

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

```
CEC01D20 2C 00 00 00 00 DA
CEC01D30 00 00 00 00 07 00
CEC01D40 03 00 26 00 00 00
CEC01D50 50 1D 80 C3 50 1D
CEC01D60 00 00 00 00 00 00
```

```
nt!_KPROCESS
+0x000 Header
+0x018 ProfileListHead
+0x028 DirectoryTableBas
+0x030 ThreadListHead
+0x040 ProcessLock
+0x048 Affinity
+0x070 ReadyListHead
+0x080 SwapListEntry
```

Поиск ключа и расшифровка

```
00 00 00 00 00 00 00 00 00 .....  
01 00 49 72 70 20 00 00 00 ..Irp ..  
3F 02 46 56 45 63 B0 6A 26 ?.FVECS°j  
DE 00 80 F8 FF FF 7C 73 DE 0.Ъшяя|s  
B4 07 80 FA FF FF C0 03 00 7.ЪъяяА.
```

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

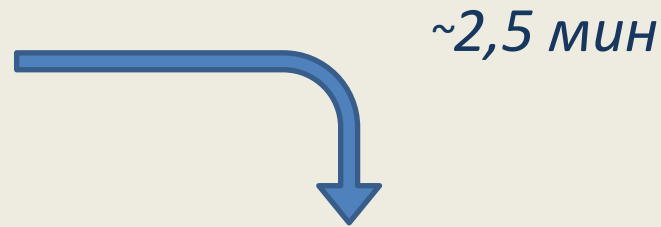
Расшифровка с LibBDE:

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

Время работы

Характеристики:

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



Ключ найден



Данные прочитаны

Итоги

✓ Процессы:

- Проверены смещения
- Исправлены вычисления

✓ Ключ:

Найден в образе памяти

✓ Расшифровка:

Реализована с помощью libbde без привязки к особенностям носителя