Name: Van Hao On

**Lab 2 – Malware**

**File: SAVED.GAM**

* **How can I determine it?**

Normally, a “\*.gam” file extension is most commonly associated with saved game file that are used by a variety of different computer gaming applications. This file allows users to control and edit the game.

**Statistics of characters:**

Example:

|  |  |  |  |
| --- | --- | --- | --- |
| **Main** | | | |
| **Attribute** | **Offset** | **Length** (in bytes) | **Modified value**  (Little endian) |
| Str | 0xC + 0x2 | 1 | 0x6300 |
| Int | 0xE + 0x2 | 1 | 0x6300 |
| Dex | 0xD + 0x2 | 1 | 0x6300 |
| HP | 0x10 + 0x2 | 2 | 0xE703 |
| Max HP | 0x12 + 0x2 | 2 | 0xE703 |
| Exp | 0x14 + 0x2 | 2 | 0x0F27 |

Note:

* Because the hex value of each attribute is written in little-endian; therefore, we need to switch the position of two bytes in an offset when we convert a decimal value to a hex value.
* While the attributes’ offset remains constant, each character will have a difference of 0x20 offset from the previous one.

For example, Shamino’s offset = Main’s offset + 0x20

* **How to get the character offset?**

Initially, we convert the character’s name into a byte array. Then, we search for the offset of that byte array in the SAVED.GAM file.

**Statistics of items and gold:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | **Offset** | **Length** (in bytes) | **Modified value**  (Little endian) |
| Gold | 0x204 | 2 | 0x0F27 |
| Keys | 0x206 | 1 | 0x6400 |
| Skull keys | 0x20B | 1 | 0x6400 |
| Germs | 0x207 | 1 | 0x6400 |
| Black badge | 0x218 | 1 | 0x0100 |
| Magic carpets | 0x20A | 1 | 0x0200 |
| Magic axes | 0x240 | 1 | 0x0A00 |

**Results**

