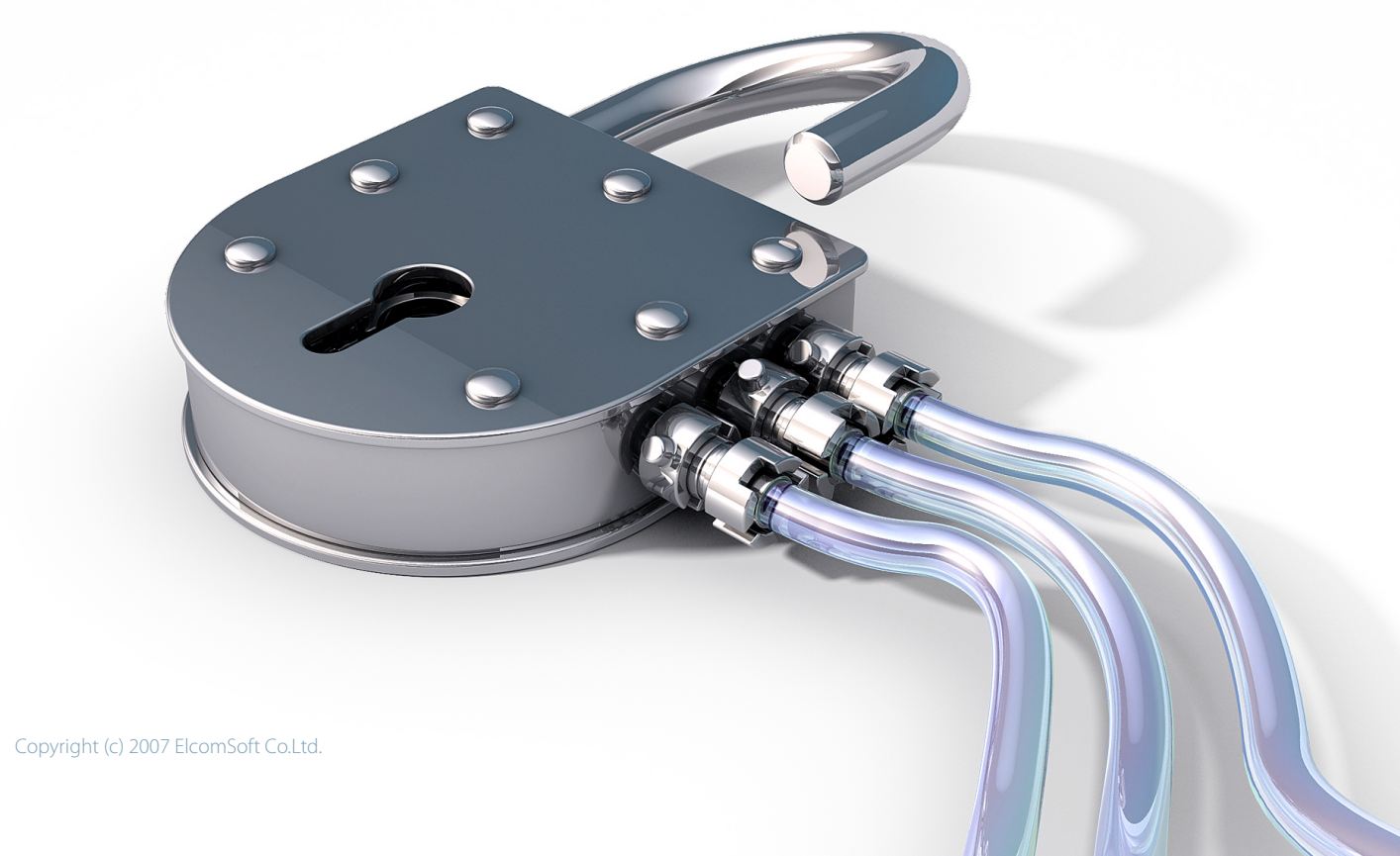
ELCOMSOFT
PROACTIVE SOFTWARE

VORTEILE UND NACHTEILE VON EFS UND EFFEKTIVE WIEDERHERSTELLUNG VERSCHLÜSSELTER DATEN

WHITEPAPER



ELCOMSOFT
PROACTIVE SOFTWARE

INHALTE

WAS IST EFS?

Eine der Innovationen unter Microsoft Windows 2000 und NTFS 5.0 – Dateisystem war die Encrypting File System (EFS) - Technologie, die dafür entwickelt wurde, Dateien auf der PC-Festplatte schnell zu verschlüsseln.

NTFS selbst hat einen eingebauten Schutz. Dennoch erforderte es schnell zusätzlichen Schutz. Der Grund war die weitverbreitete Nutzung von Tools des NTFSDos-Typs, was ermöglichte, das NTFS-Sicherheitssystem zu umgehen und Zugang durch DOS zu verschaffen; dabei wurden die Zugriffsrechte ignoriert.

Das EFS-System nutzt sowohl öffentliche, als auch private Schlüsselverschlüsselung und CryptoAPI - Bauweise. EFS kann einen beliebigen symmetrischen Datei-Verschlüsslungsalgorithmus aus der folgenden Liste nutzen: Microsoft Windows 2000 nutzte DESX, Windows XP nutzte 3DES und Windows XP SP1, 2003 und neue Windows Vista nutzen AES.

Dateiverschlüsselung erfordert nicht vom Nutzer, vorläufige Operationen durchzuführen. Während der ersten Verschüsselung der Datei werden automatisch ein Verschlüsselungszertifikat und Privatschlüssel für den Nutzer ausgestellt.

Eine der besonderen und bequemen Features von EFS ist, daß die Dateien verschlüsselt bleiben, wenn sie in einen anderen Ordner oder zum anderen NTFS-Laufwerk verschoben werden. Falls der Transfer zum anderen Dateisystem erfolgt, werden die Dateien automatisch entschlüsselt. Wenn der Nutzer neue Dateien zum verschlüsselten Ordner hinzufügt, werden sie automatisch verschlüsselt. Es besteht kein Bedarf, die Datei vor der Nutzung zu entschlüsseln, da EFS in das Betriebssystem eingebaut ist und diese Funktion automatisch ausführen wird; dabei werden alle Sicherheitsmaßnahmen befolgt.

Die Entwickler von EFS haben sich auch vor dem Risiko des Verlustes des Privatschlüssels durch den Nutzer abgesichert, zum Beispiel, im Falle einer Betriebssystem-Neuinstallation, oder wenn neue Nutzerkonten erstellt wurden. Hier kann der extra entwickelte EFS Recovery Agent benutzt werden, um Dateien zu entschlüsseln. Unter Windows 2000 ist Recovery Agent entweder vom Lokaladministrator (bei der Arbeit auf dem selbstständigen PC) oder Domain-Administrator (falls der PC innerhalb des Domains funktioniert) vorgestellt. Unter Windows XP und höher muss dies alles manuell gemacht werden.

In diesem Whitepaper beurteilen wir Vor- und Nachteile der EFS – Technologie und betrachten unterschiedliche Optionen, um die verschlüsselten Daten im Falle des Passwortverlustes oder Systemausfalls mithilfe von EFS wiederherzustellen.

EFS – VORTEILE UND NACHTEILE

Dank der EFS-Technologie können die vom ersten Nutzer erstellten Dateien nicht durch einen anderen Nutzer geöffnet werden, falls der letzte keine entsprechende Erlaubnis vorweist. Nachdem die Verschlüsselung aktiviert ist, bleibt die Datei an einem beliebigen Speicherplatz auf der Festplatte verschlüsselt, egal, wohin sie verschoben wurde. Verschlüsselung kann für beliebige Dateien, einschließlich ausführbarer Dateien, benutzt werden.

Der Nutzer mit dem Erlaubnis, die Datei zu entschlüsseln, kann mit diesen Dateien genauso, wie mit anderen, arbeiten - ohne Einschränkungen oder Schwierigkeiten. Alle anderen Nutzer werden sofort benachrichtigt, wenn sie die EFS-verschlüsselte Datei zu öffnen versuchen.

Diese Methode ist definitiv sehr bequem. Der Nutzer bekommt die Möglichkeit, den Zugang zu vertraulichen Informationen für Haushaltsmitglieder oder Kollegen, die den PC auch nutzen, sicher und schnell einzuschränken.

EFS sieht wie ein Allround-Tool aus, ist es aber nicht. Daten, die mit dieser Technologie verschlüsselt wurden, können während der Betriebssystem-Neuinstallation komplett verloren gehen.

Wir sollten uns daran erinnern, daß die Dateien auf dem Disk mit FEK (File Encryption Key) verschlüsselt sind, das in deren Eigenschaften gespeichert ist. FEK ist mit dem Hauptschlüssel verschlüsselt, der seinerseits mit den Schlüsseln dieser Nutzer verschlüsselt ist, die Zugang zu den Daten haben. Nutzerschlüssel selbst sind mit den Passwort-Hashes dieser gleichen Nutzer verschlüsselt, die Passwort-Hashes nutzen das SYSKEY-Sicherheitsfeature.

Diese Verschlüsselung sollte, laut EFS-Entwickler, zuverlässig die Daten schützen, doch in Wirklichkeit, wie unten erklärt, kann der Schutz auf die gute alte Login-Passwort-Kombination minimiert werden.

Dank dieser Verschlüsselungskette wird es unmöglich, Zugriff auf die EFS-verschlüsselten Daten auf der Festplatte zu bekommen, falls das Passwort verloren oder zurückgesetzt wurde, oder das Betriebssystem ausfällt oder neu installiert wird. Tatsächlich kann der Zugang für immer verloren gehen.

Normale Nutzer verstehen nicht ganz, wie EFS funktioniert, und zahlen oft dafür, wenn sie deren Daten verlieren. Microsoft veröffentlichte die EFS-Dokumentationen, die erklären, wie es funktioniert, und die Probleme, die bei der Verschlüsselung auftreten können. Dies alles ist allerdings für einen durchschnittlichen Nutzer schwer zu verstehen, und nur die wenigen lesen die Dokumentationen vor dem Arbeitsstart.

DATEN KÖNNEN FÜR IMMER VERLOREN GEHEN

Lasst uns verstehen, in welchen Situationen die EFS-verschlüsselten Daten verloren gehen können. Wie gefährlich kann die Situation sein? Wir analysieren es von Anfang an.

WIE KANN MAN DEN ZUGRIFF AUF EFS-VERSCHLÜSSELTE DATEN VERLIEREN?

Fast alle von uns haben schon mal die Situation erlebt, wenn es nötig ist, Windows neu zu installieren. Dies kann aufgrund des Systemausfalls, Virusangriffs oder Fehlers, der durch den Nutzer verursacht wurde, sein; oder das Passwort für das Nutzerkonto geht verloren oder das Nutzerprofil ist gelöscht. In diesem Fall sind alle verschlüsselten Daten in der alten Konfiguration wahrscheinlich verloren.

Wenn man die typischen Szenarien detailliert betrachtet:

1. **Das System bootet nicht, da ein Komponent ersetzt oder wegen eines Systemfehlers ausgefallen ist.** Zum Beispiel, ist die Hauptplatine ausser Betrieb gesetzt worden, der Boot-Abschnitt und Systemdateien sind beschädigt, die "unausgereiften" Updates oder unstabile Software wurden installiert. In diesem Fall kann die Festplatte zum anderen PC angeschlossen werden, und die Daten davon abgelesen; falls diese allerdings verschlüsselt sind, würde es nicht funktionieren.
2. **Der Systemadministrator in der Firma oder der Nutzer haben das Nutzerpasswort zurückgesetzt.** In diesem Fall ist der Zugang zu EFS-verschlüsselten Daten auch verloren.
3. **Der Nutzerprofil wurde gelöscht.** In diesem Fall sind die Dateien (und die Nutzerschlüssel) eventuell immer noch auf der Festplatte, doch das System sieht diese nicht, selbst wenn der Nutzer mit dem gleichen Namen wiederhergestellt ist, wird dem Konto ein anderes ID zugeordnet, das in dem Verschlüsselungsvorgang benutzt wird. In dieser Situation geht der Zugang zu den EFS-verschlüsselten Daten auch verloren
4. **Der Nutzer wechselte zum anderen Domain (durch den anderen Server authentifiziert).** Falls die Nutzer-Verschlüsselungsschlüssel zur Zeit des Wechsels auf dem Server gespeichert waren (normalerweise ist es der Fall), dann kann ein unprofessioneller Wechsel im Verlust des Zugriffs auf EFS-verschlüsselte Daten resultieren.
5. **System-Neuinstallation.** In diesem Fall geht der Zugang zu EFS-verschlüsselten Daten natürlich verloren. Falls eine Backup-Kopie des gesamten Systemdisks oder zumindest des Nutzerprofils („Dokumente und Einstellungen„) gemacht wurde, dann könnte der Zugang mithilfe der speziellen Software wiederhergestellt werden, jedoch nur dann, wenn die Schlüssel nicht beschädigt sind.

Es ist normal für das System, dass dieses auf einer Festplatte gespeichert ist, während die verschlüsselten Dateien auf der anderen Festplatte gespeichert sind. Wenn der Administrator das Betriebssystem neu installiert, muss das Backup von nur einer Festplatte, mit allen Daten, gemacht werden, und das System ist neu installiert. In diesem Fall sind allerdings die Schlüssel und damit der Zugang zu verschlüsselten Daten verloren.

Es muss gesagt werden, dass es einen Weg gibt, solche Situation vorzubeugen, falls vor der EFS-Nutzung EFS Recovery Agent aufgesetzt wurde; jedoch ist es für einen Durchschnittsnutzer, wie unten aufgezeigt, zu kompliziert.

WAS IST EFS RECOVERY AGENT?

EFS Recovery Agent ist der Nutzer mit Berechtigung, Daten zu entschlüsseln, die von anderem Nutzer verschlüsselt wurden; falls der Zweite Verschlüsselungs-Schlüsselzertifikate verloren hat oder das Nutzerkonto gelöscht wurde, die verschlüsselten Daten allerdings notwendig sind.

In der Regel ist Recovery Agent der Administrator, dies kann allerdings auch ein anderer Nutzer sein. Es können auch mehrere Recovery Agents sein. Um die Recovery Agent – Berechtigungen für den Nutzer zu übergeben, müssen erst Recovery Agent-Zertifikate erstellt werden; dies passiert mit dem Befehl „Chiffre /R: Dateiname"; der Pfad ist der "Dateiname" und Name des erstellten Zertifikates ohne Erweiterung.

Danach wird der Nutzer gefragt, das Passwort einzugeben, um den Privatschlüssel zu schützen, und dieses zu bestätigen (das Passwort wird nicht in der Konsole am Zugang angezeigt). Dann werden zwei Dateien mit bestimmten Namen erstellt: *.cer und *.pfx. Diese enthalten entsprechend öffentliche und private Zertifikat-Schlüssel. Nun müssen die Zertifikate zur Nutzers Ablage hinzugefügt werden, die von Recovery Agent festgelegt wird (dieser Schritt kann übersprungen werden, dann kann Recovery Agent es später machen, wenn die Wiederherstellungs-Funktionen genutzt werden müssen), indem die Datei *.pfx importiert wird (doppelklicken Sie auf den Datei-Icon, um den Zertifikat-Import-Assistenten zu öffnen). Hier muss der Administrator „Lokale Sicherheitseinstellungen „ öffnen (Start - Ausführen - secpol.msc), „Richtlinien öffentlicher Schlüssel - EFS" auswählen und im Menü „Aktion" „Agent für Wiederherstellung von verschlüsselten Daten hinzufügen" auswählen. Der Assistent für "Agent für Wiederherstellung von verschlüsselten Daten hinzufügen" wird geöffnet, und auf der zweiten Seite müssen Sie auf „Ordner ansehen" klicken und die früher erstellte *.cer – Datei auswählen.

Um den Zugang zu den verschlüsselten Dateien nach System-Neuinstallation oder nach dem Verlust des Privatschlüssels wiederherzustellen, müssen die Recovery Agents-Privatschlüssel im sicheren Ort aufbewahrt werden, beziehungsweise (falls nicht übertragen) die privaten Schlüssel aller Nutzer, die EFS benutzten, indem Sie diese vom „Privat"-Aufbewahrungsort des „Zertifikat"-Rasters (certmgr.msc) exportieren. Unter Windows Vista gibt es schliesslich einen Weg, die Schlüssel auf einer Smartcard zu speichern, was viel mehr Sicherheit bietet.

Es ist klar, dass diese Sicherheitsmassnahme mit der EFS Recovery Agent – Nutzung gegen die Prinzipien der Einfachheit spricht und untriviale Kenntnisse verlangt. Es ist kein Wunder, dass nur wenige es nutzen.

Es sollte beachtet werden, dass wenn der Administrator das Nutzerpasswort für den Lokalnutzer zurückzusetzen versucht, der Nutzer alle privaten Zertifikate und damit den Zugang zu EFS-verschlüsselten Dateien verliert (eine entsprechende Warnung erscheint, wenn dieser Vorgang versucht wird). Dasselbe passiert, wenn der Lokaladministrator spezielle Hilfsmittel benutzt, um die Passwort-Änderung zu erzwingen (z.B., ohne das alte Passwort einzugeben).

Dementsprechend ist das Risiko, die wichtigsten Daten zu verlieren, die mit EFS-Technologie verschlüsselt wurden, beim Systemausfall oder aufgrund des Administrator-/Nutzerfehlers zu verlieren, hoch und sollte immer beachtet werden.

WAS IST IM FALLE DES SYSTEMAUSFALLS ZU MACHEN?

Die typischen Situationen, in denen die EFS-verschlüsselten Daten verloren gehen, sind, wenn die Verbindung zwischen dem Betriebssystem und den Schlüsseln, die physikalisch auf der Festplatte platziert sind (vgl. Situationen, die im „Wie kann man den Zugriff auf EFS-verschlüsselte Daten verlieren?" beschrieben sind) verloren geht. In diesem Fall geben Sie bitte nicht auf – dies ist die Lösung. Es besteht eine hohe Wahrscheinlichkeit, dass der Zugriff auf die Daten wiederhergestellt werden kann. Falls allerdings die Schlüssel vom Disk gelöscht wurden und keine Backup-Kopie des Nutzerprofils oder der Nutzer-Zertifikate gemacht wurde, dann sind die Daten tatsächlich nicht wiederherstellbar.

Die Praxis zeigt, daß selbst der Export/ Import des Profils oder Zertifikate nutzvoll sein kann: die Schlüssel erscheinen wieder im System, doch der Zugang zu verschlüsselten Daten ist nicht wiederhergestellt.

Falls Sie in so eine Situation gelangen und die EFS-verschlüsselten Daten trotz der Schlüsselspeicherung unzugänglich werden, ist es dann möglich, spezialisierte Software zu nutzen, die mit großer Wahrscheinlichkeit helfen wird, den Zugriff auf die Daten wiederherzustellen.

MÖGLICHE AKTIONEN

Hier beschreiben wir die unterschiedlichen möglichen Aktionen, die Sie in dieser Situation durchführen können. Sie haben einige Optionen:

1. Booten unter anderem Konto mit Administratoren-Rechten (falls vorhanden) und mit spezieller Entschlüsselungs-Software fortfahren.
2. Festplatte physikalisch abschalten und diese auf dem anderen Arbeitsplatz installieren; dabei Entschlüsselungs-Software nutzen.
3. Booten mit dem anderen Betriebssystem, das auf gleichem PC installiert ist, falls es installiert ist, oder dieses extra für diesen Zweck installieren.

Das Wichtigste ist, Sie werden den direkten Zugang zum Disk brauchen. Im ersten Fall ist es nur für Nutzer mit Administratorenrechten möglich. Deshalb können Sie die Kontoberechtigungen erweitern, wenn das Backup-/Arbeits-Nutzerkonto nicht ausreichend ist.

SCHEMA DER DATEN-ENTSCHLÜSSELUNG

Nachdem der Zugriff zum Disk erhalten wurde, kann der nächste Schritt ausgeführt werden – direkte Entschlüsselung und Wiederherstellung der Daten. Dies kann laut folgendem Plan geschehen:

1. Suchen Sie nach dem Schlüssel und versuchen Sie, diese auf der PC-Festplatte zu entschlüsseln.
2. Suchen Sie nach verschlüsselten Dateien auf der Festplatte und versuchen Sie, diese zu entschlüsseln.

Eines der effektivsten Tools, die dafür entwickelt wurden, um EFS-geschützte Daten zu entschlüsseln, ist Advanced EFS Data Recovery. Es kann dazu benutzt werden, die Daten auf dem Problem-PC zu entschlüsseln, selbst dann, wenn einige der Nutzerschlüssel-Aufnahmen beschädigt sind.

Die Möglichkeiten und Features von Advanced EFS Data Recovery werden unten detailliert vorgestellt.

ADVANCED EFS DATA RECOVERY

Advanced EFS Data Recovery (AEFSDR) ist ein spezialisiertes Softwareprogramm zur Entschlüsselung der Dateien, die mit EFS-Technologie unter Microsoft Windows 2000 und Windows XP, Windows 2003 Server und Windows Vista verschlüsselt wurden.

Dieses Softwaretool kann benutzt werden, um die Dateien in Rekordzeit zu entschlüsseln, selbst dann, wenn das System nicht lädt oder wenn einige der Verschlüsselungs-Schlüsselaufnahmen beschädigt sind.

Selbst wenn die Datenbank mit SYSKEY geschützt ist, macht es Advanced EFS Data Recovery immer noch möglich, die Dateien zu entschlüsseln. Unter Windows 2000 ist es möglich, alle Dateien zu entschlüsseln, selbst wenn die Administrator- und Nutzerpasswörter nicht bekannt sind.

Advanced EFS Data Recovery nutzt ein Zweischrittverfahren:

1. Der erste Schritt ist die Suche nach allen EFS - Schlüsseln (Privat und Master) und der Versuch, diese zu entschlüsseln. Der erste Schritt ist die Entschlüsselung mindestens eines Schlüssels, der für die Entschlüsselung weiterer Dateien notwendig ist. Unter Windows XP und höher ist es möglich, daß das Nutzerpasswort ins AEFSDR eingegeben werden muss, das zur Verschlüsselung der Dateien oder von Recovery Agent-Passwort benutzt wird. Erst versucht das Programm, es automatisch zu machen, zum Beispiel das Passwort aus dem Cache oder Systemdateien zu extrahieren, indem es einfache Kombinationen ausprobiert (wie Passwort=Nutzername); dann führt es einen Angriff aus, indem der Angriff, der auf mittelgroßem eingebautem Wörterbuch basiert, ausgeführt wird.

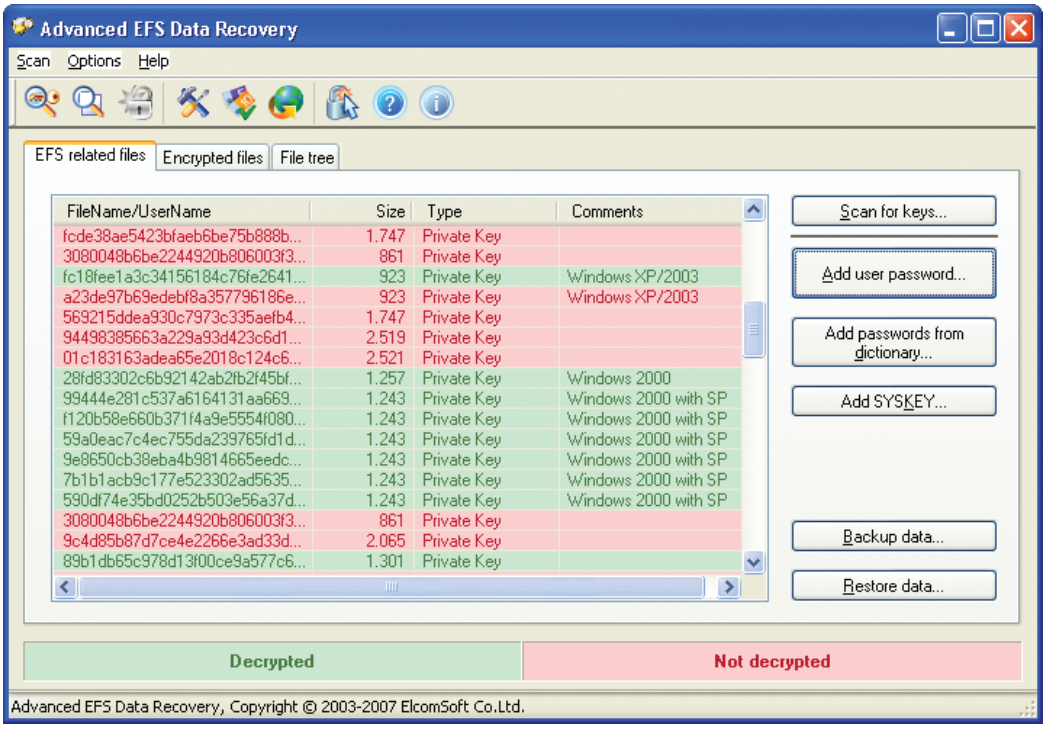


Bild. 1. Tab, der die PC-Suche und Entschlüsselung der privaten EFS-Schlüssel zeigt.

2. Im zweiten Teil führt das Programm die Suche aus, indem EFS-verschlüsselte Dateien auf der Festplatte benutzt werden, und probiert auch deren Entschlüsselung. Falls es nur wenige verschlüsselten Dateien sind und deren Position bekannt ist, kann der Nutzer manuell diese Dateien im Programm „Dateibaum" auswählen, um Zeit zu sparen.

Es könnte sich herausstellen, daß die Schlüssel auf einem Netzwerk-Server und die mit diesen Schlüsseln verschlüsselte Dateien lokal gespeichert sind. In diesem Fall nutzen Sie AEFSDR, um erst die Schlüssel, die auf dem Server gespeichert sind, abzurufen und zu entschlüsseln, und dann die Option „Backup-Daten", um die Ergebnisse in die Datei zu speichern und diese auf den Lokal-PC zu übermitteln. Somit können die Ergebnisse des ersten Arbeitsablaufs mit verschlüsselten Daten zum PC übermittelt werden, um das zweite Teil zu starten.

Der Datei-Entschlüsselungsprozess kann ziemlich lange dauern, somit ist einer der Schlüsselvorteile von Advanced EFS Data Recovery die Möglichkeit, die Systemauslastung zu verwalten. Der Nutzer kann zwischen drei Ladelevels auswählen: hoch, normal und niedrig.

Ein anderes Feature ist, daß Advanced EFS Data Recovery das neueste Microsoft Windows Vista – Betriebssystem, sowohl Windows Server 2008 unterstützt.

Schließlich ist es wichtig, über die Erfolgswirksamkeit des Produktes zu sprechen, zum Beispiel, die Wahrscheinlichkeit der erfolgreichen Datenentschlüsselung. Laut Einschätzungen von ElcomSoft-Experten kann Advanced EFS Data Recovery bis zu 99% der EFS-verschlüsselten Daten wiederherstellen, falls die Nutzerschlüssel abgerufen sind; dies ist eine sehr hohe Rate.

Die können die Testversion von Advanced EFS Data Recovery here downloaden.

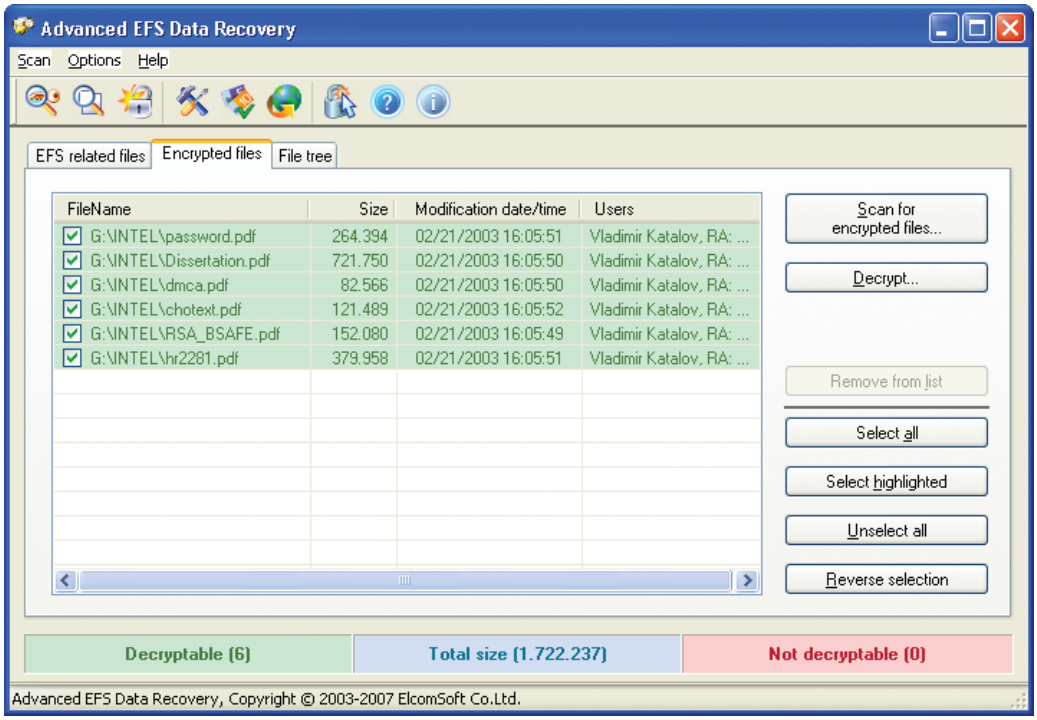


Bild. 2. Tab, der die Suchergebnisse und Dateientschlüsselung zeigt.

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