Ahogy adatbázis titkosítás esetén, úgy fájltitkosítás esetén sincs kimondott séma, amit követni lehetne, így kész megoldások kerülnek bemutatásra.

A következő dokumentumrész négy ilyen program leírását tartalmazza. Ezek a programok nem kimondottan egy-egy fájl titkosítására szolgálnak, legtöbb esetben egész meghajtókat, fájlrendszereket kódolnak, de ezek a lehető legközelebbi megoldások egyedülálló fájlok titkosításához.

A leírások nem annyira mélyre nyúlóak, célja a megoldások működésének felületes bemutatása, alkalmazott algoritmusok leírása.

BitLocker

Használatával csökkenthető az illetéktelen adathozzáférés, azáltal, hogy az operációs rendszer meghajtóján lévő összes felhasználói és rendszerfájlt titkosítja, beleértve a cserefájlokat (swap files) és hibernációs fájlokat (hibernation files), valamint ellenőrzi a rendszerindítási komponensek és a rendszerindítási konfigurációs adatok sértetlenségét.

A BitLocker AES (Advanced Encryption Standard) titkosítási algoritmust használ, 128 vagy 256 bites konfigurálható kulcshosszúsággal. Az alapértelmezett titkosítási beállítás az AES-128, de a beállítások módosíthatók.

A ’nyers adatok’ titkosítása a teljes kötet titkosítási kulcsával történik (volume encryption key), amelyet aztán a kötet főkulcsával titkosítanak.

A teljes kötet titkosítási kulcsát a kötet főkulcsa titkosítja, és a titkosított meghajtón tárolja. A kötet fő kulcsát a megfelelő kulcsvédő titkosítja és a titkosított meghajtón tárolja. Ha a BitLocker felfüggesztésre került, a kötet főkulcsának titkosításához használt kulcsot a titkosított kötet főkulccsal együtt szintén a titkosított meghajtón tárolja a rendszer.

Ez a tárolási folyamat biztosítja, hogy a kötet főkulcsa soha nem tárolódik titkosítatlanul, és védve van, hacsak nincs a BitLocker kikapcsolva. A kulcsokat redundancia érdekében a meghajtón két további helyre is elmenti. A kulcsokat a rendszerindítás-kezelő (boot manager) olvashatja és feldolgozhatja.

7-Zip

A 7-Zip támogatja az AES-256 algoritmusú titkosítást. Ez az algoritmus 256 bit hosszúságú titkosító kulcsot használ. A kulcs létrehozásához a 7-Zip egy SHA-256 hash algoritmuson alapuló deriválási függvényt (? derivation function) használ. A kulcsderiváló függvény a felhasználó által megadott jelszóból állítja elő a derivált kulcsot. Támadások ellen a jelszavak keresésének költségeinek növelése

érdekében a 7-Zip nagy számú iterációt használ, hogy előállítsa a megadott jelszóból a titkosítási kulcsot.

Tömörítési módszer beállításával használható még ZipCrypto, AES-128, AES-192 algoritmus is. A ZipCrypto-ról még nem volt szó, ez az egyik .zip jelszóvédelmi algoritmus. Natívan támogatott Windows alatt, de nem ajánlott használni, mivel viszonylag könnyen feltörhető.

Archívum létrehozása vagy frissítésekor megadható jelszó és titkosítási beállítás.

7z formátum esetében (új archiválási formátum, amely nagy tömörítési arányt biztosít) a titkosítási metódus csak AES-256 lehet.

Zip formátumhoz választható ZipCrypto vagy AES-256.

VeraCrypt

A VeraCrypt képes a rendszerpartíció vagy a teljes rendszer meghajtó titkosítására, azaz egy olyan partícióra vagy meghajtóra, amelyre a Windows telepítve van, és amelyről elindul.

Minden fájl, beleértve a Windows és az alkalmazások által a rendszerpartíción létrehozott ideiglenes fájlokat, hibernációs fájlokat, csere (swap) fájlokat is titkosítja. A Windows nagy mennyiségű potenciálisan érzékeny adatot is rögzít, például a megnyitott fájlok nevét és helyét, a futtatott alkalmazások nevét és helyét stb. Az összes ilyen log fájl és registry entry (?) mindig titkosítva van.

A rendszer titkosítása magában foglalja a rendszerindítás előtti hitelesítést, ami azt jelenti, hogy bárkinek, aki hozzáférni és használni szeretné a titkosított rendszert, olvasni és írni a rendszer meghajtón tárolt fájlokat stb., minden egyes alkalommal a Windows indítása előtt meg kell adnia a megfelelő jelszót.

Titkosítási algoritmusok közül használható az AES, Camellia, Kuznyechik, Serpent, Twofish, illetve ezeknek a kevert verziója (pl Serpent-AES). Nem volt szó a Camellia, Kuznyechik, Serpent algoritmusokról még, nagyvonalakban a leírásuk:

-Camellia: 128 bites blokkos titkosítás. A VeraCrypt a Camellia-t 24 körre használja, 256 bites kulccsal XTS üzemmódba (A VeraCrypt által a titkosított tartalmak működési módja (? mode of operation) az XTS).

-Kuznyechik: 128 bites blokkos titkosítás. A VeraCrypt a Kuznyechik 10 körre használja 256 bites kulccsal XTS üzemmódba.

-Serpent: 256 bites kulcsot és 128 bites blokkot használ XTS üzemmódba.

Hash algoritmusok közül használható RIPEMD-160 (160 bit kimeneti érték), SHA-256, SHA-512, Whirlpool (512 bit kimeneti érték), Streebog (Streebog-256 és 512. VeraCrypt csak az 512-es verzót használja, ami 512 bites kimeneti értéket állít elő).

DiskCryptor

A DiskCryptor egy nyílt titkosítási megoldás, amely az összes lemezpartíció titkosítását lehetővé teszi, beleértve a rendszerpartíciót is. Titkosítja a teljes fájlrendszert, annak minden látható és láthatatlan adatával együtt.

Program jellemzői:

-Támogatja az AES, Twofish, Serpent titkosítási algoritmusokat, beleértve ezek kombinációit is.

- A rendszerpartíciók titkosítása indítás előtti hitelesítéssel.

- Lehetőség titkosított CD- és DVD-lemezek létrehozására.

-Teljes körű támogatás a külső USB-tárolóeszközök titkosításához.