ex1.exe Malware Report

Coleman Kane - kaneca@mail.uc.edu

March 5, 2017

1 Description

This file is ex1.exe. Was reported in the Mandiant APT1 report with MD5 hash: `f7f85d7f628ce62d1d8f7b39d8940472`

According to the PE32 header, this sample was compiled on:
2011-05-30

2 Sample Hashes

- **MD5** `f7f85d7f628ce62d1d8f7b39d8940472`
- **SHA-1** `579e809c6e750605a79ae829bd88ff21781fdbec`
- **SHA-256** `1bc9ab02d06ee26a82b5bd910cf63c07b52dc83c4ab9840f83c1e8be384b9254`

3 Metadata Analysis

4 Strings Analysis

Contains references to the following URLs:

- `http://media.tzafrir.org.il/blog/index2.html`
- `http://media.aunewsonline.com/blog/index2.html`

Appears to be some commands that the attacker can use to control the tool remotely:

- `seturl2`
- `seturl1`
- `setsleep`
- `makefile`
- `mkcmdshell`
- `mkcmdload`
- `mkcmdrun`
- `mkcmddown`
- `mkcmddownrun`
- `mkcmdsleep`

Appears to use the following to denote configuration fields:

- `XXXXXYXXXXX`
- `YYYYYXYYYYY`