Elcomsoft Distributed Password Recovery entschlüsselt Passwort-Manager 1Password, KeePass, LastPass und Dashlane

Moskau, Russland – 10. August 2017 - ElcomSoft aktualisiert Distributed Password Recovery und ermöglicht die Wiederherstellung von Master-Passwörtern, die verschlüsselte Bereiche der beliebtesten Passwort-Manager 1Password, KeePass, LastPass und Dashlane schützen. Durch den Angriff auf ein einziges Master-Kennwort haben Experten die Möglichkeit, auf die gesamte Datenbank der Software zuzugreifen, die neben allen gespeicherten Passwörtern und Authentifizierungsinformationen des Benutzers auch weitere hochsensible Daten enthalten kann wie beispielsweise Abbilder von Benutzerdokumenten, personenbezogene Informationen, aber auch Nummern von Kredit-, Giro- oder Kundenkarten.

Ein Passwort für alles

Die Idee hinter allen Passwort-Management-Applikationen ist einfach: sie bieten Benutzern die Möglichkeit, ihre Passwörter zur Authentifizierung in verschiedenen Quellen sicher zu speichern, zu organisieren und zu benutzen. Da sich Benutzer dadurch nicht mehr an ihre vielen verschiedenen Passwörter erinnern müssen, wird die Verwendung von immer gleichen Kennwörtern vermieden und die Nutzung starker, einzigartiger Passwörter gefördert. Passwort-Manager sind außerdem in der Lage, für Webseiten oder andere Quellen automatisch starke Passwörter zu generieren, sodass sowohl Wörterbuch- als auch Brute-Force-Attacken wirkungslos bleiben. Die Passwörter werden in verschlüsselten Datenbanken gespeichert und können nur durch die Eingabe des Master-Passworts entschlüsselt werden.

Im Jahr 2012 führte ElcomSoft eine Studie zu den damals beliebtesten Passwort-Managern durch[1] und zeigte, dass sich im Vergleich zur Passwortspeicherung in einer Klartextdatei nur wenige als signifikant sicherer herausstellten. Seit 2017 gibt es jedoch wesentlich sichere Software-Möglichkeiten wie beispielsweise 1Password, KeePass, LastPass und Dashlane.

Alle vier Passwort-Manager verwenden dabei zur Verschlüsselung ihrer Kennwort-datenbanken starke Verschlüsselungsalgorithmen und setzen außerdem mehrere tausend Hash-Funktionen für das Master-Passwort ein, um den Schlüssel für den geschützten Bereich abzubilden. Mit anderen Worten sind die Kennwortdatenbanken vor Brute-Force-Angriffen sehr gut geschützt.

---

[1] https://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf

ELCOMSOFT
PROACTIVE SOFTWARE

Verschlüsselte Datenbanken knacken

Die Sicherheit von Benutzer-Passwortdatenbanken ist äußerst wichtig. Diese können nur durch Brute-Force-Attacken auf das Master-Passwort im Klartext entschlüsselt werden. Die Wiederherstellung dieses Passworts würde allerdings die Enthüllung der gesamten Passwort-Datenbank bedeuten, wodurch der Zugriff auf hunderte Passwörter für unterschiedliche Quellen ermöglicht würde.

Passwort-Manager verwenden aus diesem Grund mehrere tausend Iterationen, um den binären Encryption Key aus dem textbasierten Master-Passwort abzuleiten. Infolgedessen ist die Geschwindigkeit von Brute-Force-Angriffen stark eingeschränkt. Dies ist genau der Grund für die Verwendung von GPU-Einheiten in heutigen AMD- und NVIDIA-Grafikkarten, die die Wiederherstellung im Vergleich zu einer einzigen CPU 50- bis 200-fach beschleunigen. Doch auch dann liegt die Geschwindigkeit von Brute-Force-Attacken im Bereich 100.000 Passwörtern pro Sekunde, was nur die Entschlüsselung von relativ kurzen Passwörtern erlaubt. Längere und komplexere Passwörter können jedoch weiterhin mit einem Wörterbuch-Angriff entschlüsselt werden, der auf benutzerdefinierte Angriffe in Elcomsoft Distributed Password Recovery zurückgreift.

*"Wir sind bestrebt, die Bandbreite von Passwortarten, die wir brechen können, immer weiter auszubauen", sagt **Vladimir Katalov**, CEO von ElcomSoft. "Dieses Mal haben wir den Fokus auf die vier beliebtesten Passwort-Manager gelegt, sodass Experten Zugang zu geschützten Bereichen erhalten, die neben Authentifizierungsdaten der Benutzer, auch gespeicherte Logins, Passwörter und Formulare zu zahlreichen Quellen enthalten. Bei den heutigen Passwort-Managern ist hierzu lediglich die Entschlüsselung eines einzigen Master-Passworts nötig."*

Elcomsoft Distributed Password Recovery 3.40 nutzt die Leistung von GPU-beschleunigten Angriffen, die über ein Netzwerk von bis zu 10.000 Computern verteilt sind, und entschlüsselt so Master-Passwörter von 1Password, KeePass, LastPass und Dashlane. Sobald der Schlüssel wiederhergestellt ist, können Experten auf die geschützten Datenbanken der Passwort-Manager zugreifen und Passwörter, Authentifizierungsinformationen sowie weitere in der Datenbank gespeicherten Daten einsehen.

Preise und Verfügbarkeit

Elcomsoft Distributed Password Recovery ist ab sofort verfügbar. Die Lizenzierung beginnt ab 599 EUR zzgl. Mehrwertsteuer für 5 Clients, für 100 Clients kostet sie 4999 EUR zzgl. Mehrwertsteuer. Weitere Stufen sind auf Anfrage erhältlich. Kunden sind gerne eingeladen,

ElcomSoft beim Kauf von größeren Lizenzmengen zu kontaktieren. Lokale Preise können variieren.

Eine zusätzliche Lizenzoption ist ab sofort auch für kleinere Netzwerke verfügbar. Die kostengünstige Variante deckt GPU-beschleunigte distributive Ermittlung auf bis zu 5 Computern ab. Auch diese minimale 5-PC-Lizenz unterstützt bis zu 8 GPU-Kerne und bietet eine maximale Rechenleistung von 40 GPU-Kerne pro Lizenz.

Elcomsoft Distributed Password Recovery unterstützt Windows 7, 8.x, 10, sowie die entsprechenden Windows Server-Versionen.

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/