



MessageLabs[®]
Now part of Symantec

Fragmented Distribution Attack

Virus Bulletin Annual Conference 2009, Geneva

Author: Anoirel S. Issa

MessageLabs, now part of Symantec

Anoirel_issa@symantec.com

Fragmented Distribution Attack: Abstract



Through the years there has been a constant evolution of anti-virus evasion techniques. One of the latest trend that has been widely witnessed is the process code injection.

However, a technique which has not been previously disclosed and may lead to some irreversible consequences is the “Fragmented Distribution Attack”.

The scenario: An email with an attached image arrives in your mailbox from a recognized sender, you double click and open it. As expected, the image is displayed and nothing else happens. The system administrator may not have noticed anything suspicious from his system monitor logs and everything looks fine as the anti-virus product, along with the firewall, remain silent.

Under this silence, the computer is possibly being compromised by a Fragmented Distribution Attack.

Agenda

- An attempt to define the Fragmented Distribution Attack (FDA)
- Exposing the attack: case study
 - The mystery of the bodiless header
- P.O.C embedded code fragments and re-assembler
- Live variant of a fragmented distribution attack
- Consequences and possible implications
- Detecting FDA
- Conclusion

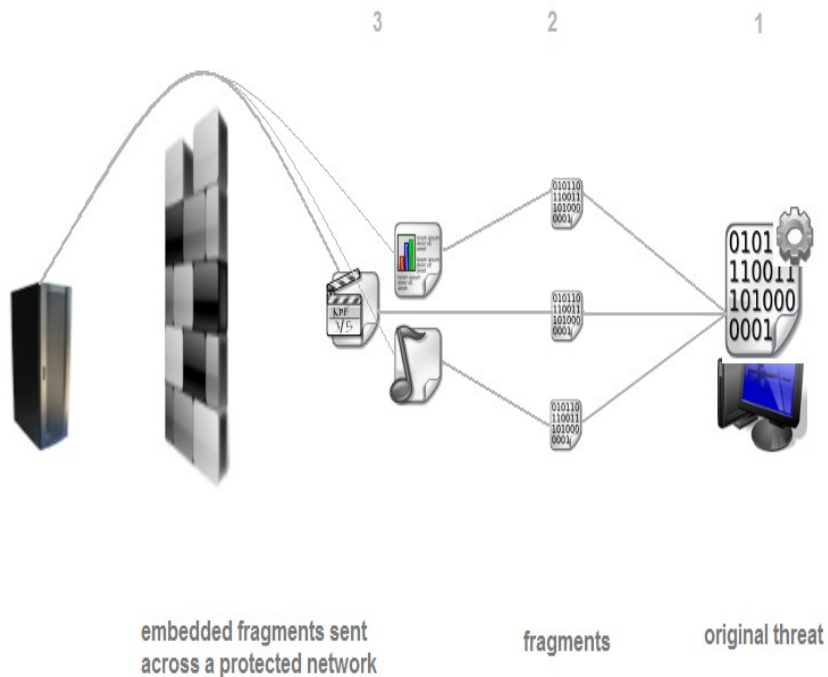
Terminology: Fragmented Distribution Attack



- A new AV evasion technique
- Aim to bypass Firewalls, IDS and Anti-virus
- Exploiting different file formats for distribution
- Code fragments embedded in innocent files
- Fragment re-assembler used to rebuild original threat
- Fragments locator – within the re-assembler

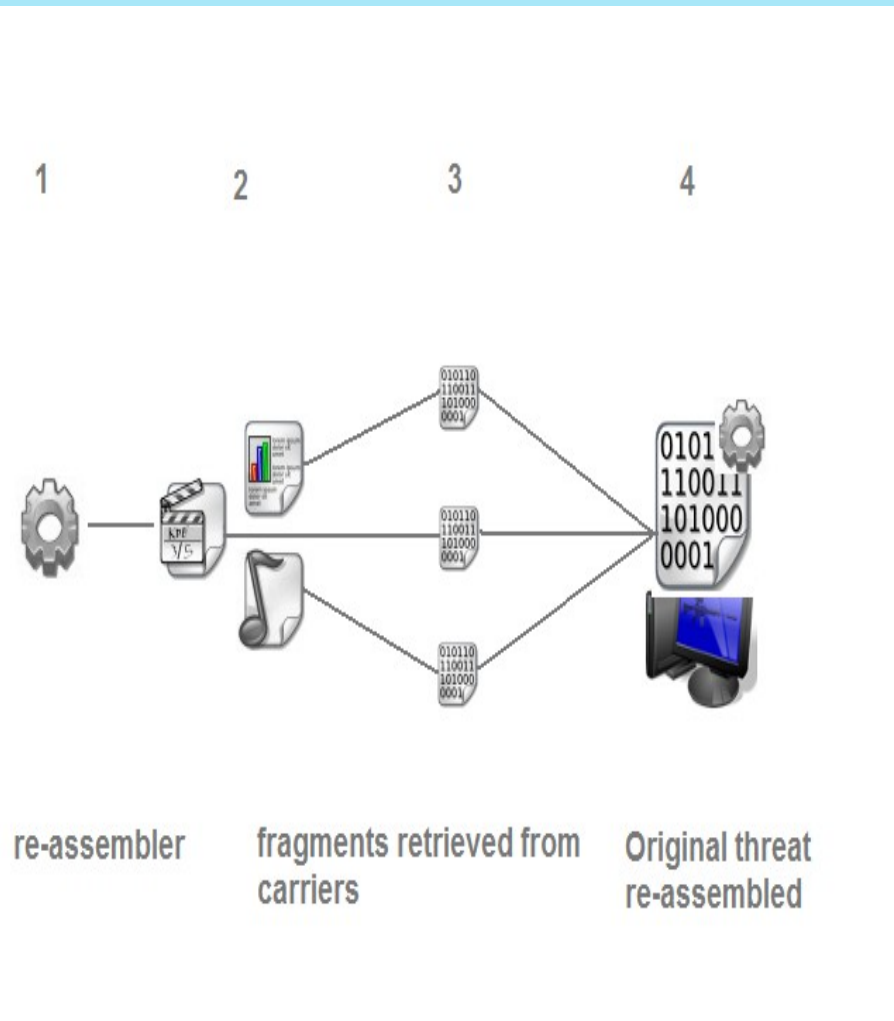
- File format exploitation and abuse
- Data fragments embedded in normal file
- Embedding code in innocent files a new method?
- Not a new technique: seen on exploits
- So what differentiates FDA to embedding technique?

A Schematic View of an FDA: Fragment Distribution



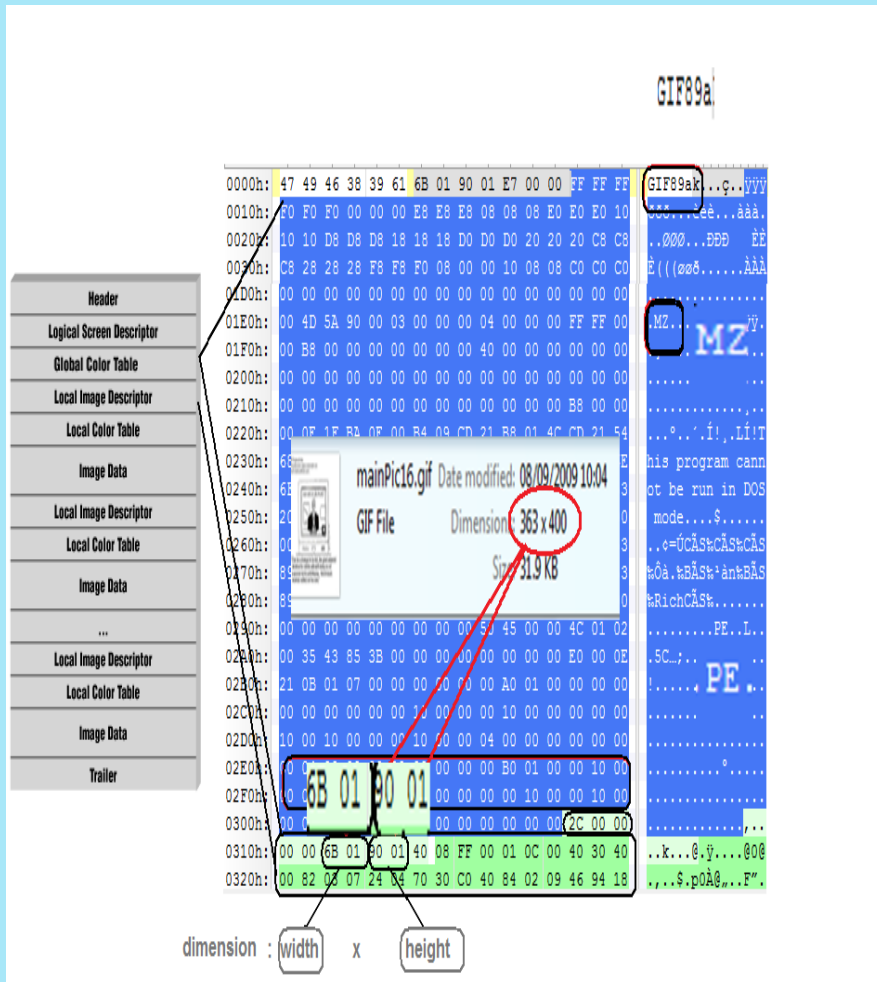
- 1 malware split in 3 fragments
- Segments embedded in innocent files
- Fragment carriers sent over the protected network

The Fragment Re-assembler



- A separate program
- Not necessarily malware
- Locates fragment carriers
- Pre-assemble fragment in memory
- May write code to disk
- Executes re-assembled code in MEM or on Disk
- System compromised

Case 1: Uncovered Live Fragment



Header

Logical Screen Descriptor

Global Color Table

Local Image Descriptor

Local Color Table

Image Data

Local Image Descriptor

Local Color Table

Image Data

...

Local Image Descriptor

Local Color Table

Image Data

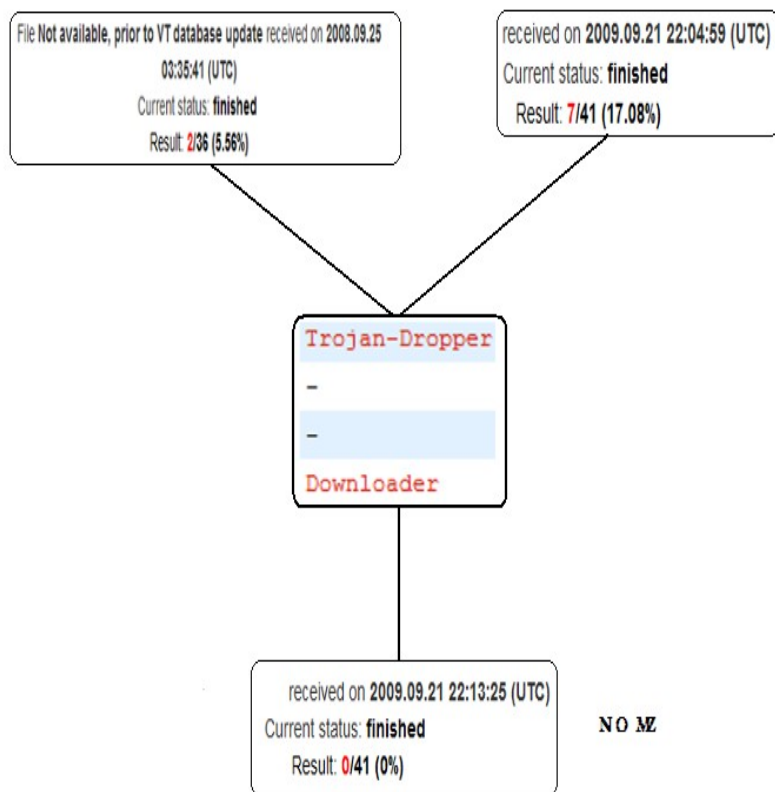
Trailer

mainPic16.gif Date modified: 08/09/2009 10:04
GIF File Dimension: 363 x 400
Size: 31.9 KB

dimension : width x height

- Embedded PE Header
- No other PE characteristics
- No encryption
- Clearly isolated fragment
- Remaining part is elsewhere
- *Possibly an FDA*

Detection of the previous live fragment



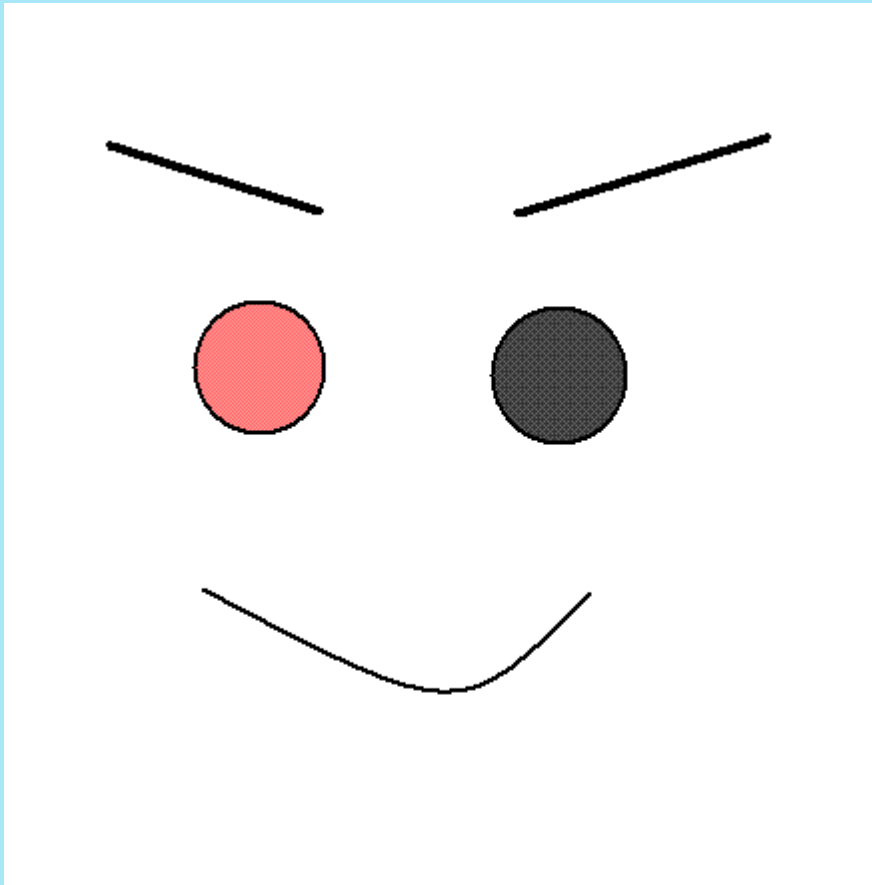
- Discovered in 2008
 - 7 AV detects the header today
 - Confusion:
 - Dropper?
 - Downloader?
 - No description
- Why ? an FDA?

What if the sample was an FDA?



- Conclusion about previous sample:
- Isolated fragment – no shellcode - no encryption
- What if our conclusion was 100% accurate?
- How would that work?
- How a single fragment of a PE file would be used and executed to compromise systems?
- FDA is the answer.
- How would an FDA work then?
- Research results and FDA POC follows

FDA Proof of concept: The Goat and the Smiling Image



To validate our deduction of FDA in the previous case we develop an FDA POC using the image in the left and a goat file

Fragment 2 & 3: Code Section & Sec Table

```
00000B90 BB DE F7 CE F7 BE FB FD EF 80 0F BC E0 07 4F F8 >>b-Í-¼úýí |.¼á.0ø
00000BA0 C2 1B FE F0 88 4F BC E2 17 CF F8 C6 3B FE F1 90 Å.þð|0%á.ÌæÆ;þñ.
00000BB0 67 4C 40 00 00 DE AD 03 6A 00 68 00 30 40 00 68 gL@.þ-.j.h.0@.h
00000BC0 05 DE AD 03 00 E8 0D 00 00 00 6A 00 E8 00 00 .0@.j.è....j.è..
00000BD0 00 DE AD 03 20 40 00 FF 25 08 20 40 00 00 00 ..ÿ%. @.ÿ%. @...
00000BE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



```
00000BA0 C2 1B FE F0 88 4F BC E2 17 CF F8 C6 3B FE F1 90 Å.þð|0%á.ÌæÆ;þñ.
00000BB0 67 4C 40 00 00 DE AD 02 00 00 00 00 00 2E 74 65 gL@.þ-.....te
00000BC0 78 74 00 00 00 DE AD 02 00 00 10 00 00 00 02 00 xt...&.....
00000BD0 00 00 04 00 00 DE AD 02 00 00 00 00 00 00 00 00 ..
00000BE0 00 20 00 00 00 DE AD 02 61 74 61 00 00 92 .rdata. .rdata.
00000BF0 00 00 20 00 00 00 00 00 06 00 00 00 .rdata.
00000C00 00 00 00 00 00 00 00 00 00 40 00 00 40 2E 04 01 .....@..@.da
00000C10 74 61 00 00 00 16 00 00 00 30 00 00 00 02 00 ta.....0.....
```

File myPicCodDaSe.gif received on 2009.09.17 15:28:47

Current status: finished

Result: 0/41 (0.00%)

File myHeadST.gif received on 2009.09.17 15:27:19 (UTC)

Current status: finished

Result: 0/41 (0%)

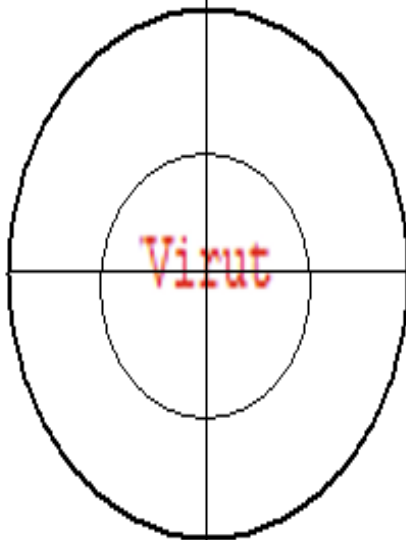
- Fragment marker “DEAD”
- Fragment order 3 - 2
- Image displays
- No detection

Extending the POC: Infectious Fragments: W32.Virut

received on **2009.09.19 18:48:31 (UTC)**

Current status: **finished**

Result: **39/41 (95.12%)**



- Not modified Virut sample
- “Unanimously” detected

A Serious Attack: Live sample



- September 09 – FDA variant seen live
 - Targeting financial institutions
 - Use old shell code technique to run re-assembler code
- Use of fragment marker
- Hacked PE header values
- Fragments of entire files
- Attack involves: Rootkit - information stealer
- Use Http to send / receive data

FDA: The Consequences



- If successfully achieved, an FDA attack can result to some serious consequences
- Depends on the victim's level of protection
- Consequence not easily predictable but can lead to:
 - Data, intellectual property leakage
 - Government, military, industrial espionage
 - Irreversible financial losses

Detecting Fragmented Distribution Attacks



- Detection would be tricky but possible
- Depend on your scan engine capabilities

Conclusion



- *Hope you enjoyed this presentation which aimed to:*
 - *bring this type of threat to light*
 - *not demonstrating malware distribution technique for hackers*

E.O.F.
Questions?
Thank you.

anoirel_issa@symantec.com
Also on LinkedIn