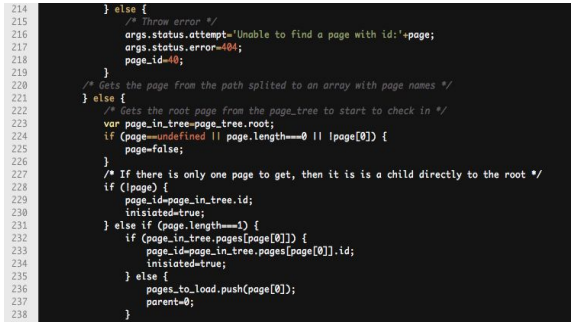
Stegosploit

By: Carlito Llena and Joseph Lee

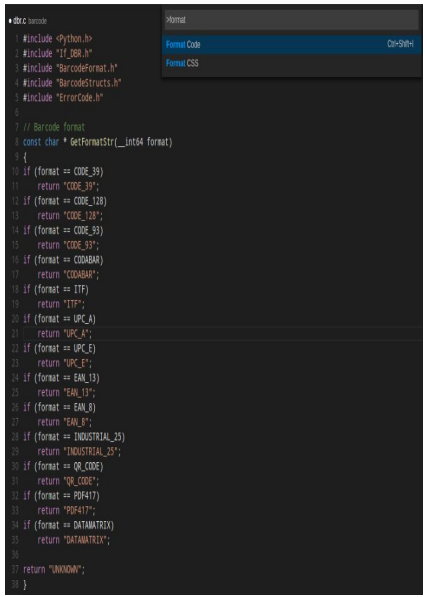
Background

Pictures are innocent...funny

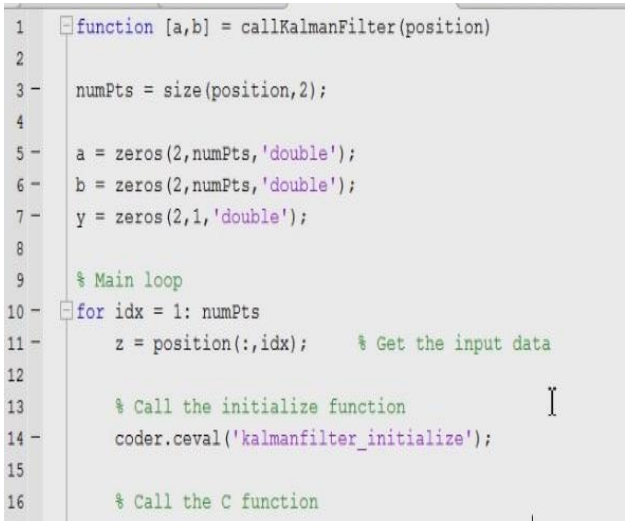
Pictures can be stylishly Malicious



```
            } else {
                /* Throw error */
                args.status.attempt='Unable to find a page with id:'+page;
                args.status.error=404;
                page_id=40;
            }
        /* Gets the page from the path splited to an array with page names */
        } else {
            /* Gets the root page from the page_tree to start to check in */
            var page_in_tree=page_tree.root;
            if (page==undefined || page.length===0 || !page[0]) {
                page=false;
            }
            /* If there is only one page to get, then it is is a child directly to the root */
            if (!page) {
                page_id=page_in_tree.id;
                inisiated=true;
            } else if (page.length===1) {
                if (page_in_tree.pages[page[0]]) {
                    page_id=page_in_tree.pages[page[0]].id;
                    inisiated=true;
                } else {
                    pages_to_load.push(page[0]);
                    parent=0;
                }
```

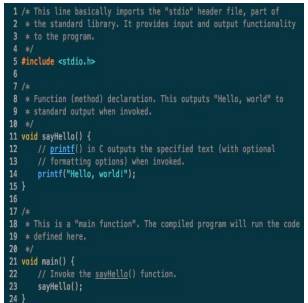


```
#include <Python.h>
#include "IF_BBR.h"
#include "BarcodeFormat.h"
#include "BarcodeStructs.h"
#include "ErrorCode.h"

// Barcode format
const char * GetFormatStr(__int64 format)
{
if (format == CODE_39)
  return "CODE_39";
if (format == CODE_128)
  return "CODE_128";
if (format == CODE_93)
  return "CODE_93";
if (format == CODABAR)
  return "CODABAR";
if (format == ITF)
  return "ITF";
if (format == UPC_A)
  return "UPC_A";
if (format == UPC_E)
  return "UPC_E";
if (format == EAN_13)
  return "EAN_13";
if (format == EAN_8)
  return "EAN_8";
if (format == INDUSTRIAL_25)
  return "INDUSTRIAL_25";
if (format == QR_CODE)
  return "QR_CODE";
if (format == PDF417)
  return "PDF417";
if (format == DATAMATRIX)
  return "DATAMATRIX";

return "UNKNOWN";
}
```



```
function [a,b] = callKalmanFilter(position)

numPts = size(position,2);

a = zeros(2,numPts,'double');
b = zeros(2,numPts,'double');
y = zeros(2,1,'double');

% Main loop
for idx = 1: numPts
    z = position(:,idx);      % Get the input data

    % Call the initialize function
    coder.ceval('kalmanfilter_initialize');

    % Call the C function
```

```
// Load required packages
var express = require('express');

// Create our Express application
var app = express();

// Create our Express router
var router = express.Router();

// Initial dummy route for testing
// http://localhost:3000/api
router.get('/', function(req, res) {
  res.json({ message: 'You are running dangerously low on beer!' });
});

// Register all our routes with /api
app.use('/api', router);

// Start the server
app.listen(3000);
```



```
/* This line basically imports the "stdio" header file, part of
 * the standard library. It provides input and output functionality
 * to the program.
 */
#include <stdio.h>

/*
 * Function (method) declaration. This outputs "Hello, world" to
 * standard output when invoked.
 */
void sayHello() {
    // printf() in C outputs the specified text (with optional
    // formatting options) when invoked.
    printf("Hello, world!");
}

/*
 * This is a "main function". The compiled program will run the code
 * defined here.
 */
void main() {
    // Invoke the sayHello() function.
    sayHello();
}
```

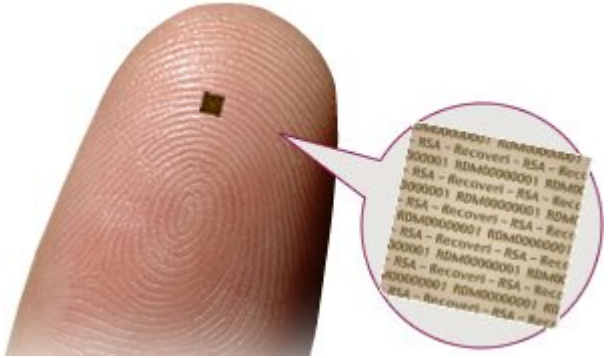
What is Stegosploit?

- Stegosploit = Steganography + Polyglot
- Stegosploit is NOT an exploit, but a way of delivering browser exploits (with style).
- Not a XSS attack or webshell
- Not a manipulation of EXIF data

What is Steganography?

- Comes from the Greek words steganos (to conceal) and graphein (writing)
- Hiding a secret message within a medium such as a picture, document or video

Morse Code knitted to a rug



Microdot, words shrunk to a tiny size, undetectable to the human eye

What is Steganography?

Another way to think about it is to contrast Steganography with Cryptography.

Cryptography hides the meaning of a message.

Steganography hides the fact that there’s a message at all.

What is Polyglot?

- In Computing/Programming context: Code written in such a way that it is a valid representation of two or more types of files.

```
#define a /*
#<?php
echo "\010Hello, world!\n";// 2> /dev/null > /dev/null \ ;
// 2> /dev/null; x=a;
$x=5; // 2> /dev/null \ ;
if (($x))
// 2> /dev/null; then
return 0;
// 2> /dev/null; fi
#define e ?>
#define b */
#include <stdio.h>
#define main() int main(void)
#define printf printf(
#define true )
#define function
function main()
{
printf "Hello, world!\n"true/* 2> /dev/null | grep -v true*/;
return 0;
}
#define c /*
main
#*/
```

Code written that can be interpreted as C, Bash script, and PHP

Bash returns
“\010Hello, world!\n
Line 5: a=5: command not found
Hello, world!”

PHP returns
“#define a /*
Hello, world!”

C returns
“Hello, world!”

Putting it all together

- Stegosploit uses **steganography** to hide code within an image file and uses the **polyglot** principle to make the browser show an image or execute the code hiding within the image file.

Vulnerability

We can make Bipolar images

These images are the same right?

Let’s call these 2 images dog.gif

How about now?

These two lines of code are unalike at all, yes?

<img src=”dog.gif”> Treats the image as an image

<script src=”dog.gif”></script> Treats the image as code

IMAJS = IMAGES + JAVASCRIPT

- We can make polyglot pictures by encoding them with Javascript or Actionscript code
- By taking advantage of that vulnerability, we are able to deliver exploits via images like bmp, jpeg, and png’s
- First coined by Saumil Shah at SyScan 2015, Singapore

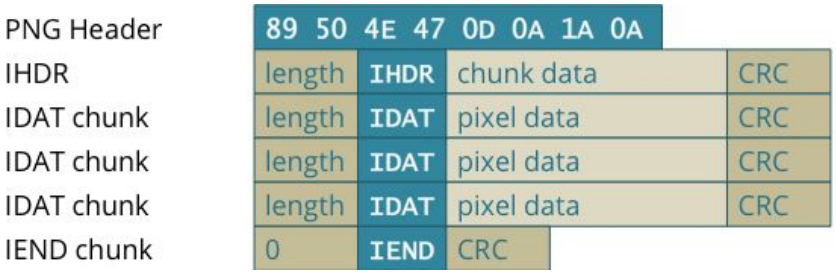
Small demo of it in action with BMP images

Headers Headers headers

- By commenting out the image data of bmp and gif data and add our own code such that our exploit will be on the website
- Jpeg images are an anomaly as we can can encode our Javascript into specific bit layers without it being visible to the naked eye

More on headers

```
47 49 46 38 39 61   HH HH   WW WW
G  I  F  8  9  a    height  width

42 4D XX XX XX XX 00 00 00 00 ........
B  M  Filesize    Empty Empty DIB data
```



Jpeg File Structure

Marker	Code	Name
FF D8	SOI	Start Of Image
FF E0	APP0	JFIF File
FF DB	DQT	Define Quantization Table
FF C0	SOF	Start Of Frame
FF C4	DHT	Define Huffman Table
FF DA	SOS	Start Of Scan
FF D9	EOI	End Of Image

Another live demo

Mitigation

As a user

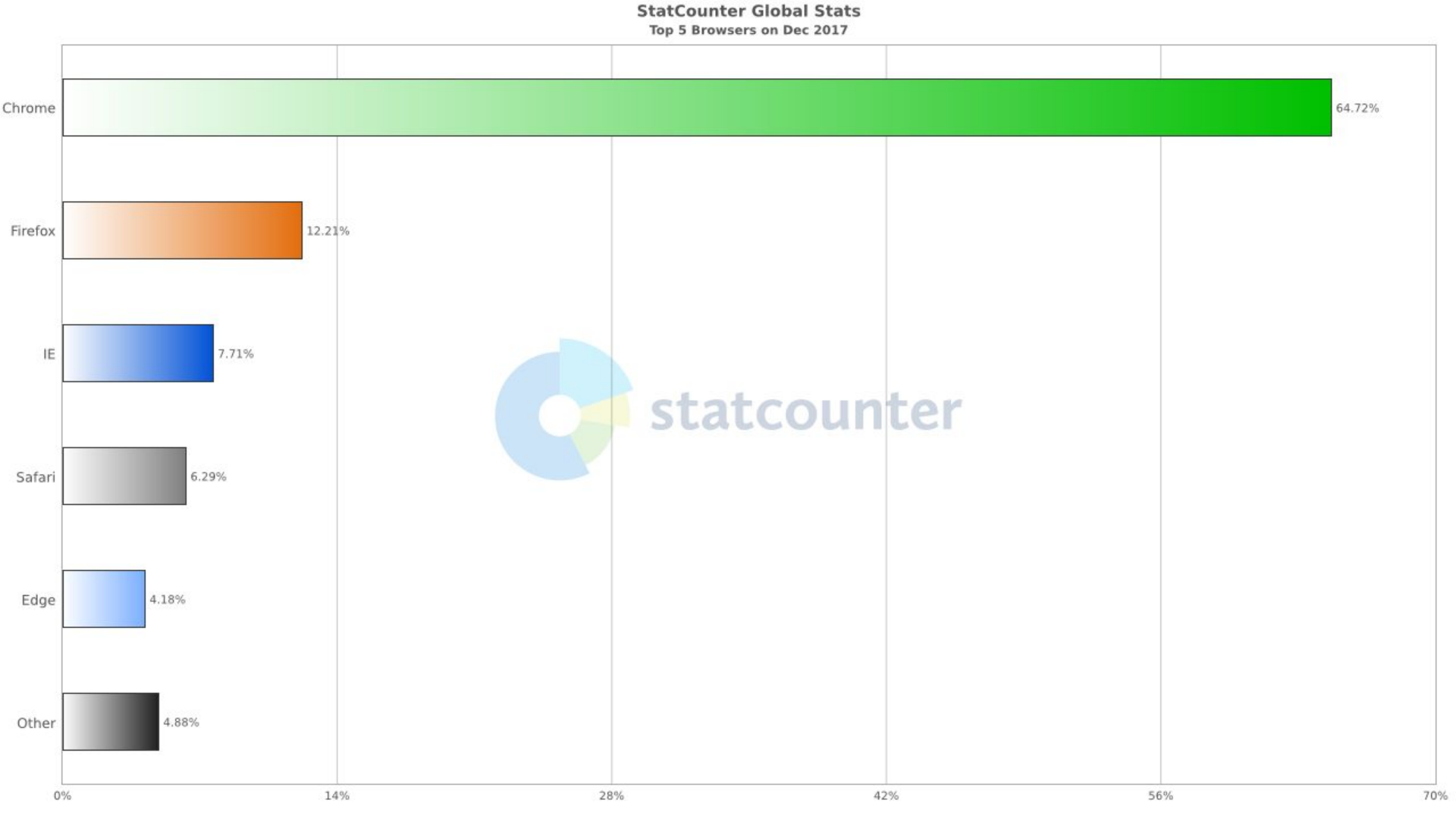
- Good browsing habits (don’t go to suspicious sites, etc.)
- Have an up-to-date browser that uses MIME type checking such as Google Chrome, Opera, Firefox, and even Microsoft Edge

Submitted at	2015-06-11 14:27:06
Filename	cammy_cinput_imajs
Comment	Stegosploit CVE-2014-0282
Filesize	239150 bytes
MD5	bfe49153a859579e52956d530c9a6093
SHA1	044fd100bcad13de52e9ceb57abb92e430e4ea33
Status	complete

Anti-Virus	Update	Detected	Signature
[VT Yara]	PeID		-
[VT Yara]	General		'dyndns_ath_ro'
[VT Yara]	Magic		-
[VT Yara]	Memory		-
[VT Yara]	Mobile		-
[VT Yara]	Trojans		-
AVG	12.0.1794.0		-
ClamAV	0.96.5		-
Comodo	1.0.2		-
Drweb	6.0.2.2 - linux		-
ESET	4.0.77		-
F-Prot	4.6.5.141		-
Ikarus	1.3.2		-
Kaspersky	8.0.1-50		-

Detected by 1 (out of 14) Anti-Virus products

WHO USES INTERNET EXPLORER ANYMORE?


StatCounter Global Stats
Top 5 Browsers on Dec 2017
Chrome
64.72%
Firefox
12.21%
IE
7.71%
Safari
6.29%
Edge
4.18%
Other
4.88%
statcounter
0%
14%
28%
42%
56%
70%

As a software Developer

- Use third party forensic analysis, steganalysis, and data sanitation software.
  - Data Sanitation(CDR) by OPSWAT
  - StegoWatch by Wetstone Technologies Inc.
  - Encase by Guidance Software Inc.
  - ILook Investigator by Perlustro and IRS
  - Stegdetect (freeware)

Approved!

As a software Developer

- If one knows the content of original image, use hashing to verify if image has been modified.
- The file size of a modified image is almost twice the size of the original.
- Think of ways to degrade quality of image so that malicious code gets corrupted.
  - QUICK FIX/HACK: Resize the image and then resize the image again to the original size.
  - QUICK FIX/HACK: Remove bit layers 0-3.
- There are steganographic algorithms that make detection hard and make the information resistant to corruption such as F5.

References

Stegosploit
http://stegosploit.info/
PoC || GTFO x08
https://www.alchemistowl.org/pocorgtfo/pocorgtfo08.pdft
SyScan'15 Singapore: Stegosploit - Hacking with Pictures
https://youtu.be/np0mPy-EHII
Steganalysis: Detecting hidden information with computer forensic analysis
https://www.sans.org/reading-room/whitepapers/stenganography/steganalysis-detecting-hidden-information-computer-forensic-analysis-1014

Questions?