[When your server ends up a Warez site]

last update: 21.June.2001

Strange logs from your FTP server

Obscure [obscure@eyeonsecurity.net]

EyeonSecurity
http://eyeonsecurity.net/

[Background information]

My experiments with ftp servers

A week before publishing this paper, I opened an anonymous ftp site on my home machine, expecting a few connections. I also wanted to see what people would do if I gave them write access. Within 3-4 days of my server being up, I got a successful connection from a remote host, which created his own directory named "_kurdt". Later on, I got another connection from a possibly different visitor, who created a different directory name "020612105639p". Checking my ftp logs, I learnt that both processes seem automated: within the same second the user has logged in, created a folder and disconnected from my ftp server. The third scan consisted of testing upload, deletion and ftp/http miss-configuration. These attacks are described in detail on the log files section.

FXP and Pub Scanning

"FXP stands for File eXchange Protocol and it let's you copy files from one FTP-server to another using a FXP-client. Normally you transfer files using the FTP protocol between your machine and a FTP-server, and the maximum transfer speed depends on the speed of your Internet connection (e.g. 56k, cable or T1). When transferring files between two remote hosts using a FXP client, the maximum transfer speed does not depend on your connection but only on the connection between the two hosts, which is usually much faster than your own connection. Because it is a direct connection you will not be able to see the progress or the transfer speed of the files." (Quoted from http://www.ultimatefxp.f2s.com/tutorials/tutorial.htm)

Technically this means that a client will initiate a PASV ftp connection from host A to host B, by giving the destination IP of host B as destination. This attack is normally described as FTP Bounce Attack.

Pub Scanning on the other hand, is about scanning for ftp sites, which allow you to upload and download your own stuff. Scanning for such ftp sites can be done either manually using a port scanner or checking each ftp site using an ftp client. Increasingly many people are using software for the sole purpose of scanning for such sites. This is described further on in the Scanning Tools section. Having such access for Warez people means that they can have large ftp sites with good bandwidth, easily accessible for trading Warez, mp3s, VCDs and more.

Difference between Warez “D00ds” and Hackers

To the unwary administrator, such activity will look like his ftp site has been hit by another evil cracker (AEC) [tm]. In reality, the methods used for pub scanning and FXP are quite similar to patterns generated by AEC people. However, the scope is quite different. While a cracker will want to penetrate the system, and maybe the network, to gain access to more machines, maybe for DDoS, which is quite popular nowadays, or to deface a site, the average Warez pub-scanner will probably want Gigabytes of storage and good bandwidth. This does not mean that exceptions do not exist. Crackers have been known to leave Warez on servers, and Warez people have also been using "exploits" (mostly exploiting miss-configuration and a few IIS exploits) to gain better access to their target hosts. In fact, with Pub-scanning becoming more sophisticated, methods used by hackers to penetrate hosts on the 'net are increasingly being used for Warez dissemination. Apart from this, it is important to note that most Warez people will use Windows as opposed to a certain section of the hacker community that prefers Linux and *BSDs.

[Conquer the ftp server]

Tools of trade

Grim's Ping is probably one of the most used tools around. Version 1.71 boasts a good number of features:

Features:

- Scan specified ports, using a proxy if you wish
- Ping 24.4.4.* IP range
- Host lookup
- Perform "Pub Find" on an infinite number of IP ranges
- Log Wingate engines found, in addition to FTPs
- Wingate usage to protect privacy
- Built in FTP client
- Log or print scan results
- Check write and delete permissions
- Check OS type and FXP/Resume capabilities
- Record speed
- Modify queue to reflect your scanning processes
- Import queue lists from other popular scanning utilities
- Autosave queue
- Many configurable options

As you can see, it supports anything a pub-scanner could wish for. Gives statistics, supports "anonymity" (as described later on) and will efficiently automate scanning for different FTP sites.

As an add-on, Grim has also included Ping Companion, which will upload space.asp, an Active Server Page that displays information about the host. It will also try to upload 1k and 1mb test files to check whether the ftp server is really capable of hosting a Warez site.

An interesting tool in use is Omega Scanner that is a *“Script Based Internet Scanner”*.

"Omega Scanner is a multi-threaded script based Internet scanner. With the advantage of scripts, Omega Scanner can be configured to scan for almost anything - from SMTP to FTP servers. The variety of scripts included with Omega Scanner shows the power of script-based Internet scanning. Omega Scanner supports proxy SOCKS4 and SOCKS5"

Numerous scripts are available for FTP pub and FXP scanning… making it another tool of choice.

Another tool worth mentioning is FlashFXP ftp client, which supports ftp-to-ftp transfer.

```
Features:
```

- `Local and Site to Site file transfers`
- `Fully recursive file transferring`
- `Fully recursive deleting`
- `FTP Proxy, Socks 4 & 5, HTTP Proxy support`
- `Grouped SITE custom commands`
- `Anti-idle keeps connection active`
- `Caching of directory lists`
- `Disconnect Dialup-Networking once transfer has completed`
- `Restore broken transfers. (reconnects and restarts file transfer)`
- `Drag-drop from Windows Explorer`
- `System tray minimize.`

Warez Trends

Tagging

Warez traders exist in groups, so that each group will have a couple of members who actively scan for pubs. Since different warez groups will target each ftp site, each group creates its own tag, to claim that ftp site as its own territory.

A tag will typically look something like "-=ACF=-" or "[DVD-R]". Grim's Ping site hosts a tag list on http://grim.virtualave.net/addtag.cgi?view . The idea is that ethical pub-scanners, respect tags and don't upload their own files if the ftp site is already in use by another group. Of course, non-ethical scanners exist, and they are sometimes called deleters.

Rating Pubs

Pubs are published on Warez bulletin boards for other users to upload and abuse. Most lists of pubs will consist of more than just IP addresses. Typical lists will include the uploadable directory, delete statistics, that is, if the uploaded files are delectable by other users, the Operating system of the ftp site, if the site is able to resume downloads and uploads (a handy feature when doing huge downloads), if it is FXPable, and the download speed. Grim's Ping Companion's space.asp, which was described earlier, will give scanners further information about the target machine including the name of logical drives, type of drive, volume name, free and total space, file system for each drive and version of IIS which is running.

Hiding files

The process of uploading Warez and other goods takes time and patience. That means that the uploader wouldn't like to have his directory deleted after a few days (or hours), by the legitimate administrator, opposing Warez groups or simply clueless roamers. For this purpose, Warez d00dz have learnt various tricks to hide their stuff.

The most commonly known method for hiding directories is to prefix the filename with a dot (.). This will hide the file on most Unix machines. Another effective method is to use the tide symbol (~). Many ftp clients will direct the user to the user directory when he tries to access ~, therefore keeping certain people out and letting others in. Adding spaces to the folder and using loads of dummy directories (maze) are other ways the pirate uses to hide the treasure.

Anonymity

Many pub-scanners are well aware of the risk involved, some of them will probably have already been tipped off by some ISP or worse, got their account stopped because of their illegal activity. Therefore, the use of anonymous proxies, mis-configured Wingate servers and socks is quite popular among the community. Some will be really paranoid and use multiple proxy servers to bounce their connection, in hope that it will take much longer to get traced back. These techniques are better covered in my other article about anonymity and other issues: "Browsing Websites at your own risk".

[Post Attack Analysis and Prevention]

This section is mostly for anyone (mostly administrators) hosting an ftp site.

Log files

During my testing, (i.e. being a honeypot), I configured Serv-U to log everything to a text file for easy manual parsing. The following entries show pub-scanner's activity:

```
[5] Thu 07Jun01 13:06:42 - (000004) Connected to 61.170.139.40 (Local address x.x.x.x)
[6] Thu 07Jun01 13:06:42 - (000004) 220 EOS FTP 2.1 Ready ...
[2] Thu 07Jun01 13:06:42 - (000004) user anonymous
[6] Thu 07Jun01 13:06:42 - (000004) 331 User name okay, please send complete E-mail
address as password.
[2] Thu 07Jun01 13:06:43 - (000004) pass ncoic77@hotmail.com
[5] Thu 07Jun01 13:06:43 - (000004) ANONYMOUS logged in, password: NCOIC77@HOTMAIL.COM
[6] Thu 07Jun01 13:06:43 - (000004) 230 User logged in, proceed.
[2] Thu 07Jun01 13:06:43 - (000004) mkd _kurdt
[6] Thu 07Jun01 13:06:43 - (000004) 257 "/_kurdt" directory created.
[5] Thu 07Jun01 13:06:44 - (000004) Closing connection for user ANONYMOUS (00:00:02
connected)
```

The above shows the first scan by an pub-scanner. "kurdt" seems to be the nickname (or tag) of the client. Doing a search for _kurdt on google, produced me with some published warez sites. So this clearly confirmed my suspicion.
Apart from that he's probably using Omega Scanner with "pub searchin' script.oss", which uses ncoic77@hotmail.com as password.

The second connection produces the following logs:

```
[5] Tue 12Jun01 10:54:40 - (000003) Connected to 213.51.52.27 (Local address x.x.x.x)
[6] Tue 12Jun01 10:54:41 - (000003) 220 EOS FTP 2.1 Ready ...
[5] Tue 12Jun01 10:54:41 - (000003) IP-Name: CP17725-A.DBSCH1.NB.NL.HOME.COM
[2] Tue 12Jun01 10:54:41 - (000003) USER anonymous
[6] Tue 12Jun01 10:54:41 - (000003) 331 User name okay, please send complete E-mail
address as password.
[2] Tue 12Jun01 10:54:41 - (000003) PASS guest@here.com
[5] Tue 12Jun01 10:54:41 - (000003) ANONYMOUS logged in, password: GUEST@HERE.COM
[6] Tue 12Jun01 10:54:41 - (000003) 230 User logged in, proceed.
```

The popular pub-scanner Grim's Ping usually sends Guest@here.com as password

```
[2] Tue 12Jun01 10:54:41 - (000003) CWD /pub/
[6] Tue 12Jun01 10:54:41 - (000003) 550 /pub: No such file or directory.
[2] Tue 12Jun01 10:54:41 - (000003) CWD /public/
[6] Tue 12Jun01 10:54:41 - (000003) 550 /public: No such file or directory.
[2] Tue 12Jun01 10:54:41 - (000003) CWD /pub/incoming/
[6] Tue 12Jun01 10:54:41 - (000003) 550 /pub/incoming: No such file or directory.
[2] Tue 12Jun01 10:54:42 - (000003) CWD /incoming/
[6] Tue 12Jun01 10:54:42 - (000003) 550 /incoming: No such file or directory.
[2] Tue 12Jun01 10:54:42 - (000003) CWD /_vti_pvt/
[6] Tue 12Jun01 10:54:42 - (000003) 550 /_vti_pvt: No such file or directory.
```

It immediately tries to search for a directory to write to.

```
[2] Tue 12Jun01 10:54:42 - (000003) CWD /
[6] Tue 12Jun01 10:54:42 - (000003) 250 Directory changed to /
[2] Tue 12Jun01 10:54:42 - (000003) MKD 020612105639p
[6] Tue 12Jun01 10:54:42 - (000003) 257 "/020612105639p" directory created.
[2] Tue 12Jun01 10:54:42 - (000003) RMD 020612105639p
[6] Tue 12Jun01 10:54:42 - (000003) 550 /020612105639p: Permission denied.
[2] Tue 12Jun01 10:54:42 - (000003) SYST
[6] Tue 12Jun01 10:54:42 - (000003) 215 UNIX Type: L8
[2] Tue 12Jun01 10:54:43 - (000003) REST 1
```

The following information about my ftp is obtained:
My ftp is writable at the root directory, directories are not deletable and
OS is UNIX.

```
[6] Tue 12Jun01 10:54:43 - (000003) 350 Restarting at 1 - send STORE or RETRIEVE to
initiate transfer.
[2] Tue 12Jun01 10:54:44 - (000003) PASV
[6] Tue 12Jun01 10:54:44 - (000003) 227 Entering Passive Mode (x,x,x,x,11,202)
[2] Tue 12Jun01 10:54:44 - (000003) PORT 207,46,133,140,1,21
```

The ip: 207.46.133.140:21 is ftp.microsoft.com. This guy is trying to test if my ftp server will allow him to FXP.

```
[6] Tue 12Jun01 10:54:44 - (000003) 200 PORT Command successful.
[2] Tue 12Jun01 10:54:44 - (000003) CWD
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
ppppp
[6] Tue 12Jun01 10:54:44 - (000003) 550
```

```
/pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
ppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
ppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
ppppp
[more similar entries]
[6] Tue 12Jun01 10:54:44 - (000003) 500 'PPPPPPPPPPPPPPPPPPPPPPPPP': command not
understood.
[5] Tue 12Jun01 10:54:44 - (000003) Closing connection for user ANONYMOUS (00:00:04
connected)
```

I think this request could be an attempt to overflow the buffer, or simply testing to see what kind of error it gets to identify the OS (and ftp server software) better. Any ideas about this one would be most welcome.

Third entry comes from the same host… the day after:

```
[5] Wed 13Jun01 14:23:49 - (000019) Connected to 213.51.52.27 (Local address x.x.x.x)
[6] Wed 13Jun01 14:23:49 - (000019) 220 EOS FTP 2.1 Ready ...
[2] Wed 13Jun01 14:23:49 - (000019) USER anonymous
[6] Wed 13Jun01 14:23:49 - (000019) 331 User name okay, please send complete E-mail
address as password.
[5] Wed 13Jun01 14:23:49 - (000019) IP-Name: CP17725-A.DBSCH1.NB.NL.HOME.COM
[2] Wed 13Jun01 14:23:49 - (000019) PASS guest@here.com
[5] Wed 13Jun01 14:23:49 - (000019) ANONYMOUS logged in, password: GUEST@HERE.COM
[6] Wed 13Jun01 14:23:49 - (000019) 230 User logged in, proceed.
```

Once again this is Grim's Ping Automated tool, with Companion software, as you will see further down.

```
[2] Wed 13Jun01 14:23:49 - (000019) CWD /
[6] Wed 13Jun01 14:23:49 - (000019) 250 Directory changed to /
[2] Wed 13Jun01 14:23:49 - (000019) TYPE I
[6] Wed 13Jun01 14:23:49 - (000019) 200 Type set to I.
[2] Wed 13Jun01 14:23:50 - (000019) PORT 213,51,52,27,17,98
[6] Wed 13Jun01 14:23:50 - (000019) 200 PORT Command successful.
[2] Wed 13Jun01 14:23:50 - (000019) STOR /1mbtest.ptf
```

The scanner uploads a 1mb test file to the root directory.

```
[6] Wed 13Jun01 14:23:50 - (000019) 150 Opening BINARY mode data connection for
1mbtest.ptf.
[4] Wed 13Jun01 14:23:50 - (000019) Receiving file d:\anonftp\1mbtest.ptf
[4] Wed 13Jun01 14:25:16 - (000019) Received file d:\anonftp\1mbtest.ptf successfully
(11.9 Kb/sec - 1048578 bytes)
[6] Wed 13Jun01 14:25:16 - (000019) 226-Maximum disk quota limited to 300000 Kbytes
[6] Wed 13Jun01 14:25:16 - (000019) Used disk quota 1024 Kbytes, available 298975 Kbytes
[6] Wed 13Jun01 14:25:16 - (000019) 226 Transfer complete.
[2] Wed 13Jun01 14:25:17 - (000019) PORT 213,51,52,27,6,55
[6] Wed 13Jun01 14:25:17 - (000019) 200 PORT Command successful.
[2] Wed 13Jun01 14:25:17 - (000019) TYPE I
[6] Wed 13Jun01 14:25:17 - (000019) 200 Type set to I.
[2] Wed 13Jun01 14:25:17 - (000019) RETR /1mbtest.ptf
```

Then it downloads the file back.

```
[6] Wed 13Jun01 14:25:17 - (000019) 150 Opening BINARY mode data connection for
1mbtest.ptf (1048578 bytes).
[3] Wed 13Jun01 14:25:17 - (000019) Sending file d:\anonftp\1mbtest.ptf
[3] Wed 13Jun01 14:26:29 - (000019) Sent file d:\anonftp\1mbtest.ptf successfully (14.3
Kb/sec - 1048578 bytes)
[6] Wed 13Jun01 14:26:29 - (000019) 226-Maximum disk quota limited to 300000 Kbytes
[6] Wed 13Jun01 14:26:29 - (000019) Used disk quota 1024 Kbytes, available 298975 Kbytes
[6] Wed 13Jun01 14:26:29 - (000019) 226 Transfer complete.
[2] Wed 13Jun01 14:26:29 - (000019) TYPE A
[6] Wed 13Jun01 14:26:29 - (000019) 200 Type set to A.
[2] Wed 13Jun01 14:26:30 - (000019) PORT 213,51,52,27,9,50
[6] Wed 13Jun01 14:26:30 - (000019) 200 PORT Command successful.
```

```
[2] Wed 13Jun01 14:26:30 - (000019) LIST -la
[6] Wed 13Jun01 14:26:30 - (000019) 150 Opening ASCII mode data connection for /bin/ls.
[6] Wed 13Jun01 14:26:30 - (000019) 226-Maximum disk quota limited to 300000 Kbytes
[6] Wed 13Jun01 14:26:30 - (000019) Used disk quota 1024 Kbytes, available 298975 Kbytes
[6] Wed 13Jun01 14:26:30 - (000019) 226 Transfer complete.
[2] Wed 13Jun01 14:26:30 - (000019) DELE /1mbtest.ptf
[6] Wed 13Jun01 14:26:30 - (000019) 250 DELE command successful.
```

And finally delete the test file. Till now the following statistics are gathered from my site: Upload/Download is enabled, my speed, deletable files (I had changed the configuration to allow deletion of files by the anonymous user).

```
[2] Wed 13Jun01 14:26:30 - (000019) TYPE A
[6] Wed 13Jun01 14:26:30 - (000019) 200 Type set to A.
[2] Wed 13Jun01 14:26:30 - (000019) PORT 213,51,52,27,9,51
[6] Wed 13Jun01 14:26:30 - (000019) 200 PORT Command successful.
[2] Wed 13Jun01 14:26:31 - (000019) STOR /space.asp
[6] Wed 13Jun01 14:26:31 - (000019) 150 Opening ASCII mode data connection for space.asp.
[4] Wed 13Jun01 14:26:31 - (000019) Receiving file d:\anonftp\space.asp
[4] Wed 13Jun01 14:26:31 - (000019) Received file d:\anonftp\space.asp successfully (4.91
Kb/sec - 2648 bytes)
[6] Wed 13Jun01 14:26:31 - (000019) 226-Maximum disk quota limited to 300000 Kbytes
[6] Wed 13Jun01 14:26:31 - (000019) Used disk quota 2 Kbytes, available 299997 Kbytes
[6] Wed 13Jun01 14:26:31 - (000019) 226 Transfer complete.
```

This file is included with Grim's Ping companion and will give out information about the ftp server, as described in the tools section.

At the same moment the following log is found from my HTTP server (IIS/5.0):

```
2001-06-13 12:26:38 213.51.52.27 - x.x.x.x 80 GET /space.asp |-|0|404_Object_Not_Found
404 -
```

Of course, if I had used the same directory for both http and ftp, the asp script would have executed and given out further information
about my machine to the scanner. Also note the timing.

```
[2] Wed 13Jun01 14:26:38 - (000019) DELE /space.asp
[6] Wed 13Jun01 14:26:38 - (000019) 250 DELE command successful.
[5] Wed 13Jun01 14:26:38 - (000019) Closing connection for user ANONYMOUS (00:02:49
connected)
```

Once the ASP files is not found on the HTTP server, the scanner just deletes the file, and leaves little or no trace of his scan and moves on to the next target.

Problems caused by FTP Pub scanning

Till now this is what I got. Maybe if I wait longer I'd find myself full of Warez and my IP address on some Warez site, IRC channel or bulletin board, with most of my bandwidth being abused, not that nice. Apart from this Corporate sites could be targeted by the software makers and accused as distributing illegal software (Warez) and similar legal issues.

Of course, when the Administrator does not set a quota for anonymous FTP servers, it is very possible that pub scanners will take up all free space. This is probably the most popular type of denial of service.

Securing your Server

Securing a server that is vulnerable to this kind of attack it pretty much straight forward for normal configurations. It should be clear that what pub-scanners are exploiting is mis-configuration of ftp (and http) servers. If there is no reason to enable anonymous users to upload files, just disable this functionality. If you need certain users to upload files, you should consider creating a user and password for this purpose, and giving them write access (maybe chroot the user).

When anonymous users are required to upload files to an FTP server, the Administrator can create a directory for anonymous connections, which allows uploads but not downloads. This will make downloaders (and probably pub-scanners) jump to the next target and simply dismiss your ftp site.

HTTP servers and anonymous FTP accounts should also have use different locations on the hard disk. Having an anonymous ftp user upload a CGI script to the http server means that depending on the configuration of the web server (we're talking about miss-configured servers here...) the user will have access to execute possibly malicious code on the target host. This attack was performed on Apache.org back in May 2000,
and has probably been around since the use of CGI scripts in HTTP.

[Conclusion]

Pub scanning seems to have become a favorite and risky pastime for many Warez dealers. This occurred maybe due to the fact that Point and Click Windows Scanners are easily available from professional looking sites. The fact that in just a week two different scanners hit my testing site, seems to indicate an increase in such scanning, and should not be under estimated by the unwary
administrator. With the increase in such activity, new tools and features in existing tools will continue to improve the art of pub scanning.

[Reference]

Prevention & Incidents

Honeynet
http://project.honeynet.org/scans/arch/scan8.txt

Cert.org tips
http://www.cert.org/tech_tips/anonymous_ftp_config.html

Same attacks way back in 1993
http://www.ciac.org/ciac/bulletins/d-19.shtml

Anonymous FTP abuses
http://www.bris.ac.uk/is/services/networks/anonftp/anonftp2.html

FTP bounce attack
http://www.insecure.org/nmap/hobbit.ftpbounce.txt

Software

Grim's Ping and other tools
http://grimsping.cjb.net/downloads.htm

Omega Scanner
http://www.ftpscanner.com/omegascanner.htm

Tutorials

Net Knowledge Base
http://www.netknowledgebase.com/

Neuromancer's Tutorial Page!
http://neuro2k.homestead.com/files/index.html (down)

The 'Art' of pub scanning
http://www.jestrix.net/tuts/scan.html

FTP RFC

FTP RFC
http://www.faqs.org/rfcs/rfc959.html

Internet Host Requirements
http://www.faqs.org/rfcs/rfc1123.html

Discussion Boards

SWL FORUM
http://swlforum.cjb.net/ (down)

Net knowledgebase forum
http://www.netknowledgebase.com/forum/index.php

Grim's Ping Forum
http://grimsping.crystallized.com/forums/

[Glossary]

FTP: File Transfer Protocol. used to transfer files between hosts, and consists of a server on one side and a client on another.

IP address: Internet protocol address. Each active machine on the Internet has an IP address.

Warez: Illegal/Copyrighted software.

FXP: File Exchange Protocol. Not a protocol in itself AFAIK, but used by pub scanners to describe the process of coping software from one server to another directly using Passive mode ftp.

PUB: Public Folder. Can allow uploading to and downloading from to exchange software and data.

Scanning: Searching for a certain type of host by checking a range of IP addresses.

Pub-scanning: Scanning for PUBs. Basically searching for an ftp site, which allows users to freely upload and download software.

Exploit: Taking advantage of a security problem.

SOCKS: Allows machines to connect to other hosts via this service.

CGI script: A server-side script, which executes custom code to extend functionality of the web server.