Hacker Defender Removal…

Since the spring of 2003 we have been the target of many attacks, many of these involve the installation of ftp servers on various Windows machines, the aim of this is for the attackers to utilise the fast bandwidth the University possesses to distribute copyrighted material such as films, games and software etc.
Sometimes these ftp servers are protected by a piece of software called HackerDefender, this software is used to hide files, processes and even ports from the user and investigating parties and is particularly difficult to infiltrate.

These instructions and removal instructions have been put together in order to allow technicians to successfully remove the HackerDefender software and the software it is protecting.
Much of the work has been carried out by Geraint Howell of CompSci who has been instrumental in creating this solution.

Detection…

Tell tale signs...
If a remote port scan says that a port is open and that port can be ftp'd into but aports (http://bagpuss.swan.ac.uk/comms/aports.exe) doesn't display the port locally you can pretty much assume a version of HackerDefender is installed.

To confirm…
Download, unzip and run the RootKit detector from the command line.
When ran this will list any issues with the PC.
http://bagpuss.swan.ac.uk/comms/RKDetectorv0[1].62.zip

To Clean…

Boot windows into Rescue mode, do one of the following:

- Insert the Windows OS Installation CD into the Drive.
- Boot from the CD
- Choose 'R' to enter the Rescue Console
- Choose the Windows installation you want to Clean from the list presented to you.
- Enter the Administrator Password.

Once in the recovery console, you have a few commands for this, including:

listsvc - lists services that can be enabled or disabled

enable <servicename> <start-type> - enables a service, with a service type,

- SERVICE_DISABLED
- SERVICE_BOOT_START
- SERVICE_SYSTEM_START
- SERVICE_AUTO_START

- SERVICE_DEMAND

disable <servicename> - disables a service, but prints out the previous start-type, which should be recorded in case you need to re-enable the service.

More info on the Recovery Console can be found here…
http://support.microsoft.com/default.aspx?scid=kb;EN-US;229716

Use listsvc to find any undesirable services, make a note of them, HackerDefender is usually called something along the lines of HackerDefender, or we have seen ZackerDefender.
Once these have been disabled you can reboot safely into full windows without HackerDefender starting up.

Clean up Trojans/payloads protected by HackerDefender...

Once the machine has rebooted search the registry for the name of the service that you disabled in the previous section, this should lead you to the executable for HackerDefender and more importantly it's .ini file (not necessarily a .ini file, but may have a different extension)

Open/Edit the ini file and in there you should find a number of files, ports and services that HackerDefender is defending. Systematically find each of these services in the registry and delete them (they will probably appear more than once), likewise find all of the referenced files and delete them also.
** See end of the Document for an example of a HackerDefender ini file. You will notice lots of spurious characters, these are added (and stripped out by HackerDefender) to evader AV sig matching.

It's also worth having a look in the registry for 'run on boot' programs too, goto this key…
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Have a look for any of these and delete them if they are present…

"spoolsvr.exe"=-
"Kernel32"=-
"GLSetIT32"=-
"iTouch.exe"=-
"Localsys.exe"=-
"explorer.exe"=-
"msiexe.exe"=-
"service"=-

Also look for anything else suspicious.

Further Reading…

The instructions for HackerDefender100 can be found here and give a good insight and explanation on how it works and perhaps how to remove it.
http://www.megasecurity.org/trojans/h/hackerdefender/Hackerdefender1.00.html

Other Related Reading…

http://www.securityfocus.com/archive/105/347406/2004-01-30/2004-02-05/2

http://madchat.org/sysadm/unix.seku/dirbreak.htm

http://members.chello.nl/s.pechler/Backdoor_stealth_proxy_server.htm

A Real HackerDefender INI File.

[H<<<idden T>>a/"ble]
>h"xdef"*
r|c<md\.ex<e::
hxdefdrv.sys
c:\WINNT\SYSTEM32\MSAGENT\Local\
MSAGENT
com1
system32
c:\RECYCLER\S-1-5-21-1368927438-52A168587-1617787245-503\
d:\RECYCLER\S-1-5-21-1368927438-52A168587-1617787245-503\
e:\RECYCLER\S-1-5-21-1368927438-52A168587-1617787245-503\
f:\RECYCLER\S-1-5-21-1368927438-52A168587-1617787245-503\
S-1-5-21-1368927438-52A168587-1617787245-503
schost.exe
schost.ini
msdiag*
SRVNY.exe
forcdos.exe
Santa*
Rhododenron.bmp

"[:\:R:o:o\:t: :P:r>:o:c<:e:s:s:e<:s:>]
h<x>d<e>:f<*
<\r\c:\m\d.\e\x\e
forcdos.exe
smnp.exe
msdiag.exe

```
/[/H/idd\en Ser:vi"ces]
Ha>:ck"er//Def\ender*
Cryptograph*

       /
[Hi:dden R/">>egKeys]
Ha:"c<kerDef\e/nder084
LE":GACY_H\ACK/ERDEFE\ND:ER084
Ha:"c<kerDef\e/nderDrv084
LE":GACY_H\ACK/ERDEFE\ND:ERDRV084
          /
\"[Hid:den\> :RegValues]"""
HackerDefender084
LEGACY_HACKERDEFENDER084
HackerDefenderDrv084
LEGACY_HACKERDEFENDERDRV084
HackerDefender073
LEGACY_HACKERDEFENDER073
Cryptograph*
          ////
:[St/\artup\ Run/]

":[\Fr<ee>> S:"<pa>ce]

"[>H<i>d"d:en<>\ P/:or:t<s"]\:
TCP:163,43958,65302

[Set/tin/:\gs]  /
P:assw\ord=k1ll3rkr1s
Ba:ckd:"oor"Shell=hxdefß$.exe
Fil:eMappin\gN/ame=_.-=[Hacker Defender]=-._
Serv:iceName=HackerDefender084
>Se|rvi:ceDisp<://la"yName=HXD Service 084
Ser>vic:eD||escr<ip:t"ion=powerful NT rootkit
Dri<ve\rN:ame=HackerDefenderDrv084
D:riv>erFileNam/e=hxdefdrv.sys

[Comments]
Hello admin, sorry for everything. I didn't damage your files, look at your files, steal your files or information. I have some morals. All that I did was take some hard disk space and soem bandwidth. Sorry once more for all your troubles. Discover the miracle of windows update and everyone will be fine :). To remove this piece of kit a reboot into safe mode will do the trick, sorry to make it so complex, but top marks for finding it to start with :)
```