Canadian spy agency creates global hacking network

Dylan Lubao
27 September 2014

A recent report in the *Globe and Mail* reveals that Canada's signals intelligence agency has developed and field-tested software that can secretly hijack a computer and then use it as a springboard to hack into other computers.

The report is based on top-secret material leaked to the German computer magazine *c't*. Titled "LANDMARK," the document adds to the list of the vast and unrestrained spying powers of the Communications Security Establishment Canada (CSEC). It also highlights the extent to which the spy agency has become a leader in electronic surveillance, heavily relied upon by the American NSA and its partners in the Five Eyes intelligence alliance to conduct mass spying operations against their geopolitical rivals and the world's population.

Multimedia slides from the leaked material show that the LANDMARK software is being used to create a level of "non-attribution" for CSEC's cyber espionage operations. By hijacking an individual's computer and then using it to hack into others, CSEC can create a vast covert data collection network that better shields its illegal activities and those of its Five Eyes partners.

Another slide demonstrates the scope of the new software. In February 2010, CSEC gave two dozen analysts up to eight hours to gather a list of potential target computers, known as Operational Relay Boxes (ORBs). Over 3,000 targets were gathered, which was seen as a good start. Using an adaptation of their OLYMPIA search engine, CSEC can trawl through large amounts of data acquired this way.

LANDMARK is not primarily oriented towards ordinary computer users, who generally lack the sophisticated tools needed to track attacks on their machines. Rather, it is clearly designed for ultra-sensitive operations, such as the targeting of the computer systems of governments or major computer and telecommunications corporations, allowing CSEC to protect its identity through the aforementioned levels of "non-attribution".

Towards the end of 2013, it was revealed that CSEC had opened offshore "covert sites at the request of the NSA" to conduct spying operations "targeting approximately 20 high-priority countries." This ties in to previously released information surrounding the STATEROOM program, through which CSEC and its Five Eyes partners mount spying operations in foreign countries from secret installations within their diplomatic offices. CSEC was also revealed to have spied on the Brazilian government in support of Canadian corporations, and assisted the NSA in spying on the 2009 G-20 meeting in London and the subsequent 2010 G-20 summit in Toronto.

Viewed against these revelations, the Harper Conservative government's vilification of rivals such as China and Russia for alleged state spying reeks of utter hypocrisy. These political provocations, which have been echoed by the opposition New Democratic Party and Liberals, are designed to erode the Canadian public's opposition to NATO preparations for war against these countries.

In perhaps the most revealing slide, it is shown that the NSA requested CSEC's help in "gaining access" to a mobile phone company's GSM network. CSEC was able to successfully infiltrate the network in under five minutes using LANDMARK. Another slide suggests that CSEC performed a similar task for the British GCHQ, which was interested in finding ORBs in Kenya.

Former NSA executive Thomas Drake summed up one of the reasons CSEC is a valued NSA partner: "Think of certain foreign agreements or relationships

that Canada actually enjoys that the United States doesn't, and under the cover of those relationships, guess what you can conduct?"

The union between CSEC and the NSA goes back decades. At the height of the Cold War, CSEC was the Five Eyes partner tasked with eavesdropping on the Soviet Union. Today, CSEC and NSA function virtually as one. According to a CSEC insider, this includes regular "exchange of liaison officers and internees, joint projects, shared activities, and a strong desire for closer collaboration in the area of cyber defense." In addition, CSEC enjoys wide access to the NSA's spying capabilities, including its newest data-mining and decryption technology. The NSA also contributes funding for joint projects.

CSEC's relationship with the NSA provides it with a means of circumventing constitutional restrictions on the interception of Canadians' private communications data. Although CSEC is legally forbidden to ask the NSA to spy on Canadians, nothing prevents it from receiving "unsolicited" private communications data acquired by the NSA.

CSEC's partnership with the NSA is part of the Canadian ruling elite's ever-deeper integration into Washington's predatory global military-security agenda. Calculating that its own imperialist interests can be best asserted through an alliance with the US, the Canadian elite has joined one US-led war after another since 1991, including the new war Obama has launched in the Middle East under the pretext of combating ISIS.

CSEC has boasted about its role in providing crucial military intelligence to the Canadian Armed Forces during its decade-long neo-colonial war in Afghanistan. While not publicly acknowledged, its spying operations are undoubtedly integrated via the NSA into Pentagon war-planning.

Given the extent of CSEC's integration into the NSA's operations, it can be safely assumed that CSEC does everything that the NSA does, albeit with a smaller global footprint.

The federal Conservative government and CSEC have already been shown to have lied shamelessly about CSEC's spying on Canadians.

For eight months, the government and CSEC stonewalled after a newspaper exposé revealed that since 2005 CSEC has been systematically spying on the metadata of Canadian's electronic communications—cell phone conversations, text messages, internet use, etc..

This all changed in February, when a new leak revealed that CSEC had been spying on WiFi users at major Canadian airports. The government was forced to change tack, baldy asserting its legal right to collect Canadians' communications "metadata." (See:HYPERLINK "http://www.wsws.org/en/articles/2014/02/04/csec-f03.html" CSEC and Harper government assert right to spy on Canadians)

The government has defended this illegal spying by claiming that information provided by metadata is innocuous and therefore not subject to legal bans on the collection of Canadians' private communications.

This is a spurious argument, as legal experts and advocates for civil rights the world over have repeatedly stressed. Metadata contains sensitive information, including names, contact info, and location data that can be used to create highly detailed profiles of an individual or group. In some cases, this data can be more revealing than the actual content of a communication, including in determining political leanings, friends and associates.

CSEC's global and domestic spying activities exemplify the Canadian elite's embrace of reaction right down the line—its aggressive imperialist foreign policy and its turn toward illegal, authoritarian forms of rule as it seeks to make the working class pay for the crisis of capitalism.