+----------+

Spies Fail to Escape Spyware in $5 Billion Bazaar for Cyber Arms
2011-12-22 00:01:00.5 GMT

By Vernon Silver

Dec. 22 (Bloomberg) -- The intelligence operative sits in a leather club chair, laptop open, one floor below the Hilton Kuala Lumpur's convention rooms, scanning the airwaves for spies.

In the salons above him, merchants of electronic interception demonstrate their gear to government agents who have descended on the Malaysian capital in early December for the Wiretapper's Ball, as this surveillance industry trade show is called.

As he tries to detect hacker threats lurking in the wireless networks, the man who helps manage a Southeast Asian country's Internet security says there's reason for paranoia.

The wares on offer include products that secretly access your Web cam, turn your cell phone into a location-tracking device, recognize your voice, mine your e-mail for anti-government sentiment and listen to supposedly secure Skype calls.

He isn't alone watching his back at this cyber-arms bazaar, whose real name is ISS World.

For three days, attendees digging into dim sum fret about losing trade secrets to hackers, or falling prey to phone interception by rival spies. They also get a tiny taste of what they've unleashed on the outside world, where their products have become weapons in the hands of regimes that use the gear to track and torture dissidents.

"I'm concerned about my calls or Internet being monitored, because that's what they sell," says Meling Mudin, 35, a Kuala Lumpur-based information-technology security consultant who takes defensive measures as he roams the exhibits. "When I make phone calls, I step out of the hotel, I don't use my computer and I also don't use the wireless services provided."

'We Meet Again'

ISS, which convenes every few months in cities from Dubai to Brasilia, is the hub of the surveillance trade. In recent years, countries such as Syria, Iran and Tunisia bulked up their monitoring by turning to some of ISS's corporate sponsors, such as Italy's Area SpA and Germany's Utimaco Safeware AG and Trovicor GmbH, a Bloomberg News investigation showed.

Business is booming, with annual revenue of $3 billion to
$5 billion growing as much as 20 percent a year, ISS organizer Jerry Lucas estimates.

Lucas, 68, an American with a PhD in physics, is perfectly cast for the part of spyware convention mastermind. With sweeping eyebrows and a bare pate that make him a look-alike of Democratic strategist James Carville, he greets an uninvited journalist at his Prague event in June with, "We've been expecting you."

On the second encounter, in Kuala Lumpur this month, he descends an escalator from the convention floor and intones:
"We meet again."

Warning Attendees

Lucas, whose conference company TeleStrategies, Inc., is based in McLean, Virginia, makes the point that his marketplace serves police who conduct criminal investigations and intelligence services that prevent terror attacks. Virtually every communications network in the world includes

wiretapping for prosecutors, or location tracking to rescue people in emergencies. And customers at ISS also include phone company executives.

Still, Lucas describes Spy vs. Spy intrigue that emerges when he convenes ISS (short for Intelligence Support Systems).

The potential for hacking has led him to warn attendees to comply with the law of host countries.

"We tell them, 'Do not bring in radio equipment that is not allowed by the government,'" says Lucas, who started ISS nine years ago.

Some gear can intercept mobile-phone or Internet transmissions, impersonating legitimate networks by sitting in the middle of the data flow.

"These guys can be your base station," Lucas says.

'Hide Your Laptop'

Attendees routinely guard against hacking, says Nikhil Gyamlani, a Munich-based developer of monitoring systems who has attended several ISS events. He says being in close contact with competitors versed in the dark arts gives them a chance to secretly copy documents saved on hard drives or sent via e-mail.

He advises preventive measures.

"Absolutely no use of wireless networks, and hide your laptop in a safe," says Gyamlani, 34, the founder of a new surveillance company, GlassCube. "The fear is very justified."

Some who haven't taken such precautions have learned to be more careful.

At ISS in Prague this year, an employee of an African telecommunications regulator was cruising Facebook on his Archos tablet computer when he found his every click being projected on a screen at the front of the room, he recalled afterwards in the lobby. He'd been using the hotel's wireless Internet.

Watching The Detectives

While ISS is closed to journalists, a Bloomberg News reporter dropped in on two 2011 installments, walking hotel corridors, sitting in bars and haunting lounges.

In Prague, at a hotel connected to a shopping mall food court, potential buyers included Thailand's Department of Special Investigation and the U.S. Drug Enforcement Administration. In the lobby, contingents from Greece and Turkey sat on opposite sides of the room.

Many conventioneers carried black canvas tote bags from Utimaco, whose systems were used in a Syrian surveillance project that was exposed this year by Bloomberg News and shut down before it could become operational.

Approaches by a journalist at ISS only triggered more paranoia among some executives. At a fourth-floor conference room rented by Trovicor in Prague, an employee, Jesper Mathiesen, not only declined to talk, but declined to trust the reporter's business card as reliable identification.

Rock Star

"Anyone can print a business card," he said, as another employee led a delegation from Serbia into the room.

In the Prague hotel's elevators, an employee of Andover, U.K.-based Gamma International rode up and down, escorting government delegations to back-to-back, appointment-only demonstrations of Gamma's FinFisher intrusion system, conducted in darkened rooms.

Once secretly planted on a target's computer, FinFisher allows remote control of the device. The tool became widely known early this year when a copy of a FinFisher proposal turned up in Egypt after the February revolution and was posted online.

The notoriety helped make the German hacker-turned- executive behind FinFisher a rock star of the ISS circuit.

Listed in the conference agendas only by his initials, MJM, he is Martin J. Muench, 30, the managing director of Gamma's German unit. One of his talks in Kuala Lumpur is titled, "Offensive IT Intelligence Information-Gathering Portfolio --An Operational Overview."

Saudi Arabia, India

At this gathering of real-life James Bonds, Muench most resembles 007 himself, as played by Sean Connery: just over six feet tall, in a trim black suit and skinny black tie.

Spotted at ISS this month, Muench declines to comment, while lighting a cigarette.

For the Malaysia event, which has 871 invited attendees from 56 countries, the Hilton lobby hosts a parade of ISS's various tribes and their telltale markings. Buyers from Saudi Arabia's interior ministry, India's cabinet secretariat and the 5-month-old state of South Sudan brandish yellow nametags that peg them as government officials. Vendors are identified by red tags.

Employees of Munich-based Trovicor are easy to pick out:
each is dressed identically, in a dark suit and a red necktie, which is custom made, marketing director Birgitt Fischer-Harrow says.

Barring Syria

"It is a Trovicor corporate identity. The company colors are black, white and Pantone 202c red," she says, referring to the precise shade of burgundy.

Trovicor is a former intelligence unit of Siemens AG and Nokia Siemens Networks. The chain of companies supplied and maintained eavesdropping systems for Syria, Bahrain, Tunisia and other countries that have battled rebellions this year, a Bloomberg News investigation showed. Fischer-Harrow says the company can't comment on contracts or clients.

Lucas says he's barred Syrian or Iranian government representatives from ISS.

Still, that hasn't stopped surveillance gear from reaching those countries, and the controversy has attracted crashers to ISS seeking to expose how the technology can be abused by repressive regimes.

In an empty hotel restaurant after lunch, Eric King, the human rights and technology adviser at London-based Privacy International, is poring over conference presentations he's obtained and tallying a growing list of suspicious technological glitches. When he tries to send an e-mail from his Apple Inc.
laptop, he gets a message that his encryption won't work.

Seeking Hackers

His paranoia builds as he also realizes that more secure 3G networks, used for phones and wireless Internet, are unavailable in the hotel. King, 22, jetlagged and wearing a wrinkled, blue button-down shirt, has a hypothesis: Someone has blocked the 3G to force everyone to use methods that would be easier to intercept.

He consults the ISS program and finds a possible culprit, "Live Demonstration of Tactical GSM Interrogation and Geo- Location System."

"We've got to get us some hackers," he says, eager to untangle what may be a nest of surveillance.

A few hours later, King heads to Kuala Lumpur's art deco Central Market to meet a Privacy International volunteer. Over a noodle dinner, she puts him in touch with a hacker who agrees to meet up the next day.

Recruiting Spies

Back at the hotel, the night is young and the paranoia is deep.

Unlike typical trade shows, this one has no social events.

No corporate-sponsored cocktail parties. No hospitality suites.

Clients and suppliers don't want to be seen with each other in public, and some countries bar their agents from mingling at the event because it's a recruiting ground for spies seeking sources, organizer Lucas says.

In some delegations, "They'll send four or five people and have one here just to watch the rest," he says.

At the Hilton's wine bar, Vintage Bank, three men from Milan-based HackingTeam are talking among themselves, drinking from brandy snifters.

Because HackingTeam sells programs that can spy on a computer's contents and activities, maybe they know something about the 3G blackout. All three say that they, too, have noticed, and also suggest an interception effort may be afoot.

In the morning, King's hacker arrives at the Hilton lobby, toting a backpack filled with wireless Internet gear and wearing a black T-shirt.

Intelligence Operative

They set up shop on a coffee table. After an hour of performing many of the same tests the intelligence operative had done at the start of the convention, the network activity comes up clean.

The hacker suggests the 3G problem might just be a spotty phone system. Later, ISS organizer Lucas says any drop in service may have been caused by heavy usage by convention-goers.

Upstairs, the operative is back in the leather club chair, this time using an iPad. Asked if this isn't risky, he says it's just for browsing websites, not e-mail or anything involving passwords. And he's got no files saved to it.

Does he have e-mail access?

He holds up a BlackBerry, and says he's running nothing sensitive through it. Then he does a double-take. The screen saver is a photo of him and his wife.

The bad guys could do face recognition, he says, looking at the picture. Kicking himself for the lapse, he walks off, the paranoia having got the best of him.

For Related News and Information:
Bloomberg's Wired for Repression series:
http://topics.bloomberg.com/wired-for-repression/
Internet industry news: NI INTERNET <GO> Top technology stories: TTOP <GO> For more on Mideast unrest: EXTRA <GO> Stories on Syria: NI SYRIA BN <GO> Projects and Investigations stories: NI PNI <GO> Exclusive stories: NI EXCLUSIVE <GO> Top regional stories: TOP MIDEAST <GO>

-- Editors: Marcia Myers, Melissa Pozsgay

To contact the reporter on this story:
Vernon Silver in Rome at +39-06-4520-6328 or vtsilver@bloomberg.net;

To contact the editor responsible for this story:
Melissa Pozsgay at +33-1-5365-5056 or mpozsgay@bloomberg.net