Malware Wars

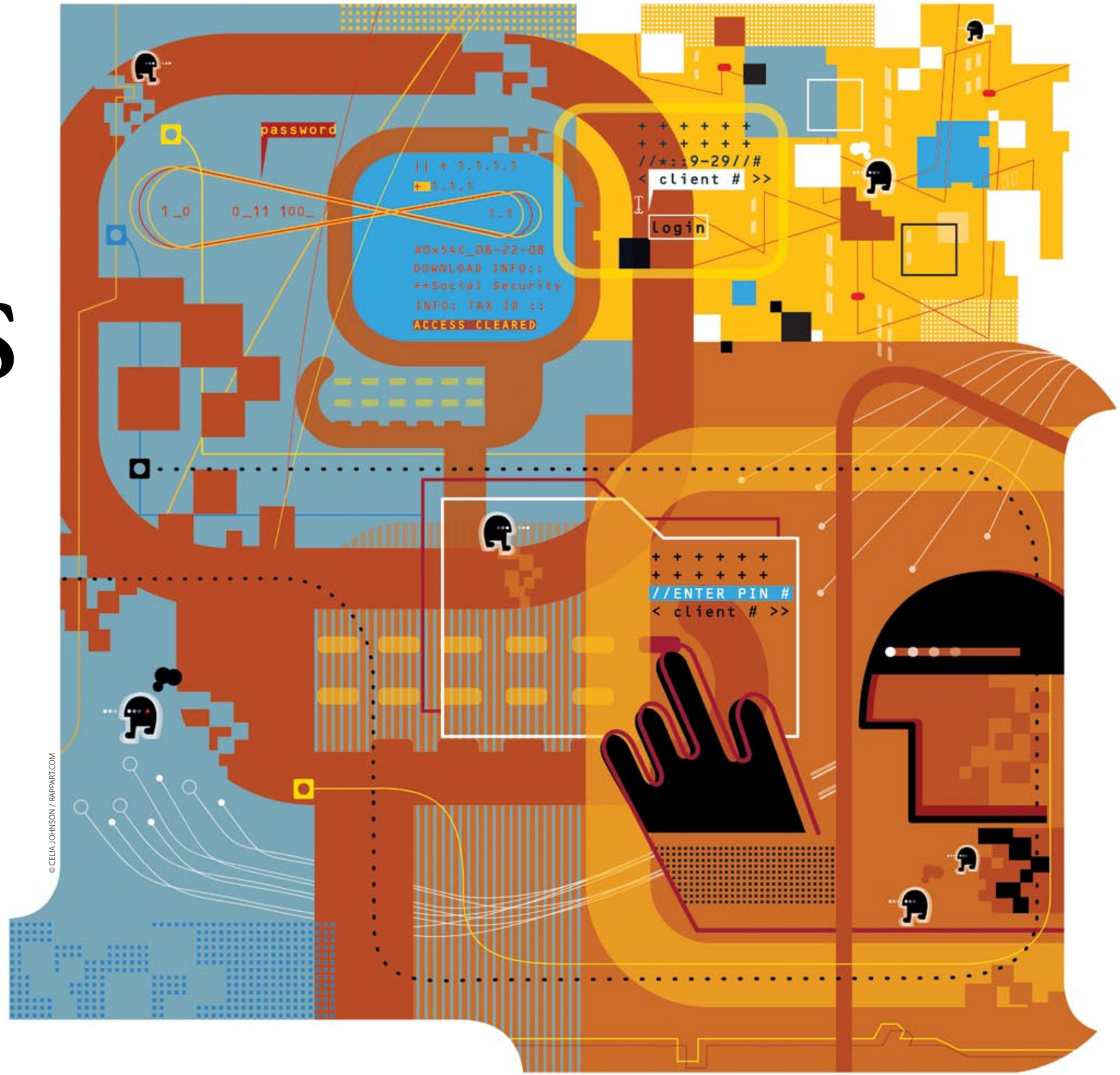
BY DEVON JACKSON

Vulnerabilities versus patches. Robustness versus phishing. Botnets versus evolvability. And complexity versus spam. Some of these terms and concepts are central to the work and philosophy of the Santa Fe Institute. Some, though, are more specific to the world of the Internet—as complex a system as any organic one.

The predators and parasites of this system are known as malware. Usually defined as software designed to infiltrate or damage a computer system without the owner's informed consent, malware (a combination of "malicious" and "software") ranges from computer worms, viruses, and identity theft to spam, spyware, and adware—as well as botnets, distributed denial-of-service attacks, phishing, pharming, and zombies. It's a multi-billion-dollar criminal industry, with its own language (called Eblish—an amalgamation of English, text messaging-speak, email-speak and whatever language happens to be native to the user, say, Nigerian, Mandarin or Romanian), and an emerging market economy. Malware's effects reach far beyond computers, and some fear that it threatens to drive the Internet, as most people know it, to extinction. That's why the Santa Fe Institute again agreed to host, for the second straight year, a workshop on how to deal with this potentially disastrous phenomenon.

This year's workshop, like the first, was organized by Matthew Williamson, a principal research scientist at Sana Security, and Eric Davis, a senior policy specialist at Google. The two-day event, entitled "Fighting Modern Malware II," included participants from academia, private corporations, and the government.

And beyond its economic and social impact, malware is the perfect lab rat for anyone interested in complexity, interconnectedness, and evolution. It's real, and it's global. As SFI Vice President Chris Wood observed, "Malware raises issues of evolvability, robustness, and diversity. It is computation in the wild."



According to a recent survey, "The 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and other Malicious Code," conducted by *Computer Economics*, a monthly information technology newsletter, the worldwide economic impact of malware is in decline: dropping from a high of $17.5 billion in damages in 2004 to $14.2 billion in 2005 to $13.3 billion in 2006. But *Computer Economics*' editors cautioned against over-optimism: "Although direct damages of malware may be declining," they wrote, "the indirect or secondary damages are likely increasing." As pointed out by Stefan Savage, associate professor of computer science and engineering at the University of California at San Diego and the director of the school's Collaborative Center for Internet Epidemiology and Defenses (a joint effort between UCSD and the International Computer Science Institute), "We really don't know precisely how big this problem is, but we know it's large and growing."

Hence, a prevailing sense of urgency (if not impending doom) among the workshop's 18 participants. "My fear is that the horses are already out of the barn and it'll be impossible to get them back in," said Howard Cox, the Department of Justice's Computer Crime Division assistant deputy chief.

"We're in the third generation of this. The juveniles of yesterday—the hackers and the Defcon wannabes—have turned into adults and have figured out, 'We can now make money at this thing.'" He noted that the economic incentive makes it almost impossible to stop people from getting into malware. "We're dealing with a criminal enterprise equivalent to the Mafia, and one that has no leader," he added.

Malware's engineers are moving at warp speed. But the guys in the white hats, as the anti-malware folks sometimes call themselves (or, alternatively, the Jedi Council), have had their hands tied. "These bad guys exist in a world without boundaries," said former Secret Service agent Robert Rodriguez, a sentiment echoed by Google's senior staff engineer,

> Malware is the perfect lab rat for anyone interested in complexity, interconnectedness, and evolution. It's real, and it's global. As SFI Vice President Chris Wood observed, "Malware raises issues of evolvability, robustness, and diversity. It is computation in the wild."

Niels Provos, an expert on honeypots—computer systems set up as traps for attackers. "The development and acceleration of malware in China and elsewhere has gotten to the point where we can't keep up," he said.

"We're just not adapting quickly enough," added Pittsburgh-based FBI agent Michael McKeown, who, like Cox, sees a trend toward organized crime and a global network. "We are doomed to be reactive," warned Savage.

Given that 80 percent of all malware attacks originate outside the U.S., American authorities often find themselves in dire need of cooperation from authorities in the country from which the malware was initiated. And the situation would be easier if other countries had similar laws to those in the U.S., or any laws at all. Many, however, have yet to even outlaw malware, much less understand it. Still, as difficult as it may be to prove that, say, someone in Latvia sent out a virus, it's Cox's belief that the laws currently in place are, for the most part, adequate. "We have the laws we need," says Cox. "What's lacking is attribution, number one, and getting data from other countries. Beyond that, we also need more reporting of Internet crimes—both from our own private businesses and from our government agencies."

And, as if to add emphasis to his point about the adequacy of existing laws, Cox recently reported to the group the arrest of Alan Ralsky, the self-proclaimed "King of Spam." Cox emphasized, "As I stated at the conference, the criminal justice process is not the first line of response in addressing malware, but to the extent that malware is a form of computer crime, this case demonstrates that even kings are not out of reach."

The Jedi Council Versus the Malwarts

So, in a world where everyone's vulnerable but no one is accountable, who should be held liable? The browser? The user? The Internet service provider (ISP)? "The decision on where you invest your effort is important," said Savage. "In malware, the problems change so quickly. Last year's problems are not this year's problems." The moving target of malware makes it hard to figure out where to invest one's efforts—viruses sent over email are not the problem they once were. Instead, attacks sent via browsers and malicious web pages are a growing threat.

Which is why it's just as important to determine *how* to invest one's effort. Given that exploiting a weakness is usually easier than patching it up, no wonder the containment, let alone defeat, of malware seems a Sisyphean task. "Our patches to fix up holes is like the whack-a-mole game, only in technological terms," said Savage.

It's a problem of scale, as well as speed—one software bug equals millions of compromised hosts. The bad guys can scale up faster because they have no laws, no rules, and no boundaries. The good guys—banks especially, agreed the Jedis—remain loath to share information with each other, with law enforcement, with their customers, or the public. Competition frustrates cooperation, and intellectual property laws, too, serve to suppress anti-malware innovations.

And the problem with most anti-malware innovations is that they tend to come at the expense of overall ease: one more lock on the door may slow down an intruder but it also slows down the owner when getting in or out—and that newfangled new lock won't come free, either. "If we introduce frictions (anti-malware actions) into the equation," said Savage, "then we introduce them into the transaction cost." The goal is to put a drag on the bad guys without imposing an equal amount of drag on the good guys. Otherwise, the future looks rather Orwellian. "My fear is that in the effort to secure the industry, we'll see people's rights trampled," said Vincent Weafer, a member of Symantec's Security Response Team. "And that there'll be these country-wide firewalls enacted under the guise of security."

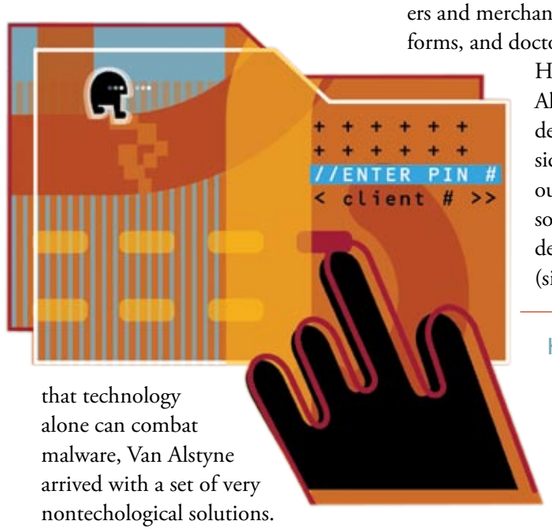
Whatever technological solutions arise out of the workshop, most of its participants more or less agree that economics drives malware. Take the incentives away, devalue them, or redirect malware engineers toward beneficent incentives, and the Internet may survive. "My hope is that we can

In this fictional scenario, an attacker (green) hires bot herders (blue) to give instructions to zombies—computers infected by their malware (white), which hit designated targets.

ABOVE : CATALOGTREENET FOR *WIRED* MAGAZINE

find economic disincentives so that people don't use malware or invest in it," said Ari Schwartz, who works on privacy and government-information issues for The Center for Democracy and Technology, a nonprofit advocacy group that helped various anti-spyware companies form a coalition.

"We need to attack their revenue streams," declared Marshall Van Alstyne, an associate professor at Boston University and visiting professor at MIT who specializes in the economics of information. An avowed skeptic



that technology alone can combat malware, Van Alstyne arrived with a set of very nontechological solutions. In a quick overview of his paper, "An Economic Response to Unsolicited Communication" (i.e., spam—which costs about $50 billion a year in losses and makes up 92 percent of all email), Van Alstyne outlined a very cogent and rather elegant three-pronged attack, based on the economic principles of information asymmetry, two-sided networks, and externalities.

Information asymmetry, he explained, exists when one party to a transaction has more information than another party. Principles of information asymmetry can be used to force the more knowledgeable party to disclose what they know. This method can help reveal someone's true intentions, for example, when they want a party to read their message or install their applet. Two-sided networks, he explained, are matching markets with two distinct user groups who provide each other with benefits. Common examples include cardholders and merchants on credit card platforms, and doctors and patients on HMO platforms. Van Alstyne, who helped develop theories of two-sided networks, pointed out that they often have sophisticated fraud-detection techniques (similar to those used to catch credit card and insurance fraud), that can be applied to fight malware. Lastly, externalities may be useful. An externality is an impact (positive or negative) on any party not involved in a given transaction. Van Alstyne showed how liability laws that are currently in place for other types of cases might be applied with success toward malware problems.

Savage, too, dealt with the economics of malware, although more from an observer's perspective than an economist's. He presented some of the mechanics of malware's underground economy. Malware has gone from being a reputation economy—in which people hacked for kudos—to a complex, stratified profit economy, in which people are innovating all the time. "They even try to phish each other and ruin each other's reputations," said Lance James, author of *Phishing Exposed* and an expert on phishing and malware who heads up Security Science Corporation's External Threat Assessment Team. (Phishing uses social engineering tactics as a way to obtain access to user names, passwords, identity information, credit cards, and other personal and corporate data; it also relies heavily on botnets, software robots that run autonomously and automatically, usually on groups of zombie computers controlled remotely.)

> How have hosts fought off parasites in the past? Hope that the host is robust enough, implied Gleichauf, Savage, and others, to withstand a parasite as nasty and evolvable as malware.

So, proposed Savage and James, the solution may be to attack the malware market, as well as its still intact reputation-based system. They also advocated attacking the malware industry economically, disrupting its efforts to launder its profits.

Is Complexity Science the Solution?

Economic solutions. Technological solutions. Legal factors, industry factors. Phishing, patching, spamming, friction. Do they work? Will they? Or does it just boil down to so much tilting at windmills? Or might it all simply be part of some grander digital design that's still evolving?

Enter Lee Altenberg, an associate professor in the Department of Information and Computer Sciences at the University of Hawaii who teaches exclusively online and specializes in evolutionary theory and population genetics. He thinks that programs behave enough like organisms that some lessons from nature might be applicable to the Internet and malware. Altenberg gently coaxed the complexity cat out of the malware bag.

A major contributor to the complexity discussion was Robert Gleichauf, a former Ph.D. candidate in anthropology who is now the Chief Technology Officer for Cisco's Security Technology Group. A realist as well as a ponderer, he is anything but blasé about the effects and potential of malware; nor does he see it as a necessary evil, or think that the death of the Internet is imminent. He does, however, believe in leveling mechanisms, and keeps an eye out for events that can lead to large evolutionary swings. "Yes, we need to minimize the impact of perturbations," says Gleichauf, "but, after all, there's a life cycle of information. Things tend to find their stasis point."

"The question is," he continued, "when you factor in the losses against the total amount of money going across the Internet, at what point is the pain of losses so high that you take action?" He asked later on, during one of the workshop's tactical sessions: "How much of malware crime levels itself out? If you can isolate these upper-tier forces—not the ankle-biters—will they regulate themselves?" And later still, he speculated, "If we stop trying to improve the Internet, our products and all things related to it, maybe they'll stop."

Robustness to the Rescue?

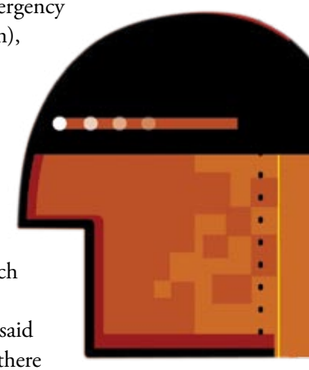
Malware is parasitic on the software, hardware, systems, and users of the Internet. How, then, have hosts fought off parasites in the past? In nature? In other economic systems? What's the proper co-evolutionary response, if any? Hope that the host is robust enough, implied Gleichauf, Savage, and others, to withstand a parasite as nasty and evolvable as malware. Gleichauf, for one, wanted more discussion on robustness. It's his belief that email systems are robust enough to survive. "But that's not so in banking," he said, "which is founded on trust, which doesn't work electronically."

Or do we latch on to a punctuating event—some major shift or development—mused Gleichauf, to escape the parasites? "Is there a punctuated event about to happen?" he asked. "Right now, that's what we're looking for at Cisco: the browser versus the mobile market," referring to the current merging of computer technology with technology that's mobile, such as phones and iPods.

Eventually, the complexity-fueled debate came back to the threat itself. "The rate of evolution for bad guys is so much higher," said Savage. "Malware has such high evolvability, it may evolve to the point where the Internet is no longer useable."

"What we're trying to do," said Gleichauf, "we're trying to maintain the functionality of old systems."

Old, antiquated, not as robust as they need be. And doomed, perhaps, though no one has yet given up. If anything, meetings such as this, and other SFI workshops, which encourage collaboration and cross-pollination, infuse participants with a renewed sense of purpose. In this case, the group will come up with a set of anti-malware action points. They will hold regular meetings, both real and virtual—that will include representatives from the banking industry, the insurance industry, U.S. CERT (the Computer Emergency Readiness Team), Amazon, eBay, Yahoo and/or Earthlink, and Microsoft. Beyond that, they also want to establish a malware research institute.



"My hope," said Davis, "is that there are livable boundaries. That there will be a malware crime rate, that's pretty much unavoidable. But people will know what to do and what not to do." That's the hope anyway. ◀

Devon Jackson is a freelance writer based in Santa Fe. He writes regularly for Southwest Art, *and has written for* Smithsonian, Outside, The New York Times *and many other magazines and newspapers. He is also the author of* Conspiranoia!