Western Governments Indirectly Admit Hackers Rule the Digital World

by Ryan Gallagher via Kismo - The Guardian UK *Wednesday, Nov 2 2011, 9:06am*
international / mass media / other press

Governments turn to hacking techniques for surveillance of citizens

> *The software companies mentioned in this story do not conform to the hacker ideal or ethic; by their own admission they seek PROFIT and have no moral problem with supplying their surveillance software to whomsoever wishes to purchase it. Real hackers have no difficulty accessing unlimited funds via their digital talents; elite hackers by nature are against all forms of social oppression and intrusions on personal privacy -- in other words surveillance states are anathema to hackers.*

In a luxury Washington, DC, hotel last month, governments from around the world gathered to discuss surveillance technology they would rather you did not know about. The annual Intelligence Support Systems (ISS) World Americas conference is a mecca for representatives from intelligence agencies and law enforcement. But to the media or members of the public, it is strictly off limits.

Gone are the days when mere telephone wiretaps satisfied authorities' intelligence needs. Behind the cloak of secrecy at the ISS World conference, tips are shared about the latest advanced "lawful interception" methods used to spy on citizens – computer hacking, covert bugging and GPS tracking. Smartphones, email, instant message services and free chat services such as Skype have revolutionised communication. This has been matched by the development of increasingly sophisticated surveillance technology.

Among the pioneers is Hampshire-based Gamma International, a core ISS World sponsor. In April, Gamma made headlines when Egyptian activists raided state security offices in Cairo and found documents revealing Gamma had in 2010 offered Hosni Mubarak's regime spy technology named FinFisher. The "IT intrusion" solutions offered by Gamma would have enabled authorities to infect targeted computers with a spyware virus so they could covertly monitor Skype conversations and other communications.

The use of such methods is more commonly associated with criminal hacking groups, who have used spyware and trojan viruses to infect computers and steal bank details or passwords. But as the internet has grown, intelligence agencies and law enforcement have adopted similar techniques.

"Traditionally communications flowed through phone companies, but consumers are increasingly using communications that operate outwith their jurisdiction. This changes the way interception is carried out ... the current method of choice would seem to be spyware, or trojan horses," said Chris Soghoian, a Washington-based surveillance and privacy expert. "There's now a thriving outsourced surveillance industry and they are there to meet the needs and wants of countries from around the world, including those who are more – and less – respectful to human rights."

In 2009, while a government employee, Soghoian attended ISS World. He made recordings of seminars and later published them online – which led him to be the subject of an investigation and, ultimately, cost him his Federal Trade Commission job. The level of secrecy around the sale of such technology by western companies, he believes, is cause for alarm.

"When there are five or six conferences held in closed locations every year, where telecommunications companies, surveillance companies and government ministers meet in secret to cut deals, buy equipment, and discuss the latest methods to intercept their citizens' communications – that I think meets the level of concern," he said. "They say that they are doing it with the best of intentions. And they say that they are doing it in a way that they have checks and balances and controls to make sure that these technologies are not being abused. But decades of history show that surveillance powers are abused – usually for political purposes."

Another company that annually attends ISS World is Italian surveillance developer Hacking Team. A small, 35-employee software house based in Milan, Hacking Team's technology – which costs more than £500,000 for a "medium-sized installation" – gives authorities the ability to break into computers or smartphones, allowing targeted systems to be remotely controlled. It can secretly enable the microphone on a targeted computer and even take clandestine snapshots using its webcam, sending the pictures and audio along with any other information – such as emails, passwords and documents – back to the authorities for inspection. The smartphone version of the software has the ability to track a person's movements via GPS as well as perform a function described as "remote audio spy", effectively turning the phone into a bug without its user's knowledge. The venture capital-backed company boasts that its technology can be used "country-wide" to monitor more than 100,000 targets simultaneously, and cannot be detected by anti-virus software.

"Information such as address books or SMS messages or images or documents might never leave the device. Such data might never be sent to the network. The only way to get it is to hack the terminal device, take control of it and finally access to the relevant data," says David Vincenzetti, founding partner of Hacking Team, who adds that the company has sold its software in 30 countries across five continents. "Our investors have set up a legal committee whose goal is to promptly and continuously advise us on the status of each country we are talking to. The committee takes into account UN resolutions, international treaties, Human Rights Watch and Amnesty International recommendations."

Three weeks ago Berlin-based hacker collective the Chaos Computer Club (CCC) exposed covert spy software used by German police forces similar to that offered by Hacking Team. The "Bundestrojaner [federal trojan]" software, which state officials confirmed had been used, gave law enforcement the power to gain complete control over an infected computer. The revelation prompted an outcry in Germany, as the use of such methods is strictly regulated under the country's constitutional law. (A court ruling in 2008 established a "basic right to the confidentiality and integrity of information-technological systems".)

"Lots of what intelligence agencies have been doing in the last few years is basically computer infiltration, getting data from computers and installing trojans on other people's computers," said Frank Rieger, a CCC spokesman. "It has become part of the game, and what we see now is a diffusion of intelligence methods into normal police work. We're seeing the same mindset creeping in. They're using the same surreptitious methods to gain knowledge without remembering that they are the police and they need to follow due process."

In the UK there is legislation governing the use of all intrusive surveillance. Covert intelligence-gathering by law enforcement or government agencies is regulated under the Regulation of Investigatory Powers Act 2000 (Ripa), which states that to intercept communications a warrant must be authorised by the home secretary and be deemed necessary and proportionate in the interests of national security, public safety or the economic wellbeing of the country. There were 1,682 interception warrants approved by the home secretary in 2010, latest official figures show.

According to Jonathan Krause, an IT security expert who previously worked for Scotland Yard's hi-tech crime unit, bugging computers is becoming an increasingly important methodology for UK law enforcement. "There are trojans that will be customer written to get past usual security, firewalls, malware scanning and anti-virus devices, but these sorts of things will only be aimed at serious criminals," he said.

Concerns remain, however, that despite export control regulations, western companies have been supplying high-tech surveillance software to countries where there is little or no legislation governing its use. In 2009, for instance, it was reported that American developer SS8 had allegedly supplied the United Arab Emirates with smartphone spyware, after about 100,000 users were sent a bogus software update by telecommunications company Etisalat. The technology, if left undetected, would have enabled authorities to bypass BlackBerry email encryption by mining communications from devices before they were sent.

Computer security researcher Jacob Appelbaum is well aware what it is like to be a target of covert surveillance. He is a core member of the Tor Project, which develops free internet anonymising software used by activists and government dissidents across the Middle East and north Africa to evade government monitoring. A former spokesman for WikiLeaks, Appelbaum has had his own personal emails scrutinised by the US government as part of an ongoing grand jury investigation into the whistleblower organisation. On 13 October he was in attendance at ISS World where he was hoping to arrange a presentation about Tor – only to be ejected after one of the surveillance companies complained about his presence.

"There's something to be said about how these guys are not interested in regulating themselves and they're interested in keeping people in the dark about what they're doing," he says. "These people are not unlike mercenaries. The companies don't care about anything, except what the law says. In this case, if the law's ambiguous, they'll do whatever the law doesn't explicitly deny. It's all about money for them, and they don't care.

"This tactical exploitation stuff, where they're breaking into people's computers, bugging them ... they make these arguments that it's good, that it saves lives," he said. "But we have examples that show this is not true. I was just in Tunisia a couple of days ago and I met people who told me that posting on Facebook resulted in death squads showing up in your house."

The growth in the use of these methods across the world, Appelbaum believes, means governments now have a vested interest in keeping computer users' security open to vulnerabilities. "Intelligence [agencies] want to keep computers weak as it makes it easier to surveil you," he says, adding that an increase in demand for such technology among law enforcement agencies is of equal concern.

"I don't actually think breaking into the computer of a terrorist is the world's worst idea – it might in fact be the only option – but these guys [surveillance technology companies] are trying to sell to any police officer," he says. "I mean, what business does the Baltimore local police have doing tactical exploitation into people's computers? They have no business doing that. They could just go to the house, serve a warrant, and take the computer. This is a kind of state terror that is simply unacceptable in my opinion."

Jerry Lucas, the president of the company behind ISS World, TeleStrategies, does not deny surveillance developers that attend his conference supply to repressive regimes. In fact, he is adamant that the manufacturers of surveillance technology, such as Gamma International, SS8 and Hacking Team, should be allowed to sell to whoever they want.

"The surveillance that we display in our conferences, and discuss how to use, is available to any country in the world," he said. "Do some countries use this technology to suppress political statements? Yes, I would say that's probably fair to say. But who are the vendors to say that the technology is not being used for good as well as for what you would consider not so good?"

Would he be comfortable in the knowledge that regimes in Zimbabwe and North Korea were purchasing this technology from western companies? "That's just not my job to determine who's a bad country and who's a good country. That's not our business, we're not politicians ... we're a for-profit company. Our business is bringing governments together who want to buy this technology."

TeleStrategies organises a number of conferences around the world, including in Europe, the Middle East and Asia Pacific. Every country has a need for the latest covert IT intrusion technology, according to Lucas, because modern criminal investigations cannot be conducted without it. He claimed "99.9% good comes from the industry" and accused the media of not covering surveillance-related issues objectively.

"I mean, you can sell cars to Libyan rebels, and those cars and trucks are used as weapons. So should General Motors and Nissan wonder, 'how is this truck going to be used?' Why don't you go after the auto makers?" he said. "It's an open market. You cannot stop the flow of surveillance equipment."

http://tinyurl.com/3vfkudf