Дешифрация образа диска с защитой Bitlocker To Go инструментами анализа дампа памяти

Грабовой Ф. Н.
344 группа
ст. преп. Ю. А. Губанов

Шифрование Bitlocker To Go

- Алгоритмы AES + Diffuser
- Ключи:
  - Full Volume Encryption Key
  - Volume Master Key
  - Recovery Key
  - External Key
  - …

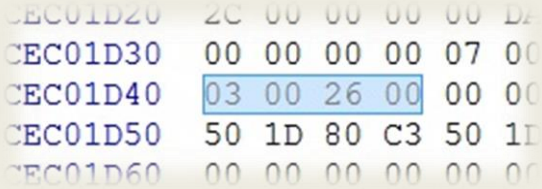
Формулировка задачи

Выполнить:

- Поиск процессов в дампе
- Поиск ключа в дампе
- Расшифровку образа носителя

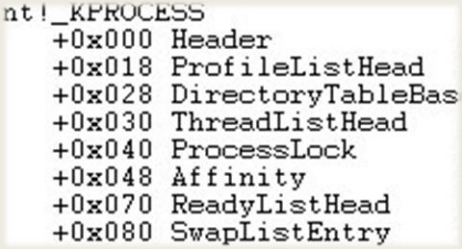
Процессы в памяти

Продолжение работы
Овчинникова Антона

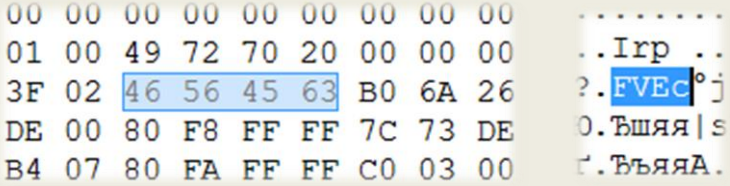


- Структуры EPROCESS
- Находятся по сигнатуре
  - По смещениям – значения параметров
- Проверяются эвристики

Программы:
Volatility
Windbg



Поиск ключа и расшифровка



- Находятся по сигнатуре
- По смещению – значения, код алгоритма

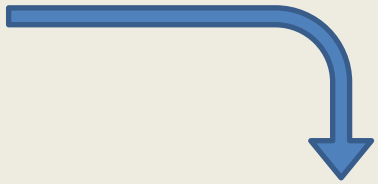
Расшифровка с LibBDE:

- Поиск entry point
- Сравнение заголовков тома (MSWIN4.1)

Время работы

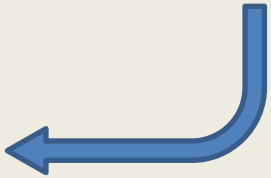
Характеристики:

- Windows 7 x86
- 4 ГБ ОЗУ
- 8 ГБ носитель



~2,5 мин

Ключ найден



~24 мин

Данные прочитаны

Итоги

✓ Процессы:

- Проверены смещения
- Исправлены вычисления

✓ Ключ:

Найден в образе памяти

✓ Расшифровка:

Реализована с помощью libbde без привязки к особенностям носителя