"OpenPuff" macht Dateien praktisch unauffindbar

23.02.2013, 08:30

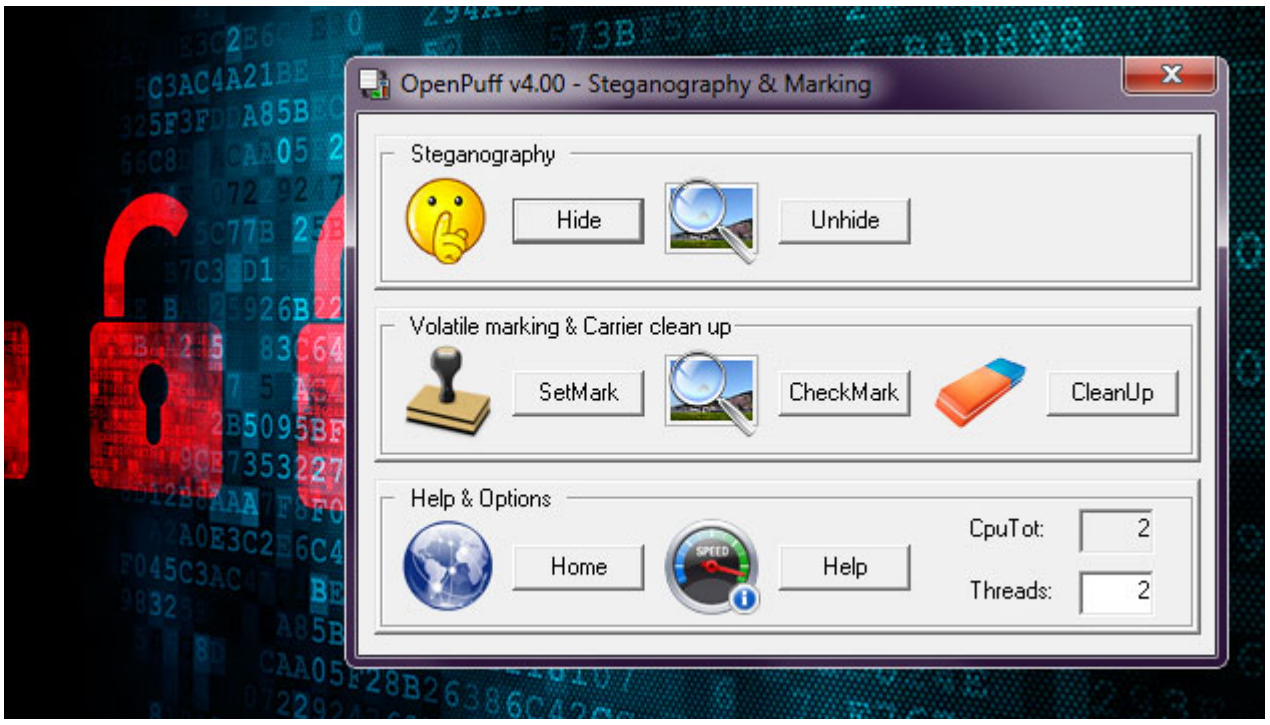

Foto: thinkstockphotos.de, embeddedsw.net

Wer ein Geheimnis bewahren möchte, der versteckt es - und zwar am besten so gut, dass es praktisch unauffindbar ist. Auf dem PC bewerkstelligt diese Aufgabe "OpenPuff": Wohl kein anderes kostenloses Tool verschlüsselt und versteckt sensible Informationen zuverlässiger als die Steganografie-Anwendung. Geheimer geht nicht.

Persönliche Informationen werden im besten Falle verschlüsselt auf dem Computer gespeichert. Doch kryptografische Verfahren haben einen entscheidenden Nachteil: Die derart vor fremdem Zugriff geschützten Dateien sind noch immer sichtbar und erwecken dadurch erst recht Aufmerksamkeit. Man denke nur an einen Passwort-Safe auf dem PC, der förmlich dazu einlädt, geknackt zu werden.

Dateien verstecken mittels Steganografie
Anders hingegen bei der sogenannten Steganografie, der "Kunst oder Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium", so Wikipedia. Das wohl beste Beispiel für ein derartiges Verfahren ist die berühmte "unsichtbare" Geheim- oder Zaubertinte aus Zitronensaft, die erst durch Erwärmen sichtbar wird. Auch nicht oder nur schwer erkennbare Wasserzeichen oder doppelte Böden, etwa in Paketen, sind der Steganographie zuzurechnen.

Anstatt nun jedoch sämtliche Online-Passwörter mit Zitronensaft auf einem Blatt Papier niederzuschreiben, sollten Nutzer mit einem Hang zu absoluter Geheimhaltung lieber zur kostenlosen Windows-Anwendung "OpenPuff" greifen. Doch was macht das kleine Tool? Ganz einfach: Es verschlüsselt eine zu schützende Datei und versteckt die digitalen Informationen in mehreren Trägerdateien, sogenannten Carriers.

Von außen nicht zu erkennen
Bei diesen Carriers handelt es sich um gewöhnliche Bild-, Audio- Video- oder Textdateien (eine Liste der von "OpenPuff" unterstützten Formate gibt es auf der Website), die – und das ist die Besonderheit – trotz der in ihnen zusätzlich gespeicherten Informationen unvermindert nutzbar sind. Fotos, Musik und Videos lassen sich also wie gehabt wiedergeben und betrachten bzw. anhören, ohne dass Außenstehende Verdacht schöpfen würden: Für sie handelt es sich um ganz gewöhnliche Dateien.

Geheimnisse verstecken - so geht's:
Um etwa ein Textdokument in anderen Dateien zu verstecken, sind bei "OpenPuff" vier Schritte nötig. Zunächst werden unter "(1)" bis zu drei voneinander unabhängige Passwörter vergeben. Nur wer sie alle kennt, kann die geheime Datei später auch wieder entschlüsseln. Auf Wunsch können auch nur ein oder zwei Passwörter vergeben werden. In diesem Fall müssen die entsprechenden Häkchen bei "Enable (B)" bzw. "Enable (C)" entfernt werden.

Unter "(2)" wird nun die zu versteckende Datei ausgewählt. Sie darf maximal 256 Megabyte groß sein. Zu beachten ist allerdings, dass die Anzahl der benötigten Trägerdateien mit zunehmender Größe der Original-Datei steigt. Wie viele Trägerdateien es letztlich braucht, um die gewünschte Datei zu versteckten, wird in Schritt drei ("3") ersichtlich.

Über den Befehl "Add" werden hier jene Dateien ausgewählt, in denen die einzelnen Informationsschnipsel gespeichert werden sollen. Entscheidend für die spätere vollständige Wiederherstellung der Original-Datei ist hierbei, dass sämtliche Trägerdateien in der richtigen Reihenfolge angeführt werden müssen, was die Entschlüsselung zusätzlich erschwert – allerdings auch für den Nutzer selbst.

Auf die falsche Fährte lenken
Wem das Ganze trotzdem noch nicht sicher genug ist, der kann nach dem Festlegen eines Komprimierungsgrades unter "(4)" auch einen zusätzlichen Köder in den Trägerdateien verstecken ("Add Decoy"). Auch er ist durch mehrere Passwörter verschlüsselt und soll Dritte im Falle einer mehr als unwahrscheinlichen Enttarnung glauben lassen, sie hätten bereits die richtige Datei entschlüsselt.

Mehrfach abgesichert
Über den Befehl "Hide Data!" wird die zu versteckende Datei schließlich auf die unter "(3)" ausgewählten Trägerdateien verteilt und zusammen mit diesen an einem definierten Ort abgespeichert, beispielsweise einem von außen harmlos wirkenden "Urlaubsbilder"-Ordner. Wer nun an die Geheimdatei gelangen möchte, muss diese zunächst nicht nur inmitten der Trägerdateien ausfindig machen, sondern anschließend auch sämtliche Passwörter und Trägerdateien sowie deren exakte Reihenfolge für die Entschlüsselung (Menübefehl "Unhide") kennen – praktisch ein Ding der Unmöglichkeit.

Vorsicht vor dem Vergessen
Nutzer laufen dadurch allerdings selbst Gefahr, ihre einmal verschlüsselten Dateien auf ewig zu verlieren. Schließlich muss gleich eine ganze Reihe von Faktoren zusammenspielen, damit die Wiederherstellung der Geheimdatei auch tatsächlich klappt. Für den täglichen Gebrauch ist "OpenPuff" daher nicht zu empfehlen, zumal sich insbesondere sehr große Dateien (beispielsweise Filme) nur sehr schwer auf andere Dateien aufteilen und in diesen verstecken lassen. In diesem Fall ist eine gewöhnliche Verschlüsselung mit einem möglichst starken Passwort sicher zielführender.

Gratis-Tool kann noch mehr
"OpenPuff" zu installieren lohnt sich aber auch für jene, die gerade nichts zu verstecken haben. Denn neben der verborgenen Speicherung mittels Steganografie ermöglicht die Freeware dem Nutzer außerdem, beliebige Daten mit unsichtbaren virtuellen Wasserzeichen zu versehen. So lässt sich die Urheberschaft von Fotos, Videos oder etwa eigens komponierten und online veröffentlichten Musikstücken einwandfrei nachweisen.