UAE case highlights ‘spyware’ innovations

By Joe Menn in San Francisco

Published: July 29 2009 19:29 | Last updated: July 29 2009 19:29

The company behind the “spyware” distributed to BlackBerry users in the United Arab Emirates as part of an apparent government surveillance effort exposed last week is neither a shady hacking outfit nor a false front for a team of spies in a bunker.

Instead, SS8 is based in Silicon Valley, backed by top-tier venture capital firm Kleiner Perkins Caufield & Byers, and largely serves law enforcement agencies.

The company, more than 15 years old, is a solid part of a growing industrial-surveillance complex that weaves together innovation in monitoring, new government cyber-security initiatives and rapid expansion in connectivity.

As more people do more online, and use phones equipped with location-finding services, law enforcement services are demanding the capability to keep better tabs on what is happening, and both established and younger companies are racing to fill that need.

In the UAE incident, a consumer investigating why his BlackBerry battery kept draining looked into the code that state telecoms operator Etisalat had just recommended for installation. He turned up a file called Interceptor, which other researchers identified as a tool for eavesdropping. BlackBerry maker Research in Motion disavowed the program, which it said originated with SS8.

It is unusual for such tools to be discovered, but they are widespread elsewhere in the telecoms network, giving regimes in Iran, China and elsewhere the ability to monitor conversations with precision.

Western law enforcement and intelligence agencies typically rely on co-operation from telecoms companies, which install surveillance gear from SS8 and others centrally.

The hardware comes from companies such as Narus, also in Silicon Valley, and can store immense amounts of e-mails in switching hubs, and check messages with flagged keywords in close to real time. As governments and the private sector look to weed out malicious cyber-attacks, such as those that brought down US and South Korean government sites this month, Narus and others are touting their ability to block designated internet traffic from suspect addresses. "People think that net surveillance and censorship are a problem with China, but the reality is it's much more pervasive in the US," said Marc Rotenberg, executive director of the nonprofit Electronic Privacy Information Center in Washington.

SS8's software is designed to integrate with scores of different networks, interfaces and protocols. It can sort through a long list of communications, including wi-fi, push-to-talk and Voice over Internet Protocol, the company says on its website. Its executives declined interview requests in the wake of the UAE uproar.

Simplified access to communications for law enforcement with warrants is mandated in the US under a law called CALEA, and equivalent rules are in place in Europe.

"In the US, carriers are required to have the capability to do certain kinds of taps, but they are not required to put tapping software into people's mobile devices," said Seth Schoen, staff technologist at the civil-liberties group Electronic Frontier Foundation. "It may be cheaper for the carrier to modify its network than to modify its devices, especially if customers are using devices not supplied to them by the carrier."

While BlackBerry e-mail traffic is encrypted, a US federal law enforcement source said it can all be recovered, most likely with a combination of access from the service provider and a key to the code from RIM. "You can get the whole suite" of services, including e-mail, voice calls, text messages and direct BlackBerry-to-BlackBerry PIN messages, which take another route, he said.

Another federal agent said US officials once had some difficulty because Research in Motion is based in Canada. That prompted approaches via the Royal Canadian Mounted Police, which had a better relationship with the company.