Bezpečnostní analýza Drive Snapshot

Michal Bambuch, Josef Kokeš

Katedra informační bezpečnosti, Fakulta informačních technologií ČVUT v Praze

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Motivace a cíl práce

Zálohování disků je nezbytné opatření pro minimalizaci rizika ztráty dat. Pro operační systém Microsoft Windows je nabízeno mnoho programů, které slouží k vytváření diskových záloh a jejich případnému obnovení. Jedním z nich je právě Drive Snapshot, kterému se ve své diplomové práci věnuji.

Cílem této diplomové práce bylo provést bezpečnostní analýzu programu Drive Snapshot s ohledem na jeho bezpečnostní funkce, jako je např. šifrování záloh, práce s šifrovacími klíči či práce s uživatelskými hesly.

Postup analýzy

Drive Snapshot je komerčním programem, ke kterému nejsou zveřejněné zdrojové kódy. Pro potřeby bezpečnostní analýzy tedy bylo nezbytné použít techniky reverzního inženýrství. Postup analýzy lze shrnout do následujících kroků:

- určení kritických částí programu – způsob generování náhodných čísel, použití kryptografických algoritmů, práce s uživatelskými hesly a kryptografickými klíči
- povrchní analýza spustitelného souboru programu
- použití technik statické a dynamické analýzy pro detailní prozkoumání kritických částí programu a vlastního souborového formátu pro vytvořenou zálohu

Výsledky reverzní analýzy

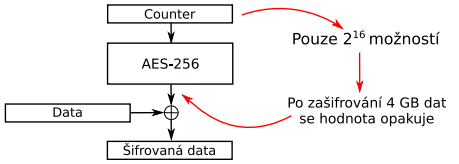
- analýza formátu souboru se zálohou
- identifikace kryptografických algoritmů
- identifikace postupu odvození šifrovacích klíčů
- identifikace způsobu generování náhodných čísel
- analýza práce s hesly a citlivými údaji
- **celkem bylo nalezeno 16 bezpečnostních zranitelností a 2 další chyby**

Nalezené bezpečnostní zranitelnosti

Velká část šifrovacího klíče je zveřejněna v souboru se zálohou

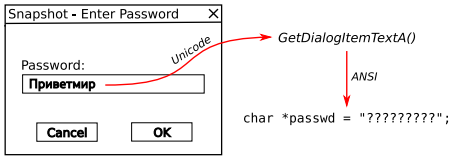
Obrázek 1: Způsob uložení šifrovacího klíče AES_KEY v souboru se zálohou. 148 z 256 bytů klíče je zveřejněno. Pro šifrování zálohy byl použit klíč AA D9 32 74 15 FE 83 30 FC 4F B5 58 21 D8 18 91 1E E7 AB DB C8 20 52 4F C6 5D DA AE 23 E2 D6 49.

Chybné použití šifrovacího režimu CTR



Obrázek 2: U šifrovacího režimu CTR nesmí být hodnoty čítače opakovány, jinak lze šifrování prolomit. Drive Snapshot používá pouze 2^{16} různých hodnot čítače, vždy po uložení 4 GB dat dojde k jejich opakování.

Možné oslabení hesla vlivem neočekávané konverze kódování



Obrázek 3: V průběhu načítání hesla z dialogového okna dochází ke konverzi kódování z Unicode do ANSI. Zadané heslo např. v azbuce je bez upozornění interně převedeno na řetězec složený z otazníků.

Možné vyzrazení části hesla nebo jeho délky v souboru se zálohou

File: *encrypted_backup.sna*

```
00F0: 4D622A002A436D64 4C696E653D22433A | Mb*.*CmdLine="C:
0100: 5C55736572735C75 7365725C4465736B | \Users\user\Desk
0110: 746F705C736E6170 73686F742E657865 | top\snapshot.exe
0120: 222020453A20463A 5C656E6372797074 | "  E: F:\encrypt
0130: 65645F6261636B75 705F434C492E736E | ed_backup_CLI.sn
0140: 61202D70773D2A2A 2076657279206C6F | a -pw=** very lo
0150: 6E67207061737377 6F7264222A005344 | ng password"*.SD
```

Obrázek 4: Pokud bylo heslo pro vytvoření šifrované zálohy zadáno přes CLI, je jeho délka zveřejněna v souboru se zálohou (počet hvězdiček odpovídá počtu znaků v hesle). Pokud heslo obsahuje mezeru, je část hesla za mezerou uložena do souboru se zálohou v čitelné podobě. Zde bylo použito heslo „A very long password“.

- Síla šifrování je závislá na výkonu počítače
- Chybná práce s citlivými údaji v paměti programu
- Možné vyzrazení hesla k použitému FTP účtu
- Odvození klíče z hesla je zranitelné na útok postranním kanálem
- Dokumentace obsahuje neplatné informace
- Web programu není dostupný přes zabezpečený protokol HTTPS
- Nedostatečné upozornění uživatele na možná rizika

Závěr

Veškeré nalezené zranitelnosti a chyby byly nahlášeny s časovým předstihem autorovi programu Drive Snapshot. Autor ocenil nahlášení chyb a přislíbil vydání nové opravené verze. Po obhájení diplomové práce došlo v srpnu 2021 k aktualizaci programu Drive Snapshot na verzi 1.49.