The New York Times

August 30, 2012

Software Meant to Fight Crime Is Used to Spy on Dissidents

By NICOLE PERLROTH

SAN FRANCISCO — Morgan Marquis-Boire works as a Google engineer and Bill Marczak is earning a Ph.D. in computer science. But this summer, the two men have been moonlighting as detectives, chasing an elusive surveillance tool from Bahrain across five continents.

What they found was the widespread use of sophisticated, off-the-shelf computer espionage software by governments with questionable records on human rights. While the software is supposedly sold for use only in criminal investigations, the two came across evidence that it was being used to target political dissidents.

The software proved to be the stuff of a spy film: it can grab images of computer screens, record Skype chats, turn on cameras and microphones and log keystrokes. The two men said they discovered mobile versions of the spyware customized for all major mobile phones.

But what made the software especially sophisticated was how well it avoided detection. Its creators specifically engineered it to elude antivirus software made by Kaspersky Lab, Symantec, F-Secure and others.

The software has been identified as FinSpy, one of the more elusive spyware tools sold in the growing market of off-the-shelf computer surveillance technologies that give governments a sophisticated plug-in monitoring operation. Research now links it to servers in more than a dozen countries, including Turkmenistan, Brunei and Bahrain, although no government acknowledges using the software for surveillance purposes.

The market for such technologies has grown to $5 billion a year from “nothing 10 years ago,” said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveillance show where law enforcement agents view the latest computer spyware.

FinSpy is made by the Gamma Group, a British company that says it sells mo
to governments solely for criminal investigations.

“This is dual-use equipment,” said Eva Galperin, of the Electronic Frontier Fo

Internet civil liberties group. “If you sell it to a country that obeys the rule of law, they may use it for law enforcement. If you sell it to a country where the rule of law is not so strong, it will be used to monitor journalists and dissidents.”

Until Mr. Marquis-Boire and Mr. Marczak stumbled upon FinSpy last May, security researchers had tried, unsuccessfully, for a year to track it down. FinSpy gained notoriety in March 2011 after protesters raided Egypt’s state security headquarters and discovered a document that appeared to be a proposal by the Gamma Group to sell FinSpy to the government of President Hosni Mubarak for $353,000. It is unclear whether that transaction was ever completed.

Martin J. Muench, a Gamma Group managing director, said his company did not disclose its customers. In an e-mail, he said the Gamma Group sold FinSpy to governments only to monitor criminals and that it was most frequently used “against pedophiles, terrorists, organized crime, kidnapping and human trafficking.”

In May, Mr. Marquis-Boire, 32, of San Francisco, and Mr. Marczak, 24, of Berkeley, Calif., volunteered to analyze some suspicious e-mails sent to three Bahraini activists. They discovered all the e-mails contained spyware that reported back to the same command-and-control server in Bahrain. The apparent use of the spyware to monitor Bahraini activists, none of whom had any criminal history, suggested that it had been used more broadly.

Bahrain has been increasingly criticized for human rights abuses. This month, a 16-year-old Bahraini protester was killed in what activists said was a brutal attack by security forces, but which Bahrain’s government framed as self-defense.

The findings of the two men came as no surprise to those in the field. “There has been a clear increase in the availability of penetrating cyberattack tools,” said Sameer Bhalotra, President Obama’s former senior director for cybersecurity who now serves as the chief operating officer of Impermium, a computer security firm. “These were once the realm of the black market and intelligence agencies. Now they are emerging more and more. The problem is that it only requires small changes to apply a surveillance tool for attack, and in this case it looks like dissidents were targeted.”

Since publishing their findings, Mr. Marquis-Boire and Mr. Marczak have started receiving malware samples from other security researchers and from activist groups that suspected they may have been targets. In several cases, the two found that the samples reported back to Web sites run by the Gamma Group. But other samples appeared to be actively snooping for foreign governments.

A second set of researchers from Rapid7, of Boston, scoured the Internet for links to the software and discovered it running in 10 more countries. Indeed, the spyware was running off EC2, an Amazon.com cloud storage service. Amazon did not return requests for clarification, but Mr. Marczak and Mr. Marquis-Boire said the server appeared to be a proxy, a way to conceal traffic.

Mr. Marquis-Boire said a Turkmenistan server running the software belonged to a range of I.P. addresses specifically assigned to the ministry of communications. It is the first clear-cut case of a government running the spyware off its own computer system. Human Rights Watch recently called Turkmenistan one of the "world's most repressive countries" and warned that dissidents faced "constant threat of government reprisal."

Ms. Galperin of the Electronic Frontier Foundation said, "Nobody in their right mind would claim it is O.K. to sell surveillance to Turkmenistan."

The Gamma Group would not confirm it sold software to Turkmenistan. A military attaché at the Turkmenistan Embassy in Washington refused to comment.

Mr. Muench, who for the last month has repeatedly denied that the researchers had pinpointed the company's spyware, sharply reversed course Wednesday.

In a statement released less than an hour after the researchers published their latest findings, Mr. Muench said that a Gamma Group server had been broken into and that several demonstration copies of FinSpy had been stolen.

By Thursday afternoon, several of the FinSpy servers began to disappear, Mr. Marczak said. Servers in Singapore, Indonesia, Mongolia and Brunei went dark, while one in Bahrain briefly shut down before reincarnating elsewhere. Mr. Marquis-Boire said that as he traced spyware from Bahrain to 14 other countries — many of them "places with tight centralized control" — he grew increasingly worried about the people on the other end.

Four months in, he sounds like a man who wants to take a break, but knows he cannot just yet: "I can't wait for the day when I can sleep in and watch movies and go to the pub instead of analyzing malware and pondering the state of the global cybersurveillance industry."