How the Boy Next Door Accidentally Built a Syrian Spy Tool

wired.com/2012/07/dark-comet-syrian-spy-tool/

Robert McMillan

Jean-Pierre Lesueur.

Photo: Jean-Pierre Lesueur

Jean-Pierre Lesueur is in many ways a typical 22-year-old computer geek. He lives outside of Paris, coding Java by day for a European company that processes airline tickets. He likes playing the piano and reading Stephen Hawking. But he's also the man who built Dark Comet – which was recently used by the Syrian government to steal information from the computers of activists fighting to overthrow it.

Dark Comet is a software application that gives you remote control over another computer, and Lesueur says he wrote it just to prove his programming cred. That meant sharing the thing with the rest of the world, and after the Syrian government grabbed the tool from the net, Lesueur found himself at the center of an international firestorm. He spoke with *Wired* Tuesday via online chat.

Sometimes, the boy next door can become a tool in a state-sponsored cyberespionage campaign. That's the power of the internet.

Although it was first developed in 2008, Dark Comet mostly stayed under the radar until it was linked to Syria earlier this year. Although Lesueur says he never intended it to be used illegally, Dark Comet is not the type of program anyone would want to discover on their PC.

In short, it's a silent spying machine. There's a password-stealing keylogger and a feature that helps it avoid detection by antivirus products. Dark Comet can be used for spying, too, quietly recording video and audio from a computer once it's installed.

According to Lesueur, Dark Comet is no worse than other hacking tools such as Metasploit or BackTrack Linux, which can be used both by legitimate security testers and criminals to launch online attacks against computers and test networks for security flaws.

Dlshad Othman first learned about Dark Comet in December, when a Syrian activist asked him to examine her computer after losing access to her e-mail, Skype, and Facebook account. After a scan, Othman discovered Dark Comet sitting on the machine's hard drive.

Dark Comet was another tool in an escalating computer espionage campaign targeting critics of the regime of Syrian President Bashar Assad. "Because most of the Syrian people started to use secure connections and they [learned how to bypass] the censorship and surveillance of the internet, so the regime found it’s better to use Trojans to arrest the people," says Othman, a Syrian activist and computer specialist who is also one of the U.S. State Department's Internet Freedom Fellows.

He and other activists believe that the information stolen via Dark Comet led to many arrests within Syria. Once one computer is infected, hackers use that activist's computer as a stepping stone to try and infect others, typically by contacting them via Skype.

That's what happened to "Osama," an activist in Damascus who declined to give his last name. About five months ago, a doctor friend of his received a file via Skype that appeared to have something to do with medicine and the Syrian revolution. "His account started to send this file to his contacts (including me) and as he is a doctor, many of his contacts trusted this file," he said.

Osama doesn't know for certain that his friend was infected with Dark Comet, but it's very likely that he was. Researchers say that between November and May, this was a preferred remote access tool of the Syrian regime.

Morgan Marquis-Boire – a researcher with Citizen Lab, a computer security research think-tank – has identified 16 separate pieces of malicious software that use Dark Comet to send information back to computers located in Syria. Typically these are Trojan horse programs, designed to look like legitimate files that activists would want to read. The Trojan might look like a .pdf file or a Skype encryption tool, but it silently installs Dark Comet in the background. Dark Comet is known as a remote administration tool. Security experts call it a RAT.

Dark Comet was packaged with malicious software that would quietly install it when victims opened this .pdf.

Image: John Scott-Railton

As word of Dark Comet's use got out, Lesueur's part-time project suddenly came under the spotlight. The Electronic Frontier Foundation, antivirus companies, and online activists "kept up steady stream of postings and reports of the use of Dark Comet in Syria," says John Scott-Railton, a doctoral student at UCLA School of Public Affairs who has worked

closely on the issue of malicious software in Syria. "I don't think that this amount of pressure has ever been placed on the developer of a RAT before. I can't imagine that [Lesueur] expected anything like this to come from his project."

At first, Lesueur wrote a removal tool, so victims could uninstall Dark Comet, but he kept the project alive. But by the end of June, he was afraid. Though he wasn't the one doing the illegal activity, it was clear that his software was being misused – not just by the Syrian government, but by untalented hackers Lesueur calls "script-kiddies."

He started to worry about being arrested. So on June 28, he took down Dark Comet. "I removed all before one day it happened," he says. "I don't want to lose my life for such a little thing."

Lesueur says the Syrian use was a factor in his decision to pull Dark Comet, but not the only one. He won't spell out the exact reason he was worried about his arrest, but two days earlier, one of the apparent authors of another remote-access tool called Blackshades was arrested in Tuscon, Arizona, on hacking and malware distribution charges. That arrest may have scared Lesueur, says Kevin Mitnick, a well-known information security consultant.

Lesueur says that it did not affect his decision. "The Blackshades author was in charge of a carding operation," he says. "It's not the same."

Blackshades, coincidentally, is now being used against the Syrian activists much in the same way that Dark Comet was, says Marquis-Boire.

Mitnick, who has used Dark Comet in security demonstrations, doesn't think Leseur should have abandoned his tool because it was being used illegally. "I don't think that's a good reason to stop development on it, because you always have bad actors," he says. "That's just a fact of life."

This isn't the first time that a software developer has dropped a tool after getting some heat. But what's unusual is that Lesueur has been remarkably candid about everything, using his real name, talking about himself in detail, and explaining why he created the tool.

Lesueur – who cut his teeth in a underground Trojan and RAT-writing forum called OpenSC – says that although he made about 2,000 euros offering technical support for Dark Comet, he didn't charge for the software and was never in it for the money. He's now working on a new remote access tool that doesn't include the controversial spying features that were in Dark Comet.

After Lesueur pulled Dark Comet, Kevin Mitnick asked him if he'd ever consider selling the source code to the tool. Lesueur said no. "I don't think he was out for money," Mitnick says. "I don't think he was doing anything illegal."

Lesueur says he just wanted to make a name for himself in the hacker scene. "The whole development process of Dark Comet was a challenge for myself," he says.

"I never imagined it would be used by a government for spying," he said. "If I had known that, I would never have created such a tool."