Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

FTP and the Warez Scene

Peer-to-peer file sharing systems, such as Gnutella, provide new ways to trade illegal software. However, software theft via FTP, Internet Relay Chat channels and bulletin boards still is prevalent. Open anonymous FTP sites on your network may be serving operating systems, application software, games, music, movies and more to users around the world. Although software theft via FTP is very common, the risk of FTP abuse can be reduced by scanning networks for anonymous FTP sites, monitoring FTP activity, and securing FT...

Copyright SANS Institute

Author Retains Full Rights

AD

FTP and the Warez Scene
Shelli Crocker

Abstract

Peer-to-peer file sharing systems, such as Gnutella, provide new ways to trade illegal software. However, software theft via FTP, Internet Relay Chat channels and bulletin boards still is prevalent. Open anonymous FTP sites on your network may be serving operating systems, application software, games, music, movies and more to users around the world.

Warez

Software theft exists in many forms: from a teen who copies a game for a friend, to a small office manager who installs a single-user application on ten workstations, to an organized crime ring that auctions illegal software on the Internet. But somewhere in this spectrum exists a vast underground software trading circle: the warez scene.

Warez is the term used for software that has been stripped of its copy protection and made available on the Internet for downloading.[1] Available warez include operating systems, applications, entertainment software (games, music, movies) and more. The warez community is an well-organized one, boasting its own search engines and Web rings to help end users locate what they want.[2] A recent FBI "Cyber Strike" investigation revealed that pirated software often appears on within a day of its public release and often before the manufacturer's official release. Pirate copies of nearly every major software release, as well as specialty items, are available. Software may be offered in exchange for uploads of other applications, or users may be charged a fee to join.[3]

There are several new peer-to-peer file-sharing systems, such as Gnutella, that provide ways to trade this illegal software. However, software theft via FTP, Internet Relay Chat channels and bulletin boards still is prevalent and should not be overlooked.

Open Anonymous FTP and FXP

Anonymous FTP may be the simplest way to transfer files via the Internet, but it is not without its problems. Abuse of anonymous FTP is quite common. The CERT Coordination Center first issued an advisory regarding anonymous FTP activity in 1993, citing a continuous stream of reports from sites that experience unwanted activities

[1] "Warez." Whatis?com: the IT-specific encyclopedia. 19 November 1999. URL: http://whatis.techtarget.com/ (14 December 2000).
[2] Cuciz, David. "Software piracy report: Part III." URL: http://www.gamespy.com/legacy/articles/spr3_b.shtm (11 December 2000).
[3] Wong, Wylie. "FBI targets BBS operators, seizes hardware in software piracy sting." 3 February 1997. Computerworld, 31(5), p24.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

within their anonymous FTP areas. One type of activity noted is use of writable areas to transfer copyrighted software and other sensitive information.[4]

Hosting open anonymous FTP sites on your network is an invitation to piracy. The most common attacks found in firewall logs are scans looking for open anonymous FTP servers.[5] Large companies and universities are popular targets due to their fast connections. Without those the warez scene wouldn't exist.[6]

There are many tutorials on the Web with detailed instructions to locate public FTP sites, or "pubs." Grim's Ping[7] is recommended as the pub scanning tool of choice. The goal in locating a pub is to load it with items for downloads using "liberated" storage. Files may then be transferred between FTP servers using an FXP (File eXchange Protocol) utility, such as FlashFXP[8]. The advantage of using FXP is that the maximum transfer speed does not depend on your connection, but only on the connection between the two hosts.[9] Files can be distributed around the Internet quickly and easily between pubs, making warez widely available.

Warning Signs

Signs of piracy on your network may not be obvious at first. FXPers take care to avoid detection. While scanning and creating pubs they may use a proxy server or a wingate to mask their source and identity. Most hide the directories they create by placing periods, spaces or tildes in the name.[10] Pubs are posted via IRC channels, boards, newsgroups and mailing lists (many of which are accessible by invitation only). When using a pub, the golden rule is to behave as a guest; tampering with the system owner's files and directories increases the chance the activity will be discovered.[11]

So what should you look for? The Software and Information Industry Association (SIIA) offers seven warning signs of piracy:

1. Increased or even massive FTP file transfer in a directory
2. Expanded directory trees
3. Excessive data transfer in a single session

---

[4] CERT Coordination Center. "CERT advisory CA-1993-10 anonymous FTP activity." CERT Advisories. 14 July 1993, rev. 8 October 1997. URL: http://www.cert.org/advisories/CA-1993-10.html (7 December 2000).
[5] Graham, Robert. "FAQ: Firewall forensics." 20 June 2000. URL: http://www.robertgraham.com/pubs/firewall-seen.html (11 December 2000).
[6] "FTP etiquette." Net Knowledge Base. URL: http://www.netknowledgebase.com/tutorials/ftpetiquette.html (7 December 2000).
[7] "Grim's Ping: Making the everyday pub scanning faster and more reliable." 23 September 2000. URL: http://grimsping.cjb.net (7 December 2000).
[8] "FlashFXP." 11 August 2000. URL: http://flashfxp.phix-it.com (11 December 2000).
[9] DrPerf. "FXP Tutorial." Xtreme-FXP. URL: http://www.directdownloads.net/Tutorials/FxP.htm (30 November 2000).
[10] "Tutorials." Ultimate FXP - The web's most complete FXP info source. 12 July 2000. URL: http://www.ultimatefxp.f2s.com/tutorials/tutorial.htm (7 December 2000).
[11] "Netiquette." Net Knowledge Base. URL: http://www.netknowledgebase.com/tutorials/netiquette.html (7 December 2000).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4. Sites labeled *Warez* or listed as involving *Cracker* or *Hacker* activity
5. The posting of serial numbers used to install software
6. Increased logging into an area
7. Numerous unusual or hidden files or directories[12]

When software piracy is discovered at your organization, SIIA provides the following advice: Review directories and files in accordance with policies and procedures that exist in your organization. Determine origin of access. Review files contents for reference to other sites or account/password combinations. Then notify sites identified, as these sites themselves may be compromised.[13]

Prevention

On a large network, new FTP sites spring up frequently. Inexperienced system administrators may run FTP services with default, open configurations. Power users may install FTP services on their desktop computers. Routine scans of your own network are essential to detect new FTP servers before the FXPers find them.

These problems not withstanding, anonymous FTP can be a valuable service if correctly configured and administered. Sites should use of the most recent version of their FTP daemon. For example, the popular War FTP Daemon has a bug that allows unrestricted access to any file on the local machine.[14] Directories, password and group files must be configured correctly. See CERT's anonymous FTP "tech tip" for details.[15]

Summary

Software theft via FTP, Internet Relay Chat channels and bulletin boards is very common on the Internet. Open anonymous FTP sites on your network may be serving operating systems, application software, games, music, movies and more to users around the world. But by scanning your own network for anonymous FTP sites, monitoring FTP activity, and securing FTP server configuration, risk of FTP abuse can be reduced.

[12] Software and Information Industry Association. "Seven warning signs of piracy: What to watch for and what's at stake." URL: http://www.siia.net/piracy/policy/int_7.asp (11 December 2000).
[13] Software and Information Industry Association. "Seven warning signs of piracy: Anonymous FTP abuses." URL: http://www.siia.net/piracy/policy/int_7_abuses.asp (11 December 2000).
[14] Aase, Jarle. "Security alert - WAR FTP daemon all versions." 4 February 2000. URL: http://war.jgaa.com/alert/ (7 December 2000).
[15] CERT Coordination Center. "Anonymous FTP configuration guidelines." CERT Tech Tips. Copyright 1996, rev. 27 July 2000. URL: http://www.cert.org/tech_tips/anonymous_ftp_config.txt (11 December 2000).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced