NET OF INSECURITY

A disaster foretold — and ignored

LOpht's warnings about the Internet drew notice but little action

Story by Craig Timberg

Published on June 22, 2015

The making of a vulnerable Internet: This story is the third of a multi-part project on the Internet's inherent vulnerabilities and why they may never be fixed.
Part 1: The story of how the Internet became so vulnerable.
Part 2: The long life of a 'quick fix.'
Part 4: How yesterday's flaws are being built into tomorrow's connected world.
Part 5: The kernel of the argument.
Read the eBook. The Threatened Net: How the Internet Became a Perilous Place

Above: L0pht hackers Brian Oblivion, Tan, Kingpin, Mudge, Weld Pond, Space Rogue and Stefan von Neumann testify before a Senate panel in 1998. (Douglas Graham/Congressional Quarterly via Getty Images)

The seven young men sitting before some of Capitol Hill's most powerful lawmakers weren't graduate students or junior analysts from some think tank. No, Space Rogue, Kingpin, Mudge and the others were hackers who had come from the mysterious environs of cyberspace to deliver a terrifying warning to the world.

Your computers, they told the panel of senators in May 1998, are not safe — not the software, not the hardware, not the networks that link them together. The companies that build these things don't care, the hackers continued, and they have no reason to care because failure costs them nothing. And the federal government has neither the skill nor the will to do anything about it.

"If you're looking for computer security, then the Internet is not the place to be," said Mudge, then 27 and looking like a biblical prophet with long brown hair flowing past his shoulders. The Internet itself, he added, could be taken down "by any of the seven individuals seated before you" with 30 minutes of well-choreographed keystrokes.

The senators — a bipartisan group including John Glenn, Joseph I. Lieberman and Fred D. Thompson — nodded gravely, making clear that they understood the gravity of the situation. "We're going to have to do something about it," Thompson said.

What happened instead was a tragedy of missed opportunity, and 17 years later the world is still paying the price in rampant insecurity.

The testimony from L0pht, as the hacker group called itself, was among the most audacious of a rising chorus of warnings delivered in the 1990s as the Internet was exploding in popularity, well on its way to becoming a potent global force for communication, commerce and criminality.

Hackers and other computer experts sounded alarms as the World Wide Web brought the transformative power of computer networking to the masses. This created a universe of risks for users and the critical real-world systems, such as power plants, rapidly going online as well.

Officials in Washington and throughout the world failed to forcefully address these problems as trouble spread across cyberspace, a vast new frontier of opportunity and lawlessness. Even today, many serious online intrusions exploit flaws in software first built in that era, such as Adobe Flash, Oracle's Java and Microsoft's Internet Explorer.

"We have the same security problems," said Space Rogue, whose real name is Cris Thomas. "There's a lot more money involved. There's a lot more awareness. But the same problems are still there."

Lopht, born of the bustling hacker scene in the Boston area, rose to prominence as a flood of new software was introducing such wonders as sound, animation and interactive games to the Web. This software, which required access to the core functions of each user's computer, also gave hackers new opportunities to manipulate machines from afar.

Breaking into networked computers became so easy that the Internet, long the realm of idealistic scientists and hobbyists, gradually grew infested with the most pragmatic of professionals: crooks, scam artists, spies and cyberwarriors. They exploited computer bugs for profit or other gain while continually looking for new vulnerabilities.

Tech companies sometimes scrambled to fix problems — often after hackers or academic researchers revealed them publicly — but few companies were willing to undertake the costly overhauls necessary to make their systems significantly more secure against future attacks. Their profits depended on other factors, such as providing consumers new features, not warding off hackers.

"In the real world, people only invest money to solve real problems, as opposed to hypothetical ones," said Dan S. Wallach, a Rice University computer science professor who has been studying online threats since the 1990s. "The thing that you're selling is not security. The thing that you're selling is something else."

The result was a culture within the tech industry often derided as "patch and pray." In other words, keep building, keep selling and send out fixes as necessary. If a system failed — causing lost data, stolen credit card numbers or time-consuming computer crashes — the burden fell not on giant, rich tech companies but on their customers.

The members of Lopht say they often experienced this cavalier attitude in their day jobs, where some toiled as humble programmers or salesmen at computer stores. When they reported bugs to software makers, company officials often asked: Does anybody else know about this?

Peiter Zatko, a.k.a. Mudge, once delighted in tweaking Microsoft as he described cracking its password security on Windows. Years later, the decline of L0pht took a toll on him. (Nick Otto for The Washington Post)

Geek heaven in a Boston loft

The hackers met online, mostly on the bulletin boards that provided computer enthusiasts with freewheeling forums for trading tips, jokes and insights about how various systems worked — and in some cases could be made to do things their creators never intended. This is the essence of hacking. It is not inherently good or evil. It can be either, or in some cases a combination of both, depending on the motives of the hackers.

L0pht's members — the exact list shifted year to year but averaged seven or eight — shared a fascination with technology and a knack for testing its limits. They would decode the program running a piece of hardware or repeatedly flood a password field with too many characters, a hack known as a "buffer overflow" that often caused systems to fail, opening the door to further manipulation.

"The difference between how it's supposed to work and how it really works is where the vulnerabilities happen," said Chris Wysopal, known as Weld Pond in his L0pht days.

The group's first clubhouse — and the inspiration for the name — was an actual loft above a carpentry shop in Boston's South End neighborhood, rented after the girlfriend of one of the hackers grew weary of all of the old computer gear littering their apartment (including several pieces resting semi-permanently in their bathroom).

Like the Internet itself, there seemed to be peril on the down-and-out streets all around L0pht's loft in this pre-gentrification era. But inside was geek heaven, with cast-off computers, a television, a couch, cold beer, a 1980s-vintage "Battlezone" arcade game and a curious array of second-hand mannequins wearing unusual adornments, including a skirt, a gas mask and the charred remnants of a police uniform that the hackers found. In a stroke of luck, the landlord paid the electrical bill each month, keeping an endless lifeline of electrons flowing to what amounted to a power-hungry computer lab.

"It was totally scary to get there, but once you got there it was like, 'Ahhhhh,' " recalled Joe Grand, a mischievous skateboarding enthusiast who was L0pht's youngest member. "It really was a refuge in a lot of ways. It really shaped my life."

Much of the gear they used — and tried to bend to their wills — had been collected from dumpsters around the tech-heavy Boston area. L0pht's members refurbished some hardware to sell at flea markets to help pay the bills, but they kept the most useful pieces, including a giant VAX computer — a hunk of 1970s-vintage technology featuring two units, each the size of a washing machine — that they somehow hauled up steep stairs and into the loft.

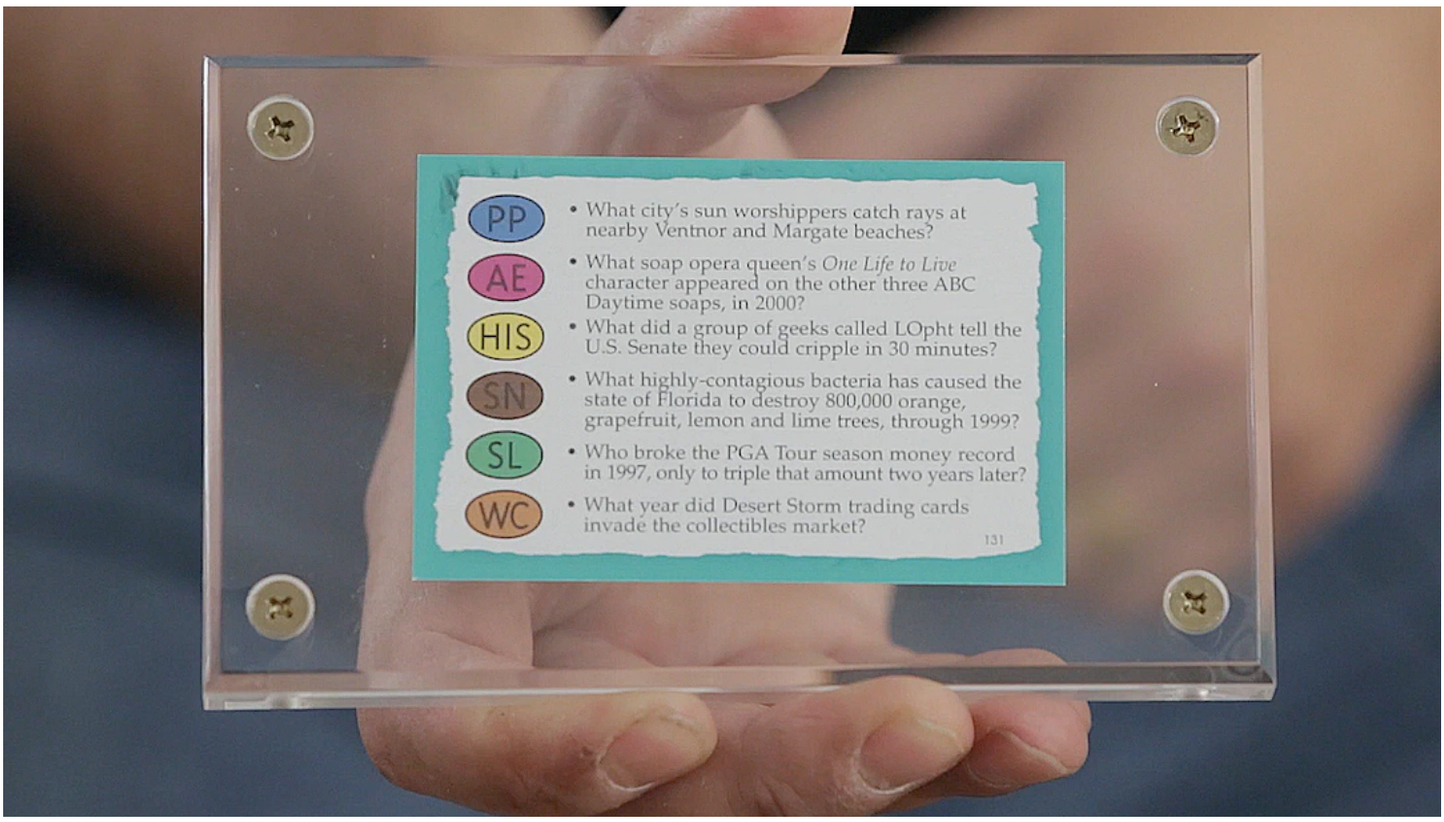
They came to particularly disdain what they considered security-by-checklist, when companies declared a product safe merely because they had implemented a specified number of standard features, such as passwords and basic cryptography. "We'd say, 'Give us one. We're going to try to break into it,' " recalled Wysopal.

They almost always did, usually after toiling late into the night in a frenzy of discovery, flooding systems with inputs that programmers had not anticipated or in any way prepared for. Paul Nash, whose hacker name was Silicosis, once discovered that he could knock computers using Microsoft's Windows operating systems offline by sending a single command — a trick he happily showed off to visitors.

When members of Lopht weren't trying to find their own bugs, they were supporting others in doing so, including through regular gatherings at a Boston bar in which anyone who revealed a new computer vulnerability got a free beer. Lopht also spread the word about security discoveries though the Hacker News Network, a popular online newsletter run by Space Rogue, a born tinkerer who had rigged up makeshift flashlights so he could read in bed at night as a kid. (He still routinely uses his hacker name today.)

Hacker News Network grew popular enough that it drew interest from advertisers. The group didn't want to sully its main Web site, Lopht.com, but was happy to collect revenue from Hacker News Network. One of the earliest ads touted the availability, for a fee, of Russian brides.

Video: How a hacker group came to Washington



Exposing bugs for all to see

Lopht partially embraced the bad-boy image of hackers, calling themselves "gray hats," a middle ground between the avowedly virtuous "white hat" hackers and the openly outlaw "black hats." The group took particular relish in trying to shame big companies, such as Microsoft, for selling products with security flaws to unsuspecting customers.

When Lopht discovered a way to crack the cryptography protecting user passwords for the Windows operating system, Mudge publicly chastised Microsoft for what he called "kindergarten crypto" and, along with Wysopal, created an easy-to-use software tool to help anyone defeat it. Lopht member Dildog developed a program with another hacker group, called Cult of the Dead Cow, to remotely control office networks running Microsoft software. The name, a spoof on the company's popular "BackOffice Server 2000" program, was "Back Orifice 2000"; the promotional materials featured an equally crude logo.

But the reality of Lopht was more conventional than the public image. Wysopal was a programmer for Lotus. Space Rogue and two others worked at CompUSA, a chain store.

Several had jobs at BBN Technologies, a venerable tech company that years earlier helped build the most important forerunner to the Internet, a Pentagon-funded project called the ARPANET.

The men used their hacker names mainly because they feared getting fired if their employers learned of their nocturnal activities. (The other reason, nearly as important, was that they wanted to make it harder for companies facing embarrassing disclosures to sue them or call the cops — real threats, then and now, for anyone doing freelance security research.)

The day jobs also provided an insider view of the burgeoning tech industry, helping the hackers find bugs in widely used business or consumer products. Companies that seemed unresponsive to complaints through formal channels often found themselves in L0pht's cross hairs. The group maintained open lines to legions of other hackers — including those working inside big tech firms — and developed disdain for a business culture they say put profit above security.

"It's get it up, get it running as fast as we can. Let's make some money," Nash said. "There's this tremendous push to get code out the door, and we'll fix it later."

L0pht also came to doubt the eagerness of companies to fix flaws even after they had been discovered. In the early years of the group, reports to official company e-mail addresses — purportedly established to solicit security concerns — often seemed to just disappear into a black hole. A particular offender, L0pht members said, was secure@microsoft.com.

They eventually discovered a reliable way to get companies' attention: Security alerts posted on L0pht.com drew notice from the world's technology journalists and eventually the companies themselves.

The downside was that plenty of "black hat" hackers also monitored L0pht's alerts, giving them time to take advantage of bugs before companies could possibly fix them. There's no way to know how many intrusions this aided, but the members of L0pht were unapologetic.

"We always thought that if we knew about it, other people probably know about it and are exploiting it," said Grand, formerly known as Kingpin.

"Black hat"/"White Hat" hackers

People who exploit flaws in computer systems. Security experts who seek to find and fix flaws often call themselves "white hat" hackers. Criminal or malicious hackers are called "black hats."

Members of L0pht, including, from left, Tan, Kingpin, Weld Pond, Mudge and Brian Oblivion, rented a van for their trip to Washington for their Senate testimony in May 1998. The hackers outside their hotel on the morning of their testimony: from left, Kingpin, Brian Oblivion, Weld Pond, Tan, Mudge (kneeling), Space Rogue and Stefan von Neumann.

Bill Gates rides 'Tidal Wave'

The 1993 arrival of the first widely popular Web browser, Mosaic, made the Internet an unstoppable cultural and commercial force. Suddenly it wasn't an exotic, far-off wonderland for the technically adept. Anybody could "surf the Web."

Over the next several years, sophisticated new programming languages such as Flash and Java dramatically expanded browsers' capabilities. Web sites began streaming video. Classic games such as "Frogger," "Super Mario Bros." and "Tetris" could be played, free of charge, on any computer that could get online.

For most users, these new features seemed almost magical. They appeared automatically, perhaps requiring just a click or two of a mouse. Soon, most computers in the world had Flash and similar programming languages on their hard drives.

Surging consumer interest was not lost on Microsoft co-founder Bill Gates, who penned a confidential memo to his top executives in May 1995 titled "The Internet Tidal Wave." The 5,500-word document demanded in sweeping, urgent terms that the company compete forcefully in the explosive new online marketplace.

"The next few years are going to be very exciting as we tackle these challenges and opportunities," Gates wrote. "The Internet is a tidal wave. It changes the rules. It is an incredible opportunity as well as incredible challenge. I am looking forward to your input on how we can improve our strategy to continue our track record of incredible success."

Gates did warn about the importance of security in the memo, saying "Our plans for security need to be strengthened." But he also said, "I want every product plan to try and go overboard on Internet features."

This priority, many critics would later say, was the most important one to Microsoft, planting the seeds of what security experts called "featuritis" — a common malady in which new features are added more quickly than they can be made secure.

This rush to innovate, to make every Microsoft product essentially an Internet product, was felt deeply throughout the company, said Billy Brackenridge, a Microsoft program manager during the 1990s. The ability to deliver new features for the company's marquee operating systems and software determined who got stock options — a key motivator for a company whose stock split seven times that decade amid a total gain of more than 9,000 percent.

"There may have been one or two guys who really cared [about security]. For the most part, it was, 'Get it out the door,' " Brackenridge recalled. "If we missed a date, that was real money. . . . If your feature didn't get in, you didn't get stock."

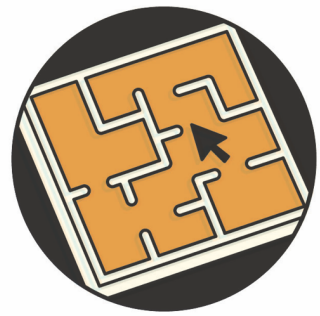
Microsoft's competitive juices fueled a furious push to develop a browser to challenge the primacy of Netscape Navigator, which was produced largely by the same team of programmers who had created Mosaic. By the mid-1990s, Navigator had more than 70 percent market share, Gates warned in his memo.

The Microsoft answer was to create Internet Explorer and to integrate the browser extensively with its dominant Windows operating system. This effort was central to the Justice Department's antitrust charges against Microsoft, which were settled in 2001.

But it had other effects more immediately noticeable to L0pht and other hackers.

As Microsoft worked to infuse Internet-related features into its products, the company created portals for hackers to discover and exploit. A particularly notorious one was a programming language called ActiveX, which like Flash and Java reached deeply into the brains of a user's computer.

"Once you go to a Web site and download some code and it executes itself . . . you have a whole new type of problem," said Giovanni Vigna, a computer scientist at the University of California at Santa Barbara and co-founder of Lastline, a security company. "Now I have running code on your machine, and I can do all sorts of interesting things."



Browser

A program that allows people to access the Web. Browsers pull information from a variety of servers across the Internet and can expose users to security risks.

Cris Thomas, a.k.a. Space Rogue, had a day job at CompUSA when he was a member of L0pht. (Bill O'Leary/The Washington Post)

700 users, 1 dumb password

At a hacker conference in August 1997, Mudge — whose real name is Peiter Zatko and who infused a zeal for showmanship into L0pht — visibly delighted in tweaking Microsoft as he described cracking the password security on Windows, at the time the standard operating system for business and government computers worldwide.

“I don’t want to be working on Microsoft products right now,” Mudge declared. “The problem is: They’re everywhere! You cannot get away from them!”

He singled out a particularly egregious security flaw — splitting a strong 14-character password field into two much weaker seven-character passwords for storage. The longer a password, the more combinations a hacker must try to break it. But Microsoft, Mudge reported, had undermined that principle by creating, in essence, two shorter and easily cracked passwords instead of one strong one.

Worse still, if the user had picked a password that was seven characters or fewer, the system stored a telltale string of characters to represent the unused portion of the password field. When hackers found this string, they knew that they already had the password halfway cracked. Mudge happily recited the odd combination of letters and numbers at the conference, with dozens of hackers looking on.

“I’m going to get that tattooed across my forehead and walk through the halls of Microsoft!” he said to laughter from the crowd.

He also announced that L0pht had discovered that a single password — “CHANGEME” — was being used by 700 users of one network the group studied.

Such antics drew fans within the hacker world, a hint of wider celebrity and the first whiff of money. L0pht sold T-shirts bearing its logo at conferences and also began selling its tool for cracking Windows passwords — called L0pht Crack — for $50 to system administrators eager to test the strength of passwords on the networks they managed.

When the members of L0pht realized how much security consultants were charging for such services, they raised the price to $150, then $500. (One of the buyers was the Government Accountability Office, a federal watchdog agency that chronicled failings of federal IT systems).

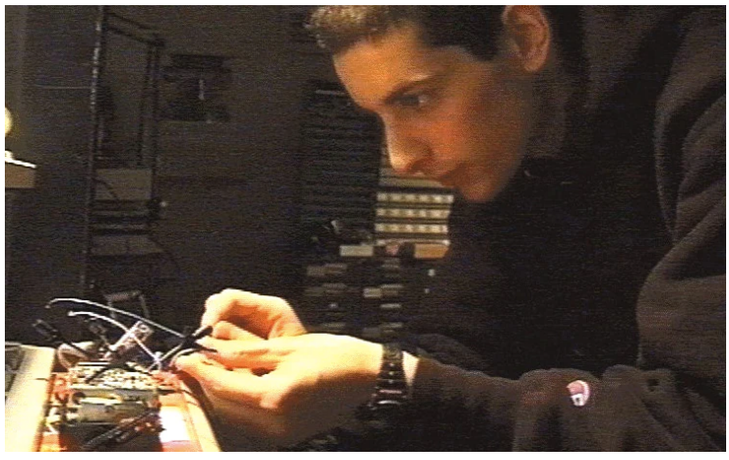
For all L0pht's drive to break systems online, members had long run their club with a certain formality. They had regular meetings, set collective priorities and handled financial matters carefully. Each hacker had his own desk and paid $100 a month toward rent; those who couldn't afford that would share desks and pay half as much.

But the money rushing into computer security got their attention. They got a first taste of it when the online ads along with sales of T-shirts and L0pht Crack meant that members no longer had to reach as deeply into their own pockets for rent or other costs. They also noticed how a rising generation of security consultants — including some doing "stress testing" using tactics much like L0pht's — were getting big paydays.

By the time L0pht appeared before the Senate in 1998, the idea of starting a real company — and earning enough profit to quit their day jobs — was starting to form within the group.

"You know," Space Rogue remembered thinking, "maybe we should get a piece of that."

This was the beginning of the end for L0pht.



Joe Grand, a.k.a. Kingpin, in 1996, modifying a radio to receive pager and police mobile data terminal transmissions. (Courtesy of Joe Grand)
A loft above a carpentry shop in Boston's South End neighborhood provided the inspiration for L0pht's name. Much of the computer hardware in the space was scavenged from Boston-area dumpsters. (Courtesy of Joe Grand)

A close call at the NSA

They had an uproariously fun trip to Washington for the Senate testimony, renting a dark green, 15-passenger van and installing an array of antennas on the roof to see what signals they could pick up along the way.

This seemed like harmless hacker fun until they made a stop at the National Cryptologic Museum, on the grounds of the National Security Agency in suburban Maryland. Zatko had visited the NSA several times before, he said, part of gradual move into federal government work. "I wanted them to have sensitivities, to know that hackers aren't the bad guys," he explained later.

But on this trip, Zatko accidentally directed the L0pht van, its roof bristling with interception equipment, to the entrance of a secure area of the NSA campus. Driving the van was L0pht member Stefan von Neumann, who appeared confused when he pulled up to a checkpoint manned by an armed military guard. When the guard saluted von Neumann, whose real name is Stefan Wuensch, he asked his fellow hackers, "What should I do?"

In unison, they shouted, “Salute back!”

But once on the grounds of the famously secret spy agency, the members of L0pht quickly grew uneasy and urged von Neumann to exit the grounds as quickly as possible. He soon did, getting the van to the museum, then onward to Washington without further incident.

The hackers testified the following day before the Senate Governmental Affairs Committee, whose staffers told L0pht that only members of federal witness protection programs had previously been allowed to testify using aliases. The hackers then took a tour of the White House, guided by National Security Council counterterrorism official Richard A. Clarke.

A cover story in Internet Week magazine, featuring Wysopal and Zatko (a.k.a. Weld Pond and Mudge), finally blew their cover at work, but they weren’t fired as they had feared. The New York Times Magazine also featured L0pht in a story, as did PBS and MTV. The hackers’ boasts about being able to take down the Internet in 30 minutes — by exploiting flaws in a key Internet routing protocol called BGP — prompted mentions from Conan O’Brien and Rush Limbaugh, who called them “long-haired nerd computer hackers.”

Even the makers of Trivial Pursuit took notice. Question: What did a group of geeks called L0pht tell the U.S. Senate they could cripple in 30 minutes?

Answer: The Internet

By the time that edition of the game hit the stores in 2000, L0pht was no longer L0pht. The hackers had joined @Stake, a security company built largely on L0pht’s fame and $10 million in venture-capital funding. They quit their day jobs to finally pursue their nocturnal hobby full time.

But they also acquired an unwelcome new set of rules and responsibilities — especially to clients who were happy to pay for their expertise but didn’t fancy getting publicly roasted whenever the hackers discovered problems.

“The community we came from thought we were selling out to the Man, which of course we were,” Wysopal recalled.

Among the biggest companies to hire @Stake — and demand nondisclosure agreements about what they found — was L0pht’s longtime nemesis: Microsoft.

Chris Wysopal, known as Weld Pond during his L0pht days, stands in front of a projection of the group's Web home page. Wysopal and a fellow L0pht hacker, Dildog, founded the security company Veracode in 2006. (Bill O'Leary/The Washington Post)

Dropping the ax

As business realities set in, Space Rogue was the first casualty. He had run the operations side of Lopht and also Hacker News Network. But the venture capitalists had their own operational guys, and they weren't keen on publicly affiliating themselves with the word "hacker."

So the online newsletter became a sanitized corporate Web site called "Security News Network," and Space Rogue got a job in @Stake's marketing department — far from the center of gravity where Mudge, Kingpin, Weld Pond and the others worked. Space Rogue was fired soon after.

The company confiscated his laptop computer and unceremoniously escorted him out the door for reasons he says he still doesn't understand. By the time Space Rogue got home, his Lopht.com accounts had been shut down. He had no idea — and still doesn't — whether any of his fellow hackers spoke up for him or fought the firing.

"That was a bad part of my life. . . . I lost six of my best friends," Space Rogue recalled. "It was really devastating to me. It took me a long time to recover from that."

The dot-com bubble, which had pushed tech companies' valuations into the stratosphere, burst about the same time, sweeping away weak companies like Pets.com and squeezing revenue throughout the industry. The chief executive of @Stake, who was brought in to provide something like parental supervision to Lopht, ordered Wysopal to single out a member of the group for a layoff in order to balance out cuts elsewhere in the company.

Wysopal said he reluctantly dropped the ax on Brian Oblivion, one of Lopht's charter members, whose real name is Brian Hassick. The firing came the day before Hassick's son was to be baptized; he and Wysopal did not speak again for months.

As the bonds at the heart of Lopht deteriorated, Zatko mysteriously disappeared. Though not a founding member of the group, he had been its most public face during the rise to fame.

If Lopht was something akin to the Beatles of the hacker world — combining serious chops with an instinct for self-promotion — Zatko was the mercurial, boundary-busting John Lennon to Wysopal's even-keeled Paul McCartney.

But as @Stake struggled, Zatko developed severe anxiety, made worse by a bad reaction to medicine that was supposed to ease his symptoms, he said. Zatko ended up in a psychiatric ward for several days. None of the members of Lopht came to visit, a source of enduring frustration to him. (They say they didn't know what was happening, only that he was missing from work.)

"The Lopht was my only family," Zatko recalled. "It killed me. . . . It was absolutely atrocious."

Though Zatko gradually recovered, the decline of @Stake continued. Space Rogue threatened a lawsuit to reclaim lost wages and his remaining share of the initial venture-capital funding. (He eventually settled with enough to buy a car, cover his lawyer's fees and put a down payment on a condominium, he says.)

Perhaps an even lower point for @Stake came in September 2003, when the company fired its chief technology officer, the respected security guru Dan Geer, after he co-authored a study on how Microsoft's dominance of the software industry undermined security. Geer learned of his dismissal through a news release issued by @Stake, according to news reports at the time.

When Symantec, a larger security firm, bought the remains of @Stake in 2004, it was a mercy killing.

"Everything we stood for had been nibbled away little by little by little until we were left with nothing," Grand said. "We needed to be able to speak the truth about everybody. That didn't last very long. . . . Eventually we just got on our knees for everybody."

As L0pht was collapsing, security on the Internet took a turn for the worse. The waning days of the 20th century featured huge investments toward fixing the Y2K bug — based on the alarming possibility that programs designed to recognize years by only two digits, such as "99," would suddenly crash when they saw "00."

But the problems that would soon bedevil computing were not accidental, like the Y2K bug. The black hats were on the rise.

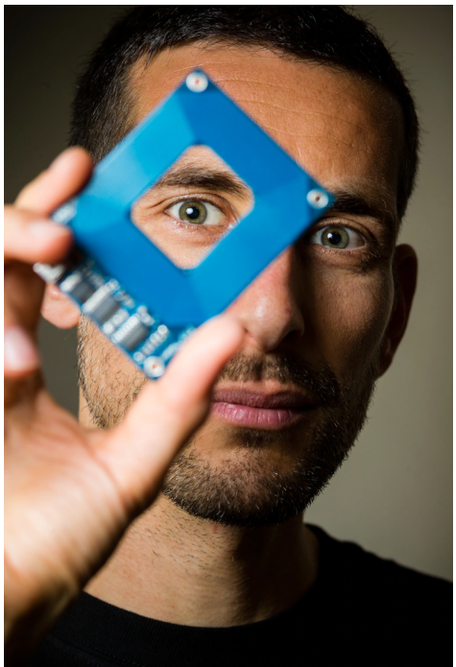
Among the first security disasters of the next decade, the ILOVEYOU worm, arrived in May 2000 and apparently was the work of a pair of computer programmers from the Philippines.

The virus exploited a feature in Microsoft Outlook to send malicious code to each new victim's contact lists.

Soon, an estimated 10 percent of the world's computers were infected, snarling networks for the Pentagon, the British Parliament and many private companies. Estimates of damage and cleanup costs topped $20 billion. Many other worms — with names such as Pikachu, Anna Kournikova and Nimda — also exploited flaws in Microsoft products.

On Dec. 8, 2000, one day after the anniversary of the surprise Japanese attack on U.S. Navy forces in 1941, Clarke — the National Security Council official who had once given L0pht a tour of the White House — appeared at a conference organized by Microsoft. He warned that if the government didn't improve computer security, the nation might suffer a "digital Pearl Harbor."

'Hackers are like water'



L0pht's legacy is a mixed one. The group was among the pioneers of a system called "responsible disclosure," still widely used today, in which researchers who find bugs give companies a set amount of time to make fixes before security flaws are announced to the world. Some companies now go a step further, offering cash rewards called "bug bounties" to encourage hackers to search for problems — and ideally find them ahead of criminals and spies.

Microsoft eventually became more serious about security. It didn't have much choice: Major customers told Gates to either do better or lose their business. In a memo in January 2002 — something of a bookend to the one from 1995 — Gates declared that a new security initiative was "the highest priority for all the work we are doing."

The move initially drew some skepticism. "When I told friends I was going to Microsoft to do security . . . most of them laughed at me because I used 'Microsoft' and 'security' in the same sentence," said Scott Charney, a former Justice Department official hired in 2002. He is now corporate vice president for Trustworthy Computing at Microsoft.

Joe Grand, who formerly used the hacker name Kingpin, at his home in Portland, Ore., with an RFID card reader he designed. (Leah Nash for The Washington Post)

Microsoft pulled thousands of engineers off of product development to overhaul the company's systems for designing and building software. Gates sent one group of officials to a retreat at a historic wooden home more commonly used for weddings, in nearby Bellevue, Wash., about a 15-minute drive from Microsoft's headquarters in Redmond. Charney said, "Basically some people were sent there and told, don't come back until you have an answer."

But the Internet did not suddenly become secure. The company's newfound focus on security took years to bear fruit, most notably with the arrival of Windows Vista in 2006 and Office 2010 a few years later. Because of a need for "backward compatibility" — meaning older and newer versions of Microsoft products work easily together — old flaws lingered in the online world for many years after they were fixed in newly released software.

The federal government in the past year finally has replaced hundreds of thousands of computers running Windows XP — an operating system first released in 2001, months before Gates's call to arms on product security — after the company withdrew free support after nearly 13 years.

But as Microsoft's products became more secure, hackers began feasting on alternative targets that did not get similar overhauls.

"Hackers are like water," said Vigna, the computer scientist at the University of California at Santa Barbara. "They always go for the path of least resistance. . . . If you put a plug in place, they will find another crack."

At the root is an issue raised by L0pht in its Senate testimony: The business incentives within the tech industry favor growth over security. And once companies get big enough that security is a major concern — as eventually happened to Microsoft — it's extremely difficult to retrofit rigorous protections into systems built without them.

Thompson, the Tennessee Republican who chaired the Senate panel in 1998 and left Congress in 2003, said in a recent interview that Internet security is the kind of problem the government has trouble fixing. "Number one, it's very difficult, and number two, there's no immediate political payoff for anyone."

Paul Nash, a.k.a. Silicosis, left, and Chris Wysopal, a.k.a. Weld Pond. The members of L0pht eventually quit their day jobs to join @Stake, a security company. “The community we came from thought we were selling out to the Man, which of course we were,” Wysopal says. (Bill O'Leary/The Washington Post)

The rise of the black hats

Some industry critics favor strict government standards and legal liability for failures, as long have existed for many critical offline systems such as cars, elevators and airplanes. Others would create an independent group, a tech industry equivalent to Underwriters Laboratories, which certifies the safety of electronic devices worldwide. Or perhaps insurance companies, which ultimately foot the bill for many cybersecurity incidents, may some day demand better safety practices from their clients, as insurers long have done for homes and cars.

But others have argued that demands for greater security could damp innovation and make tech products harder to use. Given the industry’s increasingly central role in the national economy — and the massive expansion in tech lobbying power in Washington in recent years — tough new laws or regulations remain difficult to imagine.

“The only way to get in front of the security problem is to build better software,” said Gary McGraw, chief technology official for Cigital, a Northern Virginia-based firm that has worked on software security since the 1990s. “Until we start building security in, we’ll always play catch-up.”

L0pht itself has rebounded a bit, releasing an updated version of L0pht Crack in 2009. The main Web site is still running, if a bit dated looking. The Hacker News Network regained its name and its edge.

Wysopal and fellow L0pht hacker Dildog founded a security company, Veracode, in 2006. Zatko, after recovering from severe anxiety, rejoined BBN Technologies. He later spent three years directing cybersecurity research at the Defense Advanced Research Projects Agency, the Pentagon agency that created the forerunner to the Internet decades ago, before becoming deputy director for a research team at Google.

Most of the others still work on computer security issues. They had a reunion of sorts in the summer of 2014 at Space Rogue’s wedding in Philadelphia. The emotional wounds from the @Stake debacle have scarred over if not disappeared.

As for the security issues they once highlighted for the U.S. government and the world, the news is far worse. Hackers — the black-hat kind — have consistently outrun efforts to impose security.

Wysopal offered this grim precedent: Cities were once vulnerable to disastrous fires, which raged through dense clusters of mostly wooden buildings. It took a giant fire in Chicago to spur government officials into serious reforms, including limits on new wooden structures, a more robust water supply for suppressing blazes and an overhaul to the city’s fire department.

“The market didn’t solve the problem of cities burning down,” Wysopal said, predicting that Internet security may require a historic disaster to force change. “It seems to me that the market isn’t really going to solve this one on its own.”

But here’s a frightening fact: The push to create tough new fire-safety standards did not start after the Great Chicago Fire in 1871, which killed hundreds of people and left 100,000 homeless. It took a second fire, nearly three years later in 1874, to get officials in Chicago to finally make real changes.

Comments

Discussion Policy

Credits

Story by Craig Timberg