WikiLeaks email release reveals hacking by governments worldwide

Mike Head
13 July 2015

WikiLeaks last week published more than one million emails from the Italian surveillance malware vendor Hacking Team, shedding further light on the extent of the spying being conducted by governments around the world against their populations.

Emails in the searchable database disclose the company's negotiations with intelligence and police agencies to supply some of the advanced technology used to secretly hack into, take control over and monitor computers and smart phones.

In its emails, Hacking Team boasts that its programs can "attack, infect and monitor target PCs and smart phones, in a stealth way" and "bypass encryption, collect relevant data out of any device, and keep monitoring your targets wherever they are, even outside your monitoring domain."

At least 46 countries are identified as purchasing, or preparing to purchase, Hacking Team software. The list features Western powers, such as the United States, Britain and Australia, along with openly repressive regimes around the world, including military dictatorships such as Egypt and Thailand.

On July 5 the company's Twitter account was reportedly compromised. Over 400GB of data, featuring internal emails, invoices and source codes were revealed via BitTorrent. Revelations so far include that Hacking Team works with the major imperialist spy agencies, together with police units such as Bangladesh's Rapid Action Battalion, a paramilitary agency notorious for torture and extrajudicial killings.

The US is a customer via the FBI, the military and the Drug Enforcement Agency. Police agencies in the United Kingdom have trialled Hacking Team's technology, despite acknowledging that its use could be illegal. Australia's purchasers include the main domestic spy agency, the Australian Security Intelligence Organisation (ASIO), and the Australian Federal Police (AFP).

According to a survey of the database published by the *Intercept* web site, Hacking Team's biggest sales in recent years have come from these countries, in descending order of sales: Mexico, Italy, Morocco, Saudi Arabia, Chile, Hungary, Malaysia, UAE, the US, Singapore, Kazakhstan, Sudan, Uzbekistan, Panama, Ethiopia, Egypt, Luxembourg, Czech Republic, South Korea, Mongolia, Vietnam, Spain, Ecuador, Oman, Switzerland, Thailand, Russia, Nigeria, Turkey, Cyprus, Honduras, Azerbaijan, Colombia, Poland, and Bahrain.

The company was pushing for contracts in Brazil, Belarus, Guatemala, Israel, Kuwait, Finland, Georgia, Greece, India, Turkmenistan, Kyrgyzstan and elsewhere. Several intelligence and police agencies in India sought technology that was not just target-specific, but could create a sweeping net of surveillance.

One Hacking Team email sent to Maharashtra police provided an insight into the far-reaching capabilities of the company's Remote Control System (RCS) to manipulate and monitor computer networks and smart phones.

"It allows you to covertly collect data from the most common desktop operating systems, such as: Windows, OS X, Linux," the email claimed. "Furthermore, Remote Control System can monitor all the modern smart phones: Android, iOS, Blackberry, Windows phone. Once a target is infected, you can access all the information, including: Skype calls, Facebook, Twitter, WhatsApp, Line, Viber and many more—device location, files, screenshots, microphone, virtual currencies and much more."

A brochure for RCS stated: "Take control of your

targets and monitor them regardless of encryption and mobility ... Remote Control System is invisible to the user, evades anti-virus and firewalls, and doesn't affect the devices' performance or battery life."

Other promotional material emphasised that RCS could remotely activate microphones and cameras and send the data back for analysis, and monitor people logging in to Gmail and Facebook.

Emails relating to Australia showed company representatives identifying state and territory police forces, and a Victorian state anti-corruption body, as well as ASIO and the AFP, as being in confidential negotiations with Hacking Team. Victoria's anti-corruption commission was considering signing a $500,000 contract for monitoring software as recently as two weeks ago.

Another email chain named a Canberra company, Criterion Solutions, signing a non-disclosure agreement for access to information about the RCS program last November. The Hacking Team's Singaporean representatives later said Criterion Solutions was acting for ASIO.

For further exposing the surveillance being conducted against millions of people internationally, WikiLeaks and its founder, Julian Assange, will come under renewed assault by the governments and agencies involved. WikiLeaks is already being branded as "criminal," while the anti-democratic operations of the so-called security agencies are regarded as legitimate.

Eric Rabe, the chief marketing and communications officer for Hacking Team, told the Australian Broadcasting Corporation that the hacking of the company's data was "reckless and dangerous." It was "a criminal attack" conducted with "no regard for public safety." Rabe insisted that Hacking Team's services helped police and investigators "keep the rest of us safe."

In reality, as documented by previous WikiLeaks releases, the US and its allies are engaged in criminal activities on a worldwide scale, including massacres, torture, regime-change operations and illegal bugging. In addition, their mass surveillance operations, spanning the globe, have been laid bare by US National Security Agency whistleblower Edward Snowden.

The UK-based Privacy International expressed shock at the scale of the Hacking Team's operations disclosed by WikiLeaks. The organisation suggested that Western governments had not realised the "full picture" and needed to "ensure the integrity of their contractors." It urged them to confine access to surveillance technology to "governments with strong human rights records," rather than "governments with awful human rights records."

The truth of the matter is that the US and other Western imperialist powers are leading the establishment of police-state conditions, ripping up basic legal and democratic rights in the process. Amid mounting political and social discontent, they are the most intent of all governments on utilising the technology now available to establish the scaffolding of a police state.

In Australia, the Abbott government, with the Labor Party's bipartisan support, has pushed through parliament four major surveillance bills in the past six months, on the pretext of combating the threat of ISIS terrorism. The very first bill, brought forward last September, specifically allows ASIO to use listening, optical and tracking devices without warrants, and hack into and "disrupt" entire computer networks, while imposing lengthy jail terms for whistleblowers and journalists who alert the public to the undercover operations.

The fourth bill, passed this year despite widespread popular opposition, compels all Internet providers and social media platforms, including Google and Facebook, to retain vast amounts of data for two years so that the security services can trawl through it, permitting them to compile a full picture of everyone's spending habits, political views, friends and associates and geographical locations.