In battle against cyberattacks, these hackers wear the 'white hats'

May 2 2013, by Erik Lacitis

He's 26, likes industrial and electronic music, has a bleached-blond Mohawk haircut and sometimes, Mikhail Davidov said, he starts his day "at the crack of noon." The late hours are in front of a computer, working on reverse engineering, tearing apart computer programs to find their vulnerabilities.

Sometimes he works 18 hours straight. "There are few hackers out there who are 'morning people,' " Davidov said.

These days, the front lines for security don't only include soldiers carrying weapons.

They include computer whiz kids like Davidov, who works for the Leviathan Security Group, a 20-person firm that operates out of second-floor offices in a renovated 1918 building in Seattle.

Chad Thunberg, chief operating officer of Leviathan, said he can relate to Davidov, remembering his own younger days.

Thunberg, who is 35 and married with two children, said, "I'm considered a grandpa in my industry. There was a time when I was the Mikhail equivalent. You live and breathe security."

Cyberattacks are costing corporations - and consumers - a lot. In a six-year span starting in 2005, data breaches in 33 countries, including the U.S., cost the firms involved more than $156 billion, according to the

nonprofit Digital Forensics Association.

Every second, in various parts of the world, there are 18 cybercrime victims - some 1.6 million a day - according to a 2012 Norton by Symantec study.

On Friday, the Wenatchee World newspaper reported that a Leavenworth, Wash., hospital said hackers stole more than $1 million from the hospital's electronic bank account. The Chelan County, Wash., treasurer said it had been able to retrieve about $133,000 by notifying recipient bank accounts, most in the Midwest and East Coast.

And the Associated Press reported that LivingSocial, an online deals site, said Friday that its website was hacked and the personal data of more than 50 million customers may have been affected - names, email addresses, date of birth of some users and encrypted passwords.

Then there are the Chinese hackers, who blasted into the news in February when Mandiant, an Internet security firm, released a report saying that a group linked to the People's Liberation Army had systemically stolen confidential data from at least 141 American firms.

In his State of the Union address, President Barack Obama warned, "Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions and our air traffic control systems."

That makes Internet security a booming industry, at an estimated nearly $1 billion a year in 2012, according to the consulting firm Frost & Sullivan.

Another "white hat" hacker is Adam Cecchetti, 31, who used to work at Leviathan and then in 2010 became one of the founders of Deja vu Security, which operates out of a second-floor renovated loft in Seattle's

Capitol Hill. Sometimes, he has colored his hair blue.

Davidov and Cecchetti are on the front lines of fighting off the "black hat" hackers. Yes, that is how they describe their enemy.

The latter includes those sending out phishing emails that look like they came from a legitimate source but are fakes trying to get your passwords and credit-card information.

Or maybe they are black hats trying to compromise a company's website just so they can boast about it in hacker circles.

For the white hats, their unique skill at finding where a program is vulnerable and how to close the digital doors that the black hats use to penetrate a website is worth $120,000 to $130,000 a year, Thunberg said.

"Companies are being attacked by bad people, and if they want to defend themselves, they have to attract these scarce people," he said. "There are maybe 1,000 individuals of this nature in the world. They have this unique hacker mind-set."

Their clients aren't exactly keen to publicize that they seek Internet security, said Thunberg, and that's often written into their contracts with Leviathan. Thunberg said his company's average contract size is for around $70,000. Citing privacy, he said only that most are Fortune 1000 companies.

But one client that didn't mind talking is a Washington, D.C.-based company called Silent Circle. For $20 a month, it offers a service that encrypts voice, text and video on a user's smartphone, tablet or computer.

Their customers, said Jon Callas, Silent Circle's chief technical officer, include U.S. businesses "doing work in China and Eastern Europe and other places where they don't want their phone calls tapped."

His company, Callas said, hired Leviathan to evaluate the encrypting software for vulnerabilities and fix them.

"They helped us find problems before anybody else did," said Callas.

At Deja vu Security, Cecchetti said, work that they've done includes posing as new employees at a financial institution, given the standard access to computers. Firms routinely give computer "administrative privileges" to only a handful of individuals.

But, Cecchetti said, "within a couple of weeks, we had basically control of the entire organization and could access pretty much anything we wanted."

Deja vu put together "a very large report" on how to fix things, he said.

Hackers such as Davidov and Cecchetti have certain similarities. For one thing, they started tinkering with computers when they were kids, and that passion never stopped.

Cecchetti grew up in Greensburg, Pa. He helped start a computer club in high school and said that although he ran track and played soccer, "I was plenty nerdy."

As a teen in the 1990s, he was programming video games and went on to creating simple websites, before they had become ubiquitous.

Cecchetti earned a master's from Carnegie Mellon University in electrical and computer engineering, and ended up in Seattle in 2005,

working for Amazon to keep black hats from breaking in.

Davidov is the son of Russian immigrants. His father worked at a tech firm in Moscow and got a visa to come to the U.S. in 1995, moving the family to Woodinville, Wash.

But even in the old country, when he was 5, Davidov said, he was using a computer his father brought home, "playing little DOS games," the early operating system.

By his teen years, Davidov was hacking into video games so he could beat them.

Having promised his parents that he'd go to college, Davidov enrolled at the DigiPen Institute of Technology in Redmond, Wash., and earned a four-year degree in "Real-Time Interactive Simulation."

Said Davidov, "That means I know video games."

It is the ability to look at programs over, under, sideways and down that makes a Davidov so valuable, and in such short supply.

At the University of Washington's renowned Computer Science and Engineering program, out of nearly 50 faculty members, "we have one full-time faculty member, Yoshiro Kohno, who is a superstar in computer security, but we're hoping to grow in that area in the near future," said its chairman, Hank Levy.

But even with more college classes in cybersecurity, it is real-world experience that is needed, said Davidov. Outside of a school's lab, he said, it all gets "much grander in scope."

There are also personal aspects, he said, such as when he delivers a

report to developers who had spent a long time working on a program, and he points out its security flaws.

The developers, he said, "can get a little defensive, and it can become a little confrontational."

For both Davidov and Cecchetti, it was a conscious, and simple, decision to become a white hat.

Said Cecchetti, "I'm not in this business to harm people, or to take Grandma's savings, or deface somebody's website."

There is plenty of money to be made in Internet security.

"Things are very good," Cecchetti said about Deja vu, which has a staff of a dozen.

Companies pay for security because getting hacked can cost plenty.

At Leviathan, on one of the brick walls are a dozen or so framed exotic bugs. Chad Thunberg, as one of Leviathan's bosses at the 20-person company, said that every time the company finds "a big-deal" bug in software, up goes another display insect.

At Deja vu, a small gong gets banged when there is some good news.

"Deja vu" is a very specific reference point in the hacker mentality. Cecchetti said it's from the 1999 movie "The Matrix," which he figures he's seen 10 or 20 times. The hero, played by Keanu Reeves, is a hacker in a future time in which humans live in an artificial reality.

In the movie, Reeves sees a black cat walk by, and then immediately sees the same black cat walk by again.

"Whoa. Deja vu," he says.

It turns out that "deja vu" is a glitch in the matrix, and happens when something is changed in that cyberspace reality. The logo for Deja vu Security even has a black cat.

Cecchetti now is one of those who hires, and said that when interviewing applicants, he wants to know, "Can they see things from the perspective of a hacker, gleeful to see how things are made? They need to want to peel away the layers. What happens if I make a very small change in the system?"

If you can do that, you can come to the office in any hairstyle you want.

"It's usually a little bit of a shock," Davidov said about how some clients react to his Mohawk.

"But once they start seeing the output of the work we do, they find it almost endearing."