Fun With JavaScript DeObfuscation

Adnan Mohd Shukor
Mahmud Ab Rahman
MyCERT, CyberSecurity Malaysia
JavaScript Fun Facts #1

Java != JavaScript
JavaScript Fun Facts #2

• Only in browsers?
JavaScript

• JavaScript® (sometimes shortened to JS) is a lightweight, object-oriented language, most known as the scripting language for web pages, but used in many non-browser environments as well.

• Executed on client side – Code will be downloaded and execute on the client applications

• Obfuscation as protection
• Obfuscated JavaScript is Everywhere
Obfuscated JavaScript is Everywhere

– Browser exploit
• **Obfuscated JavaScript is Everywhere**
  – PDF Reader Exploit
Obfuscated JavaScript is Everywhere
– Injected into Database + Browser Exploit
Common Type of Obfuscations

- 1 liner
- Base64
- Escape/Unescape
Common Type of Obfuscations

- 1 liner
Common Type of Obfuscations

• 1 liner – JS Beautifier eg: http://jsbeautifier.org/
Common Type of Obfuscations

• Base64

```html
<script>
    eval(atob("YWNlcml0b3IhIaCEgQmFzZTY0KQgPyIiQw=="));
</script>
```
Common Type of Obfuscations

- **Base64**
  - Using webbased tool to decode the string
    - Eg: http://home2.paulschou.net/tools/xlate/
  - Scripting kungfu anyone?

```ruby
gerubyr --e 'require "Base64"; puts
  Base64.decode64("YWxlcnQoIkh1aCEgQmFzZTY0KCGgPyIpOw==")'
> alert("Huh! Base64() ?");
```
Common Type of Obfuscations

- Escape/Unescape
Common Type of Obfuscations

• Escape/Unescape
  – Using webbased tool to decode the string
    • Eg: http://www.tareeinternet.com/scripts/unescape.html
  – Yet another scripting kungfu?
Modern JavaScript Obfuscations

• javascriptobfuscator.com Obfuscation
• eval(function(p,a,c,k,e,r) Obfuscation
• JSidle Obfuscation
• (+[]) Obfuscation
• $=\sim[] Obfuscation
Modern JavaScript Obfuscations

• With a lil help from:
  – Firebug JavaScript Console
    • console.log()
    • console.debug()
    • console.info()
    • console.warn()
    • console.error()
  – SpiderMonkey
  – print()
  – alert()
  – <textarea>
Modern JavaScript Obfuscations

• javascriptobfuscator.com Obfuscation
  – Web based + FREE
  – Converted to HEX
Modern JavaScript Obfuscations

- javascriptobfuscator.com Obfuscation
  - Convert from HEX manually :P
  - Using <textarea>
  - Hook the obvious function(s)
Modern JavaScript Obfuscations

• `eval(function(p,a,c,k,e,r){e=String;if(!"\".replace(/\^/,String))\{while(c--)r[c]=k[c]\};k=[function(e){return r[e]}];e=function(){return `\w +`};c=1};while(c--)if(k[c])p=p.replace(new RegExp(`\b`+e(c)+`\b","g`),k[c]);return p)`

– AKA Edwards Packer
– Web based + FREE
Modern JavaScript Obfuscations

• `eval(function(p,a,c,k,e,r) Obfuscation`
  – Using `<textarea>`
  – Hook the eval function
    • `alert()`
    • `console.log()`
    • `print <= for SpiderMonkey`
Modern JavaScript Obfuscations

- JSidle Obfuscation
  - By Sven T.
  - Obfuscation + time factor
  - Appearance: HITB magazine, Volume 1, Issue 3
  - Proposed (by the author) to be integrated into Metasploit
Modern JavaScript Obfuscations

- JSidle Obfuscation

```javascript
var hexcomp=function hex comp(o){return rtt2Hex(rtt2Comp(str2rtt utf8(o)))
function hex o comp(o){
return rtt2Hex(rtt2comp(str2rty utf8(o)))
function rtt2comp(t){
return t.hex comp()}
function rtt2comp(t){
return t.hex comp()}
function hex comp(t){
return t.hex comp()}
function str2rty utf8(t){
return t.hex comp()}
function str2rty utf8(t){
return t.hex comp()}
function str2rty utf8(t){
return t.hex comp()}
}
var str1(utf8(o))}{
var str1(utf8(o))}{
var str1(utf8(o))}{
var str1(utf8(o))}{
var str1(utf8(o))}
}```
Modern JavaScript Obfuscations

• JSidle Obfuscation
  – Hook the eval function
    • alert()
    • console.log()
    • print <= for SpiderMonkey
Modern JavaScript Obfuscations

• (+[]) Obfuscation
  – AKA JSF*ck Obfuscation
  – By Sifoo Yosuke HASEGAWA
  – UTF-8.jp guy
  – Encode with only 6 letters - []()!+
  – Master of weird symbol based obfuscation
Modern JavaScript Obfuscations

• (+[]) Obfuscation
Modern JavaScript Obfuscations

• (+[]) Obfuscation
  – Hook the function constructor
    • alert()
    • console.log
Modern JavaScript Obfuscations

• $=\sim[\] Obfuscation
  – AKA jjencode
  – By Sifoo Yosuke HASEGAWA
  – UTF-8.jp guy
  – Encode with symbol
  – For some reason, also called as “Dollar sign encode”
Modern JavaScript Obfuscations

- $=\sim[]$ Obfuscation

```javascript
<script>
// Obfuscated code
</script>
```
Modern JavaScript Obfuscations

• $=\sim[]$ Obfuscation
  – Hook the function constructor
    • alert()
    • console.log
  – Octal decode in 2\textsuperscript{nd} iteration
That is not the end!

- JavaScript is now full with emotion that can be express via emoticon

![Image](image.png)
That is not the end!

- JavaScript aware that you are analyzing them
  - userAgent
  - chrome://firebug/content/
  - chrome://jsdeobfuscator/content/