> For the Inner Circle,
> cracking software is a
> challenge. For the wannabe
> underground, collecting it
> is an obsession. For the
> software industry, it's a
> billion-dollar nightmare.

Sunday morning, 7 a.m., somewhere in US Eastern Standard Time: Mad Hatter gets up, has a glass of Seagram's Ginger Ale and a cigarette, and checks his machine, which has been running automated scripts all night. He looks for errors and then reads his email. He has 30 messages from all over the world: some fan mail, a couple of flames, a few snippets of interesting information, three or four requests - some clear, some PGP- encoded. After a quick espresso and another cigarette, he surveys the contents of a few private FTP sites, filters through a bunch of new files, and then reroutes the good stuff to his newsreader. After breakfast with the family, another wave of automated scripts kicks in. The ISDN connection hums to life. A steady stream of bytes departs his machine 128 Kbps and vanishes into the ether. By the end of the day Mad Hatter, a ringleader of the software piracy group called the Inner Circle, will have poured 300 Mbytes of illegal "warez" onto the Internet.

Monday morning, 9 a.m., Greenwich Mean Time: Phil arrives for work in Bracknell, England, in a suit and tie, just back from a few days in Switzerland. Inside Novell UK's glossy five-story headquarters, he lets himself into his office. It looks like a mad, bad bedroom - shiny desktops and derelict ones, disemboweled minitowers and battered servers, every last expansion slot distended with DAT machines, CD-ROM burners, extra hard drives. A metal shelf unit contains a rack of monitors, some video equipment, spare keyboards. Everything is wired insanely to a single ISDN line. After a coffee, Phil boots up and skims his email. Twenty minutes later he has ceased to be Phil. For the next week, he will pretend to be a trader, a courier, a cracker, a newbie, a lamer, a lurker, a leecher. He is an undercover Internet detective, a "technical investigator." He spends his days roving the Net, finding people like Mad Hatter - and busting them.

This is a story about a universe with two parallel, overlapping worlds. One is the familiar, dull world of the software industry, with its development costs, marketing teams, profit, and loss. Phil's world, at least part of the day.

And then there is warez world, the Mad Hatter's world, a strange place of IRC channels and Usenet groups, of thrills, prestige, and fear. A world of expert crackers who strip the protection from expensive new software and upload copies onto the Net within days of its release. A world of wannabes and collectors, whose hard drives are stuffed like stamp albums, with programs they'll never use. And a world of profit pirates, who do exactly what the software makers say: rip off other people's stuff and sell it for their own benefit.

In Phil's world, software is a valuable tool that commands high prices - programs like QuarkXPress, Windows NT, and AutoCAD, costing thousands of dollars a shot. But in Mad Hatter's world, those sticker prices means nothing - except inasmuch as more expensive programs are harder to crack, and that makes them the most desirable, spectacular trophies of all.

In Phil's world, warez are a menace. In warez world, Phil is...

> Filthy lucre

Phil's world is full of nasty numbers. Antipiracy organizations like the Software Publishers Association and Business Software Alliance estimate that more than US$5 million worth of software is cracked and uploaded daily to the Net, where anyone can download it free of charge. A running scoreboard on the BSA Web site charts the industry's losses to piracy: $482 a second, $28,900 a minute, $1.7 million an hour, $41.6 million a day, $291.5 million a week. A lot of that is garden-variety unlicensed copying and Far East-style counterfeiting. But an estimated one-third leaks out through warez world, which can be anywhere there's a computer, a phone, and a modem.

This is bad news for the business. Think of the lost revenue! The lost customers! "It's a frightening scenario out there," says Martin Smith, Novell's product-licensing manager for Europe, the Middle East, and Africa. "We are seeing a very, very rapid development of crime on the Internet."

He's not being paranoid: look at the thousands of messages that pour through alt.binaries.warez.ibm-pc and the other Usenet sites that are the warez world's pulsing heart. In a typical week, you'll see Microsoft Office Pro and Visual C++, Autodesk 3D Studio MAX, SoftImage 3D, SoundForge, Cakewalk Pro Audio, WordPerfect, Adobe Photoshop 4.0 - virtually every high-end package in existence. All this plus impossibly early betas and alphas. Add a smattering of mundane Web tools, Net apps, registered shareware, games, and utilities, and you have everything for the forward-looking computer user.

Warez world's volumes are impressive, too - a good 65 Mbytes a day of freshly cracked, quality new releases, chopped into disk-sized portions (to make it from one hop to the next without clogging the servers), compressed, and uploaded. Postings can vary from a few bytes (for a crack) to hundreds of megabytes. The nine main warez sites alone account for 30 to 40 percent of the traffic on Usenet, an average of more than 500 Mbytes in downloads every 24 hours, according to OpNet.

Bad news indeed for Phil and his friends, gazing at those endless dollar signs. But warez world's leading citizens say that filthy lucre is beside the point - at least for them and the hungry collectors they supply.

"No money ever exchanges hands in our forum," says California Red, one of a half dozen of the Mad Hatter's Inner Circle colleagues gathered for an IRC chat.

"We're on the nonprofit side of the warez feeding chain," insists another, TAG (The Analog Guy).

"It's a trade. You give what you have, get something you need. No money needed," adds Clickety.

"We're not in it for the money. I would never sell something I got from warez," California Red reiterates.

"Never made a dime," says Mad Hatter.

Even Phil admits these are not the people responsible - not directly, anyhow - for the 500-Mbyte, $50 bundled software CD-ROMs from Asia that are the industry's most prominent nightmare. Warez crackers, traders, and collectors don't pirate software to make a living: they pirate software because they can. The more the manufacturers harden a product, with tricky serial numbers and anticopy systems, the more fun it becomes to break. Theft? No: it's a game, a pissing contest; a bunch of dicks and a ruler. It's a hobby, an act of bloodless terrorism. It's "Fuck you, Microsoft." It's about having something the other guy doesn't. It's about telling him that you have something he doesn't and

forcing him to trade something he has for something you don't.

In other words, it's an addiction. Listen to a typical dialog on an IRC warez trading channel:

"What you got?"

"Cubase three."

"What's that?"

"A music program."

"I got it. What else?"

"No, but it's Cubase three-oh-three - the latest bugfix."

"Shit. Gimme."

"It's not a patch. It's another seven meg download."

"Don't care. I want it."

Warez traders scour the newsgroups every night, planting requests, downloading file parts they don't need. Warezheads feel unfulfilled unless they've swelled their coffers by at least one application a day. They don't need this Java Development Kit tool, or that Photoshop plug- in - the thrill is in creating the new subdirectory and placing the tightly packed and zipped file cleanly, reverently, into the collection. They may even install it. Then toy absentmindedly with its toolbars and palettes before tucking it away and never running it again.

Look at Michael, an 18-year-old warez junkie who's also into weight lifting. In the evenings, while his friends pursue women, he's either at the gym or home at his machine, combing the planet for the latest dot releases of 3D Studio MAX. "I bought a Zip drive so I could store it all. The SoftImage rip is 20 disks. It took me three months to get the entire set." A directory called WAREZ on his D: drive has $50,000 worth of cracked software, more than any one person could ever use, ludicrous amounts of applications. The more high-end and toolbar-tastic the app, the better. Without technical support or manuals, he hasn't a clue how to use most of it. But it's there and will stay there. "Warez give you a weird kind of feeling," he says. "You end up collecting programs you don't need and never use. Just so you can say, 'I've got this or I've got that.' Or 'My version of Photoshop is higher than yours.'"

Mad Hatter knows the feeling. "It's an obsessive game. We see it every day - people begging for something to 'finish their collection.'" He's not much better himself. "When I was out of work on disability, I was totally motivated by the thrill of massive uploads, uploading at least 40 Mbytes a day for four months straight." Fellow Inner Circle member Clickety used to spend 12 hours a day online until college got "awful heavy." Another, Abraxas, spends 6 to 10 hours online on weekdays, 12 to 16 on weekends. But Mad Hatter - who runs the semi-tongue-in-cheek, semi-poker-faced discussion group alt.support.warez. recovery - is making progress: he's down to 30 Mbytes a day. "My computer is online 24 hours a day," he says. "A warez pirate is always online."

> As gods

For Joe Warez Addict at the end of the cracked software food chain, membership in a group like the Inner Circle is the ultimate collectible. A way to legitimize their addiction, work for the common good, and, of course, get a nice fresh supply of warez. The drug addict becomes dealer. A sizable chunk of Mad Hatter's daily mail is begging letters. "I hope that if I ask this question, you will not be offended in any way. But can I join the Inner Circle? I mean, I respect the Inner Circle ... but never got a chance to join it. I was just wondering, can I? Please mail me back ASAP."

Needless to say, this lone obsessive didn't get his chance. Joining the Inner Circle is nigh on impossible. Reaching its members, though, is easy enough. They keep a high profile, both in posting files on Usenet and flaming lamers. When I first tried to contact them I thought that they weren't so good at answering email, but it turned out their provider had just been taken offline for illegal spamming. They relocated en masse, and my mail had been lost in transit. So I posted a message to one of their newsgroups, made sure it was correctly labeled, politely worded, and not crossposted (a cardinal sin anywhere on Usenet). A reply arrived within eight hours. Mad Hatter was more than happy to talk, but not on the phone, not in person, and not on conventional IRC. "It has a bit of a habit of advertising my IP address," he said. He and six other Inner Circle members set up their own IRC server, configured a secret channel, and arranged a mutually convenient time for a live interview. We met and talked for nine hours, in the bizarre overlapping conversational style of IRC. They were frank and open, friendly and articulate - and, like any new start-up, flattered by the attention.

A 17-strong force, the Inner Circle has its own iconography and its own ideals. Its members are warez gods. They preach, police, advise, flame. Their commandments? Good manners, good use of bandwidth, and good warez. Give unto others as you would have them give unto you. When the Inner Circle is not sourcing warez from secret sites, its members are hunting and gathering from more conventional sources. Clickety borrows fresh stuff from his clients. A few have attended Microsoft Solution seminars. "Some of us are actual beta testers, too," says Mad Hatter. "That's got to be scary for the developers." One way or another, they help maintain the steady flow of warez onto Usenet. From there, various wannabes, lamers, and aspirants copy their work to countless BBSes, FTP sites, and Web pages.

These are not pimply teenagers devoid of social life and graces, little ferrets who talk in bIFF text and make napalm out of soap and lightbulbs; they're not downloading porn or being careful not to wake their parents or spelling "cool" as "kewl." According to the interviews I conducted, not one member is younger than 20; Clickety-Clack is the youngest at 23. Most are 30-plus. Champion uploader Digital has been happily married for 22 of his 46 years. Most are well-adjusted white males with day jobs and thoroughly nuclear families. Founding member Abraxas has three kids, one over 18. Mad Hatter runs a small business from home. Technical guru TAG is a computer animator. Irrelevant maintains commercial real estate. They're spread all over the United States. A few are concentrated around Orlando, Florida. Two or three others are California-based. For obvious reasons, that's as precise as they like to get.

The Inner Circle was born of a sense of outrage that their beloved pirate-wares newsgroups were going to pot. Warez had been around for more than a decade, but the growth of the Internet was bringing clueless newbies onto the boards. Warez needed a code of ethics and a group of leaders to set some examples. The leaders would

be the best crackers - some of whom became the Inner Circle.

"We took over alt.binaries.pictures.leek in early '96," explains Abraxas, "and then leaked the first Nashville [Windows 97] beta. The groups were being overrun by clueless people. They needed help. They were wasting Internet resources. Perhaps if we could encourage responsible use of the available bandwidth, the whole Usenet warez 'scene' might last a while longer. Warez was around before we were, and will be after, but we wanted to help people and preserve resources using common sense."

As enforcers of the warez code, the Inner Circle can be swift and sure. In April 1996, a pirate gang called Nomad, convinced that posts to warez groups were being suppressed, decided to get themselves some unsupervised elbow room. They selected an antiwork newsgroup - alt.binaries.slack, relatively empty and off the beaten track - where software could be slipped past news providers who had firewalled the usual warez forums. Within 24 hours, the forum was flooded with the latest releases. The slackers bestirred themselves from their apathy and fought back, posting files that told the pirates politely to push off. The warez kept coming. Then the Inner Circle waded in on the slackers' side and castigated the invaders for their poor manners. The pirates left meekly - though as a parting gift, one of them posted Microsoft NT, Beta 3, all 48 Mbytes of it, in 5,734 parts. The slackers' newsfeed was clogged for days.

A slightly disturbing revelation came out of the slacker invasion. "After the first attempted takeover, we discovered just how scary search engines like Deja News and AltaVista were," explains TAG. "You could dig up real email addresses pretty easy on about 75 percent of people posting warez." A worried TAG hacked into the code of Forte Agent, an industry standard newsreader already cracked to bypass the shareware cripples, and stripped away the X-newsreader header, giving posters far greater anonymity. As a side effect, the patch also reduced email spams by two-thirds. "The hack went over so well with even nonwarez people that Forte eventually incorporated it into Agent as a feature," TAG says proudly, "although I don't think they'll be giving us credit."

By mid-'96, Mad Hatter decided that police work was getting to be too much of a chore. The newsfeed was being clogged by lamers, requesters, and partials posters with "room-temperature IQs." Those genuinely into warez were seeing less and less complete software uploaded; in its place were hundreds of stray disks and clammy begging posts. In a rare fit of pique, Mad Hatter took his revenge.

"If I continue to see the 'here's what I have' threads," he wrote, "I will stop uploading here. I will not help and will laugh my ass off that everyone is suffering. If for some reason you doubt that I make a difference, it's your loss, as I personally have uploaded 85 percent of all the shit that's getting posted now when it was zero day or still fresh. Keep fighting over stale shit - I like to watch; keep posting partials, and I'll stop upping my 100 to 300 Mbytes a week. In fact, I think I'll stop now."

And stop the Inner Circle did. "We became burnt out on educating the masses," Mad Hatter says. Instead, a range of guaranteed lamer-free encrypted newsgroups was created for posting PGP-encoded warez, for Inner Circle-approved members only. Those on the select interested- parties list are given the codes to unlock the software, and anyone can apply to join. Requirement: a reasonable knowledge of PGP. "Hopefully this is a sign you won't be totally incompetent if you choose to post," says TAG. At the last count, the IPL had 500 subscribers, happily trading warez under the protection of the latest in antilamer technology.

New economy

Warez on Usenet are basically gifts - testimony to the power and stature of the giver. Files are posted for all to download, free. Just fire up your newsreader, point it at an appropriate forum, and a list like a home-shopping catalog of the latest software spills down your screen. There is no pressure, but if you download and you like the vibe, you are expected to join the community and contribute uploads whenever possible.

On the freewheeling IRC chat forums, warez are no longer gifts - they're trade goods. The rewards are greater, but you've got to work for them. The IRC channels are 24-hour stock exchanges cum street markets: FreeWarez, Warez96, Warez4Free, WarezSitez, WarezAppz, and WarezGamez. There are private channels, hidden areas, and invite-only piracy parties. And there are no free lunches - every piece of software has to be paid for, in software. The more recent the application, the higher its value. The ultimate bartering tools are zero-day warez - software released by a commercial house in the last 24 hours, cracked if necessary and uploaded. The prizes for good zero-day warez vary; you may get instant download status on a particular server, logins and passwords for exclusive FTP sites, or admission to the ranks of a powerful cartel like the Inner Circle.

"Zero-day sites are very Ã‰lite stuff," explains paid-up Ã‰litist TAG. "People can get access only if they can move a few hundred Mbytes a day. Most are invite only. The average IRC warez trader doesn't get that kind of access unless he puts a lot of effort into it." Zero-day warez trading is a fraught business; competition between groups often leads to malpractice. "You get a lot of first releases with bad cracks," says TAG, "just so someone can say they released first. Then two days later, you get a working crack. We get most of our freshest stuff from private FTP and courier drop sites."

If your software collection is more mundane, you can trade one piece directly for another. But with so many unpoliced egos in one place, this can be risky. People will often welsh on deals, allowing you to pass them a file and then disappearing into the ether. Cunning traders will barter with "trojans" - zipped-up files of gunk, realistic enough to carry out half the transaction. In extreme cases, someone may feed you a virus.

A step down from zero-day warez are drop sites, where fresh cracks can be found for the cost of a download. Some drop sites run on the trader's own machine; others piggyback on government or corporate mainframes, shareware mirrors, and university networks. Often they're only in existence for 24 hours, or on weekends when the sysops are at home.

Wherever you end up, you'll be struck by the extreme politesse and measured courtesy, united by a common language. "Greets m8. Have appz, gamez and crackz on 129.102.1.3. Looking for Pshop 4.0 beta. L8ter." "Have 1.5 gigs of warez on anonymous T1. Upload for leech access. msg me for more info. No lamers."

Real money

Back in Phil's world, they can't quite cope with the idea of this ferocious brag-driven barter economy cloaked in courtesy. The SPA and the BSA just don't believe it. "Considering the amount of time they dedicate, they must be making a return to justify it," says Phil. Casual observers of the BSA's Web site may well be convinced, if only because they're stunned by the money that's involved - or seems to be. Fifteen point five billion dollars a year! But those figures are based on the assumption that if piracy were stopped, someone would be willing to pay for every pirated copy in circulation.

"Billions of dollars?" scoffs East London BBS operator Time Bandit. "I know guys who have thousands and thousands of pounds worth of software, but the values are meaningless. Win95 may cost, like, Â£75 in the shops, but in warez, it's worthless. It's just another file that you might swap for another program, which might cost four grand. How much it costs in real money is meaningless."

How do you ram home sales figures and quarterly losses to a bunch of teenagers who see warez trading as their passport to acceptance on the scurrilous side of a brave new world? How do you convince middle-aged men who see incandescently expensive software as monopoly money in a vast, global boardgame that what they're doing is "harmful"? In the software industry's latest campaign, you scare them - or try. The BSA's mandate used to be "not to capture pirates, but to eradicate piracy." Now exemplary punishment is the big thing.

To do that, the BSA and the SPA are willing to push the law to its limits. Prosecuting clear offenders - warez-vending BBS operators and FTP-site pirates, for instance - is one thing; suing ISPs for carrying Web pages containing pirate links and cracks is another. A typical case was against C2Net, a Buffalo, New York-based ISP that the SPA sued for doing just that. In what smacked of a token prosecution - or, in the words of C2Net's president, Sameer Parekh, "legal terrorism" - the action by Adobe, Claris, and Traveling Software, under the aegis of the SPA, held the provider responsible as "publishers" for the contents of its server, and for the activities of individual account holders. The SPA eventually backed off but threatens to revive the suit if C2Net and other ISPs don't agree to monitor their users for copyright infringement. C2Net says it will not give in to litigious "bullying."

And then there are straightforward busts. On January 12, 1996, Microsoft and Novell jointly announced a settlement with Scott W. Morris, who was "doing business as the Assassin's Guild BBS ... billed ... as the worldwide headquarters for two large pirate groups, Pirates With Attitude (PWA) and Razor 1911." According to the statement, "marshals seized 13 computers, 11 modems, a satellite dish, 9 gigabytes of online data, and over 40 gigabytes of offline data storage dating back to 1992.... Mr. Morris agrees to assist Microsoft and Novell in their continuing BBS investigations."

Phil, our undercover Internet detective, wasn't responsible for that particular drama, but he's been integral to others. His latest victory was in Zurich - "a landmark case against individuals and organizations distributing unlicensed software on the Internet," he calls it. A 27- year-old computer technician who helpfully called himself "The Pirate" was running an FTP site filled to the brim with warez, including US$60,000 worth of unlicensed Novell software. Phil, impersonating a trader, infiltrated the site (admittedly no great feat), collected evidence, then handed it over to the Swiss police. He accompanied them on the raid to ensure no evidence was damaged. "He was one of a new breed who advertise on the Internet," says Phil. "He made his files available via email requests and telnet." Swiss police also raided the home of a BBS called M-E-M-O, run by "The Shadow," a friend of The Pirate. Unfortunately, The Shadow was on holiday with his parents. The family returned two weeks later to find their front door broken down; the son was arrested. If convicted, the young pirates face up to three years in jail and possible $80,000 fines.

The Pirate's mistake - aside from his suicidal choice of nickname - was to plant himself geographically. Phil, a former corporate network manager, was able to trace him through his FTP site's IP address. Phil knows his networks; this makes him the perfect undercover agent - and one of Novell UK's most envied employees. "I play on the Net all day," he says, "and get paid for it."

There's a bit more to it than that. Phil and his counterparts in Asia and the US are deployed to infiltrate pirate groups; to study IRC; to get under the skin of the lamers, the dabblers, and the professionals; to chat, seduce, charm, and interact with the denizens of this bizarre over-underworld. Phil talks to traders in their own language, understands the tricks and traps. After busting The Pirate, he says, "we were talking and he was moaning about the sluggishness of his network. I pointed out that, aside from using LANtastic, he was using a 75-ohm terminator on the back of his file server, slowing the whole thing down."

Now that he's back from ZÃ¼rich, Phil will be getting some new toys: the spoils of war. In many jurisdictions, any hardware deemed to be part of an illegal setup can be taken by investigators and - if part of a civil prosecution - can be worked in as part of the settlement. Once sucked dry of evidence and incriminating data, the cannibalized machines are moved to Bracknell and hooked up to the network.

But despite the resources at his disposal and his status as a network ninja, Phil doesn't always get his man. "If there's a person out there who has a decent level of technological awareness of the ways he can be located, it's quite true to say he could successfully hide himself, or use a system where it would be impossible to track him. It's technically possible for them to bounce their messages all around the world and have us running around like blue-arsed flies." It's a reluctant admission, but then Phil is one person pitted against thousands.

Successful prosecutions aren't always that easy either. Take David LaMacchia, an MIT engineering student who turned two of the school's servers into drop sites and downloaded an estimated $1 million worth of pirated software. LaMacchia was arrested in 1995, only to have the case thrown out by a judge who ruled that no "commercial motive" was involved. Prosecutors tried charging him with wire fraud, but this was ruled an unacceptable stretching of the law. LaMacchia walked free.

"Bringing Internet cases through the judicial system is a nightmare," says Novell's Martin Smith. "Try talking to a judge about 'dynamically allocated IP addresses.' We don't have a chance."

Tell that to the former warez traders of America Online, which had a meteoric history as a pirate mecca. For years, instructions on how to crack AOL's security and obtain free accounts were a Usenet staple. Online, "freewarez" chat rooms were packed with traders, 24 hours a day. Megabytes of warez were kept in permanent circulation.

Then came the crackdown of 1996, a dark period in warez history. Goaded by software-industry watchdogs, AOL introduced countermeasures to disinfect its system; alt.binaries.warez was removed from the Internet newsfeed. CATwatch automated sentinels were placed on AOL's warez chat channels, logging off anyone who entered. "Free" accounts were traced and nuked. Michael, the weight-lifting trader and also an AOL veteran, says everyone thought that "the FBI had infiltrated the warez groups, and we were all going to get busted." On the cusp of the big time - a top pirate outfit named Hybrid had a position open - Michael had been hoping to prove himself by doing a CD rip of the soccer game Euro 96. "I was halfway through removing the FMV and CD audio. I reckon I could've got it down from 58 disks to 9. But then everything went haywire."

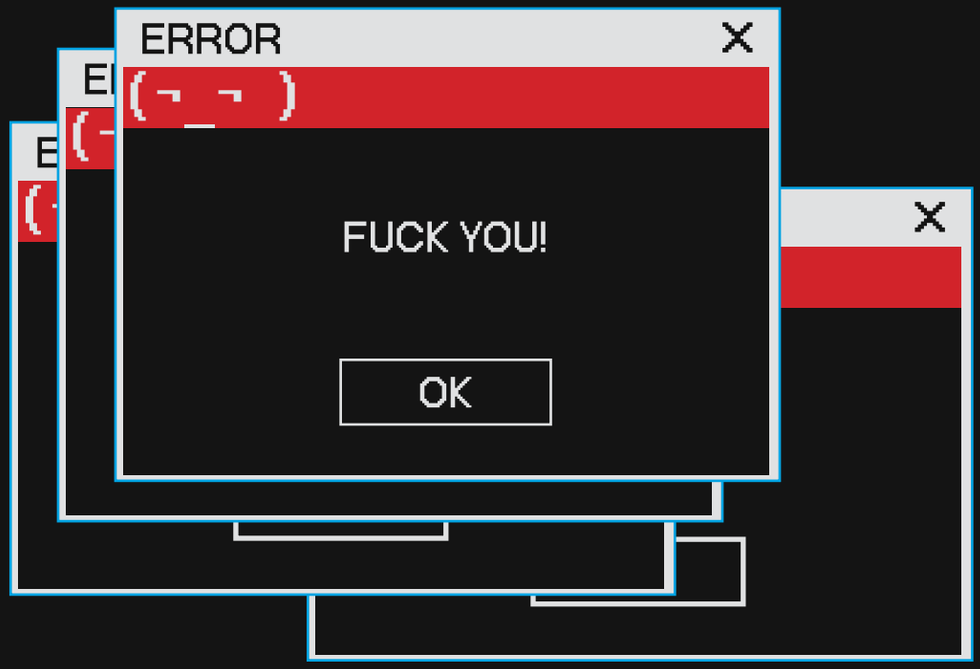
Profit-driven crackers are actually the easiest to catch: they have links to the real world, starting with the money trail from credit cards. And the easiest prey of all are BBSes, with their telltale telephone connections. In January, FBIagents led by the bureau's San Francisco-based International Computer Crime Squad raided homes and businesses in California and half a dozen other states. They seized computers, hard drives, and modems, though no arrests were made. Along with Adobe, Autodesk, and other BSA stalwarts, the list of software companies involved included Sega and Sony - a hint that the targets included gold-disk dupers who counterfeit mass-market videogames.

Mad Hatter was not impressed. "Wow, I'm in hiding," he cracked the day after the raids. But "Cyber Strike" was, as BSAvice president Bob Kruger said later in a statement, "the most ambitious law enforcement action to date against Internet piracy" - specifically, the first UScase in which the FBI, rather than local police, took the lead. And that can't help but augment the BSA's number-one antipiracy tactic for 1997: creating the "perception of threat." And even warez gods don't necessarily want the FBI on their case.

But bluster aside, people like Mad Hatter are intrinsically - and deliberately - much harder to catch. The most prestigious pirate groups - Razor 1911, DOD, Pirates With Attitude, the Inner Circle - are tightly knit clubs whose members have known each other for years and call each other "good friends" - though they rarely, if ever, meet. Joining is no easy task. Positions become vacant only when members quit or are busted, or a vote is taken to expand operations. Kudos and reputation are everything. Unofficial homepages can be found here and there, constructed by acolytes who celebrate the groups' best releases and victories. These are often padded out with cryptic biographies and obituaries for those busted by the cops ("We feel for ya!"). Despite the boasting, and the draping of their releases with corporate motifs - logos, front ends, graphics, even signature tunes and Java applets - crackers' true identities typically remain secret, even to one another.

The anonymity, however, works both ways. Cloaked in his own secret identity, Phil says he has managed to get deep within several major groups in the past 18 months and is skimming the surface of several others. He can convincingly portray himself as a caring, sharing warez god. "You make some good friends," he says with a smile. And, it seems, you can end up pretty impressed. "

"Some of these people are very talented. The logic and programming behind their setups are just amazing". Or maybe he's just bluffing?"



> Warez and whyfores

In Phil's world, warez dealers are thieves. In warez world, the software companies are the criminals.

"Most products you buy from a store can be returned if you are unsatisfied," reads the beautifully crafted Warez FAQ, on the Inner Circle's Web site. "Software cannot." The Inner Circle thus can claim to have a practical motivation - providing "a place to find something you might want to evaluate before purchasing." All right. "I personally have bought progs that I demo'd first from warez," declares Clickety. "I have more warez than I could ever hope to install on my poor drives. Tested a lot of crap also that I was glad I didn't pay for - deleted it right off the bat. I have recommended software to clients based upon using a pirate version at home."

"Software developers have families, and should be able to support them," reads the Warez FAQ. "We do advocate buying your own software if you really like it and use it heavily," adds Mad Hatter.

As Phil and his friends are well aware, the line between piracy and ownership is very blurred. For example, it's commonplace for 3-D animators and modelers to use pirated, cracked, or at least unlicensed copies of their office software at home, for overtime or experimentation. In some minds, it's even a "necessary evil," a slightly arcane marketing strategy, a rather reckless approach to branding - look at Netscape. Indeed, many software executives privately acknowledge that piracy - especially the attention it brings to new releases - can be a valuable way to develop markets.

Novell's Martin Smith might disagree. He spends "99.9 percent" of his time fighting piracy, and he worries that the next generation of browsers will seamlessly marry the Web with Usenet. "The newsgroups will be a lot more accessible," he says, with something close to resignation, "which is going to make the whole thing a lot more widespread and give these guys a much bigger market. There's not much we can do, other than encourage ISPs not to take them."

The difficulty is that, once it's up, a Usenet post can generally be canceled only by the author or a sysop from the post's point of origin, "server zero." Even if a cancel is issued, it takes time to ripple across the network. A warez regular would be able to grab the file before it was vaped. Some servers refuse on principle to honor cancels. "Even the most diehard warez hater in news.admin.hierarchy would defend your right to be safe from cancels," claims TAG. Many commercial ISPs have taken the industry's encouragement and dropped the warez groups, but lots of free servers are carrying on. And things aren't helped by the lack of a clear legal framework. Imagine the scenario: a program that belongs to a UScompany is uploaded via a router in Canada to a server in South Africa, where it is downloaded by a Norwegian operating out of Germany using a US-based anonymous remailer, then burnt onto a CD in the UK and sold in Bulgaria. "How would you prosecute that mess?" asks Smith. "It's a jurisdictional nightmare."

And the profit pirates are getting more creative. Smith cites the Web page of one warez guru, offering a premium-line phone number: for $3 a minute, you can listen to details about the best

warez FTP sites, their addresses, and their login passwords. “Updated every three days for your convenience,” it declares. It also makes provisions for those dialing from outside the US. The selling of information that leads to illegal use of information - a difficult case to prosecute.

“Our strategy is to bring a critical mass of prosecutions,” says Smith. “We’ll take out some people who’re downloading this material - the gnats - and then we’ll take out some of the larger, more organized guys. The people who are packaging it up and zipping it onto CD-ROMs.” Which might work in a world where software was always bought on CD-ROM. But in pushing ever deeper into electronic commerce, where more and more real commercial software (browsers, little applets) is being given out for free, where the Internet is the ultimate distribution network, this looks a little ropey. Friction-free markets and friction-free piracy run in tandem. The Inner Circle already has its PGP-encoded giveaway mall in place.

Smith knows all this. There’s just not much he can do about it. “All it needs is one server in one country where there are no laws to counter copyright theft, and there are plenty who will - the likes of Libya, Bulgaria, and Iran. One country with a decent enough telephone infrastructure is enough to undo a hundred busts in the West.” Even if laws are constitutional or enforced, larger biases come into play. “Try asking a Saudi policeman to arrest a Saudi software pirate on behalf of an American company. Forget it.”

> Dingle my dongle

The alternative to policing is burglar-proofing: making things harder to crack. In principle, you might think that the gazillion-dollar software industry would be able to produce uncrackable software. In practice, it can't, although it certainly keeps trying.

Take the dongle, for example. It is the summit of copy protection, an explicit melding of software and hardware. Without the right hardware key - the dongle - plugged into the machine's parallel port, the software won't run. And without the right software, the dongle is a mindless doorstop. Calls to the dongle are woven into the code at the lowest level. "The program may call the dongle every 150 mouseclicks, or every time you print, or every time you select flesh tones as your desktop color scheme," says one dongle expert. If the response to the call is false or not forthcoming, the program shuts down. All communications between the two are encrypted by uncrackable algorithms. Internal security fuses ensure that any attempt to hack the dongle mechanically will cause it to self-destruct. "Nothing short of an electron microscope," says the expert, "could extract the algorithm from that mess."

The biggest player in the dongle market is Rainbow Technologies, whose Sentinel hardware keys are used by 55 percent of all protected software. There are 8 million Sentinel keys attached to 8 million printer ports the world over. The company calls it "the world's most effective way to stop piracy" - a clarion call to crackers if ever there was.

The logical approach to cracking a hardware key is to create a "pseudodongle" - a chunk of code that sits in memory, giving the correct answers to any query. To do this, a cracker would have to monitor and trap traffic to-ing and fro-ing across the parallel port, then use this information to build an infallible query response table. Unfortunately, if the query is, say, six characters long, it can have more than 280 trillion responses (281,474,976,710,700 to be exact). With the speed of modern machines, this would take approximately 44,627 years to collate. With the SentinelSuperPro dongle ("the most secure and flexible protection available") the query length can be 56 characters - requiring a mere 10 125 years (in theory) for a complete table. However, the dongle in SentinelSuperPro for Autodesk 3D Studio MAX was cracked in just under seven days of its retail release - substantially less than the 44 millennia emblazoned on the sales brochures. Other expensive high-end applications that use Sentinel - including NewTek's LightWave 5 and Microsoft's SoftImage - have ended up the same way: cracked, repackaged, and redistributed to every corner of the Internet within weeks of their release. How? Instead of attempting to simulate the dongle, expert crackers simply remove its tendrils from the program code, unraveling the relationship skein by skein, function by function, call by call, until the application ceases to need the dongle to function. Then it's ready for anyone and everyone to use - or, more likely, gawk at.

Nobody says this is easy. There may be only three or four crackers in the world who could manage such an opus. But with the Internet to transmit the result, only one needs to succeed.

With the latest wave of dongles, warez world looked to Russia to get the job done - and a shadowy group called DOD "won" the contract. The self- styled "Warez Bearz of Russia and Beyond," DOD appears to have arms throughout Europe, Asia, and the US. It undid Microsoft SoftImage's dongle protection in two weeks, which wasn't easy. The crew riotously celebrated in their "NFO" file: "Totally awesome work of glorious DOD cracker - Replicator after five other crackers gave up! We decided not a do a crack patch 'coz it will take too much time to code it ... you ask why? 'Coz there are only 72 (!!!) EXEs patched. All options now work 100%!"

NFO files do more than brag or supply installation instructions; they testify that the ware is a bona fide release, guaranteed to work. And this is more

than just posturing; a group's reputation is paramount. Each release is painstakingly beta-tested. These are their products now, their labors of love. Nobody wants to find a "bad crack" in his hands after a seven-hour download. Nobody wants to be accused of being "unprofessional." Nobody wants the ignominy of anything like the bad crack for Autodesk's 3D Studio that made the rounds in 1992. For all intents and purposes it ran correctly, all features seemed 100 percent functional. Except that the dedongled program slowly and subtly corrupted any 3-D model built with it. After a few hours of use, a mesh would become a crumpled mass of broken triangles, irrevocably damaged. Cleverly, Autodesk had used the dongle to create a dynamic vector table within the program. Without the table, the program struggled to create mathematically accurate geometry - and eventually failed. Many a dodgy CAD house saw its cost-cutting measures end in ruin. Autodesk support forums and newsgroups were flooded with strangely unregistered users moaning about the "bug in their version of 3D Studio." A rectified "100 percent cracked" version appeared soon after, but the damage was done. The Myth of the Bad Crack was born, and the pirate groups' reputations tarnished.

But the pirates bounced back. They always do. And there's no reason to think that there's any way to stop them. Software security people are at an intrinsic disadvantage. Compare their job to that of securing something in the real world that's valuable and under threat - a bank, say. Typically, only one set of armed robbers will hold up a bank at a time, and they'll get only one crack at it. Imagine an army of robbers, all in different parts of the world, all attacking the same bank at the same time. And in the comfort of their own homes. Not just once, but over and over again. Imagine that each set of robbers is competing against every other, racing to be first in. Imagine, too, that some of the robbers are so technically adept that they could have built the alarms, the safe, and even the jewels themselves. And that they have cracked more than 30 banks with the same protection system. And that they're learning from all their failures, because they're never caught. No security could realistically resist such an onslaught. It may be that the only way to avoid having your software cracked is to put no protection whatsoever on it. No challenge, no crack.

Popularity only feeds the frenzy. *Doom* is a good example. In 1993, id Software distributed the original shareware version of its nasty-guns-in-nasty-dungeons masterpiece on bulletin boards, CompuServe, and a then-little-known system called the Internet. Downloaded by more than 6 million people worldwide, *Doom* was a trailblazer in the world of modem marketing. The shareware gave you a third of the game: if you liked it, you had to buy the rest on disks. Millions did.

Doom and its makers became a dream target. Weeks before *Doom II*'s release, the sequel was available on the Internet - not as shareware, but warez. And not just as a teaser, but the whole damn thing. "Yeah, that was leaked," says Mike Wilson, id's then-vice president of marketing, now CEO at Ion Storm. "Can't tell you how much that hurt." The leaked copy was rapidly traced - rumors abounded that the version was a review copy fingerprinted to a British PC games magazine - but too late. It was already on Usenet, doing the rounds on IRC, filling up FTP sites. The pirates were in ecstasy and id was left with recoding the final retail release, to ensure future patches and upgrades would not work on the pirated version. Then they shut the stable door. No more external beta testing; no more prelaunch reviews. "We assured ourselves it would never happen again," says Wilson. "No copy of our games would leave the building."

Nice try. *Quake, Doom's* much-anticipated follow-up, turned up on an FTP server in Finland three days before the shareware come-on was due to be released. The pirate version was a final beta of the full game - complete with eerily empty unfinished levels and bare, unartworked walls. Within hours, it had been funneled to sites all over the globe. IRC was swamped with traders and couriers desperate to download.

"Somebody actually broke into our then poorly secured network and started to download it right before our eyes," Wilson recalls. "We managed to stop the transfer before he got all of it. We traced the call, got his name and address. He was pretty scared, but, of course, it was some kid. We didn't pursue that one. It hurt, but not enough to put some little kid in jail."

When the legitimate *Quake* hit the stores last year, it was initially in the form of an encrypted CD, which let you play a shareware version for free but would only unlock the rest on receipt of a password, available for purchase by phone. The encryption scheme, an industry standard called TestDrive, was eventually cracked by a lone European pirate called Agony. And id's crown jewel was now available, courtesy a 29K program. "In order to unlock the full version, you are supposed to call 1-800-IDGAMES," Agony gloated in a posting. "Hahahahahah."

"We knew it was going to be hacked," says Wilson. "We of all people knew. But we thought it was safe enough, certainly safer than *Doom II*." And, truth to tell, it didn't matter too much. The gap between the game's release and the warez version becoming widespread was enough for id to sell the copies they expected. "Copy-protection schemes are just speed bumps," laments Wilson.

Nobody really knows how much actual damage cracking does to the software companies. But as the industry rolls apprehensively toward the uncertain future of an ever-more frictionless electronic marketplace, almost everyone thinks piracy will increase. "The level of activity out there is overwhelming. We know that we have to take action to take control of it. We will continue to bring a critical mass of prosecutions," says Novell UK's Smith. He doesn't sound all that convinced.

Somewhere back on the US East Coast, Mad Hatter has a final swig of ginger ale and settles down to bed with his wife, White Rabbit. She thinks his obsession is a wasted resource, but didn't complain when he installed the latest version of Quicken on *her* computer - a cracked copy, of course. "We are all family men, married with children, day jobs, dedicated accounts, and multiple phone lines," Mad Hatter says. "Our kids have been looking over our shoulders for years. They will be the next couriers, the next warez gods."


NEW HIGH SCORE!
THE WAREZ GAME
Obtain
Crack
Pack
Release

Scene Glossary

0-day

As in 0sec access to a release. It means someone has access to a release immediately

Crack

Software cracking is the modification of software to remove encoded copy prevention (*DRM*).

1337

Leet-speak a contraction of “elite speak” — a form of slang communication that uses text and numbers. Often, the numbers “1337” or “31337” are used to mean “leet” of “eleet” for the digits’ resemblance to “e,” “l,” and “t.”

Leeching

Downloading a lot without uploading. Also can be used as a noun often used as a derogatory term. Being a leech is frowned upon

NFO

A .nfo file is a textfile with information about the release.

Ripping

Ripping is the process of extracting digital content, such as audio or video files, from a physical source like a CD, DVD, or Blu-ray disc, and converting it into a digital file format. This allows you to store, share, and play the content on various devices without the need for the original physical media.

DRM

Digital Rights Management. Programming routines that aim to make it impossible, illegally, to copy an artefact. *Cracks* aim to circumvent DRM/TPM.

Courier

An individual who moves *releases* between sites to build ratio credit for download and to participate in *courier charts* Competitive scoring systems that rank *couriers*. The act of transferring a release, in competition with other couriers, is called *“racing.”* Previously, in earlier BBSs, a courier was also referred to as a *“broker.”*

Dupecheck

A database of previous scene releases, allowing a *release group* to ascertain whether a release is a duplicate of a previous work.

Release Group

A set of individuals working together to create *releases*. A *release* is A pirate artefact, be it music, movies, software, games,etc

Nuke

Both a noun and a verb. In its noun form, this refers to a “bad” release that has been marked as a rule violation at either the topsite-level (a violation of individual site rules) or Scene-level (a violation of release rule standards). Nuke as a verb refers to the act of marking a release as bad using the “site nuke” command. The *NukeNet* is an inter-site system for nuking releases. A *Nuker* has the role of *Nuking* releases.

Topsite

An FTP server with a high-speed internet connection and vast amounts of storage space. It has *affiliates, couriers, siteops* (site operators)*, nukers,* and other user categories. It is ranked according to various criteria for participation in *courier charts*.

Internet Relay Chat

(IRC) A distributed online chat system used by Sceners to communicate with one another. Site bots also post updates to the IRC channels of topsites.

Internal

A *release* designed only for dissemination amongmembers of the release group itself. Such releases are not beholden to the same standards (e.g., dupecheck) as public releases.