GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

FTP and the Warez Scene

Shelli Crocker
December 14, 2000

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. 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. 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.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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

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. Large companies and universities are popular targets due to their fast connections. Without those the warez scene wouldn't exist.

There are many tutorials on the Web with detailed instructions to locate public FTP sites, or "pubs." Grim's Ping 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. 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. 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. 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.

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. 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

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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.

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. Directories, password and group files must be configured correctly. See CERT's anonymous FTP "tech tip" for details.

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.

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.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(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).

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 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS