

Trickbot

Alföldi Mátyás

June 12, 2020

Contents

Introduction	2
Initial VT report check	3
Static Analysis	4
0.1 imgpaper.png	4

Introduction

File: imgpaper.png

VT: <https://www.virustotal.com/gui/file/934c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a/detection>

Initial VT report check

Sections:

- .text section seems to have a decently high entropy, so there will most likely be an unpacking process.
- .rsrc section is quite big, with a close to 8 entropy, signaling that it is definitely packed.

Interesting Imports:

- advapi32.dll
 - Various registry related api calls + Get/SetFileSecurity
- kernel32.dll
 - Virtual* functions
 - Resource handling functions (for the unpacking)
 - Heap related functions
 - File operations (like Read/Write file)
 - Library loading/unloading
 - SetUnhandledExceptionFilter + UnhandledExceptionFilter combo
 - Various Get* functions for information gathering
- WINSPOOL.DRV (This in itself is strange)

Static Analysis

0.1 `imgpaper.png`