GlobalResearch
Center for Research on Globalization

Hacking the Hacking Team: The Innards of the Surveillance Industry

By Dr. Binoy Kampmark
Global Research, July 08, 2015
Region: USA
Theme: Intelligence

"Surveillance companies like Hacking Team have shown they are incapable of responsibly regulating themselves, putting profit over ethics time after time."

Eric King, Deputy Director Privacy International, Jul 7, 2015

What goes around can come around with inexorable force. An Italian hackers-for-hire company called the Hacking Team, selling software to facilitate surveillance, has been, in turn, hacked. In this self-assuming ecology, such companies will have to expect that what they allow others to do will be used on them in time.

The firm specialises in the sale of malicious software and technologies on a large scale, supplying a range of intelligence agencies and governments. It's stated aim is clear and mercenary in promise: "We provide effective, easy-to-use offensive technology to the worldwide law enforcement and technology companies."

On Sunday night, the hackers in question got busy changing the Twitter account of the company from The Hacking Team to The Hacked Team, with its transformed, stated purpose being, "Developing ineffective, easy-to-pwn offensive technology to compromise the operations of the worldwide law enforcement and intelligence communities."[1]

For twelve hours, the company's site was steered, a period which saw the release and distribution of company data, including a range of juicy titbits. "Since we have nothing to hide," went the message, "we're publishing all our e-mails, files and source code." The posted link effectively published a 400 gigabyte trove of internal documents, including customer invoices, executive emails and promised source code.

The surveillance industry is teaming with such technology, because clients keen to monitor their citizens and employees will always find the most readily available, and purchasable route. The business incentive is dressed up in champagne-reception styled promise: we provide the best services money can buy. We go to the shows. We go to the workshops and stump valuable software. All to satisfy the peeping tom impulse of state bureaucracy.

The client list is worth exploring, given that the company's persistent denial about selling to customers with a patchy record. The University of Toronto's Citizen Lab's report last year claimed to find traces of the Hacking Team's apparently untraceable software in 21 countries.[2] Company spokesman Eric Rabe dismissed the suggestions, citing a diligent internal system policing any abuse.

He also proved steadfast on the issue of not revealing client names, claiming that doing so would "jeopardise the confidentiality necessary for necessary law-enforcement and

intelligence operations" (*Mashable*, Feb 24, 2014).

The human rights dimension was certainly not absent from internal company correspondence. The Hacking Team's Operations Manager, Daniele Milan, expressed concern in an email (Mar 19) to various members of the company, including Rabe, about the impact of "Citizen Lab/HRW reports." Of specific concern was Ethiopia, whose agency had been "reckless and clumsy" in using their software against the Ethiopian Satellite Television Service and Ethiopian journalists in the United States.[3] "What's worst is that we can be sure that if we allow them to continue, more [bad publicity] will come." The customer, seemingly, is not always right.

As was revealed in the information dump, the list includes such states as Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakhstan, Morocco, Nigeria, Oman, Saudi Arabia and Sudan. They also count among them various agencies – the DEA, the US Department of Defence, and the FBI. (Unsurprising to note that one of the firm's three head offices is based in Annapolis, Maryland, deep in the US intelligence cluster.)

Counted among the invoices is one for $1 million made out to the Information Network Security Agency of Ethiopia, a country not exactly flowering with protections for its journalists. Sudan also features for an invoice at half the price. Both had agencies keen to obtain the spyware tool called the Remote Control System. The RCS is described amongst the Hacking Team's own materials as "a solution designed to evade encryption by means of an agent directly installed on the device".

While the event is still raw, the company has been in the sites of investigative journalists and students of the surveillance industry. Cora Currier and Morgan Marquis-Boire published an expose in *The Intercept* in October last year outlining the uses of RCS software in various manuals.[4] Meant for government technicians and analysts, they cover the activation of cameras, password collection, log typing, and noting Skype calls and emails.

The Hacking Team's RCS 9 Analyst's Guide is replete with the functionality of tapping, a step-by-step process on how "targets" are assigned and "operations" conducted.[5]

As Currier and Marquis-Boire explain, these manuals also list means of infecting devices via wifi networks, streaming video, USB sticks, and email attachments. Even the modestly trained technician would be able to operate these without fear of detection.

The surveillance industry has no codes of fidelity or borders of control. It is simply a business over nourished by peeping tom patrons. Caught in this tawdry mix are users of such technologies who simply want that rather frayed liberty of privacy to be protected. Not all who use encryption tools seek to trick the law and its suspicious officials.

FBI Director James Comey may well be concerned about "criminals and terrorists" liking "nothing more" than to have access to encryption defeating devices (*Guardian*, Oct 17, 2014). His obsession here lies with making sure such companies "build lawful intercept capabilities for law enforcement." But Comey is being fundamentally naïve. The Hacking Team and those of its ilk have an interest, less in principles of liberty, than bottom lines of profit. In this industry, buyers, not moralists, matter above all else.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email:bkampmark@gmail.com

Notes

[1] http://www.v3.co.uk/v3-uk/news/2416392/government-surveillance-software-firm--hacking-team-hit-by-hack-and-data-leak

[2] http://mashable.com/2014/02/23/hacking-team-spyware-governments/

[3] https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists--targeted-spyware/

[4] https://firstlook.org/theintercept/2014/10/30/hacking-team/

[5] https://firstlook.org/theintercept/2014/10/30/hacking-team/#manuals

---