Australian police, spy agencies flocked to Italian hacking company

Oscar Grenfell
15 July 2015

Among the revelations contained in more than a million emails from the Italian surveillance malware vendor Hacking Team released by WikiLeaks last week, is that a host of Australian police, intelligence and government agencies actively sought out the dubious company, with some apparently purchasing its hacking programs.

Hacking Team products, which included capabilities to remotely take control of computers and mobile phones, have been purchased by police agencies in Britain, the US, and a host of repressive regimes around the world.

The ties between Australian state agencies, and the Italian company, underscore the massive buildup of police and intelligence capabilities and powers, directed against fundamental democratic rights, under the rubric of the fraudulent "war on terror."

According to the leaked emails, which include Hacking Team's accounts, the Australian Federal Police (AFP) was a client of the company until 2011. Invoices from November 2009, and February 2010 indicate that the AFP paid some €245,000 for the company's offensive hacking products.

The software that the AFP apparently purchased facilitates hacking into encrypted emails, Skype calls, and data stored on a computer, and provides the ability to turn on and monitor microphones and cameras on mobile phones and computers. The software also enables the sending of viruses and malicious software.

The main domestic spy agency, the Australian Security Intelligence Agency (ASIO), also appears to have solicited the Italian hacking company. The leaked emails indicate that a Canberra-based company named Criterion Solutions signed a non-disclosure agreement in November 2014 for information about Hacking Team's programs. According to the ABC, Hacking Team's Malaysian representatives have since indicated that Criterion Solutions was representing ASIO in the negotiations.

Hacking Team reportedly provided a briefing to the 2014 National Security Conference, an event attended by government officials.

Australian state police forces also sought out the Italian company. The New South Wales (NSW) police sent a request for a price list of Hacking Team's products in July 2013, while the Northern Territory (NT) police solicited a briefing on the company's services in November 2014. A Hacking Team report on that meeting indicates that abilities to hack into Gmail, and Facebook accounts, along with opening encrypted files on a thumb drive, accessing online banking and many other invasive measures were all demonstrated.

The Victorian Independent Broad-based Anti-corruption Commission (IBAC) also had dealings with Hacking Team, and was apparently considering signing a $500,000 contract with the company in late June.

The latest leaks are not the first time it has been revealed that government and police authorities purchased hacking software from private companies. In September 2014, documents released by WikiLeaks exposed the NSW police as a client of the German-based FinFisher company, which provides hacking software that performs a similar function to Hacking Team's products. The leaks indicated that NSW police had first acquired licenses to FinFisher's products in late 2011, and had in all paid some $2.6 million to the company.

Successive Coalition and Labor governments at the state and federal level have boosted police and intelligence funding, as part of a broader assault on basic democratic rights. Since 2001, these agencies have been provided with ever-broader powers to

monitor, detain and harass ordinary people on the flimsiest of pretexts.

Between 2007 and 2013, the Labor governments of Prime Ministers Kevin Rudd and Julia Gillard boosted the budget of ASIO alone by 27 percent, and increased its staffing by 32 percent. The Labor government spent some $18 billion on “national security matters” beginning in 2008.

Last October, the unanimous support for the build-up of police powers within the political establishment was on display, with the passage of the National Security Legislation Amendment Bill, which further expanded ASIO’s powers.

The bill, which was supported by the Labor Party opposition, gave the spy agency the power to monitor, hack, and take control of computer networks of any size, and included anti-whistleblower provisions that could see journalists imprisoned for 10 years for exposing ASIO’s activities. Not a single vote was cast against the legislation, at its final reading in the House of Representatives.

The Coalition government, backed by Labor, also announced the boosting of funding for the security services by some $630 million over four years, including $200 million for ASIO.

The ramping up of funding for the police and intelligence agencies has been accompanied by attempts to whip up hysteria over “terrorism.” In September last year, Australian police and ASIO officers conducted the largest anti-terror raids in the country’s history involving some 800 personnel. The media issued lurid stories aimed at stoking fear, but only one person was charged, and on dubious grounds. Since then, the “terror threat level” has been raised, and further incidents, including the police killing of 17-year-old Numan Haider, and massive police mobilisation for the Sydney Siege last December, have been invoked to advocate ever more repressive powers.

The use by police and government authorities of hacking software takes place in the context of Australia’s complete integration into the US-led global spying operation exposed by whistleblower Edward Snowden in 2013. The National Security Agency (NSA) actively spies on the communications of millions of people, in the US and around the world, along with government officials, and even heads of state.

Snowden’s revelations included information that the Australian Signals Directorate (ASD), was playing a direct role in the NSA’s harvesting of hundreds of millions of email address lists, and “buddy lists” from instant messaging devices. The ASD, along with telecommunications firm Telstra, also play a critical role in the NSA’s data collection by assisting it to plug into the undersea cables that carry internet traffic and other electronic communications from the region.

At the same time, government and law enforcement authorities issue hundreds of thousands of requests for telecommunications data, without requiring a warrant or judicial oversight. In 2011–12, government and police bodies, excluding ASIO issued 293,501 such requests.

Australian authorities have also been directly implicated in the US-led espionage activities directed against foreign governments, with the ASD and NSA establishing “listening” posts in capitals throughout Asia. Among those spied on was Indonesian President Susilo Bambang Yudhoyono.

The Abbott government, with the full support of the Labor Party opposition is continuing to ramp up the assault on the fundamental democratic right to privacy. In March, it passed legislation with bipartisan support mandating that telecommunications providers retain internet and phone data for two years, during which time it will be searchable by the intelligence and security agencies.