SUNDAY TIMES NEWS BY MATTHEW SAVIDES AND ANDRÉ JURGENS, 2015-07-12

SA spies' scary shopping list revealed

Image: Gallo Images/ Thinkstock

WikiLeaks lays bare SA police and SARS agents' inquiries about espionage software

- *The software is 'designed to attack, infect and monitor PCs and smartphones in a stealth way'*

A MASSIVE security breach by hackers has provided a rare glimpse into the world of clandestine government snooping — and revealed that South African authorities showed an interest in buying highly sophisticated spyware.

What is more frightening is the possibility that the spy equipment could be used illegally to obtain information on ordinary citizens.

This emerged in a massive dump of a million confidential e-mails and documents by WikiLeaks after they were taken by hackers last weekend from controversial Italian surveillance and security firm Hacking Team.

The documents reveal details of elaborate software used in murky espionage operations and show that members of the South African Police Service and the South African Revenue Service tried to acquire some of these programs. The software of interest to the law enforcers and the taxman would allow spying on a grand scale, granting them access to private details of their targets.

The software would allow the agencies to:

- Remotely grab files and e-mail messages off computers using Apple, Windows and Linux operating platforms;
- Monitor cellphone Skype calls and instant messages on platforms such as WhatsApp and Viber;
- Access Facebook, Twitter and social media accounts; and
- Take screen grabs off a cellphone, track its location and activate the phone's microphone to turn it into a bugging device.

The leaked documents include e-mail correspondence between a **xxxx** in police crime intelligence and **xxxx**, a key account manager at Hacking Team. **xxxx** inquired about a "commercial proposal" submitted by the company to sell Remote Control System to the police in 2011.

The software, which has since been updated under the code name Galileo, is "designed to attack, infect and monitor target PCs and smartphones in a stealth way".

It cannot be detected and works on Android, BlackBerry, Apple and Windows phones. It can track the location of the phone, grab files off the device, and turn the phone into a bugging device.

"Your quotation was submitted to Lieutenant-General **xxxx**. Before he could provide me with instructions, the following happened," **xxxx** wrote back to the firm in 2011, adding a link to a news article about the former crime intelligence boss being embroiled in a love-triangle murder investigation. The chain of correspondence does not indicate if the police purchased the software.

Cyber security expert **xxxx** said the law did allow the sort of tools Hacking Team offered, but that it had to be carefully monitored and used only after following due process.

"It becomes a problem when these tools are used abusively, cracking down on journalists or activists instead. The big problem with Hacking Team was that they knowingly sold these tools to governments with a proven track record of trampling on their people's rights.

"Tools like this, by analogy, are closest to wiretaps. The man in the street can't wiretap people; police can, with the right piece of paper. SARS can when acting under judicial mandates. Hacking Team was selling 'easy wiretaps' to anyone, and this is the complaint," he said.

National police spokesman Lieutenant-General **xxxx** was unable to answer detailed questions about the e-mails yesterday due to difficulties contacting the relevant parties.

xxxx, national president of the Security Association of South Africa, said he suspected the police already had access to the type of data that the company was offering to help extract.

And a lot of cellphone service providers also had access to data that police could tap into.

He said it was of the utmost importance that the police operated within the law.

"Our privacy acts are quite strong. [For this technology to be used] the law would have to change, or it would have to be used in conjunction with a court order," said **xxxx**.

Another e-mail, from **xxxx** — a former member of a rogue spy unit at SARS — on July 24 last year, asked for information about concealing "smartphone infections".

xxxx wrote: "Will appreciate it if you could send me information regarding the smartphone infections. The information must be as comprehensive as possible, e.g. is it necessary to 'Root' Android smartphones, can the infection be concealed in a MMS, etc. I would also want to know what the minimum quantity licences would be that we have to acquire and what the annual maintenance fee [would] be for updates."

The Sunday Times revealed in May that **xxxx** had submitted an affidavit to the Hawks admitting to spying on the National Prosecuting Authority. Affidavits by SARS employees said the former Directorate of Special Operations, better known as the Scorpions, paid **xxxx** sums of R900 000 and R250 000 to buy surveillance equipment.

SARS spokesman **xxxx** said yesterday the organisation was "not aware of such correspondence and is highly shocked by such allegations. SARS does not have records for such purchases. We, however, cannot speak on behalf of **xxxx**."

Other e-mails sent to Hacking Team include an inquiry from police Colonel **xxxx** on July 24 last year asking: "Where is Gmail located and how do I subpoena them to provide information for evidence purpose [s]?"

Company CEO **xxxx** alerted colleagues: "Please find a help request from a military guy in South Africa. Yes, such a request indicates that this guy is close to clueless. HOWEVER, we could exploit his request in order to establish a commercial contact."

In turn, **xxxx** e-mailed **xxxx**, saying it was "not possible to force Google to provide you with information related to one of their users". However, "what you can do, in order to bypass this bottleneck, is to infect the device of your suspect/target", he said.

Hacking Team's customers are intelligence agencies and governments around the world — including some with questionable human rights records — who use its software to fight crime. But it has also been used to snoop on political activists.

Besides the leaked documents, hackers stole the source code used to build spy software sold by the company, previously only available to government agencies. "Hacking Team's investigation has determined that sufficient code was released to permit anyone to deploy the software against any target of their choice. Before the attack, Hacking Team could control who had access to the technology . . . Now, because of the work of criminals, that ability to control who uses the technology has been lost. Terrorists, extortionists and others can deploy this technology at will if they have the technical ability to do so," said a spokesman.

Although the company has previously denied selling software to repressive regimes, the Guardian reports that the leaked documents appear to show that among its clients are several repressive states known to conduct "aggressive surveillance of citizens, activists and journalists both domestically and overseas".