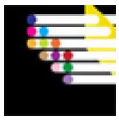
<< Back to Article

WIRED MAGAZINE: 16.12

Secret Geek A-Team Hacks Back, Defends Worldwide Web

By Joshua Davis 11.24.08

Kaminsky was alone in his Seattle apartment when he discovered a security vulnerability that could leave banks, online retailers, and ISPs open to hackers.
Photo: John Keatley



How to Plug the Hole in the Internet

In June 2005, a balding, slightly overweight, perpetually T-shirt-clad 26-year-old computer consultant named Dan Kaminsky decided to get in shape. He began by scanning the Internet for workout tips and read that five minutes of sprinting was the equivalent of a half-hour jog. This seemed like a great shortcut—an elegant exercise hack—so he bought some running shoes at the nearest Niketown. That same afternoon, he laced up his new kicks and burst out the front door of his Seattle apartment building for his first five-minute workout. He took a few strides, slipped on a concrete ramp and crashed to the sidewalk, shattering his left elbow.

He spent the next few weeks stuck at home in a Percocet-tinged haze. Before the injury, he'd spent his days testing the inner workings of software programs. Tech companies hired him to root out security holes before hackers could find them. Kaminsky did it well. He had a knack for breaking things—bones and software alike.

But now, laid up in bed, he couldn't think clearly. His mind drifted. Running hadn't worked out so well. Should he buy a stationary bike? Maybe one of those recumbent jobs would be best. He thought about partying in Las Vegas ... mmm, martinis ... and recalled a trick he'd figured out for getting free Wi-Fi at Starbucks.

As his arm healed, the details of that Starbucks hack kept nagging at him. He remembered that he had gotten into Starbucks' locked network using the domain name system, or DNS. When someone types google .com into a browser, DNS has a list of exactly where Google's servers are and directs the traffic to them. It's like directory assistance for the Internet. At Starbucks, the port for the low-bandwidth DNS connection—port 53—was left open to route customers to the *Pay for Starbucks Wi-Fi* Web page.

So, rather than pay, Kaminsky used port 53 to access the open DNS connection and get online. It was free but super-slow, and his friends mocked him mercilessly. To Kaminsky that was an irresistible challenge. After weeks of studying the minutiae of DNS and refining his hack, he was finally able to stream a 12-second animated video of Darth Vader dancing a jig with Michael Flatley. (The clip paired the Lord of the Sith with the Lord of the Dance.)

That was more than a year ago, but it still made him smile. DNS was the unglamorous underbelly of the Internet, but it had amazing powers. Kaminsky felt drawn to the obscure, often-ignored protocol all over again.

Maybe the painkillers loosened something in his mind, because as Kaminsky began to think more deeply about DNS he became convinced that something wasn't right. He couldn't quite figure it out, but the feeling stuck with him even after he stopped taking the pain pills. He returned to work full time and bought a recumbent stationary bike. He got hired to test the security of Windows Vista before it was released, repeatedly punching holes in it for Microsoft. Still, in the back of his mind, he was sure that the entire DNS system was vulnerable to attack.

Then last January, on a drizzly Sunday afternoon, he flopped down on his bed, flipped open his laptop, and started playing games with DNS. He used a software program called Scapy to fire random queries at the system. He liked to see how it would respond and decided to ask for the location of a series of nonexistent Web pages at a Fortune 500 company. Then he tried to trick his DNS server in San Diego into thinking that he knew the location of the bogus pages.

Suddenly it worked. The server accepted one of the fake pages as real. But so what? He could now supply fake information for a page nobody would ever visit. Then he realized that the server was willing to accept more information from him. Since he had supplied data about one of the company's Web pages, it believed that he was an authoritative source for *general* information about the company's domain. The server didn't know that the Web page didn't exist—it was listening to Kaminsky now, as if it had been hypnotized.

When DNS was created in 1983, it was designed to be helpful and trusting—it's directory assistance, after all. It was a time before hacker conventions and Internet banking. Plus, there were only a few hundred servers to keep track of. Today, the humble protocol stores the location of a billion Web addresses and routes every piece of Internet traffic in the world.

Security specialists have been revamping and strengthening DNS for more than two decades. But buried beneath all this tinkering, Kaminsky had just discovered a vestige of that original helpful and trusting program. He was now face-to-face with the behemoth's almost childlike core, and it was perfectly content to accept any information he wanted to supply about the location of the Fortune 500 company's servers.

Paul Vixie organized experts from around the world to address the DNS security flaw.
Photo: John Keatley

Kaminsky froze. This was far more serious than anything he could have imagined. It was the ultimate hack. He was looking at an error coded into the heart of the Internet's infrastructure. This was not a security hole in Windows or a software bug in a Cisco router. This would allow him to reassign any Web address, reroute anyone's email, take over banking sites, or simply scramble the entire global system. The question was: Should he try it?

The vulnerability gave him the power to transfer millions out of bank accounts worldwide. He lived in a barren one-bedroom apartment and owned almost nothing. He rented the bed he was lying on as well as the couch and table in the living room. The walls were bare. His refrigerator generally contained little more than a few forgotten slices of processed cheese and a couple of Rockstar energy drinks. Maybe it was time to upgrade his lifestyle.

Or, for the sheer geeky joy of it, he could reroute all of .com into his laptop, the digital equivalent of channeling the Mississippi into a bathtub. It was a moment hackers around the world dream of—a tool that could give them unimaginable power. But maybe it was best simply to close his laptop and forget it. He could pretend he hadn't just stumbled over a skeleton key to the Net. Life would certainly be less complicated. If he stole money, he'd risk prison. If he told the world, he'd be the messenger of doom, potentially triggering a collapse of Web-based commerce.

But who was he kidding? He was just some guy. The problem had been coded into Internet architecture in 1983. It was 2008. Somebody must have fixed it by now. He typed a quick series of commands and pressed enter. When he tried to access the Fortune 500 company's Web site, he was redirected to an address he himself had specified.

"Oh shit," he mumbled. "I just broke the Internet."

Paul Vixie, one of the creators of the most widely used DNS software, stepped out of a conference in San Jose. A curious email had just popped up on his laptop. A guy named Kaminsky said he'd found a serious flaw in DNS and wanted to talk. He sent along his phone number.

Vixie had been working with DNS since the 1980s and had helped solve some serious problems over the years. He was president of the Internet Systems Consortium, a nonprofit that distributed BIND 9, his DNS software. At 44, he was considered the godfather of DNS. If there was a fundamental error in DNS, he probably would have fixed it long ago.

But to be on the safe side, Vixie decided to call Kaminsky. He picked up immediately and within minutes had outlined the flaw. A series of emotions swept over Vixie. What he was hearing shouldn't be possible, and yet everything the kid said was logical. By the end of the third minute, Vixie realized that Kaminsky had uncovered something that the best minds in computer science had overlooked. This affected not just BIND 9 but almost all DNS software. Vixie felt a deep flush of embarrassment, followed by a sense of pure panic.

"The first thing I want to say to you," Vixie told Kaminsky, trying to contain the flood of feeling, "is never, ever repeat what you just told me over a cell phone."

Vixie knew how easy it was to eavesdrop on a cell signal, and he had heard enough to know that he was facing a problem of global significance. If the information were intercepted by the wrong people, the wired world could be held ransom. Hackers could wreak havoc. Billions of dollars were at stake, and Vixie wasn't going to take any risks.

From that moment on, they would talk only on landlines, in person, or via heavily encrypted email. If the information in an email were accidentally copied onto a hard drive, that hard drive would have to be completely erased, Vixie said. Secrecy was critical. They had to find a solution before the problem became public.

Andreas Gustafsson knew something was seriously wrong. Vixie had emailed the 43-year-old DNS researcher in Espoo, Finland, asking to talk at 7 pm on a hardwired line. No cell phones.

Gustafsson hurried into the freezing March evening—his only landline was the fax in his office a brisk mile walk away. When he arrived, he saw that the machine didn't have a handset. Luckily, he had an analog phone lying around. He plugged it in, and soon it let off an old-fashioned metallic ring.

Gustafsson hadn't spoken to Vixie in years, but Vixie began the conversation by reading aloud a series of numbers—a code that would later allow him to authenticate Gustafsson's emails and prove that he was communicating with the right person. Gustafsson responded with his own authenticating code. With that out of the way, Vixie got to his point: *Find a flight to Seattle now*.

Wouter Wijngaards got a call as well, and the message was the same. The Dutch open source programmer took the train to the airport in Amsterdam, got on a 10-hour flight to Seattle, and arrived at the Silver Cloud Inn in Redmond, Washington,

on March 29. He had traveled all the way from Europe, and he didn't even know why. Like Gustafsson, he had simply been told to show up in Building Nine on the Microsoft campus at 10 am on March 31.

In the lobby of the Silver Cloud, Wijngaards met Florian Weimer, a German DNS researcher he knew. Weimer was talking with Chad Dougherty, the DNS point man from Carnegie Mellon's Software Engineering Institute. Wijngaards joined the conversation—they were trying to figure out where to have dinner. Nobody talked about why some of the world's leading DNS experts happened to bump into one another near the front desk of this generic US hotel. Vixie had sworn each of them to secrecy. They simply went out for Vietnamese food and avoided saying anything about DNS.

The next morning, Kaminsky strode to the front of the conference room at Microsoft headquarters before Vixie could introduce him or even welcome the assembled heavy hitters. The 16 people in the room represented Cisco Systems, Microsoft, and the most important designers of modern DNS software.

Vixie was prepared to say a few words, but Kaminsky assumed that everyone was there to hear what he had to say. After all, he'd earned the spotlight. He hadn't sold the discovery to the Russian mob. He hadn't used it to take over banks. He hadn't destroyed the Internet. He was actually losing money on the whole thing: As a freelance computer consultant, he had taken time off work to save the world. In return, he deserved to bask in the glory of discovery. Maybe his name would be heralded around the world.

Kaminsky started by laying out the timeline. He had discovered a devastating flaw in DNS and would explain the details in a moment. But first he wanted the group to know that they didn't have much time. On August 6, he was going to a hacker convention in Las Vegas, where he would stand before the world and unveil his amazing discovery. If there was a solution, they'd better figure it out by then.

But did Kaminsky have the goods? DNS attacks were nothing new and were considered difficult to execute. The most practical attack—widely known as cache poisoning—required a hacker to submit data to a DNS server at the exact moment that it updated its records. If he succeeded, he could change the records. But, like sperm swimming toward an egg, whichever packet got there first—legitimate or malicious—locked everything else out. If the attacker lost the race, he would have to wait until the server updated again, a moment that might not come for days. And even if he timed it just right, the server required a 16-bit ID number. The hacker had a 1-in-65,536 chance of guessing it correctly. It could take years to successfully compromise just one domain.

The experts watched as Kaminsky opened his laptop and connected the overhead projector. He had created a "weaponized" version of his attack on this vulnerability to demonstrate its power. A mass of data flashed onscreen and told the story. In less than 10 seconds, Kaminsky had compromised a server running BIND 9, Vixie's DNS routing software, which controls 80 percent of Internet traffic. It was undeniable proof that Kaminsky had the power to take down large swaths of the Internet.

The tension in the room rose as Kaminsky kept talking. The flaw jeopardized more than just the integrity of Web sites. It would allow an attacker to channel email as well. A hacker could redirect almost anyone's correspondence, from a single user's to everything coming and going between multinational corporations. He could quietly copy it before sending it along to its original destination. The victims would never know they had been compromised.

This had serious implications. Since many "forgot my password" buttons on banking sites rely on email to verify identity, an attacker could press the button, intercept the email, and change the password to anything he wanted. He would then have total access to that bank account.

"We're hosed," Wijngaards thought.

It got worse. Most Internet commerce transactions are encrypted. The encryption is provided by companies like VeriSign. Online vendors visit the VeriSign site and buy the encryption; customers can then be confident that their transactions are secure.

But not anymore. Kaminsky's exploit would allow an attacker to redirect VeriSign's Web traffic to an exact functioning replica of the VeriSign site. The hacker could then offer his own encryption, which, of course, he could unlock later. Unsuspecting vendors would install the encryption and think themselves safe and ready for business. A cornerstone of secure Internet communication was in danger of being destroyed.

David Ulevitch smiled despite himself. The founder of OpenDNS, a company that operates DNS servers worldwide, was witnessing a tour de force—the geek equivalent of Michael Phelps winning his eighth gold medal. As far as Ulevitch was concerned, there had never been a vulnerability of this magnitude that was so easy to use. "This is an amazingly catastrophic attack," he marveled with a mix of grave concern and giddy awe.

It was a difficult flight back to San Francisco for Sandy Wilbourn, vice president of engineering for Nominum, a company hired by broadband providers to supply 150 million customers with DNS service. What he heard in Redmond was

overwhelming—a 9 out of 10 on the scale of disasters. He might have given it a 10, but it was likely to keep getting worse. He was going to give this one some room to grow.

One of Wilbourn's immediate concerns was that about 40 percent of the country's broadband Internet ran through his servers. If word of the vulnerability leaked, hackers could quickly compromise those servers.

In his Redwood City, California, office, he isolated a hard drive so no one else in the company could access it. Then he called in his three top engineers, shut the door, and told them that what he was about to say couldn't be shared with anyone—not at home, not at the company. Even their interoffice email would have to be encrypted from now on.

Their task: Make a change to the basic functioning of Nominum's DNS servers. They and their customers would have to do it without the usual testing or feedback from outside the group. The implementation—the day the alteration went live to millions of people—would be its first real-world test.

It was a daunting task, but everyone who had been in Redmond had agreed to do the same thing. They would do it secretly, and then, all together on July 8, they would release their patches. If hackers didn't know there was a gaping DNS security hole before, they would know then. They just wouldn't know exactly what it was. Nominum and the other DNS software vendors would have to persuade their customers—Internet service providers from regional players such as Cablevision to giants like Comcast—to upgrade fast. It would be a race to get servers patched before hackers figured it out.

Though the Redmond group had agreed to act in concert, the patch—called the source port randomization solution—didn't satisfy everyone. It was only a short-term fix, turning what had been a 1-in-65,536 chance of success into a 1-in-4 billion shot.

Still, a hacker could use an automated system to flood a server with an endless stream of guesses. With a high-speed connection, a week of nonstop attacking would likely succeed. Observant network operators would see the spike in traffic and could easily block it. But, if overlooked, the attack could still work. The patch only papered over the fundamental flaw that Kaminsky had exposed.

On July 8, Nominum, Microsoft, Cisco, Sun Microsystems, Ubuntu, and Red Hat, among many others, released source port randomization patches. Wilbourn called it the largest multivendor patch in the history of the Internet. The ISPs and broadband carriers like Verizon and Comcast that had been asked to install it wanted to know what the problem was. Wilbourn told them it was extremely important that they deploy the patch, but the reason would remain a secret until Kaminsky delivered his talk in Las Vegas.

Even as Kaminsky was giving interviews about the urgency of patching to media outlets from the *Los Angeles Times* to CNET, the computer security industry rebelled. "Those of us ... who have to advise management cannot tell our executives 'trust Dan,'" wrote one network administrator on a security mailing list. On one blog, an anonymous poster wrote this to Kaminsky: "You ask people not to speculate so your talk isn't blown but then you whore out minor details to every newspaper/magazine/publishing house so your name can go all over Google and gain five minutes of fame? This is why people hate you and wish you would work at McDonald's instead."

With a backlash building, Kaminsky decided to reach out to a few influential security experts in hopes of winning them over. He set up a conference call with Rich Mogull, founder of Securosis, a well-respected security firm; researcher Dino Dai Zovi; and Thomas Ptacek, a detractor who would later accuse Vixie and Kaminsky of forming a cabal.

The call occurred July 9. Kaminsky agreed to reveal the vulnerability if Mogull, Dai Zovi, and Ptacek would keep it secret until the Vegas talk August 6. They agreed, and Kaminsky's presentation laid it out for them. The security experts were stunned. Mogull wrote, "This is absolutely one of the most exceptional research projects I've seen." And in a blog post Ptacek wrote, "Dan's got the goods. *It's really f'ing good*."

And then, on July 21, a complete description of the exploit appeared on the Web site of Ptacek's company. He claimed it was an accident but acknowledged that he had prepared a description of the hack so he could release it concurrently with Kaminsky. By the time he removed it, the description had traversed the Web. The DNS community had kept the secret for months. The computer security community couldn't keep it 12 days.

About a week later, an AT&T server in Texas was infiltrated using the Kaminsky method. The attacker took over google.com—when AT&T Internet subscribers in the Austin area tried to navigate to Google, they were redirected to a Google look-alike that covertly clicked ads. Whoever was behind the attack probably profited from the resulting increase in ad revenue.

Every day counted now. While Kaminsky, Vixie, and the others pleaded with network operators to install the patch, it's likely that other hacks occurred. But the beauty of the Kaminsky attack, as it was now known, was that it left little trace. A good hacker could reroute email, reset passwords, and transfer money out of accounts quickly. Banks were unlikely to announce the intrusions—online theft is bad PR. Better to just cover the victims' losses.

On August 6, hundreds of people crammed into a conference room at Caesars Palace to hear Kaminsky speak. The seats filled up quickly, leaving a scrum of spectators standing shoulder to shoulder in the back. A group of security experts had mockingly nominated Kaminsky for the Most Overhyped Bug award, and many wanted to know the truth: Was the massive patching effort justified, or was Kaminsky just an arrogant, media-hungry braggart?

While his grandmother handed out homemade Swedish lace cookies, Kaminsky took the stage wearing a black T-shirt featuring an image of Pac-Man at a dinner table. He tried for modesty. "Who am I?" he asked rhetorically. "Some guy. I do code."

The self-deprecation didn't suit him. He had the swagger of a rock star and adopted the tone of a misunderstood genius. After detailing the scope of the DNS problem, he stood defiantly in front of a bullet point summary of the attack and said, "People called BS on me. This is my reply."

By this time, hundreds of millions of Internet users were protected. The bomb had been defused. The problem was, there was little agreement on what the long-term solution should be. Most discussion centered around the concept of authenticating every bit of DNS traffic. It would mean that every computer in the world—from iPhones to corporate server arrays—would have to carry DNS authentication software. The root server could guarantee that it was communicating with the real .com name server, and .com would receive cryptological assurance that it was dealing with, say, the real Google. An impostor packet wouldn't be able to authenticate itself, putting an end to DNS attacks. The procedure is called DNSSEC and has high-profile proponents, including Vixie and the US government.

But implementing a massive and complicated protocol like DNSSEC isn't easy. Vixie has actually been trying to persuade people for years, and even he hasn't succeeded. Either way, the point might turn out to be moot. Kaminsky ended his Las Vegas talk by hinting that even darker security problems lay ahead. It was the type of grandstanding that has made him a polarizing figure in the computer security community. "There is no saving the Internet," he said. "There is postponing the inevitable for a little longer."

Then he sauntered off the stage and ate one of his grandma's cookies.

Contributing editor Joshua Davis(www.joshuadavis.net) *wrote about the rescue of the foundering Cougar Ace in issue 16.03.*