

Chris Cortner

Phil 308 – Term Paper

12/10/2008

The Warez Scene

In this paper I present a general overview of what is known as “the warez scene.” The beginning of the paper gives a brief introduction to the experience of the end user while the rest describes the organization and operations of the scene, legal challenges it has faced, and some of the ethical considerations regarding software piracy. This is a subject with which I have some personal knowledge, not as an insider, but as someone who has been exposed to it from a very young age. I would like to note that I do not condone or excuse the practice of software piracy.

The word “warez” is modern slang for pirated software, music, movies or any illegal collection of copyrighted content made available in digital form. The word itself has a double meaning. In one connotation, “warez” is short for software, but it also refers to the wares that a merchant has to offer (“WareZ”). The “z” at the end of the word comes from leetspeak, or “elite speak.” This is the practice of obfuscating words by purposely misspelling them and replacing characters with numbers or symbols that resemble the letters they replace. The word “leet” itself is often changed in this manner and spelled l337. Software pirates adopted leetspeak for use in online conversation and for obfuscating the names of pirated software. For example, a program called Super Spreadsheet 2000 may have been renamed “=-Sup3r_Spr3ad5h337_2000=-.” The name of the program is still human-readable, but it is not likely to show up in an online search, if for example a software company was trying to locate illegal copies of its software (“WareZ”).

Software piracy has boomed with the rise of the Internet. FTP (File Transfer Protocol), Usenet, and other more recent technologies such as peer-to-peer networks have moved the ability to easily and illegally obtain copies of warez from the domain of the technically gifted to that of the common person. Modern tools for digital piracy can now be downloaded from commercial companies, and users of these programs can obtain from those companies, or from online communities, support in how to use them. The accessibility and professional sheen of these products, in addition to their ease of use, has added an air of legitimacy to the act of software piracy. Today if people wish to download a new, unreleased movie, they can simply type its name into their favorite tool and if the movie is available, click to download it. Take Usenet, for example. Usenet was one of the original applications of the Internet and was intended for online discussion. A Usenet server, also referred to as a news server, hosts discussion groups. A user connects to his news server with a news reader program to retrieve and post messages to whichever discussion groups he is interested in. These groups are synchronized among news servers around the world, an arrangement that allows people separated by vast distances to communicate about topics of shared interest.

It wasn't long, though, before clever hackers devised a way of using this technology for the distribution of warez. A file to be posted online is first cut into hundreds or thousands of chunks and these are in turn converted into ASCII text by a process called uuencoding. Each chunk is then posted on a discussion group as a message. Certain news groups are usually devoted entirely to warez and their names make them easy to find. Usenet groups have names based on the topics they cover. For example, there is an astronomy discussion group called sci.astro. Warez newsgroups typically have names starting with "alt.binaries." The group alt.binaries.gamez, for instance, is devoted to pirated games. In order to download a file from one

of these groups, a person tags all of the files' chunks, downloads them, and then uses a program called a uudecoder to reassemble them into the original file. This entire process was manual, required several different programs, and the knowledge to use each one. Today there are websites such as www.newzbin.com, which indexes the files on Usenet and gives an individual the ability to search for a program and then download a “.nzb” file containing indexes for all of the pieces of the program and the groups from which to download them. To use the .nzb file, one simply opens it with a program such as Grabit, available from www.shemes.com, which takes care of downloading and reassembling the individual messages into the original files. In fact, this is more complicated than many of the other methods for obtaining warez such as BitTorrent, discussed later. I suspect this is one of the reasons that Usenet as a tool for “warez’ing” remains somewhat obscure (“What is Usenet?”).

Given the modern conception of software piracy, it is small wonder that few people realize how much organization is involved. The people involved in the creation and distribution of warez are referred to collectively as “the scene” or “the warez scene.” The scene consists of various groups and individuals with different functions in bringing out a release. Some of them, like courier groups or cracking groups, may function on their own, but often larger organizations called release groups will manage the entire process (“Warez (scene)”). Release groups compete with each other to bring releases to the scene first and every one is tagged with information identifying who was responsible for the end product. This information is found in an “.nfo” file, which almost always accompanies a release. In addition to the group’s name, .nfo files contain information about the individual release such as the title of the software, the company that produced it, aliases of the individuals involved, information on how any copy protection was

broken, instructions on how to install the release, etc. These files also will advertise for services that the group requires. Here is an example of such an advertisement:

```

B UUUU° °UUUU B
°ZUUUB°BU° °UB°BUUUZ°
°ZUUU° 2 2 °UUUZ° °° Ü
°UUUU° Ü ÜZÜ Ü °ZUUZ° ° ° °ZUUZ° ÜZÜ Ü °UUUU°
°UUU°BU °UU B °Ü °UUU° °UUU° °Ü B °UU° UB°UUU°
°UUUZ° °UU ° UUU° UUB °UUU° UUUZ BUU °UUU°°UU° ZUUU°
°UUUZ°°UU°°ZUUUB° UUZ°°UUU° ... TBE NEWS ... °UUU °ZUU° BUUZ °UU°°ZUUU°
ZUUUZUUZ°ZUUZ° UU°UUUU° ~~~~~ °UUUU°UU° °ZUUZ°ZUUZUUUZ°
°BUUUUB° °ZUUU° °UUUUU° UUUUU° °UUUZ° °BUUUUB°
BB Ü °BBB BBB BBB Ü BBB° BB
°B ° B B ° B

```

We got several positions to fill, if at least one of the following characteristics fits to you:

1. You work at any reseller, distributor or software company and have access to new software
2. You are a talented cracker (Dongles, SecuROM, VOB/Protectcd, ppc...)

Here the group is asking for people who are able to be suppliers and crackers. In order for a movie, song, or piece of software to be released, a legitimate copy must first be secured. This is the job of the supplier. Once a copy has been obtained through legitimate or illegitimate means, the supplier hands it off to a release group via an Internet drop site. According to the DOJ, suppliers are often “company insiders who have access to final versions of the companies [sic]

new software products before their public release date” (“Illegal 'warez' organizations and Internet piracy”), (“Releasegroup Structure”), (“Warez(scene)”).

Once a release group has secured a copy of a piece of software, they are then faced with the challenge of circumventing any copy protection the product may have. This is the role of the cracker, whose job is by far the most technically challenging, and these people are almost without exception skilled programmers (“Software cracking”). Software companies spend a large amount of time and money on copy-protection schemes and crackers so far have been very successful at breaking almost everything the software industry has thrown at them. I will discuss a few common copy-protection schemes here and the methods used to bypass them.

One common method of copy protection is the use of a serial-number system in a process called registration. In order to unlock or activate a piece of software, a user must enter a number, which itself is often generated via a mathematical algorithm known as a hash function. This algorithm takes one piece of information such as the user's name and converts it into a unique number or code. Companies will often invent their own hash functions. Without knowing the details, it is impossible to guess a serial number for a given input. One method used to bypass this form of copy protection is to distribute the software with a known serial number. However, there may not always be one that is known, or programs may “call home” by contacting the manufacturer over the Internet and checking that the number has not already been used. This makes it necessary for the cracker to write a program called a key generator, or keygen for short, which allows a user to enter the input and generate the corresponding serial number. To write a keygen, the cracker must figure out, often through reverse engineering, the algorithm used by the manufacturer. Keygens used to be more common than they are today, partly due to the ability of

programs to activate online. Nowadays, during registration the program checks with the manufacturer that the key was indeed supplied by the company and not generated by someone else. Keys can also be checked against a list of known pirated keys in a sort of online activation blacklist.

Another variant of this form of copy protection involves a challenge response system where the user must enter, online or over the phone, a special code supplied with the software. The manufacturer then supplies a response code that must be entered into the program. This type of protection can also be defeated via a keygen, but because of the increased complexity, programs called cracks, which modify the original program, are often used instead.

Another and more difficult-to-break form of copy protection is the dongle. Because of their efficacy, dongles are often used to protect very expensive programs. A dongle is a phallic piece of hardware that must be connected to a computer for a program to work. Modern dongles are usually connected to one of a PC's USB ports. A simple type contains an encrypted software license key. Crackers can sometimes circumvent these types of dongles by writing cracks that modify the program in such a way that the portion of the program's code that checks the license key is bypassed. The difficulty of this task depends on how securely the dongle code in the program was written and on the skill of the hacker, but it is generally considered simpler than cracking another class of dongles known as cryptoprocessors. A cryptoprocessor dongle contains a specialized microprocessor and is responsible for executing a portion of the program's code. Without the dongle, the program cannot run because a piece of hardware required to run it is missing ("Dongle").

One interesting case of dongle protection is the confrontation that went on between Steinberg, a manufacturer of audio software, and a cracking group named H20. Steinberg's bread-and-butter product is a program called Cubase. This is a type of program called a DAW or Digital Audio Workstation that allows a person to produce music on their computer. Cubase has evolved through many releases since 1989 and most of these have involved some sort of dongle protection, all versions of which were routinely broken by crackers until the release of Cubase SX 3.1. This program, which used a new cryptoprocessor dongle from a company called Syncrosoft, proved a real challenge to the audiowarez (music warez) scene. Finally, nine months after the release, an eternity in the warez world, H20 released a crack. Their solution was to write a dongle emulator, a program that replicates the function of a processor in software. H20's emulator perfectly replicated the function of the cryptoprocessor on Syncrosoft's dongle. This was considered a monumental achievement in the audiowarez scene. Not only did it require an astonishing amount of technical knowledge about the inner workings of the dongle, but they also had to break the encryption protecting its contents in the first place. How they achieved all this was never made public, though it has been speculated that they did it with inside knowledge. H20 was so proud of their achievement that they made it a point to publicly gloat prior to releasing the cracked version of Cubase onto the scene. In a teaser music video posted before doing that, H20 taunted Syncrosoft by playing samples of a Syncrosoft commercial extolling the benefits of their copy protection product while displaying images, many vulgar, meant to express how thoroughly they had beaten Syncrosoft's system (Steinberg Cubase), (H20 SYNCHROSOFT TRAILER), (Syncrosoft eLicenser).

Distribution of a release onto the scene is the job of the courier and is the final link in the chain of events. A courier, who may be a member of a group formed expressly for this purpose,

is often the low man on the totem pole in the warez scene. A courier can gain the trust of release groups by quickly and efficiently distributing releases of software (“Topsite (warez)”). Two of the original ways to distribute pirated software were via floppy disks and BBS's. Floppy disks would be enclosed in envelopes and mailed between groups or individuals in a practice called mail trading. This was particularly popular in Europe (“Warez (scene)”). BBS warez trading, on the other hand, was slightly more convenient. Couriers would connect to warez BBS's, which often appeared as legitimate BBS's to those without “privileged” accounts, to upload the latest releases. Once software was on a BBS, it could be downloaded by other groups or individuals. Historically, the main distribution channel for warez, which still exists today, is through FTP servers, which became the direct successor to the use of BBS's. FTP or File Transfer Protocol is a technology whose sole purpose is to make online storage and retrieval of files easy. Files from an FTP server can be downloaded and uploaded with a program called an FTP client. Warez groups store their loot on high-speed, often compromised FTP servers known as Topsites. These are seeded with a group's releases by the couriers and serve as hubs for distribution into the wider warez scene. Warez groups often become affiliates of several Topsites in order to have their releases distributed efficiently. Because many groups upload their releases onto these servers, the collection of warez on a Topsite would become very large (“Topsite (warez)”). According to the DOJ, some of the Topsites hosted as many as 25,000 individual titles (“Illegal ‘warez’ organizations and Internet piracy”). These collections remain available until the sites are discovered and taken down. Therefore, measures are taken to prevent them from being discovered. The simplest is the obfuscation of filenames, as discussed in the beginning of this paper. Another is by limiting access to the sites to specific IP addresses and allowing communication with the site through secure encrypted connections only (“Topsite (warez)”).

After a release is uploaded into the warez scene, it is made available to the common person. Today the primary method for the public to access warez is through the use of peer-to-peer networks, file-trading systems where users transfer files among each other. Two of the originals that gained wide public acceptance were Napster and Kazaa. These programs allowed users to search for files and then download them from whoever happened to have a copy. Napster was used purely for trading music, but Kazaa hosted files of every type: software, movies, music and more. Because of legal pressures, today Napster and Kazaa have both become legitimate businesses (“Kazaa site becomes legal service”), (“Napster”).

The current preferred peer-to-peer technology is BitTorrent. In this protocol, a file is available as a series of chunks. When a person initially shares a file on the BitTorrent network, that person becomes known as a seeder for that file. To do this, the seeder creates a torrent file, which is then uploaded to a special server known as a tracker. Other users can then download this torrent, which enables them to retrieve chunks from the seeder. Every chunk that the user downloads then becomes available to other users on the BitTorrent network and less of the file needs to be downloaded from the original seeder. Once a user has all the parts of the file he is downloading, then he becomes a seeder as well. Because every user is a download source, the more popular the torrent, the faster the download of that files will be. Torrents often end up on multiple trackers and the decentralized nature of the file transfers makes it almost impossible to discover the actual origin of the file (“Warez”), (“The BitTorrent Protocol Specification”).

In this country and most modern nations, software piracy is illegal and in many countries such as the United States, the law is enforced. It is therefore in the best interest of software pirates to maintain their anonymity online. There are several ways in which they do this. First,

the members of a warez group seldom know each other and only refer to each other through aliases. Second, communication occurs anonymously. One of the primary methods for doing this is through the use of IRC channels. IRC or Internet Relay Chat is a protocol that allows a person to join “channels,” which are chat rooms where they can communicate with many other users simultaneously. Warez groups will often have their own IRC channels that are invite-only, meaning that unless someone lets you join, you cannot see the discussions in that channel. IRC channels are hosted on IRC servers (“TopSite (warez)”), (“The IRC Prelude”). When connecting to these servers, software pirates take care to ensure that their connection cannot be traced back to them. This is often done with the use of shell accounts and proxies. A shell account is an account on a remote computer, usually a Unix or Linux machine, that a person can connect to in order to run programs. These shell accounts can be secured either legitimately and often for a fee, or by hacking into a host. From the shell account the user can then run an IRC client to connect to the IRC server. In this way, if the connection is traced, it is only back to the Shell account. Furthermore, it is desirable for the user to find shell accounts that do not keep connection logs, as this will prevent the account from being easily traced to his actual location. If the shell account server does keep logs, steps will often be taken by the user to disrupt the logging. Proxy servers accomplish the same effect through different means. A proxy server is a computer that will reroute a connection, making that connection appear as if it came from the proxy server.

Even though people on the scene are careful to prevent their activities from being traced, busts do occur. An investigation of note is Operation Buccaneer, which was started in 2001 and is ongoing today. This is a coordinated international effort headed by the U.S. Department of Justice and the U.S. Customs Service. Raids have been conducted at five U.S. universities,

several software companies and in Canada, Britain, Australia, Finland, Norway and Sweden. As a result, seventeen people were convicted on felony charges of conspiracy, aiding and abetting, and criminal copyright infringement. Additionally, many servers containing terabytes of data were confiscated.

Operation Buccaneer directly targeted release groups. One of the more famous groups whose members were prosecuted as a result of the bust was called Razor1911. They have been around since the early 1980's, when they gained fame cracking video games for the Commodore 64 computer system ("Razor 1911"). Razor1911 was referred to by the D.O.J as "the Oldest Game Software Piracy Ring on the Internet." The amount of software seized was estimated to be worth "hundreds of millions of dollars." The results of this bust were significant for the scene. Here is a snippet from an article on CNET:

"This is a bad hit for warez," one self-described 18-year-old programmer, who has been a member of the community for four years, wrote in an on-line chat with CNET News.com.

"Right now, every scene is at a standstill. Every one of them."

Operation Buccaneer was effective because it targeted the release groups. Fourteen months of investigation allowed undercover agents to infiltrate the scene and after the busts, the defendants were willing to divulge sensitive scene information to law enforcement officials. Other operations, which can be read about on the D.O.J website, such as Operation Fastlink and Operation Site Down, have chipped away at the warez community, but have had little overall effect as software piracy is more rampant than ever ("Former Leader of Razor 1911, the Oldest Game Software Piracy Ring on the Internet, Sentenced"), ("The Investigation"), ("FBI raids cripple software pirates"), ("Operation Buccaneer").

So what are the ethical implications of software piracy? There are many reasons that people engage in this activity. A common justification is that the software costs too much and is of poorer and poorer quality. In the video game industry, for example, it is not uncommon for a game to be unusable right out of the box. The buyer must go online and download a patch before the game can even be played. A Google search for “video game patch” will return literally thousands of results of patches that fix major issues such as game crashes and computer lockups. Rampant bugs such as these are obviously frustrating for computer users, but does it justify what is legally recognized as theft? Let's evaluate this scenario from a Rule Utilitarian perspective. Even if we disregard the fact that most people agree theft is wrong, it is obvious that when people steal software, the profits of the software companies are affected. It has been estimated that as of 2003, losses due to software piracy added up to 10 billion dollars a year. The software companies in turn have little choice but to raise prices, which hurts all software consumers (“How cyber piracy affects you”). Also, with fewer people purchasing software, there is pressure on manufacturers to bring their software to the market even quicker in order to compete with other companies in a smaller market. This results in rushed products with more bugs. The solution actually contributes to the problem. When looked at from this perspective alone, it is clear that software piracy is unethical.

Another reason used to justify this behavior is that given the price of software, a person should have the opportunity to try a piece of it before they purchase it. I myself have purchased programs many times only to be disappointed by their quality. Unlike other types of products, most retailers do not allow refunds on software. If you are dissatisfied, you are out the purchase price. This line of reasoning is often used by the release groups themselves. The audiowarez group H20, for instance, uses the slogan “Try Before Buy” with their releases and usually posts a

note in their .nfo files and software installers to “Never make money with warezed software.” While I am more sympathetic to this point of view, I think the temptation to continue using a piece of software after pirating it is too great to resist. The incentive to purchase a legitimate copy is very small when you already have a free working copy. While I can only speak for myself, and acknowledging that the problems with modern software are significant, I believe the above excuses are really examples of self-deception used by people to absolve themselves of guilt over stealing. As stated at the beginning of this paper, software piracy has become very easy and the number of people doing it makes it very unlikely that any one individual will get caught. Pirating software has become somewhat of a social norm. While I agree it is wrong, it remains to be seen what the end result of “the software companies vs. the scene” will be. I suspect that like Prohibition and the war on drugs, the result could be the status quo.

Glossary

BBS	An acronym for Bulletin Board System. A BBS is a computer system running special software that allows users to connect to it via a modem. Once connected, they can perform various tasks such as downloading files, posting to discussion groups, and playing games. BBS's were popular before the rise of the Internet, but are rarely in use today.
BitTorrent	A popular and widely used peer-to-peer file-sharing system. Files to be shared are divided between the users sharing and downloading them. As a user obtains chunks of the file, those chunks become available to the BitTorrent "swarm." Because each user contributes their portion of the download to the network, the more popular a file is, the faster that file can be downloaded.
Courier	A person responsible for distributing "warez" onto the "scene."
Crack	A program written by a cracker for the purpose of bypassing another program's copy protection.
Cracker	The person with the responsibility of cracking a program's copy protection scheme.
Dongle	A hardware-based form of copy protection. A dongle is an external device that connects to a computer running the copy-protected software. Dongles use various methods of protection such as hosting encrypted license keys and providing them to the software when required.
FTP	File Transfer Protocol. A protocol which defines a method for hosting files on the internet. FTP specifies a host-client system in which the files being hosted are visible in a directory structure to the client.
IRC	Internet Relay Chat. An Internet application in which "Chat rooms" are hosted on a network of servers. Users with IRC client programs can connect to these to communicate and share files with each other.
Kazaa	An early popular peer-to-peer application used for sharing files. Kazaa was notorious for being packaged with malware.
Keygen	A program used to generate a license key for use in defeating the copy protection of programs that require them.
License key	A number or series of digits and/or letters used as a form of copy protection. It is also known as a serial number. A serial number can be unique to an individual user or organization.
Napster	The first widely popularized peer-to-peer application. Napster was used for sharing music files with other users.

NZB file	A file format used by modern Usenet client software. An NZB file lists all of the individual pieces of an encoded file and the newsgroups from which they can be downloaded.
Peer-to-peer networks	Peer-to-peer networking is a model in which the client programs communicate directly with each other. This is in contrast to the traditional server-client model in which client computers connect to another computer known as a server.
Proxy server	A computer which “proxies” internet connections for another computer. Computers running their internet connections through a proxy server are essentially invisible to the Internet. Their connections appear to be coming from the proxy server itself.
Shell account	A text-based account on a remote computer. A shell account allows the hosting computer to be used remotely.
Supplier(s)	Individuals or organizations which supply original copies of software, music, and video to the warez scene.
The scene	The collective name for operations and individuals involved in the illegal procurement and distribution of digital copy-protected material.
Topsite	Usually an FTP server, it serves as a major hub for the storage and dissemination of warez.
Usenet	An Internet application in which “news servers” host “newsgroups,” which are online discussion groups. Each newsgroup is dedicated to a specific topic. Users can subscribe to the newsgroups in which they are interested. The original purpose of Usenet was perverted as users found ways to post files instead of messages to the newsgroups. This allows Usenet to be used for the sharing of warez.
Warez	Refers to pirated software, music, movies or any other digital copyrighted product.

Bibliography

“The BitTorrent Protocol Specification.” *BitTorrent.org*. 28 February 2008, 10 Dec 2008

<http://www.bittorrent.org/beps/bep_0003.html>

“FBI raids cripple software pirates.” *CNET News*. 19 Dec 2001 11:50 PST. 10 Dec 2008

<<http://news.cnet.com/2100-1023-277226.html>>

“Dongle.” *Wikipedia, The Free Encyclopedia*. 3 Dec 2008, 16:33 UTC. 10 Dec 2008

<<http://en.wikipedia.org/w/index.php?title=Dongle&oldid=255654561>>.

“How cyber piracy affects you”. *BBC NEWS*. 9 April 2003, 10:18 GMT. 10 Dec 2008

<http://news.bbc.co.uk/2/hi/uk_news/2924531.stm>

“Illegal ‘warez’ organizations and Internet piracy.” *Operation Buccaneer*. 10 Dec 2008

<<http://www.usdoj.gov/criminal/cybercrime/ob/OBorg&pr.htm>>

“The Investigation.” *Operation Buccaneer*. 10 Dec 2008

<<http://www.cybercrime.gov/ob/OBinvest.htm>>

“The IRC Prelude.” *irchelp.org* 1 June 2000. 10 Dec 2008

<<http://www.irchelp.org/irchelp/new2irc.html>>

“Kazaa site becomes legal service.” *BBC NEWS*. 27 July 2006, 11:51 GMT. 10 Dec 2008

<<http://news.bbc.co.uk/1/hi/sci/tech/5220406.stm>>

“leetspeak” *Netlingo The Internet Dictionary*. 2008, 10 Dec 2008

<<http://www.netlingo.com/lookup.cfm?term=leetspeak>>

“Napster.” *Wikipedia, The Free Encyclopedia*. 8 Dec 2008, 04:31 UTC. 11 Dec 2008

<<http://en.wikipedia.org/w/index.php?title=Napster&oldid=256559605>>

“Operation Buccaneer.” *Wikipedia, The Free Encyclopedia*. 19 Sep 2008, 02:56 UTC. 11 Dec

2008 <http://en.wikipedia.org/w/index.php?title=Operation_Buccaneer&oldid=239450040>.

“Razor 1911.” *Wikipedia, The Free Encyclopedia*. 8 Dec 2008, 19:55 UTC. 11 Dec 2008

<http://en.wikipedia.org/w/index.php?title=Razor_1911&oldid=256680368>.

“Software cracking.” *Wikipedia, The Free Encyclopedia*. 25 Nov 2008, 03:37 UTC. 10 Dec 2008

<http://en.wikipedia.org/w/index.php?title=Software_cracking&oldid=253934926>.

“Steinberg Cubase.” *Wikipedia, The Free Encyclopedia*. 5 Dec 2008, 00:04 UTC. 10 Dec 2008

<http://en.wikipedia.org/w/index.php?title=Steinberg_Cubase&oldid=255941293>.

“Syncrosoft eLicenser.” *Syncrosoft crypto & security solutions*. 10 Dec 2008

<http://www.syncrosoft.com/Syncrosoft_eLicenser-78-30.html>

"Topsite (warez)." *Wikipedia, The Free Encyclopedia*. 23 Nov 2008, 20:27 UTC. 11 Dec 2008
<[http://en.wikipedia.org/w/index.php?title=Topsite_\(warez\)&oldid=253651190](http://en.wikipedia.org/w/index.php?title=Topsite_(warez)&oldid=253651190)>.

"Warez." *Wikipedia, The Free Encyclopedia*. 7 Dec 2008, 16:20 UTC. 10 Dec 2008
<<http://en.wikipedia.org/w/index.php?title=Warez&oldid=256435533>>

"Warez (scene)." *Wikipedia, The Free Encyclopedia*. 15 Nov 2008, 02:30 UTC. 11 Dec 2008
<[http://en.wikipedia.org/w/index.php?title=Warez_\(scene\)&oldid=251891055](http://en.wikipedia.org/w/index.php?title=Warez_(scene)&oldid=251891055)>

"What is Usenet?" *faqs.org*. 10 Dec 2008
<<http://www.faqs.org/faqs/usenet/what-is/part1/>>

"Former Leader of Razor 1911, the Oldest Game Software Piracy Ring on the Internet,
Sentenced." *U.S. Department of Justice*. 6 June 2003. 10 Dec 2008
<http://www.cybercrime.gov/pitmanSent.htm>>