angeschlossen sein, um die Erstellung von Paarung zu vermeiden. Unverschlüsselte Sicherungskopien sollen nicht erstellt werden.

BlackBerry-Benutzer sollen ein Sicherheitspasswort (Device Passwort) einrichten und dafür sorgen, dass die Verschlüsselung der Speicherkarte ausgeschaltet ist oder dass die Optionen "Verschlüsseln mit dem Device Key" oder "Verschlüsseln mit dem Device Key und Device Passwort" gewählt sind, um den Angreifer an der Gewinnung des Kennworts durch den Inhalt der Media-Karte zu hindern. Unverschlüsselte Sicherungskopien des Geräts sollen nicht erstellt werden.

Die Whitepaper ist verfügbar unter http://www.elcomsoft.com/download/BH-EU-2012-WP.pdf

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, Microsoft Gold Independent Software Vendor Partner, ISV und Intel Premier Elite Partner. Mehr auf http://www.elcomsoft.de/

© 2012 ElcomSoft Co. Ltd.