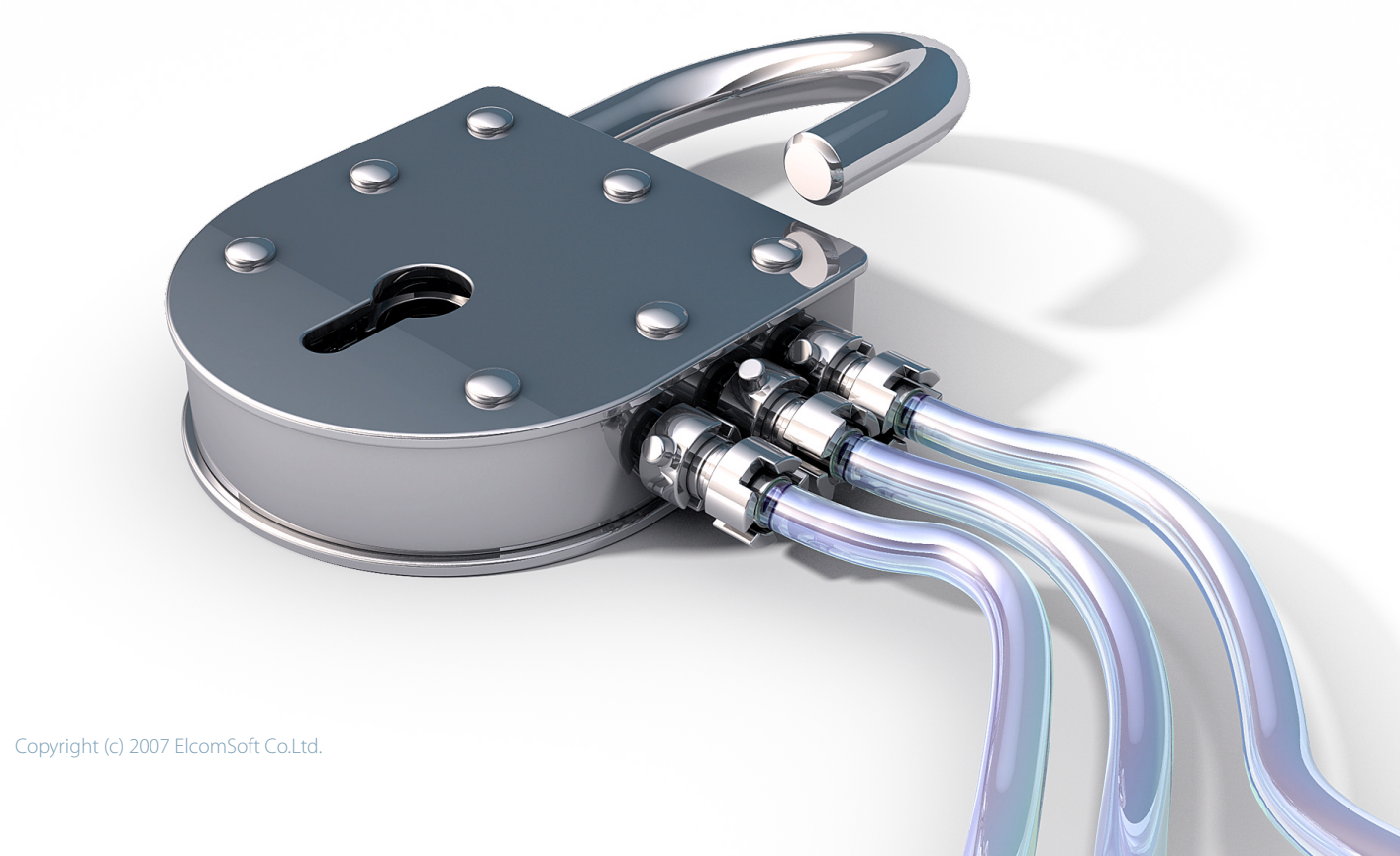
ELCOMSOFT
PROACTIVE SOFTWARE

SESAM, ÖFFNE DICH!

EINE EINFACHE METHODE ZUR WIEDERHERSTELLUNG VON KENNWÖRTERN FÜR DEN ZUGRIFF AUF DATEIEN, ANWENDUNGEN UND DATENBANKEN



ELCOMSOFT
PROACTIVE SOFTWARE

INHALT

INFORMATION – DER SCHLÜSSEL ZU RICHTIGEN ENTSCHEIDUNGEN

Heute hören wir ständig Wörter wie „Informationszeitalter", „Informationstechnologie", „wer über Informationen verfügt, beherrscht die Welt" usw. In unserem Bewusstsein sitzt der Gedanke fest, dass Information das einzig Wichtige ist.

Was bedeutet das und ist die Information an sich so wichtig? Das trifft nicht ganz den Kern. Wir brauchen Informationen, um Entscheidungen zu fällen. Das ist wahrhaftig wichtig. Eine richtige Entscheidung ist der Weg zum Erfolg in jedem Geschäft. Aus diesem Grund ist der Besitz von Information in der modernen Geschäftswelt ein Wettbewerbsvorteil.

Es ist nicht verwunderlich, dass dem Schutz von Informationen erhöhte Aufmerksamkeit zuteil wird. Auf dem aktuellen Soft- und Hardwaremarkt werden zahlreiche Lösungen angeboten, die den Zugriff zu Informationen einschränken und Datenlecks verhindern: Tools zur Kontrolle des Zugriffs und der Authentifizierung, Systeme zum Verhindern von Hacker-Attacken, Programme zum Erstellen von Reservekopien, Antiviren-Software und andere.

Das einfachste und für jeden Anwender zugänglichste Instrument bleibt nach wie vor der Passwortschutz, der den unbefugten Zugriff zu den Systemen, Dokumenten und Datenbanken verhindert. Jeder von uns verwendet am Arbeitsplatz ein Kennwort, um sich ins System einzuloggen, Datenbanken einzusehen usw. Es ist bekannt, dass die empfindlichste Stelle eines jeden Informationssystems der Mensch ist. Der Passwortschutz bildet dabei keine Ausnahme. Wie oft haben Sie selbst das eine oder andere Kennwort vergessen? Bei der Vielzahl von Kennwörtern, die heutzutage jeder Computeranwender im Kopf haben muss, ist das jedoch kein Wunder.

Wenn das Kennwort aus dem einen oder anderem Grund verloren wurde, gibt es keinen Zugang zu den Informationen.

SIE HABEN KEINEN ZUGRIFF…

Verkaufs- und Finanzdaten, Kundendatenbanken, die Rechenschaftslegung der Buchhaltung und Verwaltung, analytische Berichte und Prognosen – all diese Daten sind sowohl für eine erfolgreiche Unternehmensführung als auch für strategische Entscheidungen über die weitere Geschäftsentwicklung unentbehrlich.

In der Regel ist ohne ein Kennwort der Zugriff auf diese Informationen unmöglich. Der Passwortschutz dieser Daten zählt zur elementaren Sicherheits-Police eines jeden Unternehmens. Was jedoch tun, wenn der Zugriff zu diesen Daten nötig, das Kennwort aber unbekannt ist? Ständig entstehen solche Situationen.

Erstes Beispiel: Sie selbst haben das Kennwort vergessen. Geben Sie zu, dass dies bereits vorkam? Als verantwortungsbewusster Mensch haben Sie Ihr Kennwort nicht auf die letzte Seite Ihres Kalenders geschrieben, sondern sich entschieden, es im Gedächtnis zu speichern und einfache Assoziationen zu benutzen, beispielsweise, Ihr Lieblingsgericht + Ihr Geburtsdatum. Mit dem Geburtsdatum ist es ein Leichtes, aber das Gericht …? Seit dem letzten Urlaub auf Kreta schwirren nur griechische Salate in Ihrem Kopf umher und die Anmeldung im System schlägt immer wieder fehl.

Zweites Beispiel: der Salesmanager hat gekündigt, ohne das Kennwort für die Lieferberichte zu hinterlassen. Zum jetzigen Zeitpunkt ist keine Verbindung mit ihm möglich, da er sich gerade einen alten Traum erfüllt und sich auf einer 90tägigen Pilgerreise in Tibet befindet. Die Vertragspartner drohen, die Verträge zu kündigen, wenn Sie nicht schnellstens die Rechnungen zahlen. Unklar ist nur, welche Daten Sie zugrunde legen sollen. Kommt Ihnen diese Situation bekannt vor?

Nicht selten entstehen Situationen, wo Mitarbeiter entlassen werden, weil sie in Finanz-machenschaften verwickelt waren oder für Mitbewerber tätig wurden. In diesen Fällen ist es sinnlos zu erwarten, dass dieser Mitarbeiter das Kennwort zu seinen Dokumenten preisgibt. Der Zugang zu diesen Informationen ist jedoch nötig, und möglichst sofort.

Das Problem ist also offensichtlich: um Zugriff zu Informationen zu bekommen und aktuelle Geschäftsaufgaben zu lösen, muss das verlorene Kennwort wiederhergestellt werden. In den meisten Fällen ist das möglich.

WIE KANN MAN DIESE DENKAUFGABE LÖSEN?

GUTE UND DIVERSE KENNWÖRTER

Das Problem der verlorenen Kennwörter besteht, seit der Passwortschutz erfunden wurde. Längst beschäftigen sich die Softwarehersteller mit dieser Frage. Deshalb gibt es auf dem heutigen Markt eine Reihe von Softwarelösungen zur Wiederherstellung der Kennwörter.

Legen wir aber die Erzählung über die Methoden, die von diesen Programmen zur Lösung des Kennwortproblems verwendet werden, zunächst beiseite. Klären wir zu Beginn, welche Kennwörter es grundsätzlich gibt und welche zusätzliche Information bei der Suche des Kennwortes nützlich sein könnte.

In der Regeln können im Kennwort folgende Symbole verwendet werden: 26 lateinische Kleinbuchstaben (a…z), 26 lateinische Großbuchstaben (A…Z), 10 Zahlen (0…9), 33 Sonderzeichen (!@#$%^ u.ä.) – insgesamt 95 Symbole in verschiedener Kombination. In einigen Fällen werden die Sonderzeichen ausgeschlossen, wodurch sich die Zahl der möglichen Kennwortvarianten weiter reduziert. Wir sollten auch nicht vergessen, dass die Kennwörter unterschiedlich lang sein können, was dann kritisch wird, wenn das Kennwort nicht wiederhergestellt oder annulliert, sondern nur über die Brute-Force-Methode (einfaches Ausprobieren) herausgefunden werden kann.

Darüber hinaus kann die Kenntnis der menschlichen Psychologie ein großes Hilfsmittel bei der Suche des Kennwortes sein. Trotz zahlreicher Einschränkungen, die den Passwortschutz verstärken sollen (minimale Passwortlänge, regelmäßiges Wechseln des Kennwortes usw.), missachten viele Anwender die elementaren Sicherheitsregeln und beweisen damit ein weiteres Mal die Existenz des bereits erwähnten Phänomens des„schwachen Gliedes", welches in der gegebenen Situation der Mensch ist.

Die meisten Kennwörter bestehen aus Wörtern und Symbolen aus der Muttersprache oder einer anderen bekannten Sprache des Menschen. Häufig haben die Wörter einen Bezug zum persönlichen Leben des Anwenders: Geburtsdatum, Name des Hundes, Telefon- oder Kontonummer usw. Ein neues Kennwort ist oft nur eine geringfügige Modifikation des vorherigen Kennwortes. Eben auf diese Weise löst die überwiegende Mehrheit der Anwender für sich das Problem des regelmäßigen Wechselns des Kennwortes, wie es in der Sicherheits-Police des Unternehmens vorgesehen ist. Eine letzte, aber wichtige Bemerkung: häufig hinterlegen die Menschen einen Zettel mit dem Kennwort direkt auf ihrem Arbeitsplatz oder speichern es auf ihrem Computer in einer separaten Datei, obwohl eine derartige Medizin gegen das Vergessen das endgültige Ende der Idee des Passwortschutzes bedeutet.

Folglich erleichtern die Kenntnis der Anforderungen an das Kennwort (mögliche Zusammensetzung der Symbole und Länge) sowie das Vorhandensein einiger Angaben über den Anwender die Suche des unbekannten Kennworts erheblich. Die Technologien, die in der speziellen Software zur Wiederherstellung von Kennwörtern verwendet werden, berücksichtigen die Möglichkeit der Verwendung dieser Informationen.

AUCH DIR HELFEN WIR AUF DIE BEINE…

Bis heute werden von der Software die folgenden Hauptmethoden zur Suche von Kennwörtern verwendet: die Brute-Force-Methode (einfaches Durchprobieren), Brute-Force mit Maske (Durchprobieren mit Maske), Dictionary-Attacke (Wörterbuch-Angriff), Key-Search-Methode (Durchprobieren der Chiffrier-Schlüssel – hier kann es weniger Varianten als beim Durchprobieren der Kennwörter geben) und die so genannte Rainbow-Attacke. In einigen Fällen werden andere Methoden zur Wiederherstellung des Zugriffs zu den Dateien verwendet – beispielsweise die so genannte Plaintext-Attacke (auf Grundlage des bekannten Inhaltes). Betrachten wir einige dieser Methoden ausführlicher.

Brute-Force-Methode

Kern der Brute-Force-Methode, des direkten Ausprobierens, ist einfach: das Programm probiert alle möglichen Kombinationen der Symbole aus, bis das gesuchte Kennwort gefunden wird. Man kann die Suche etwas einschränken, indem man die Anzahl der Symbole im Kennwort eingibt, die Symboltypen (Buchstaben, Zahlen, Sonderzeichen) oder aber Symbole eingibt, mit denen die Suche begonnen werden soll.

Wie viel Zeit wird es wohl benötigen, um das verlorene Kennwort über die Methode der „rohen Gewalt" (brute force) wiederherzustellen? Dies hängt von der Länge des Kennwortes ab, von den verwendeten Symbolen, der Leistungsfähigkeit des Computers, aber auch vom Typ des Dokuments, für welches das Kennwort gesucht wird.

Natürlich kann es passieren, dass das richtige Kennwort schnell gefunden wird und nicht alle möglichen Kombinationen ausprobiert werden müssen. Aber davon sollte man besser nicht ausgehen. Beim Lösen der Aufgabe auf einem gewöhnlichen Computer kann die Rechnung Jahre dauern! Die Brute-Force-Methode ist die aufwendigste Methode, deshalb sollte man nur dann auf sie zurückgreifen, wenn es keine anderen Alternativen gibt.

Brute-Force mit Maske

Wenn Sie selbst das Kennwort erstellt haben, kann es immer die Chance geben, es mit einer Maske wiederherzustellen, indem die Suche stark eingegrenzt wird. Möglicherweise erinnern sie sich an die Länge des Kennwortes und an einige Symbole. Jede Information ist hilfreich.

Beispiel: Sie sind überzeugt davon, dass Sie nur Zahlen und lateinische Kleinbuchstaben verwendet haben. Demzufolge können Sonderzeichen und lateinische Großbuchstaben bei der Suche ausgeschlossen werden. Es wäre nicht schlecht, wenn Sie wissen, auf welcher Position das eine oder andere Symbol im Kennwort stand. Wenn Sie z.B. wissen, dass das Kennwort aus 10 Symbolen bestand, mit „a" begann und mit „2007" endete, kann man für die Suche die Maske „a?????2007" erstellen. Unbekannte Symbole sind in der Maske mit Fragezeichen gekennzeichnet.

Die Bedeutung der Verwendung der Maske ist offensichtlich: das Programm muss eine geringere Anzahl möglicher Kombinationen ausprobieren, somit verkürzt sich die Zeit, in der das Kennwort gefunden werden kann.

Leider sind nicht so oft Details des Kennwortes bekannt, und eine Maske kann entsprechend nur selten verwendet werden. Zum Glück gibt es eine weitere Methode zur Wiederherstellung des Kennwortes, die sehr gute Ergebnisse liefert.

Dictionary-Attacke

Angenommen, Sie haben Informationen über mögliche Wörter oder Namen, die im Kennwort verwendet wurden. In diesem Fall kann man die Dictionary-Methode anwenden.

Häufig verwenden die Anwender gewöhnliche Wörter für die Erstellung ihrer Kennwörter. In der Regel sind das Wörter aus der englischen Sprache: open, access, password usw., denn es ist viel leichter, sich ein solches Kennwort zu merken, als die sinnlose Kombination von Buchstaben und Zahlen. In Wirklichkeit vergisst man dieses Kennwort jedoch genauso, wie alle anderen, nur ist seine Wiederherstellung leichter.

Woher nimmt man ein derartiges Wörterbuch (oder genauer, eine solche Wortliste). Erstens, kann es Bestandteil des Lieferpaketes sein. Zweitens, kann man im Internet suchen – auf den FTP-Servern kann man die unterschiedlichsten Listen allgemein gebräuchlicher Wörter und ihrer Modifikationen finden, thematische Listen (Tiere, Fußballmannschaften u.a.), Abkürzungen usw. Drittens, kann man selbst ein kleines Wörterbuch erstellen.

Die Vorzüge dieser Methode sind offensichtlich. Die Liste der Wörter, welche die Anwender als Kennwörter eingeben, ist sehr eingeschränkt und übersteigt selten hundert Wörter. Für einen modernen Computer ist das Ausprobieren von hunderttausend Varianten eine leibhaftige Bagatelle. Aus diesem Grunde sollte man die Dictionary-Methode zuerst ausprobieren. Es kann durchaus sein, dass sie schnell zum Erfolg führt.

Rainbow-Attacke

Die Zeitdauer, die man für die Suche nach dem Kennwort benötigt, ist der wichtigste Parameter der Wiederherstellung. Wir wissen bereits, dass bei einem einfachen Ausprobieren alle möglichen Varianten des Kennworts durchgegangen werden, und bei komplizierten Kombinationen erfordert dies viel zu viel Zeit. Wenn man mit Monaten oder Jahren der Ermittlung rechnen muss, strebt die Zweckmäßigkeit dieses Unterfangens gen Null.

Zur Lösung eben dieses Problems wurde die so genannte Rainbow-Attacke (rainbow attack) erfunden, deren wichtigste Idee in der Verwendung von Vorausermittlungen bei der Kennwortsuche besteht. Der Gedanke des Austauschs ressourcenintensiver Ermittlungen gegen die gewöhnliche Suche nach einer zuvor erstellten Suchtabelle (lookup table) ist nicht neu. Suchtabellen werden in Fällen genutzt, wo es viel leichter ist, die Daten aus dem Speicher zu extrahieren, als zu erstellen.

Bei Durchführung der Rainbow-Attacke werden die Ergebnisse der Vorausermittlungen von möglichen Varianten des Kennworts für eine bestimmte Symbolauswahl verwendet. In einer Zeit, die mit dem Knacken eines Kennworts über die Brute-Force-Methode vergleichbar ist, erhält man Tabellen, nach denen man mit einer sehr hohen Wahrscheinlichkeit tausendmal schneller ein beliebiges Kennwort aus dem überprüften Bereich findet. Der Aufbau von Rainbow-Tabellen nicht aus einer Auswahl von Symbolen, sondern einer Auswahl von Wörterbüchern, erlaubt die Wiederherstellung von Kennwörtern praktisch unbegrenzter Länge.

Die Rainbow-Tabellen sind kleiner als gewöhnliche Suchtabellen: es geht schon nicht mehr um Terabytes, sondern um Gigabytes des Speichers. Die Reduzierung der Tabellengröße wird aufgrund ihrer Optimierung erreicht. Der Gerechtigkeit halber müssen wir zugeben, dass die Zeit zur Wiederherstellung des Kennworts dabei zunimmt, und die Chance etwas abnimmt, aber das Ergebnis lohnt sich dafür. Beispiel: bei Verwendung einer Tabelle für sieben alpha-numerische Symbole (für ihre Erstellung braucht man etwa eine Woche), erlaubt die Methode der Rainbow-Attacke die Wiederherstellung praktisch jedes aus sieben alpha-numerischen Symbolen bestehenden Kennworts innerhalb von 20-30 Sekunden. Bei Verwendung der Brute-Force-Methode benötigt man in diesem Fall mehr als einen Tag. Der Vorteil ist offensichtlich.

Da die Vorbereitung dieser Tabellen die Kosten des Programms wesentlich erhöht, wird die Methode der Rainbow-Attacke hauptsächlich in Unternehmenslösungen angewendet. Außerdem sollte man nicht vergessen, dass die Wahrscheinlichkeit der Wiederherstellung eines Kennworts mittels der Rainbow-Attacke geringer ist, als bei der Verwendung gewöhnlicher Methoden. Das ist der Preis für die Geschwindigkeit.

WIR WÄHLEN DAS BESTE

Die Frage über die Zweckmäßigkeit des Erwerbs eines Programms zur schnellen Wiederherstellung von Kennwörtern steht nicht. Ein solches Tool sollte jeder System-Administrator stets griffbereit haben. Die Anschaffungskosten werden beim ersten Vorfall eines Kennwortverlustes um ein Vielfaches wieder eingespielt.

Worauf sollten Sie bei der Auswahl einer Lösung der Klasse password recovery achten?

Erstens, wie hoch ist, laut Hersteller, die Wahrscheinlichkeit der Wiederherstellung des Kennworts? Dies ist das wichtigste Kriterium für die Bewertung der Effektivität der Lösung. Denn dafür kaufen Sie die Lösung. Die Chancen für einen Erfolg hängen vom Typ des Dokuments ab, für welches das Kennwort gesucht wird, sowie von der Leistungsfähigkeit des Computers. Außerdem werden die Anwender zunehmend vorsichtiger und wählen immer sicherere Kennwörter. Dennoch liegt die Wahrscheinlichkeit in der Regel bei 80%. Dies ist eine annehmbare Richtgröße. Für einige Kennwortvarianten und Dokumente garantieren die Hersteller sogar eine 99%ige Wahrscheinlichkeit.

Zweitens sollten Sie Ihre Aufmerksamkeit auf das Spektrum der unterstützten Betriebssysteme, Programmversionen, Dateiformate, Sprachen und Kodierungen richten. Es ist schwer vorauszusagen, mit welcher Microsoft Word oder Adobe Acrobat Version des Dokumentes Sie bei der Wiederherstellung des Kennworts konfrontiert werden, ganz zu schweigen von Kodierungen, wie beispielsweise hieroglyphische oder arabische Sprachen. Bringen Sie auch in Erfahrung, wie schnell die Unterstützung von neuen Programmversionen ergänzt wird. Denn wenn im Programm die Unterstützung, beispielsweise von Office 2007 fehlt, kann es wertlos sein – die Zeit drängt.

Drittens, fragen Sie nach der Geschwindigkeit der Wiederherstellung des Kennworts. Natürlich variiert die Zeitdauer des Herausfindens des Kennworts von der Leistungsfähigkeit Ihres Computers. In der Regel geben die Hersteller einige Durchschnittswerte bekannt. Sie sollten hierbei herausfinden, ob es sich bei der Zeitdauer um Minuten, Tage, Wochen oder Monate handelt.

Und - letztens – bietet das Programm die Möglichkeit der verteilten Wiederherstellung? Diese Lösungsmethode für arbeitsaufwendige Rechenaufgaben sieht die Bündelung der Rechenleistung verteilter lokaler und entfernter Rechner im Netzwerk vor. Diese Methode wird auch zum Knacken von Kennwörtern genutzt. Den Zugriff auf einige Dokumente und Anwendungen (z.B. das ICQ- oder Google Talk-Kennwort, das lokal gespeichert ist) kann man auf einem gewöhnlichen Computer in kürzester Zeit wiederherstellen. Für das Knacken anderer Kennwörter reichen die Ressourcen eines Computers nicht mehr aus – egal, um welche Frist es sich handelt. PGP-Kennwörter, beispielsweise, sind so unangreifbar, dass ihre Wiederherstellung nur über verteilte Rechenleistung möglich ist.

Dies sind die Hauptkriterien für die Auswahl einer Lösung zur Wiederherstellung verlorener Kennwörter.

ELCOMSOFT BEGINNT UND GEWINNT

Das russische Unternehmen Elcomsoft bietet seinen Kunden ein breites Spektrum von Lösungen zur Wiederherstellung von Kennwörtern für beliebige Systeme – begonnen bei Office-Anwendungen und Instant Messengern bis zu Systemkennwörtern von Windows und Archiven.

Dank der einzigartigen Technologien sowie einem Expertenteam mit jahrelanger Erfahrung im Bereich der Kryptologie entwickelt Elcomsoft hochwertige Programme der Klasse password recovery. Die Wahrscheinlichkeit, ein Kennwort in Abhängigkeit von seiner Länge, seinem Schwierigkeitsgrad und der für die Anwendung benutzten Verschlüsselungs-technologie wiederherzustellen, beträgt über 80%.

Die Produktpalette genügt den Bedürfnissen beliebiger Kunden – vom Heimanwender, der sein ICQ-Kennwort vergessen hat, bis zu großen Unternehmenskunden, für welche die Wiederherstellung der Systemkennwörter für Windows, der Zugang zu verschlüsselten Microsoft Office Dokumenten oder das Löschen der Einschränkung von Adobe Acrobat Dateien erforderlich ist. Separate Anwendungen in einem Paket gebündelt, erlauben die Auswahl mehrerer Produkte zu einem attraktiven Preis.

Um Kennwörter für eine große Anzahl von Dokumenten sowie lange und komplizierte Kennwörter in einer annehmbaren Zeitspanne zu finden, besteht die Möglichkeit der verteilten Wiederherstellung unter Einbeziehung sowohl lokaler als auch entfernter Ressourcen.

Betrachten wir die wichtigsten Produkte des Unternehmens Elcomsoft ausführlich, um eine Vorstellung über die Möglichkeiten dieser Anwendungen und den Schwierigkeitsgrad der zu lösenden Aufgaben zu erhalten.

MICROSOFT OFFICE DOKUMENTE

Advanced Office Password Recovery

Zur Wiederherstellung von Kennwörtern für Dateien / Dokumente, die in Microsoft Office-Anwendungen erstellt wurden, bietet das Unternehmen die Lösung Advanced Office Password Recovery (Abb.1).

Die Mehrheit der Kennwörter wird blitzschnell über direkte Dekodierung gefunden. Dabei spielt die Version von Microsoft Office keine Rolle - Advanced Office Password Recovery stellt Kennwörter für Dokumente wieder her, die mit einem beliebigen gängigen Betriebssystem erstellt wurden: Office 95, Office 97, Office 2000, Office XP, Office 2003 Beta, Office 2003, Office 2007. Darüber hinaus können Sie die Kennwörter für Microsoft Money, Microsoft Visio, Microsoft Backup und das Kennwort für Internet Explorer Content Advisor wiederherstellen.

Das Programm wird in drei Varianten geliefert: Home, Standard und Professional, die sich durch die Auswahl der zu unterstützenden Anwendungen voneinander unterscheiden. Die Version Professional, die für große Unternehmen bestimmt ist, kann über 30 Kennwort-Typen in 14 verschiedenen Anwendungen wiederherstellen.

Ausführliche Information über Advanced Office Password Recovery erhalten Sie auf der Webseite von Elcomsoft. Hier können Sie außerdem eine Testversion des Programms herunterladen.

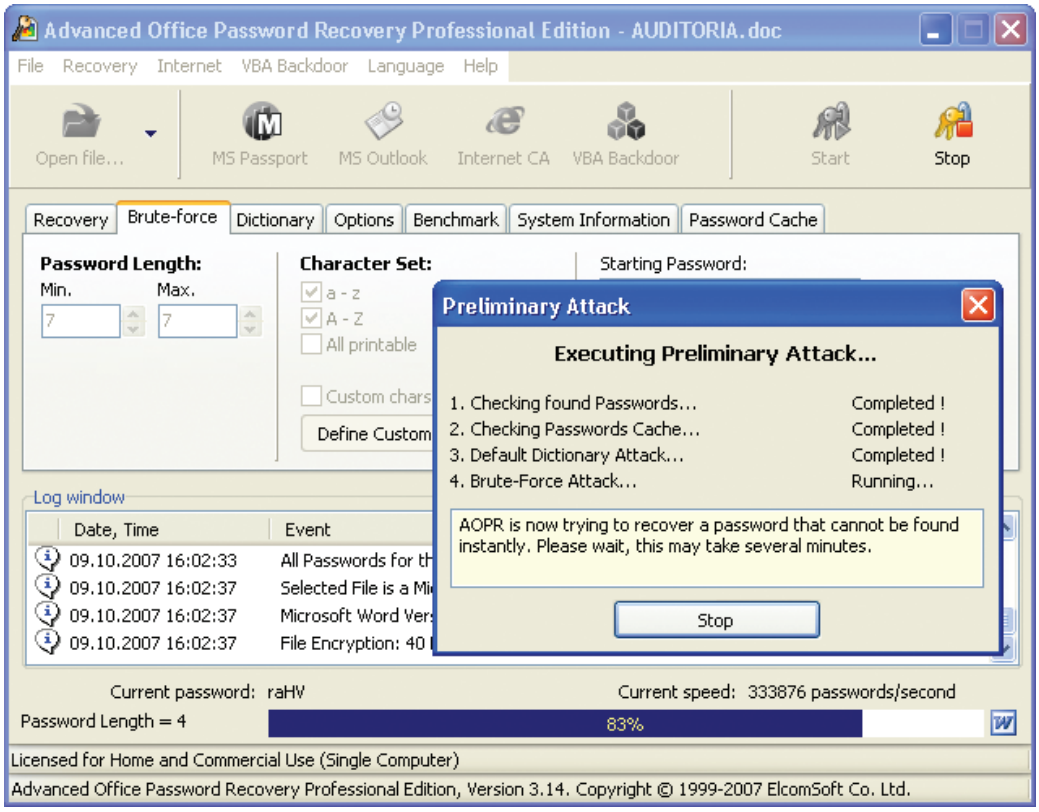


Abb.1 Vorausgehende Attacke zur Wiederherstellung des Kennworts zum Öffnen eines Microsoft Word 2003 Dokuments.

Advanced Office Password Breaker

Wenn es um die Wiederherstellung der Kennwörter von Word- und Excel-Dateien geht, sollten Sie auf das Programm Advanced Office Password Breaker aufmerksam werden. Mit diesem Programm können Sie Word und Excel 97/2000-Dateien entschlüsseln, bei denen der Schutz zum Öffnen der Dateien eingestellt ist.

Dank der Tatsache, dass in Microsoft Office 97/2003 40-bit Schlüssel zum Verschlüsseln verwendet werden, garantiert das Programm das Öffnen des Dokuments. Dabei spielen die Länge und der Schwierigkeitsgrad des Kennworts keine Rolle. Durchschnittlich dauert die Entschlüsselung etwa zwei Wochen.

Eine Testversion des Programms können Sie von der Webseite herunterladen.

Beachten Sie, dass man zur Entschlüsselung von Microsoft Office XP Dokumenten, die mit Crypto-Provider geschützt sind, das Programm Advanced Office Password Recovery verwenden muss, da für diese Dokumente nur ein Ausprobieren aller Verschlüsselungen möglich ist.

E-MAIL-CLIENTS UND INSTANT-MESSENGER

Advanced Mailbox Password Recovery

Weit verbreitet ist der Verlust der Anmelde- und Kennwortinformationen für E-Mail-Clients. Eine einfache und schnelle Lösung dieses Problems bietet das Produkt Advanced Mailbox Password Recovery von Elcomsoft. Das Programm hilft, die lokal gespeicherten Kennwörter für die E-Mail-Einträge wiederherzustellen.

Die Liste der unterstützten E-Mail-Clients ist beeindruckend: Microsoft Internet Mail And News, Eudora, The-Bat!, Netscape Navigator/Communicator Mail, Pegasus mail, Calypso mail, FoxMail, Phoenix Mail, IncrediMail, @nyMail, QuickMail Pro, MailThem, Opera mail, Kaufman Mail Warrior, Becky! Internet Mail. Das Programm enthält auch einen POP3- und IMAP-Server-Emulator, der es erlaubt, das POP3/IMAP-Kennwort von jedem E-Mail-Client zu bekommen.

Eine Testversion des Programms können Sie von der Webseite herunterladen.

Advanced Instant Messengers Password Recovery

Zu den häufigsten Vorfällen im Bereich der Authentisierung zählt der Verlust des Kennwortes zum Instant-Messenger ICQ. Da diese Kommunikationsmethode bei den meisten Menschen in erster Linie persönlichen Charakter trägt, wird mit der Einhaltung von Diskretion eher frei umgegangen. Bei Verlust des Kennworts muss die Person sich nur vor sich selbst verantworten. Dennoch ist der Verlust einer „schönen" ICQ-Nummer und der Verlust der History des Schriftverkehrs nicht gerade angenehm.

Eben für diese Fälle bietet das Unternehmen Elcomsoft das Produkt Advanced Instant Messengers Password Recovery an - ein Programm zur Wiederherstellung von (lokal gespeicherten) Anmelde- und Kennwortinformationen für über 30 Instant Messenger, wie ICQ, Miranda, QIP, Google Talk, Trillian, Mail.Ru Agent.

Alle Kennwörter werden sofort mittels direkter Codierung gefunden (dafür ist es erforderlich, dass das Kennwort lokal gespeichert ist). Das gesuchte Kennwort kann nicht nur aus lateinischen Symbolen bestehen – man kann auch Kennwörter in anderen Fremdsprachen wiederherstellen. Die Testversion des Programms hat einige Einschränkungen, Sie erhalten jedoch eine Vorstellung über die Möglichkeiten des Programms.

ADOBE ACROBAT UND INTUIT QUICKEN DOKUMENTE

Advanced Intuit Password Recovery

Die vom Unternehmen Intuit entwickelten Programme der Familie Quicken sind für die Bearbeitung und Speicherung von Informationen über Finanzoperationen bestimmt. Diese Anwendungen werden von Banken, Audit- und Buchhaltungsunternehmen verwendet und ermöglichen die Führung der Steuerstatistik und die Kontrolle der persönlichen Finanzen. Muss man noch erklären, wie ernst der Verlust eines Kennworts zu dieser Information ist?

Das Programm Advanced Intuit Password Recovery ist ein Programm zur Wiederherstellung verlorener oder vergessener Kennwörter zu Dateien von Intuit Quicken Versionen 4 bis 2008, Quicken Lawyer (Portfolios, *.PFL) und QuickBooks (*.QBW, *.QBA) Versionen von 3 bis 2007 (Abb.2).

Bei Dokumenten, die in 2003 oder späteren Versionen der Anwendung erstellt wurden, nutzt Intuit vervollkommnete Verschlüsselungsalgorithmen. Auch wenn alternative Produkte nur die Probier-Technologie verwenden, bietet Advanced Intuit Password Recovery die sofortige Entschlüsselung der Dokumente an.

Eine Testversion des Programms können Sie von der Webseite herunterladen.

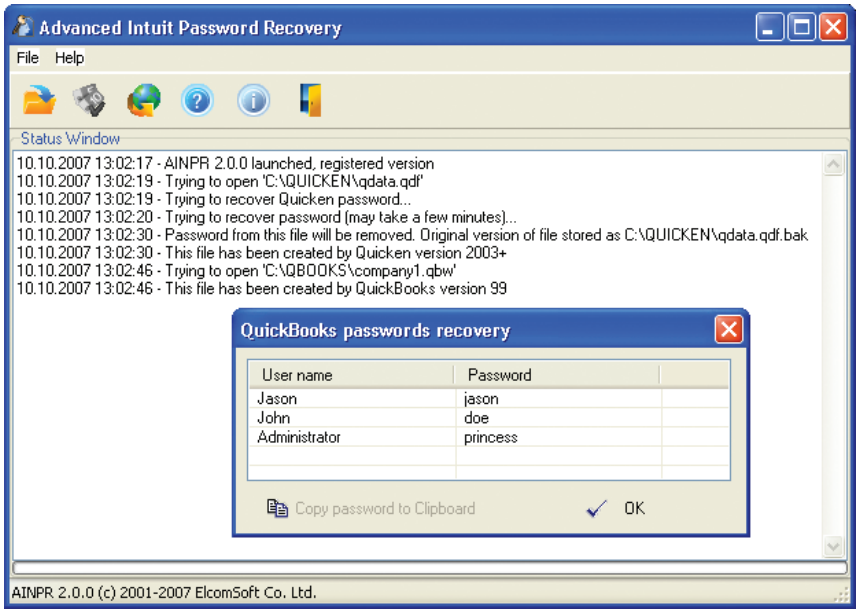


Abb.2 Ergebnis der Kennwortsuche von QuickBooks-Anwendern.

Advanced PDF Password Recovery

Das Dateiformat PDF ist so bekannt, dass sich kaum ein Mensch findet, der nicht mindestens einmal mit Adobe Acrobat Dateien gearbeitet hat. Demnach wissen Sie genau, mit welchem Problem die Anwender häufig konfrontiert werden: mit dem Schutz durch ein Owner-Kennwort, um diese Dateien zu bearbeiten, ändern oder zu drucken. Häufig wird zudem ein User-Kennwort gesetzt, um die Dateien zu öffnen.

Elcomsoft hat ein separates Programm zur Lösung dieses Problems entwickelt: Advanced PDF Password Recovery. Die Anwendung unterstützt alle Versionen und alle Verschlüsselungsalgorithmen von Adobe Acrobat von 3.x bis 8.x und erlaubt, PDF-Dateien zu öffnen und entfernt die Funktionsbeschränkungen der Datei, die im PDF-Format vorgesehen sind. Funktionsbeschränkungen werden sofort entfernt, unabhängig vom Komplexität des gesetzten Kennwortes. Für die Wiederherstellung des Kennworts können sowohl die Brute-Force-Methode, die Dictionary-Attacke als auch die Key Search Attacke verwendet werden.

Drei Editionen stehen Ihnen zur Verfügung: Standard, Professional, Enterprise. Die Basisedition des Programms (Standard) entfernt die Funktionsbeschränkungen der Datei zum Bearbeiten und Drucken. Die Professional-Edition erlaubt es zudem, die Nutzer- und Owner–Passwörter zu suchen. Die Enterprise-Edition basiert auf der Professional-Edition und verfügt über eine gehobene Key Search attack. Eine neue Rainbow-Table-Methode verringert die Zeit bis zur Wiederherstellung von Nutzer-Passwörtern mit 40-Bit-Verschlüsselung auf wenige Minuten. Die dafür benötigten, vorberechneten Tabellen werden auf einer DVD per Express-Mail angeliefert.

Die Möglichkeiten des Programms können Sie am Beispiel einer Testversion bewerten.

Archive

Elcomsoft bietet mehrere separate Lösungen zur Wiederherstellung von Kennwörtern in Archiven an: Advanced ZIP Password Recovery, Advanced ARJ Password Recovery, Advanced ACE Password Recovery und Advanced RAR Password Recovery. Sie können aber auch alle in einem integrierten Paket Advanced Archive Password Recovery erworben werden. Dadurch wird das Wiederherstellen von Kennwörtern in allen bekannten Archiven ermöglicht: ZIP (PKZIP, WinZIP), ARJ/WinARJ, RAR/WinRAR и ACE/WinACE.

Gegenwärtig ist diese Software die leistungsfähigste auf dem Markt für Software zur Wiederherstellung von Kennwörtern in Archiven. Zu den Vorzügen des Programms zählen die garantierte Wiederherstellung der Inhalte der meisten passwortgeschützten WinZIP Archive, unabhängig von der Komplexität des Passworts, das weltweit schnellste Ausprobieren von Kennwörtern in ZIP, ARJ und RAR-Archiven (ca. 15 Millionen Kennwörter pro Sekunde auf den modernen P-IV Prescott Prozessoren), die Entschlüsselung von WinZIP Archiven mit der resistenten AES-Verschlüsselung. Für ZIP und ARJ-Archive ist die so genannte known plaintext attack (Attacke auf bekannte Inhalte) vorgesehen. Ist der Inhalt wenigstens einer Datei des ZIP-Archivs bekannt, wird das Kennwort in wenigen Stunden gefunden, unabhängig von seiner Länge und Kompliziertheit.

Eine Testversion des Programms können Sie von der Webseite herunterladen.

ANDERE OFFICE-ANWENDUNGEN

Die Produktpalette von Elcomsoft beinhaltet Programme zur Wiederherstellung von Kennwörtern in anderen Office-Anwendungen.

Advanced Lotus Password Recovery ist ein Programm zur Wiederherstellung verloren gegangener oder vergessener Kennwörter für Dateien/Dokumente, die in IBM/Lotus-Anwendungen erstellt wurden: Organizer, WordPro, 1-2-3, Approach и Freelance Graphics. Es werden alle Programmversionen von IBM Lotus unterstützt. Darüber hinaus stellt das Programm den Zugriff auf FTP- und Proxy-Sites wieder her. Alle Kennwörter werden mittels direkter Decodierung sofort gefunden, unabhängig von der Sprache. Eine 30-tägige Testversion können Sie hier herunterladen.

Wenn Sie für Ihre Arbeit Corel WordPerfect Office verwenden, so sollten Sie über den Erwerb von Advanced WordPerfect Office Password Recovery nachdenken, einem Programm zur Wiederherstellung verlorener oder vergessener Kennwörter für Corel WordPerfect Office Dokumente der Formate *.wp, *.wpd, *.qpw, *.wb?, *.wq?, *.db. Alle Versionen von WordPerfect Office und seine Komponenten und Schutzmodi werden unterstützt; die Kennwörter werden sofort oder innerhalb weniger Minuten wiederhergestellt. Kennwörter in Fremdsprachen werden unterstützt. Eine 30-tägige Testversion können Sie hier herunterladen.

VERTEILTE WIEDERHERSTELLUNG

Über den Vorteil der verteilten Wiederherstellung komplizierter Kennwörter haben wir weiter oben bereits berichtet. Die Lösung Elcomsoft Distributed Password Recovery ist für die verteilte Wiederherstellung vergessener oder verloren gegangener Kennwörter verschiedener Dokumente konzipiert. Die Software bündelt die Rechenleistung verteilter Rechner im lokalen und globalen Netzwerk und kann so effizienter und schneller arbeiten.

Mit der Hilfe dieses Programms können Sie die Kennwörter für praktisch alle Microsoft Office Dokumente wiederherstellen sowie die Kennwörter für Microsoft Money, Microsoft OneNote, Adobe Acrobat, Intuit Quicken, Lotus Notes, User-Passwörter der Anwender von Windows 2000/XP/2003/Vista, Schlüssel vom Format PGP (*.skr), PGP Disk (*.pgd) u.a.

Das Programm besteht aus drei Komponenten: Server, Agent und Konsole. Der Server (Abb.3) wird auf einem der Computer im Netzwerk installiert und verwaltet den Prozess des Ausprobierens der Kennwörter. Auf beliebige Computer im Netzwerk kann ein Agent installiert werden, der eine bestimmte „Portion" Kennwörter ausprobiert, die vom Server bestimmt werden. Dann wird auf einem beliebigen Computer im Netzwerk die Konsole gestartet, die den Server verwaltet. Der Server erhält seine Aufgabe von der Konsole und verteilt sie an die Agenten. Die Konsole ist ihrerseits dafür konzipiert, den Server, mit dem sie verbunden ist, und die Agenten, die auf dem Server registriert sind, zu verwalten. Die Agenten werden auf dem Server registriert, wenn sie sich zum ersten Mal mit ihm verbinden. Für den Server und den Agenten können Sie Testversionen von der Webseite herunterladen.

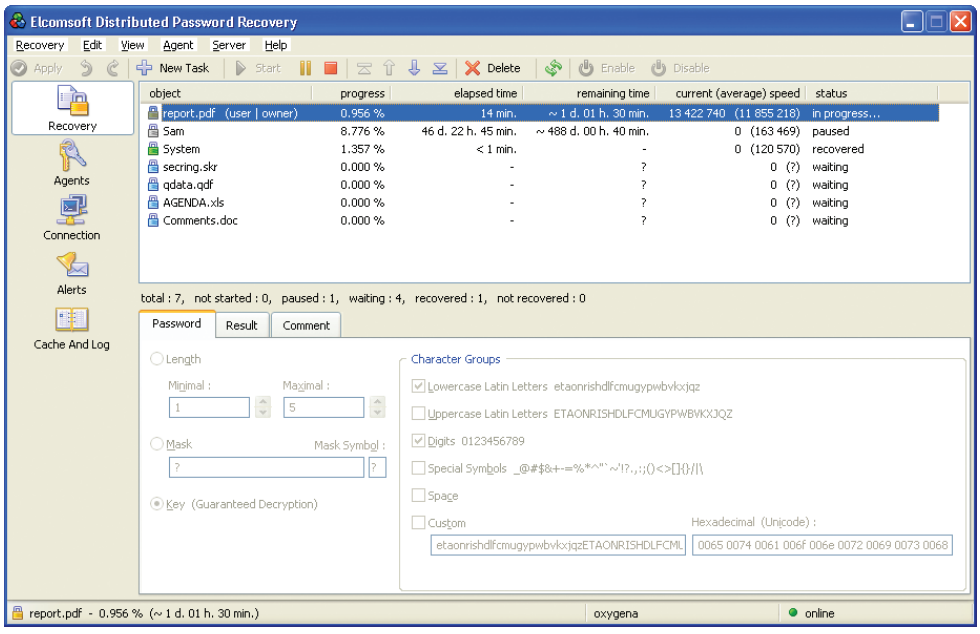


Abb.3 Hauptfenster der Elcomsoft Distributed Password Recovery (Komponente „Server").

ÜBER ELCOMSOFT

Der 1990 gegründete russische Software-Entwickler ElcomSoft Co. Ltd. zählt zu den führenden Experten im Bereich Software zur Sicherheitsprüfung und Wiederherstellung von Passwörtern und Kennungen, mit denen sie Windows-Netzwerke sichern bzw. auf wichtige Dokumente zugreifen können. Dank der einzigartigen Technologien genießen die Produkte des Unternehmens weltweite Anerkennung.

Zu den Kunden von ElcomSoft zählen weltbekannte Unternehmen aus folgenden Branchen:

High Tech: Microsoft, Adobe, IBM, Cisco
Regierungseinrichtungen: FBI, CIA, US Army, US Navy, Department of Defence
Consulting-Unternehmen: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finanzdienstleistungen: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telekommunikation: France Telecom, BT, AT&T
Versicherungen: Allianz, Mitsui Sumitomo
Handel: Wal-Mart, Best Buy, Woolworth
Medien & Unterhaltung: Sony Entertainment
Hersteller: Volkswagen, Siemens, Boeing
Energie: Lukoil, Statoil
Pharmazie: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

Das Unternehmen ist Microsoft Gold Certified Partner, Intel Software Partner, Mitglied der Russian Cryptologie Association (RCA), des Computer Security Institute (CSI) und der Association of Shareware Professionals (ASP).

Auf die technologischen Errungenschaften von Elcomsoft wird in vielen bekannten Büchern Bezug genommen, beispielsweise, in der Microsoft-Enzyklopädie „Microsoft Encyclopedia of Security", „The art of deception" (Kevin Mitnick), „IT Auditing: Using Controls to Protect Information Assets" (Chris Davis) und „Hacking exposed" (Stuart McClure).

Mehr über Elcomsoft können Sie auf der Webseite des Unternehmens erfahren.

ADRESSE:

ElcomSoft Co. Ltd.
Zvezdnyi blvd. 21, Office 541
129085 Moskau

FAX:

USA (toll-free): +1 (866) 448-2703
Großbritannien: +44 (870) 831-2983
Deutschland: +49 18054820050734

WEBSEITEN:

http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr