The New York Times
nytimes.com

PRINTER-FRIENDLY FORMAT
SPONSORED BY
IN AMERICA
NOW PLAYING IN SELECT THEATRES

February 8, 2004

The Virus Underground

By CLIVE THOMPSON

This is how easy it has become.

Mario stubs out his cigarette and sits down at the desk in his bedroom. He pops into his laptop the CD of Iron Maiden's "Number of the Beast," his latest favorite album. "I really like it," he says. "My girlfriend bought it for me." He gestures to the 15-year-old girl with straight dark hair lounging on his neatly made bed, and she throws back a shy smile. Mario, 16, is a secondary-school student in a small town in the foothills of southern Austria. (He didn't want me to use his last name.) His shiny shoulder-length hair covers half his face and his sleepy green eyes, making him look like a very young, languid Mick Jagger. On his wall he has an enormous poster of Anna Kournikova -- which, he admits sheepishly, his girlfriend is not thrilled about. Downstairs, his mother is cleaning up after dinner. She isn't thrilled these days, either. But what bothers her isn't Mario's poster. It's his hobby.

When Mario is bored -- and out here in the countryside, surrounded by soaring snowcapped mountains and little else, he's bored a lot -- he likes to sit at his laptop and create computer viruses and worms. Online, he goes by the name Second Part to Hell, and he has written more than 150 examples of what computer experts call "malware": tiny programs that exist solely to self-replicate, infecting computers hooked up to the Internet. Sometimes these programs cause damage, and sometimes they don't. Mario says he prefers to create viruses that don't intentionally wreck data, because simple destruction is too easy. "Anyone can rewrite a hard drive with one or two lines of code," he says. "It makes no sense. It's really lame." Besides which, it's mean, he says, and he likes to be friendly.

But still -- just to see if he could do it -- a year ago he created a rather dangerous tool: a program that autogenerates viruses. It's called a Batch Trojan Generator, and anyone can download it freely from Mario's Web site. With a few simple mouse clicks, you can use the tool to create your own malicious "Trojan horse." Like its ancient namesake, a Trojan virus arrives in someone's e-mail looking like a gift, a JPEG picture or a video, for example, but actually bearing dangerous cargo.

Mario starts up the tool to show me how it works. A little box appears on his laptop screen, politely asking me to name my Trojan. I call it the "Clive" virus. Then it asks me what I'd like the virus to do. Shall the Trojan Horse format drive C:? Yes, I click. Shall the Trojan Horse overwrite every file? Yes. It asks me if I'd like to have the virus activate the next time the computer is restarted, and I say yes again.

Then it's done. The generator spits out the virus onto Mario's hard drive, a tiny 3k file. Mario's generator also displays a stern notice warning that spreading your creation is illegal. The generator, he says, is just for educational purposes, a way to help curious programmers learn how Trojans work.

But of course I could ignore that advice. I could give this virus an enticing name, like "britney--spears--wedding--clip.mpeg," to fool people into thinking it's a video. If I were to e-mail it to a victim, and if he

clicked on it -- and didn't have up-to-date antivirus software, which many people don't -- then disaster would strike his computer. The virus would activate. It would quietly reach into the victim's Microsoft Windows operating system and insert new commands telling the computer to erase its own hard drive. The next time the victim started up his computer, the machine would find those new commands, assume they were part of the normal Windows operating system and guilelessly follow them. Poof: everything on his hard drive would vanish -- e-mail, pictures, documents, games.

I've never contemplated writing a virus before. Even if I had, I wouldn't have known how to do it. But thanks to a teenager in Austria, it took me less than a minute to master the art.

Mario drags the virus over to the trash bin on his computer's desktop and discards it. "I don't think we should touch that," he says hastily.

Computer experts called 2003 "the Year of the Worm." For 12 months, digital infections swarmed across the Internet with the intensity of a biblical plague. It began in January, when the Slammer worm infected nearly 75,000 servers in 10 minutes, clogging Bank of America's A.T.M. network and causing sporadic flight delays. In the summer, the Blaster worm struck, spreading by exploiting a flaw in Windows; it carried taunting messages directed at Bill Gates, infected hundreds of thousands of computers and tried to use them to bombard a Microsoft Web site with data. Then in August, a worm called Sobig.F exploded with even more force, spreading via e-mail that it generated by stealing addresses from victims' computers. It propagated so rapidly that at one point, one out of every 17 e-mail messages traveling through the Internet was a copy of Sobig.F. The computer-security firm mi2g estimated that the worldwide cost of these attacks in 2003, including clean-up and lost productivity, was at least $82 billion (though such estimates have been criticized for being inflated).

The pace of contagion seems to be escalating. When the Mydoom.A e-mail virus struck in late January, it spread even faster than Sobig.F; at its peak, experts estimated, one out of every five e-mail messages was a copy of Mydoom.A. It also carried a nasty payload: it reprogrammed victim computers to attack the Web site of SCO, a software firm vilified by geeks in the "open source" software community.

You might assume that the blame -- and the legal repercussions -- for the destruction would land directly at the feet of people like Mario. But as the police around the globe have cracked down on cybercrime in the past few years, virus writers have become more cautious, or at least more crafty. These days, many elite writers do not spread their works at all. Instead, they "publish" them, posting their code on Web sites, often with detailed descriptions of how the program works. Essentially, they leave their viruses lying around for anyone to use.

Invariably, someone does. The people who release the viruses are often anonymous mischief-makers, or "script kiddies." That's a derisive term for aspiring young hackers, usually teenagers or curious college students, who don't yet have the skill to program computers but like to pretend they do. They download the viruses, claim to have written them themselves and then set them free in an attempt to assume the role of a fearsome digital menace. Script kiddies often have only a dim idea of how the code works and little concern for how a digital plague can rage out of control.

Our modern virus epidemic is thus born of a symbiotic relationship between the people smart enough to write a virus and the people dumb enough -- or malicious enough -- to spread it. Without these two groups of people, many viruses would never see the light of day. Script kiddies, for example, were responsible for some of the damage the Blaster worm caused. The original version of Blaster, which struck on Aug. 11, was clearly written by a skilled programmer (who is still unknown and at large).

Three days later, a second version of Blaster circulated online, infecting an estimated 7,000 computers. This time the F.B.I. tracked the release to Jeffrey Lee Parson, an 18-year-old in Minnesota who had found, slightly altered and re-released the Blaster code, prosecutors claim. Parson may have been seeking notoriety, or he may have had no clue how much damage the worm could cause: he did nothing to hide his identity and even included a reference to his personal Web site in the code. (He was arrested and charged with intentionally causing damage to computers; when his trial begins, probably this spring, he faces up to 10 years in jail.) A few weeks later, a similar scene unfolded: another variant of Blaster was found in the wild. This time it was traced to a college student in Romania who had also left obvious clues to his identity in the code.

This development worries security experts, because it means that virus-writing is no longer exclusively a high-skill profession. By so freely sharing their work, the elite virus writers have made it easy for almost anyone to wreak havoc online. When the damage occurs, as it inevitably does, the original authors just shrug. *We may have created the monster,* they'll say, *but we didn't set it loose*. This dodge infuriates security professionals and the police, who say it is legally precise but morally corrupt. "When they publish a virus online, they *know* someone's going to release it," says Eugene Spafford, a computer-science professor and security expert at Purdue University. Like a collection of young Dr. Frankensteins, the virus writers are increasingly creating forces they cannot control -- and for which they explicitly refuse to take responsibility.

"Where's the beer?" Philet0ast3r wondered.

An hour earlier, he had dispatched three friends to pick up another case, but they were nowhere in sight. He looked out over the controlled chaos of his tiny one-bedroom apartment in small-town Bavaria. (Most of the virus writers I visited live in Europe; there have been very few active in the United States since 9/11, because of fears of prosecution.) Philet0ast3r's party was crammed with 20 friends who were blasting the punk band Deftones, playing cards, smoking furiously and arguing about politics. It was a Saturday night. Three girls sat on the floor, rolling another girl's hair into thick dreadlocks, the hairstyle of choice among the crowd. Philet0ast3r himself -- a 21-year-old with a small silver hoop piercing his lower lip -- wears his brown hair in thick dreads. (Philet0ast3r is an online handle; he didn't want me to use his name.)

Philet0ast3r's friends finally arrived with a fresh case of ale, and his blue eyes lit up. He flicked open a bottle using the edge of his cigarette lighter and toasted the others. A tall blond friend in a jacket festooned with anti-Nike logos put his arm around Philet0ast3r and beamed.

"This guy," he proclaimed, "is the best at Visual Basic."

In the virus underground, that's love. Visual Basic is a computer language popular among malware authors for its simplicity; Philet0ast3r has used it to create several of the two dozen viruses he's written. From this tiny tourist town, he works as an assistant in a home for the mentally disabled and in his spare time runs an international virus-writers' group called the "Ready Rangers Liberation Front." He founded the group three years ago with a few bored high-school friends in his even tinier hometown nearby. I met him, like everyone profiled in this article, online, first e-mailing him, then chatting in an Internet Relay Chat channel where virus writers meet and trade tips and war stories.

Philet0ast3r got interested in malware the same way most virus authors do: his own computer was hit by a virus. He wanted to know how it worked and began hunting down virus-writers' Web sites. He discovered years' worth of viruses online, all easily downloadable, as well as primers full of coding

tricks. He spent long evenings hanging out in online chat rooms, asking questions, and soon began writing his own worms.

One might assume Philet0ast3r would favor destructive viruses, given the fact that his apartment is decorated top-to-bottom with anticorporate stickers. But Philet0ast3r's viruses, like those of many malware writers, are often surprisingly mild things carrying goofy payloads. One worm does nothing but display a picture of a raised middle finger on your computer screen, then sheepishly apologize for the gesture. ("Hey, this is not meant to you! I just wanted to show my payload.") Another one he is currently developing will install two artificial intelligence chat-agents on your computer; they appear in a pop-up window, talking to each other nervously about whether your antivirus software is going to catch and delete them. Philet0ast3r said he was also working on something sneakier: a "keylogger." It's a Trojan virus that monitors every keystroke its victim types -- including passwords and confidential e-mail messages -- then secretly mails out copies to whoever planted the virus. Anyone who spreads this Trojan would be able to quickly harvest huge amounts of sensitive personal information.

Technically, "viruses" and "worms" are slightly different things. When a virus arrives on your computer, it disguises itself. It might look like an OutKast song ("hey--ya.mp3"), but if you look more closely, you'll see it has an unusual suffix, like "hey--ya.mp3.exe." That's because it isn't an MP3 file at all. It's a tiny program, and when you click on it, it will reprogram parts of your computer to do something new, like display a message. A virus cannot kick-start itself; a human needs to be fooled into clicking on it. This turns virus writers into armchair psychologists, always hunting for new tricks to dupe someone into activating a virus. ("All virus-spreading," one virus writer said caustically, "is based on the idiotic behavior of the users.")

Worms, in contrast, usually do not require any human intervention to spread. That means they can travel at the breakneck pace of computers themselves. Unlike a virus, a worm generally does not alter or destroy data on a computer. Its danger lies in its speed: when a worm multiplies, it often generates enough traffic to brown out Internet servers, like air-conditioners bringing down the power grid on a hot summer day. The most popular worms today are "mass mailers," which attack a victim's computer, swipe the addresses out of Microsoft Outlook (the world's most common e-mail program) and send a copy of the worm to everyone in the victim's address book. These days, the distinction between worm and virus is breaking down. A worm will carry a virus with it, dropping it onto the victim's hard drive to do its work, then e-mailing itself off to a new target.

The most ferocious threats today are "network worms," which exploit a particular flaw in a software product (often one by Microsoft). The author of Slammer, for example, noticed a flaw in Microsoft's SQL Server, an online database commonly used by businesses and governments. The Slammer worm would find an unprotected SQL server, then would fire bursts of information at it, flooding the server's data "buffer," like a cup filled to the brim with water. Once its buffer was full, the server could be tricked into sending out thousands of new copies of the worm to other servers. Normally, a server should not allow an outside agent to control it that way, but Microsoft had neglected to defend against such an attack. Using that flaw, Slammer flooded the Internet with 55 million blasts of data per second and in only 10 minutes colonized almost all vulnerable machines. The attacks slowed the 911 system in Bellevue, Wash., a Seattle suburb, to such a degree that operators had to resort to a manual method of tracking calls.

Philet0ast3r said he isn't interested in producing a network worm, but he said it wouldn't be hard if he wanted to do it. He would scour the Web sites where computer-security professionals report any new software vulnerabilities they discover. Often, these security white papers will explain the flaw in such detail that they practically provide a road map on how to write a worm that exploits it. "Then I would

use it," he concluded. "It's that simple."

Computer-science experts have a phrase for that type of fast-spreading epidemic: "a Warhol worm," in honor of Andy Warhol's prediction that everyone would be famous for 15 minutes. "In computer terms, 15 minutes is a really long time," says Nicholas Weaver, a researcher at the International Computer Science Institute in Berkeley, who coined the Warhol term. "The worm moves faster than humans can respond." He suspects that even more damaging worms are on the way. All a worm writer needs to do is find a significant new flaw in a Microsoft product, then write some code that exploits it. Even Microsoft admits that there are flaws the company doesn't yet know about.

Virus writers are especially hostile toward Microsoft, the perennial whipping boy of the geek world. From their (somewhat self-serving) point of view, Microsoft is to blame for the worm epidemic, because the company frequently leaves flaws in its products that allow malware to spread. Microsoft markets its products to less expert computer users, cultivating precisely the sort of gullible victims who click on disguised virus attachments. But it is Microsoft's success that really makes it such an attractive target: since more than 90 percent of desktop computers run Windows, worm writers target Microsoft in order to hit the largest possible number of victims. (By relying so exclusively on Microsoft products, virus authors say, we have created a digital monoculture, a dangerous thinning of the Internet's gene pool.)

Microsoft officials disagree that their programs are poor quality, of course. And it is also possible that their products are targeted because it has become cool to do so. "There's sort of a natural tendency to go after the biggest dog," says Phil Reitinger, senior security strategist for Microsoft. Reitinger says that the company is working to make its products more secure. But Microsoft is now so angry that it has launched a counterattack. Last fall, Microsoft set up a $5 million fund to pay for information leading to the capture of writers who target Windows machines. So far, the company has announced $250,000 bounties for the creators of Blaster, Sobig.F and Mydoom.B.

The motivations of the top virus writers can often seem paradoxical. They spend hours dreaming up new strategies to infect computers, then hours more bringing them to reality. Yet when they're done, most of them say they have little interest in turning their creations free. (In fact, 99 percent of all malware never successfully spreads in the wild, either because it expressly wasn't designed to do so or because the author was inept and misprogrammed his virus.) Though Philet0ast3r is proud of his keylogger, he said he does not intend to release it into the wild. His reason is partly one of self-protection; he wouldn't want the police to trace it back to him. But he also said he does not ethically believe in damaging someone else's computer.

So why write a worm, if you're not going to spread it?

For the sheer intellectual challenge, Philet0ast3r replied, the fun of producing something "really cool." For the top worm writers, the goal is to make something that's brand-new, never seen before. Replicating an existing virus is "lame," the worst of all possible insults. A truly innovative worm, Philet0ast3r said, "is like art." To allow his malware to travel swiftly online, the virus writer must keep its code short and efficient, like a poet elegantly packing as much creativity as possible into the tight format of a sonnet. "One condition of art," he noted, "is doing good things with less."

When he gets stuck on a particularly thorny problem, Philet0ast3r will sometimes call for help from other members of the Ready Rangers Liberation Front (which includes Mario). Another friend in another country, whom Philet0ast3r has never actually met, is helping him complete his keylogger by

writing a few crucial bits of code that will hide the tool from its victim's view. When they're done, they'll publish their invention in their group's zine, a semiannual anthology of the members' best work.

The virus scene is oddly gentlemanly, almost like the amateur scientist societies of Victorian Britain, where colleagues presented papers in an attempt to win that most elusive of social currencies: street cred. In fact, I didn't meet anyone who gloated about his own talent until I met Benny. He is a member of 29A, a super-elite cadre within the virus underground, a handful of coders around the world whose malware is so innovative that even antivirus experts grudgingly admit they're impressed. Based in the Czech Republic, Benny, clean-cut and wide-eyed, has been writing viruses for five years, making him a veteran in the field at age 21. "The main thing that I'm most proud of, and that no one else can say, is that I always come up with a new idea," he said, ushering me into a bedroom so neat that it looked as if he'd stacked his magazines using a ruler and level. "Each worm shows something different, something new that hadn't been done before by anyone."

Benny -- that's his handle, not his real name -- is most famous for having written a virus that infected Windows 2000 two weeks before Windows 2000 was released. He'd met a Microsoft employee months earlier who boasted that the new operating system would be "more secure than ever"; Benny wrote (but says he didn't release) the virus specifically to humiliate the company. "Microsoft," he said with a laugh, "wasn't enthusiastic." He also wrote Leviathan, the first virus to use "multithreading," a technique that makes the computer execute several commands at once, like a juggler handling multiple balls. It greatly speeds up the pace at which viruses can spread. Benny published that invention in his group's zine, and now many of the most virulent bugs have adopted the technique, including last summer's infamous Sobig.F.

For a virus author, a successful worm brings the sort of fame that a particularly daring piece of graffiti used to produce: the author's name, automatically replicating itself in cyberspace. When antivirus companies post on their Web sites a new "alert" warning of a fresh menace, the thrill for the author is like getting a great book review: something to crow about and e-mail around to your friends. Writing malware, as one author e-mailed me, is like creating artificial life. A virus, he wrote, is "a humble little creature with only the intention to avoid extinction and survive."

Quite apart from the intellectual fun of programming, though, the virus scene is attractive partly because it's very social. When Philet0ast3r drops by a virus-writers chat channel late at night after work, the conversation is as likely to be about music, politics or girls as the latest in worm technology. "They're not talking about viruses -- they're talking about relationships or ordering pizza," says Sarah Gordon, a senior research fellow at Symantec, an antivirus company, who is one of the only researchers in the world who has interviewed hundreds of virus writers about their motivations. Very occasionally, malware authors even meet up face to face for a party; Philet0ast3r once took a road trip for a beer-addled weekend of coding, and when I visited Mario, we met up with another Austrian virus writer and discussed code for hours at a bar.

The virus community attracts a lot of smart but alienated young men, libertarian types who are often flummoxed by the social nuances of life. While the virus scene isn't dominated by those characters, it certainly has its share -- and they are often the ones with a genuine chip on their shoulder.

"I am a social reject," admitted Vorgon (as he called himself), a virus writer in Toronto with whom I exchanged messages one night in an online chat channel. He studied computer science in college but couldn't find a computer job after sending out 400 resumes. With "no friends, not much family" and no girlfriend for years, he became depressed. He attempted suicide, he said, by walking out one frigid winter night into a nearby forest for five hours with no jacket on. But then he got into the virus-writing

scene and found a community. "I met a lot of cool people who were interested in what I did," he wrote. "They made me feel good again." He called his first virus FirstBorn to celebrate his new identity. Later, he saw that one of his worms had been written up as an alert on an antivirus site, and it thrilled him. "Kinda like when I got my first girlfriend," he wrote. "I was god for a couple days." He began work on another worm, trying to recapture the feeling. "I spent three months working on it just so I could have those couple of days of godliness."

Vorgon is still angry about life. His next worm, he wrote, will try to specifically target the people who wouldn't hire him. It will have a "spidering" engine that crawls Web-page links, trying to find likely e-mail addresses for human-resource managers, "like careers@microsoft.com, for example." Then it will send them a fake resume infected with the worm. (He hasn't yet decided on a payload, and he hasn't ruled out a destructive one.) "This is a revenge worm," he explained -- for "not hiring me, and hiring some loser that is not even half the programmer I am."

Many people might wonder why virus writers aren't simply rounded up and arrested for producing their creations. But in most countries, writing viruses is not illegal. Indeed, in the United States some legal scholars argue that it is protected as free speech. Software is a type of language, and writing a program is akin to writing a recipe for beef stew. It is merely a bunch of instructions for the computer to follow, in the same way that a recipe is a set of instructions for a cook to follow. A virus or worm becomes illegal only when it is activated -- when someone sends it to a victim and starts it spreading in the wild, and it does measurable damage to computer systems. The top malware authors are acutely aware of this distinction. Most every virus-writer Web site includes a disclaimer stating that it exists purely for educational purposes, and that if a visitor downloads a virus to spread, the responsibility is entirely the visitor's. Benny's main virus-writing computer at home has no Internet connection at all; he has walled it off like an airlocked biological-weapons lab, so that nothing can escape, even by accident.

Virus writers argue that they shouldn't be held accountable for other people's actions. They are merely pursuing an interest in writing self-replicating computer code. "I'm not responsible for people who do silly things and distribute them among their friends," Benny said defiantly. "I'm not responsible for those. What I like to do is programming, and I like to show it to people -- who may then do something with it." A young woman who goes by the handle Gigabyte told me in an online chat room that if the authorities wanted to arrest her and other virus writers, then "they should arrest the creators of guns as well."

One of the youngest virus writers I visited was Stephen Mathieson, a 16-year-old in Detroit whose screen name is Kefi. He also belongs to Philet0ast3r's Ready Rangers Liberation Front. A year ago, Mathieson became annoyed when he found members of another virus-writers group called Catfish_VX plagiarizing his code. So he wrote Evion, a worm specifically designed to taunt the Catfish guys. He put it up on his Web site for everyone to see. Like most of Mathieson's work, the worm had no destructive intent. It merely popped up a few cocky messages, including: *Catfish_VX are lamers. This virus was constructed for them to steal.*

Someone did in fact steal it, because pretty soon Mathieson heard reports of it being spotted in the wild. To this day, he does not know who circulated Evion. But he suspects it was probably a random troublemaker, a script kiddie who swiped it from his site. "The kids," he said, shaking his head, "just cut and paste."

Quite aside from the strangeness of listening to a 16-year-old complain about "the kids," Mathieson's rhetoric glosses over a charged ethical and legal debate. It is tempting to wonder if the leading malware

authors are lying -- whether they do in fact circulate their worms on the sly, obsessed with a desire to see whether they will really work. While security officials say that may occasionally happen, they also say the top virus writers are quite likely telling the truth. "If you're writing important virus code, you're probably well trained," says David Perry, global director of education for Trend Micro, an antivirus company. "You know a number of tricks to write good code, but you don't want to go to prison. You have an income and stuff. It takes someone unaware of the consequences to release a virus."

But worm authors are hardly absolved of blame. By putting their code freely on the Web, virus writers essentially dangle temptation in front of every disgruntled teenager who goes online looking for a way to rebel. A cynic might say that malware authors rely on clueless script kiddies the same way that a drug dealer uses 13-year-olds to carry illegal goods -- passing the liability off to a hapless mule.

"You've got several levels here," says Marc Rogers, a former police officer who now researches computer forensics at Purdue University. "You've got the guys who write it, and they know they shouldn't release it because it's illegal. So they put it out there knowing that some script kiddie who wants to feel like a big shot in the virus underground will put it out. They know these neophytes will jump on it. So they're grinning ear to ear, because their baby, their creation, is out there. But they didn't officially release it, so they don't get in trouble." He says he thinks that the original authors are just as blameworthy as the spreaders.

Sarah Gordon of Symantec also says the authors are ethically naive. "If you're going to say it's an artistic statement, there are more responsible ways to be artistic than to create code that costs people millions," she says. Critics like Reitinger, the Microsoft security chief, are even harsher. "To me, it's online arson," he says. "Launching a virus is no different from burning down a building. There are people who would never toss a Molotov cocktail into a warehouse, but they wouldn't think for a second about launching a virus."

What makes this issue particularly fuzzy is the nature of computer code. It skews the traditional intellectual question about studying dangerous topics. Academics who research nuclear-fission techniques, for example, worry that their research could help a terrorist make a weapon. Many publish their findings anyway, believing that the mere knowledge of how fission works won't help Al Qaeda get access to uranium or rocket parts.

But computer code is a different type of knowledge. The code for a virus is itself the weapon. You could read it in the same way you read a book, to help educate yourself about malware. Or you could set it running, turning it instantly into an active agent. Computer code blurs the line between speech and act. "It's like taking a gun and sticking bullets in it and sitting it on the counter and saying, 'Hey, free gun!'" Rogers says.

Some academics have pondered whether virus authors could be charged under conspiracy laws. Creating a virus, they theorize, might be considered a form of abetting a crime by providing materials. Ken Dunham, the head of "malicious code intelligence" for iDefense, a computer security company, notes that there are certainly many examples of virus authors assisting newcomers. He has been in chat rooms, he says, "where I can see people saying, 'How can I find vulnerable hosts?' And another guy says, 'Oh, go here, you can use this tool.' They're helping each other out."

There are virus writers who appreciate these complexities. But they are certain that the viruses they write count as protected speech. They insist they have a right to explore their interests. Indeed, a number of them say they are making the world a better place, because they openly expose the weaknesses of computer systems. When Philet0ast3r or Mario or Mathieson finishes a new virus, they

say, they will immediately e-mail a copy of it to antivirus companies. That way, they explained, the companies can program their software to recognize and delete the virus should some script kiddie ever release it into the wild. This is further proof that they mean no harm with their hobby, as Mathieson pointed out. On the contrary, he said, their virus-writing strengthens the "immune system" of the Internet.

These moral nuances fall apart in the case of virus authors who are themselves willing to release worms into the wild. They're more rare, for obvious reasons. Usually they are overseas, in countries where the police are less concerned with software crimes. One such author is Melhacker, a young man who reportedly lives in Malaysia and has expressed sympathy for Osama bin Laden. Antivirus companies have linked him to the development of several worms, including one that claims to come from the "Qaeda network." Before the Iraq war, he told a computer magazine that he would release a virulent worm if the United States attacked Iraq -- a threat that proved hollow. When I e-mailed him, he described his favorite type of worm payload: "Stolen information from other people." He won't say which of his viruses he has himself spread and refuses to comment on his connection to the Qaeda worm. But in December on Indovirus.net, a discussion board for virus writers, Melhacker urged other writers to "try to make it in the wild" and to release their viruses in cybercafes, presumably to avoid detection. He also told them to stop sending in their work to antivirus companies.

Mathieson wrote a critical post in response, arguing that a good virus writer shouldn't need to spread his work. Virus authors are, in fact, sometimes quite chagrined when someone puts a dangerous worm into circulation, because it can cause a public backlash that hurts the entire virus community. When the Melissa virus raged out of control in 1999, many Internet service providers immediately shut down the Web sites of malware creators. Virus writers stormed online to pillory the Melissa author for turning his creation loose. "We don't need any more grief," one wrote.

If you ask cyberpolice and security experts about their greatest fears, they are not the traditional virus writers, like Mario or Philet0ast3r or Benny. For better or worse, those authors are a known quantity. What keeps antivirus people awake at night these days is an entirely new threat: worms created for explicit criminal purposes.

These began to emerge last year. Sobig in particular alarmed virus researchers. It was released six separate times throughout 2003, and each time the worm was programmed to shut itself off permanently after a few days or weeks. Every time the worm appeared anew, it had been altered in a way that suggested a single author had been tinkering with it, observing its behavior in the wild, then killing off his creation to prepare a new and more insidious version. "It was a set of very well-controlled experiments," says Mikko Hypponen, the director of antivirus research at F-Secure, a computer security company. "The code is high quality. It's been tested well. It really works in the real world." By the time the latest variant, Sobig.F, appeared in August, the worm was programmed to install a back door that would allow the author to assume control of the victim's computer. To what purpose? Experts say its author has used the captured machines to send spam and might also be stealing financial information from the victims' computers.

No one has any clue who wrote Sobig. The writers of this new class of worm leave none of the traces of their identities that malware authors traditionally include in their code, like their screen names or "greetz," shout-out hellos to their cyberfriends. Because criminal authors actively spread their creations, they are cautious about tipping their hand. "The F.B.I. is out for the Sobig guy with both claws, and they want to make an example of him," David Perry notes. "He's not going to mouth off." Dunham of iDefense says his online research has turned up "anecdotal evidence" that the Sobig author comes from

Russia or elsewhere in Europe. Others suspect China or other parts of Asia. It seems unlikely that Sobig came from the United States, because American police forces have been the most proactive of any worldwide in hunting those who spread malware. Many experts believe the Sobig author will release a new variant sometime this year.

Sobig was not alone. A variant of the Mimail worm, which appeared last spring, would install a fake pop-up screen on a computer pretending to be from PayPal, an online e-commerce firm. It would claim that PayPal had lost the victim's credit-card or banking details and ask him to type it in again. When he did, the worm would forward the information to the worm's still-unknown author. Another worm, called Bugbear.B, was programmed to employ sophisticated password-guessing strategies at banks and brokerages to steal personal information. "It was specifically designed to target financial institutions," said Vincent Weafer, senior director of Symantec.

The era of the stealth worm is upon us. None of these pieces of malware were destructive or designed to cripple the Internet with too much traffic. On the contrary, they were designed to be unobtrusive, to slip into the background, the better to secretly harvest data. Five years ago, the biggest danger was the "Chernobyl" virus, which deleted your hard drive. But the prevalence of hard-drive-destroying viruses has steadily declined to almost zero. Malware authors have learned a lesson that biologists have long known: the best way for a virus to spread is to ensure its host remains alive.

"It's like comparing Ebola to AIDS," says Joe Wells, an antivirus researcher and founder of WildList, a long-established virus-tracking group. "They both do the same thing. Except one does it in three days, and the other lingers and lingers and lingers. But which is worse? The ones that linger are the ones that spread the most."

In essence, the long years of experimentation have served as a sort of Darwinian evolutionary contest, in which virus writers have gradually figured out the best strategies for survival.

Given the pace of virus development, we are probably going to see even nastier criminal attacks in the future. Some academics have predicted the rise of "cryptoviruses" -- malware that invades your computer and encrypts all your files, making them unreadable. "The only way to get the data back will be to pay a ransom," says Stuart Schechter, a doctoral candidate in computer security at Harvard. (One night on a discussion board I stumbled across a few virus writers casually discussing this very concept.) Antivirus companies are writing research papers that worry about the rising threat of "metamorphic" worms -- ones that can shift their shapes so radically that antivirus companies cannot recognize they're a piece of malware. Some experimental metamorphic code has been published by Z0mbie, a reclusive Russian member of the 29A virus-writing group. And mobile-phone viruses are probably also only a few years away. A phone virus could secretly place 3 a.m. calls to a toll number, sticking you with thousand-dollar charges that the virus's author would collect. Or it could drown 911 in phantom calls. As Marty Lindner, a cybersecurity expert at CERT/CC, a federally financed computer research center, puts it, "The sky's the limit."

The profusion of viruses has even become a national-security issue. Government officials worry that terrorists could easily launch viruses that cripple American telecommunications, sowing confusion in advance of a physical 9/11-style attack. Paula Scalingi, the former director of the Department of Energy's Office of Critical Infrastructure Protection, now works as a consultant running disaster-preparedness exercises. Last year she helped organize "Purple Crescent" in New Orleans, an exercise that modeled a terrorist strike against the city's annual Jazz and Heritage Festival. The simulation includes a physical attack but also uses a worm unleashed by the terrorists designed to cripple communications and sow confusion nationwide. The physical attack winds up flooding New Orleans;

the cyberattack makes hospital care chaotic. "They have trouble communicating, they can't get staff in, it's hard for them to order supplies," she says. "The impact of worms and viruses can be prodigious."

This new age of criminal viruses puts traditional malware authors in a politically precarious spot. Police forces are under more pressure than ever to take any worm seriously, regardless of the motivations of the author.

A young Spaniard named Antonio discovered that last fall. He is a quiet 23-year-old computer professional who lives near Madrid. Last August, he read about the Blaster worm and how it exploited a Microsoft flaw. He became intrigued, and after poking around on a few virus sites, found some sample code that worked the same way. He downloaded it and began tinkering to see how it worked.

Then on Nov. 14, as he left to go to work, Spanish police met him at his door. They told him the anti-virus company Panda Software had discovered his worm had spread to 120,000 computers. When Panda analyzed the worm code, it quickly discovered that the program pointed to a site Antonio had developed. Panda forwarded the information to the police, who hunted Antonio down via his Internet service provider. The police stripped his house of every computer -- including his roommate's -- and threw Antonio in jail. After two days, they let him out, upon which Antonio's employer immediately fired him. "I have very little money," he said when I met him in December. "If I don't have a job in a little time, in a few months I can't pay the rent. I will have to go to my parents."

The Spanish court is currently considering what charges to press. Antonio's lawyer, Javier Maestre, argued that the worm had no dangerous payload and did no damage to any of the computers it infected. He suspects Antonio is being targeted by the police, who want to pretend they've made an important cyberbust, and by an antivirus company seeking publicity.

Artificial life can spin out of control -- and when it does, it can take real life with it. Antonio says he did not actually intend to release his worm at all. The worm spreads by scanning computers for the Blaster vulnerability, then sending a copy of itself to any open target. Antonio maintains he thought he was playing it safe, because his computer was not directly connected to the Internet. His roommate's computer had the Internet connection, and a local network -- a set of cables connecting their computers together -- allowed Antonio to share the signal.

But what Antonio didn't realize, he says, was that his worm would regard his friend's computer as a foreign target. It spawned a copy of itself in his friend's machine. From there it leapfrogged onto the Internet -- and out into the wild. His creation had come to life and, like Frankenstein's monster, decided upon a path of its own.

Clive Thompson writes frequently about science and technology. His last article for the magazine was about mobile-phone culture.

Copyright 2004 The New York Times Company | Home | Privacy Policy | Search | Corrections | Help | Back to Top

Ryan McGinley for The New York Times

Mario, a k a Second Part to Hell, Austrian virus writer.

Ryan McGinley for The New York Times

Benny, Czech Republic. 21-year-old master of malware and member of the international virus-writing group 29A.

Ryan McGinley for The New York Times

Stephen Mathieson, Detroit. The 16-year-old virus writer is dismissive of hackers who release other people's viruses: "The kids just cut and paste."