Warez All that Pirated Software Coming From?

Date: Nov 1, 2002 By Seth Fogie. Article is provided courtesy of Prentice Hall PTR.

In this world of casual piracy, many people have forgotten or just never realized where many software releases originate. Seth Fogie looks at the past, present, and future of the warez industry; and illustrates the simple fact that "free" software is here to stay.

NOTE

The purpose of this article is to provide an *educational* overview of warez. The author is not taking a stance on the legality, morality, or any other *.ality on the issues surrounding the subject of warez and pirated software. In addition, no software was pirated, cracked, or otherwise illegally obtained during the writing of this article.

Software piracy is one of the hottest subjects in today's computerized culture. With the upheaval of Napster and the subsequent spread of peer-to-peer programs, the casual sharing of software has become a world-wide pastime. All it takes is a few minutes on a DSL connection, and KazaA (or KazaA-Lite for those people who don't want adware) and any 10-year-old kid can have the latest pop song hit in their possession. As if deeply offending the music industry isn't enough, the same avenues taken to obtain *cheap* music also holds a vast number of software games and applications—some worth over $10,000.

While it may be common knowledge that these items are available online, what isn't commonly known is the complexity of the process that many of these "releases" go through before they hit the file-sharing mainstream. For example, on September 15, 2002, Unreal Tournament 2003 was available to download online. What makes this surprising is that the game was not even available in stores, and wouldn't be for at least 10 more days. However, if you looked in the right places, you could find a fully functional version of Unreal Tournament in 65 x 15MB files ready to be downloaded and installed. And if you were worried about serial numbers or time limits, this was no problem! Another quick download of the Unreal 2003 patch and the newly *found* game would be semi-fully registered.

At this point, several questions might be on your mind. One, how and why was this game available for *free* before it was officially released? Second, where did a patch come from that makes any protection obsolete? And third, why are there 65 files!? This article will touch on each of these questions and more as we take a walk through the software-piracy process.

Warez Overview

Casual piracy has been around since before most of the readers of this article were even out of high school. It all started many years ago, when the purchase of a PC became a reality for homeowners. In those days, software was passed around like a good joke. One person would buy it, and they would subsequently make copies of it on their 5-1/4-inch floppy drive. They would then pass this copy on to their friends and family members. Obviously, we aren't talking about some highly technical routine or process. However, the ease of software duplication made it equally as obvious to software developers that they should incorporate some form of protection into their software.

Thus, the concept of the install-counter and serial number was applied to software development. Most everyone is familiar with serial numbers, which are used as digital keys to unlock software. Install-counters, which many are not aware of, keep track of how many times a product is installed and restricts any installations over a set number (allowing for reinstalls). In theory, this should stop the spread of the files by ensuring that a program is restricted to its local area. However, it didn't take long after protection was introduced that a cracking subculture was formed to handle this obstacle to free software. While the initial cracks were nothing more than finding ways around software protection, such as making copies of software before installation or just copying installed files straight from a computer, this attempt at curbing the free distribution of software lead to advanced protection techniques, and eventually encouraged the creation of advanced cracking groups. It was about this time that pirated software picked up a nickname: *warez*. Obviously related to the word "softwares", warez became a slang word used to describe all software obtained for free through the digital

underground.

As technology changed, the floppy disk size changed from 5-1/4-inch to 3-1/2-inch. It was during this time that the dialup Internet started to become more popular—and with it the Bulletin Board System (BBS). Using a modem and phone connection, something many of the kids today will never have to experience, a computer user could connect to another computer and upload, download, or just look through someone else's files. At this point, piracy began to pick up speed as more and more people were turned on to the online experience.

Now, instead of relying on a friend at school to hook you up with the latest copy of whatever hot game was out, you could dial up a BBS and download the warez'd game. Unfortunately, this often required the use of a long-distance line, which was quite costly. However, in the same way that copy protection created a need for crackers, the need for free phone service created a need for phone hackers, also known as *phreakers*.

While this is beyond the scope of this article, phreaking is the "art" of obtaining phone service for free. If a person could achieve this, they could essentially dial up any BBS in the world and download whatever files existed at that site without worrying about long-distance phone service. I am quite sure that many an unsuspecting victim complained to their phone company about huge phone bills as a result of their phone line being hijacked for BBS purposes.

The BBS eventually evolved into the Internet we know today. However, this development brought with it a whole new wave of threats for the software makers. No longer did users have to connect to a remote BBS to download software; instead, they could simply use an Internet connection through Prodigy or another Internet Service Provider (ISP) to connect to a remote computer, thus avoiding long-distance calls. However, this freedom was short-lived because the introduction of the CD-ROM threw a small wrench into the piracy industry...at least, it first appeared that way.

The biggest problem software developers had, prior to CDs, was size limitation on their software. For example, Windows 95 came on roughly 30 floppies, which was expensive to ship and produce. Although other programs didn't typically take as many floppies, more money was wasted on getting the program to the consumer with each additional floppy. However, this increase in size also helped to reduce the ease at which a program could be freely passed out to others. Therefore, once the CD hit the market, developers quickly bloated their software with large files, making it very annoying for software pirates to spread the software around. For example, can you imagine how long it would take to download Windows 95 on a blazingly fast 14.4K modem (or if you were lucky, a 28.8K modem)? The need for a solution once again caused another evolution of the software underground, however, from which the art of packing 600MB into 50MB became a viable skill.

Currently, software piracy has taken on a new life, and there seems to be no end in sight. Thanks to connections that can deliver a program in a few hours using high-speed Internet connections and the creation of simple peer-to-peer programs that make sharing software as easy as pointing and clicking, anyone can find the latest copy of Photoshop 7 or Dreamweaver MX to add to their personal collection of software. This technological advance has also impacted the piracy underground, in which it is possible to pass full CD images from one computer to another, thus eliminating the need for repacking. Although the packing of software is no longer as serious an issue, protection is becoming more advanced with phone-home registrations processes—as used by Microsoft's Windows XP. Again, software-cracking is beyond the scope of this article, but it will be touched on briefly in the next few pages.

Obtaining Warez

> "PARADiGM is looking to fill its ranks. Contact us now if:-you can supply unreleased new games"

This is a portion of a text file that was included with a warez'd game. The warez group, PARADiGM, uses the nfo file (nfo for information) included with the release of a game to gather supporters for its group. This example illustrates the value that unreleased games have within the warez community. If a group can release a game before it hits the shelves, it will "one up" the other groups. However, this takes having connections with the right people in the right places. A mole in a software-development shop or at the CD factory can easily, with low risk, pass the program on to the warez group. In return, the mole gets access to an infinite supply of free software provided by other such moles; they're all free, and *fully* operational (with the right crack).

However, if a software release is not well-known, or if there are no moles waiting to pass on the goods, the next obvious place to get free software is from a slightly crooked software store employee. All it takes is one night with a CD, which is typically a perk of

working in a software store, and a program can be copied and uploaded to a waiting warez group. While this method may not carry the same weight as "pre-release," if a group can get the program to the warez underground first, it can still gain some respect points. However, this takes having a cracker on staff that can quickly take a protected CD and strip off any protection schemes built into it.

Cracking

The art of cracking could fill a book by itself. In short, this is the process of debugging a program, with one small twist on the concept of debugging. Instead of targeting errors in a program, crackers target the key points in a program that perform security and anti-piracy checks. This is done using programs such as IDA Pro, Hex editors, and Softice to systemically work through a program and follow each execution thread to its end. By using cracking tools and knowing how to hook into a program, a good debugger can produce a crack for a program in a few hours. This type of activity is so productive that almost EVERY software title available for purchase (or download) has a corresponding crack that disables any anti-piracy protection.

For example, Warcraft 3, which hit the shelves this summer, can be downloaded in its full form from various sites online. Included in the unpacked files is a folder labeled "Razor1911" (another warez group). This folder includes two programs written by crackers that are used to bypass the piracy checks of the game. The first is a key-generator program that creates random serial numbers that are needed by the Warcraft 3 game to validate the installation software. In addition to this little program, the main executable files of Warcraft 3 have replacement files that were altered to allow Warcraft 3 to run without an original CD.

Needless to say, software developers are aware of these cracks, and are constantly searching for ways to stop crackers from subverting their protection schemes. Due to this vigilance, the warez groups need dedicated and smart crackers who are willing to debug software and find the loopholes in the software needed to bypass the latest protections. In addition, these same crackers need to be able to understand Assembler language and to re-create algorithm-type functions to create serial generators such as the one used with Warcraft.

Like the call for help for PARADiGM provided, the following is an example of a shout out for assistance from another major warez group, ORIGIN.

> "We are also currently looking for several PROVEN crackers and trainer makers to join the team. Can you do SAFEDISC/C-DILLA or SECUROM or VOB protections? What about quality menu driven trainers? Contact us NOW! Use the contact information below."

Safedisc/C-Dilla, SecureROM, and VOB are all protection methods used by software distributors to stop people from making illegal copies of their CDs. If a CD is copied, and one of these methods of protection is used on the CD, the copy won't be accepted by the game as a legitimate copy. Using proprietary methods for hiding data in subchannels or disguising the data in other ways, CD protection schemes attempt to thwart would-be pirates from making copies.

Unfortunately, each of these methods leaves its signature behind on the CD, which makes detecting it rather easy. For example, Safedisc/C-Dilla can be quickly spotted because the CD will typically contain a file named "00000001.TMP".

Ironically, many of these disks can still be copied by just using the right CD-creation software. There are even "backup" programs available that will allow a person to copy their CD as a single file and then mount the file as a fake CD-ROM. For example, Daemontools.com provides one such program that is fully legal as a CD backup tool, but also can be *abused* to bypass all of the major protection schemes.

Packing

Once a program is cracked, it is time for packaging. While broadband users have an easy time downloading 600+ MB files, the rest of the world has to be able to download files using their 56K dialup connection. Obviously, attempting to download a 600MB file would not prove to be very successful, and if it were, the time required would extend into days (if not weeks) for most titles.

To assist these users, there are rules that most e*lite* warez groups abide by when releasing a program. At times, these groups form an alliance that is then used to set a standard. For awhile, one such group was known as the Faction, which had a set of 10 rules that standardized the release of games. While there are various releases that don't follow these guidelines, the warez groups attempt to stick to the rules. In fact, these pseudo rules often become a point of competition for many warez groups. The number

of files, total size of release, and number of features left in the release are important in determining the quality of the release.

To clarify the ripping process, let's walk through the steps required to turn a 600MB game into a 200MB release. The first thing a group would have to do is determine how to circumvent the piracy protection. This typically doesn't add in any space, but must be considered and included in the final release. Next, a group must determine what the final release can do without. Obviously, any additional extras such as DirectX installation files can be immediately removed. Next, all the sound files, which more often than not are extra-large WAV files, are converted to MP3 files, and a converter program is added to reconvert the MP3s back to WAV files on your computer. Next, the game is examined for movie files, sound files, song files, or any other files that are not necessary for game play. If a game can do without a certain type of file, it is removed, and a patch is included that ensures the game won't attempt to use a missing file. However, a warez group will be very cautious about removing any of these files because it affects the quality of the release. Fortunately, a warez group can gain back some points by providing a separate release that includes just the sound or movie files.

Once the game has been laid bare, an installation script is written, and an installer is added to the files, the installation process becomes a simple point-click operation. For example, Figure 1 shows an old installer used by the CLASS group. This installer and others are available at shareandenjoy.com for you to view and be amused by. One of the things to observe in this example is the subtle hint ("Myth sucks") that is delicately placed in the snow. Again, this example illustrates the deep love shared between the various warez groups.

Figure 1 CLASS warez installer (notice "Myth sucks" in the snow).

NOTE

there is no guarantee that the files on this site are not riddled with Trojans or viruses.

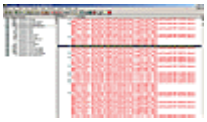
At this point, the final task of taking all the files and packaging them up into distributable sections is undertaken. Again, there are rules and guidelines provided that determine how many of these files can exist and how big each file can be. Early in the days of warez, the file size was small (1.44MB) due to limitations on download speed. However, this size has increased several times and is currently at about 15MB. In addition to the size limit, the entire package must fit in a limited number of files. This is to facilitate the spread of the files to dialup modem users; just imagine the annoyance of trying to download a 200MB file! Thanks to some organizations, a computer user can now just download a series of 15MB files, one at a time; and because the files are statically sized, incomplete files are easily spotted and can be replaced.

It should be noted that the last few years of the 20th century brought an ISO scene that did much of the same type of gathering and cracking activities. This evolved into the current bin/cue scene, which is just another format for CD image creation. Regardless of the label, all formats of warez require the same basic steps of collection, cracking, packing, and distribution; with slight variations at each stage.

Distribution

Distribution of warez is by far the most commonly known stage that all pirated software goes through. In short, this is the point of no return for the program that has been obtained, cracked, and packaged. Once at this stage, a warez'd program becomes part of the public domain, regardless of any legal issues. Using a seemingly unending supply of methods, pirated software spreads like wildfire: First through the warez underground and then onto the Internet via file sharing program, FTP sites, and even commercial file storage service sites.

When first released, the warez'd program is used by couriers as a bartering power for other newly released programs. This ensures that the major groups all have the latest games, applications, and movies. From here, the warez spreads in several directions. Private FTP sites are typically updated next, with IRC channels soon to follow. After this, file-sharing services such as Direct Connect, KaZaa, and Bearshare are updated with final posts to the alt.binary news groups (see Figure 2 for an example of Warcraft 3 posted in a newsgroup). Once these locations are all spreading the release, the World Wide Web becomes the last in a long string of distribution methods.



Warcraft 3 posted in a newsgroup.

If you are wondering why anyone would bother setting up websites and uploading mass amounts of data to the WWW, the answer is

two-fold. First, the Internet provides a quick and relatively anonymous playground for warez distribution. The second and most common reason is based on the fact that warez attracts surfers like a hacker conference attacks black-shirted computer geeks. Due to this, most of the popular warez sites are completely surrounded by porn advertisements, which is ironically one of the most popular reasons people get online in the first place. In fact, some warez sites will send a browser into a spastic fit of porn overload as a warez site triggers popup after popup. And if the initial barrage of smut isn't enough to annoy the warez searcher, 10 more popups take its place when the unsuspecting surfer attempts to close a window. In other words, a warez search can quickly become a frustrating power struggle between man and machine, typically resulting in the infamous three finger salute (Ctrl-Alt-Del).

While this is a very annoying experience for the surfer, the deceitful warez provider is happily collecting cash for each window that opens and each click that occurs. In addition to the direct financial rewards, each site is in a competition to get to the top of several "Top ##" lists, which helps to increase the number of visitors coming back into the porn trap. Note that if this ever happens, the quickest and easiest thing to do is hit Alt-F4, which will close the active windows one at a time until order is once again resumed.

Regardless of all the misleading sites, if a person diligently searches long enough, they will eventually find a site that has working downloads. However, even these sites are performing digital sleight-of-hand tricks; if a person looks close enough, they will see that most of the files they are downloading are not actually coming from the site where they are. Using various tricks of the trade—which involve using Java-based proxy programs, sites such as GeoCities and Yahoo, online file sharing services, and even hacked computers—warez distributors can post their files anonymously and without fear of legal repercussion. After all, they are only providing links to the warez, not the warez itself. While these downloads are usually spotted by the true host and taken offline within hours, they still manage to serve up thousands of files a day.

The Future

The point of this article is to illustrate the amount of time, expertise, and dedication that goes into the distribution of warez. Hackers and crackers have always been at the forefront of technology. Without their dedication and rebellious activities, this world would not have many of the items we take for granted, including the methods and techniques by which warez is created and spread. For example, peer-to-peer software is now being eyed by businesses as a viable method for making money. To illustrate, Napster was recently targeted by a porn company as a potential method of creating a peer-to-peer porn distribution service.

While warez seems to be growing at a phenomenal rate, there are several attempts being made to stop the cracking and spread of pirated software. However, they are mostly targeted at the more common means of distribution, such as KaZaa; and by strong-arm tactics, as demonstrated by the infamous Business Software Alliance. In addition, the FBI is targeting some of the more well-known warez groups, such as the recently dismembered Drink or Die. Regardless of the attempts of various governments, will this actually make an impact on the spread of pirated software?

The answer to this is a resounding no. The simple fact remains that hackers and crackers remain one step ahead of the rest of the world in using new technologies and abstract concepts to their advantage. For example, imagine that there is just one small country in which hacking, cracking, piracy, and porn was legal. Not only legal, but what if a country made this its sole method of financial income? Well, this has already happened! HavenCo, Inc. (http://www.havenco.com) operates out of a small but completely government-free pseudo-country. The following is the ONLY rule regarding the storage of files on their servers, which can be had for the low price of $7,500 a year:

> "Unacceptable publications include, but are not limited to: Material that is unlawful in the jurisdiction of the server. For instance, if a customer's machine is hosted on Sealand by HavenCo, content which is illegal in Sealand may not be published or housed on that server. Sealand's laws prohibit child pornography. Sealand currently has no regulations regarding copyright, patents, libel, restrictions on political speech, non-disclosure agreements, cryptography, restrictions on maintaining customer records, tax or mandatory licensing, DMCA, music sharing services, or other issues; child pornography is the only content explicitly prohibited. At the present time, child pornography is not precisely defined; HavenCo is obeying rules similar to those of the United States, specifically a prohibition on any depiction of those under 18 in a sexual context."

In other words, pirated software can *legally* be stored on their servers. In addition to earth-based server farms, how long will it be until some company figures out a way to make a profit from a similar rules-free server farm in outer space that can be accessed by satellite? And if alternative physical locations aren't enough, a new storage technique was recently found that uses ICMP (a data protocol) to store data *on* the Internet itself. In other words, at any one time there is a huge amount of data *in transit* on the Internet that could be used to hold various amounts of information. While this technique of storage is relatively new, hiding data between the cracks of the Internet is just one abstract method of distributing warez that demonstrates the futility of the many activities of the DCMA and RIAA. If a U.S. citizen can remotely control a computer in another country, are they actually breaking an American law?

In addition to the alternative methods of distributing warez, what would happen if software companies created their own cracks and gave them to the warez underground for distribution? This, in fact, has already happened! While many may find this hard to believe, one such company has taken the outlook that providing their own warez'd copy of their software will help market their name. What better way to break into the global market than to familiarize a huge base of highly technical hackers and crackers with your company's name!?

Summary

In this article, we outlined the process in which a game or application becomes warez. This is no simple and unorganized hobby that has successfully provided *free* software to the world. The release of a warez'd program takes skills and talents that most people don't even know exist, much less understand.

While the spread of warez is deemed a solvable problem, this has not yet proved to be true. The solution will not be found by plugging up the methods of distribution with legal maneuvering or counter-hacking efforts, as the RIAA is attempting to legalize. The answer will instead be found in an equally abstract or plainly simple idea that defeats the very nature of warez itself. For example, if every company provided its software for free, warez would by definition no longer be necessary. Of course, this idea isn't a realistic possibility at this time, due to conventional methods of thinking and a general lack of creativity.

Another possible solution, which is being used by major hardware creators, is to incorporate anti-piracy schemes into the very hardware required to run software. However, this too has so far met with failure, as can be seen by the complete dissemination of Microsoft's Xbox and its conversion into a cheap computer able to run Linux.

Regardless of the efforts of governments, corporations, and lobbying organizations, the general public has spoken. People want their software, music, and movies; and they are willing to do whatever it takes to get it. The prohibition of alcohol had the reverse effect of pushing drinking into the very core of the rebellious American public. This resulted in the widespread distribution and use of alcohol, and eventually led to the acceptance of drinking and reversal of the law that restricted it in the first place. Prohibition didn't stop the American people from drinking alcohol because the demand was too great, and the public didn't take it seriously. Could this historical example provide an illustration of what is to come for warez?
