# Advanced Heap Spraying Techniques

## Recognize-Security

By Moshe Ben Abu, January 12 2010

# Who Am I?

Moshe Ben Abu *(a.k.a Trancer)*

- Aug 2006 - Nov 2009 at BugSec Ltd.
- Nov 2009 - Now - Independent security expert
- Website: www.rec-sec.com

| | |
|---|---|
| Email | - mtrancer@gmail.com |
| Twitter | - http://twitter.com/Trancer00t |
| LinkedIn | - http://il.linkedin.com/in/trancer |

# Heap Spraying

- Heap spraying is an exploitation technique that increases the exploitability of memory corruption vulnerabilities.

- Allocation of many objects ("blocks") containing malicious code (+ NOP sled) in the heap.

- Increasing the attacker's chance to jump to a location within the heap, successfully executing malicious code.

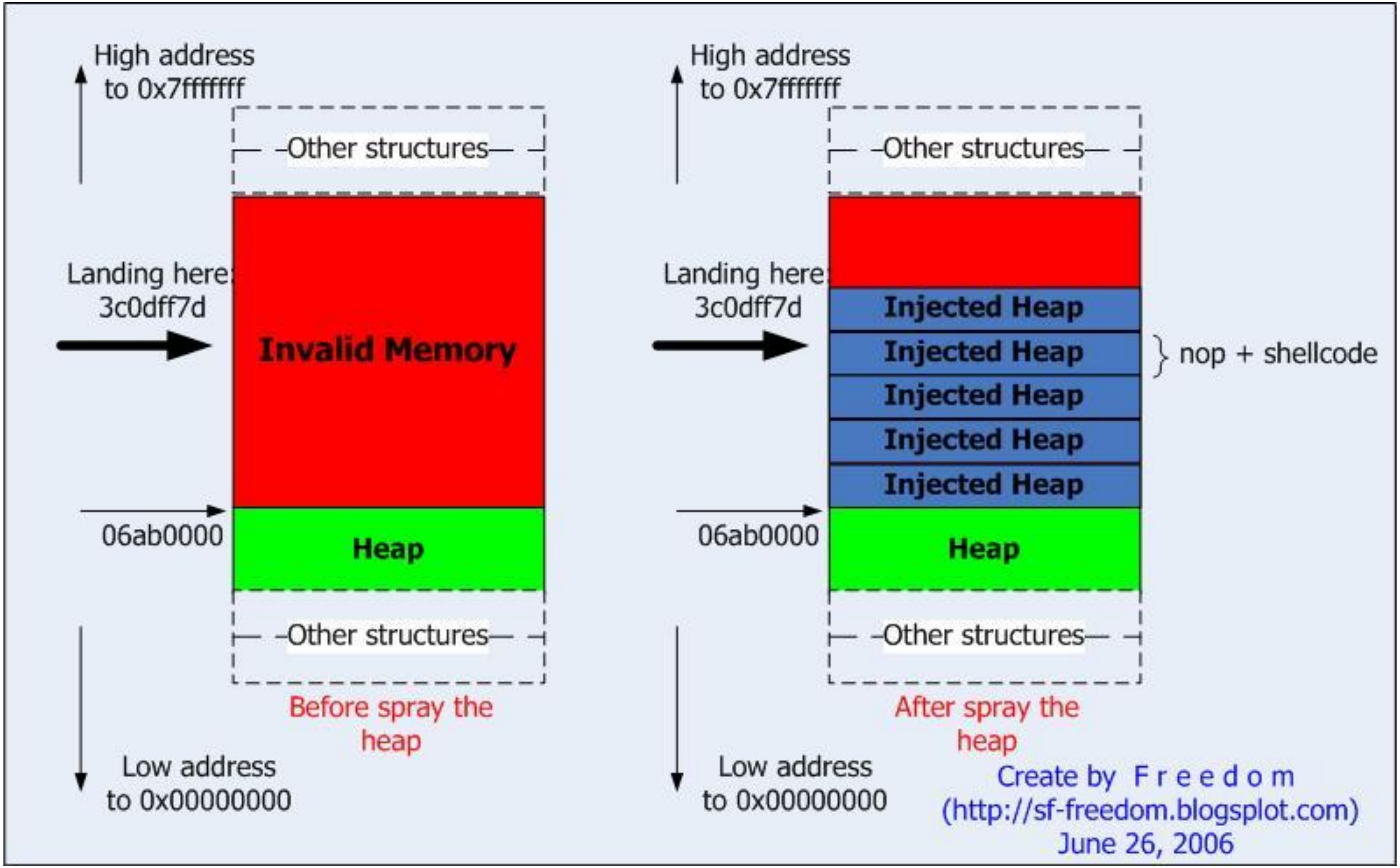
# Heap Spraying

- 2001 - exploiting a remote Microsoft IIS buffer overflow vulnerability (MS01-033).

- 2004 - SkyLined Internet Explorer IFRAME tag buffer overflow exploit.

- 2005..2010 - Owning the planet - Heap Sparying used in (almost) every “drive-by” exploit: Internet Explorer, Firefox, Opera, Safari, Adobe Acrobat Reader and etc’.

# Heap Spraying



Create by Freedom
(http://sf-freedom.blogsplot.com)
June 26, 2006

# Known Heap Spraying Techniques

Microsoft Internet Explorer

# JavaScript

- Created by SkyLined (2004).

- Most used Heap Spray technique today (doesn’t depend on external plugins).

- Very easy to detect.

# JavaScript

```
var shellcode = unescape("%u03eb%ueb59%ue805%ufff8%uffff%u4949...");
var bigblock = unescape("%u0c0c%u0c0c");
var headersize = 20;
var slackspace = headersize + shellcode.length;
while (bigblock.length < slackspace) bigblock += bigblock;
var fillblock = bigblock.substring(0,slackspace);
var block = bigblock.substring(0,bigblock.length - slackspace);
while (block.length + slackspace < 0x40000) block = block + block +
   fillblock;
var memory = new Array();
for (i = 0; i < 500; i++){ memory[i] = block + shellcode }
```

# Java Virtual Machine

- Created by Ph4nt0m Security Team (2007).
- Recreated by Alexander Sotirov and Mark Dowd (2008) – bypassing DEP and ASLR.
- Java Runtime Environment installed on 75% - 85% Internet enabled desktops.
- Not very common.

# .NET DLL Memory Technique

- Created by Alexander Sotirov and Mark Dowd (2008) – bypassing DEP and ASLR.
- Microsoft disabled .NET User Controls on Internet Explorer 8 RTM (Internet Zone and Restricted Sites Zone).
- Exploited in-the-wild.

# ActionScript Virtual Machine

- Exploited in-the-wild + Roee Hay CVE-2009-1869 exploit (2009).

- Flash Player installed on 99% Internet enabled desktops.

# New Heap Spraying Techniques

# Bitmap Heap Spraying

- Using Bitmap files (.bmp) to spray the heap.
- Discussed by Michael Sutton and Greg MacManus of iDefense (2006) but no actual attack.
- Doesn’t depend on external plugins.
- No AV detection.
- Heavy bandwidth load (2.25MB per file x 100 = 225MB), but don’t worry, we have gzip.
- Internet Explorer only?
- Work in progress.

# Bitmap Heap Spray Demo

# Silverlight Heap Spraying

- Using Microsoft Silverlight controls (.xap files) to spray the heap.
- Created by Meron Sellem.
- Silverlight installed on ??% Internet enabled desktops.
- No AV detection.
- Almost no bandwidth load (download malicious control once, load it multiple times).
- Work in progress.

# Silverlight Heap Spray Demo

# Questions?

Further questions, feedback, suggestions, nude pictures:
mtrancer@gmail.com

www.rec-sec.com