Despite exposure, new nations joining cyberespionage game

October 15 2015, byRaphael Satter

In this Oct. 13, 2014, file photo, pro-democracy activists, from left, Moosa Abd-Ali Ali, Saeed Al-Shehabi and Jaafar Al Hasabi listen during a news conference in London. The three activists said they had been hacked by Bahrain's government while living in Britain. The three men were at the heart of a criminal complaint, filed with British police by London-based Privacy International, alleging that Bahrain's government infected their computers with FinFisher, a powerful piece of espionage software. Researchers have since identified a new group of smaller, poorer nations as users of spy software, suggesting that a recent series of leaks and lawsuits hasn't deterred governments from investing in off-the-shelf cyberespionage products. (AP Photo/Matt Dunham, File)

Researchers say some smaller, poorer nations are now using spy software, suggesting that recent data leaks and lawsuits have not deterred governments from investing in off-the-shelf cyberespionage products.

Internet watchdog group Citizen Lab said in a report Thursday that it had found 33 "likely government users" of FinFisher, one of the world's best-known purveyors of spyware. A report released separately by London-based Privacy International on Thursday said the same spyware had seen use in Uganda to hack, intimidate and blackmail members of the opposition.

Business appears good for FinFisher, despite a damaging hack last year which exposed reams of client information and other confidential data.

"They seem to have a healthy client base, despite the fact that they were hacked and customer data was exposed," Citizen Lab's Bill Marczak wrote in an email. "Far from observing a drop in FinFisher servers, we're detecting more than ever before."

FinFisher did not return messages seeking comment on the findings.

Like many malicious programs, FinFisher's products work by infecting their targets' computers and phones, copying messages, recording conversations and even activating webcams.

On its website, the Munich-based company say the spyware helps law enforcement and intelligence agencies bring criminals to justice. Among the documents leaked last year was a brochure touting the software's success in breaking up organized crime and human-trafficking rings, but FinFisher's tools have also been found spying on journalists, human rights defenders and lawyers.

Privacy International's report said FinFisher had been deployed against

opponents of Ugandan President Yoweri Museveni during 2012 protests against his government. The advocacy group published what it said was a leaked Ugandan presidential briefing which boasted that "hordes of data" had been gathered by the spyware.

One objective, the seven-page briefing said, was "to manage and control the media houses and opposition politicians, which in the worst case scenario, may involve blackmailing them especially after personal information is in our hands."

The briefing, marked "SECRET," went on to say that FinFisher's tools had been deployed in hotels, government agencies and even the country's parliament. "Impudent opposition politicians" were among the spyware's top targets, the memo said.

There was no immediate way to independently authenticate the briefing, although Privacy International has a record of publishing genuine material about surveillance companies' operations. Ugandan government spokesman Ofwono Opondo did immediately respond to calls for comment.

Hacking impudent opponents doesn't come cheap. Among the documents leaked last year was a price list suggesting that a suite of FinFisher products—including a full set of attack software, booby-trapped thumb drives and nearly a dozen different training courses—retailed for some 3 million euros ($3.5 million.)

That price tag doesn't seem to have put off Uganda or other government agencies in Paraguay, Kenya, Macedonia and Bangladesh. The latter were four were among the countries newly identified as likely users of FinFisher by Citizen Lab, which is based at the University of Toronto's Munk School of Global Affairs and has long kept tabs on government hacking.

In Bangladesh, researchers found a FinFisher server in an Internet Protocol address block used by the country's Directorate General of Forces Intelligence. In Kenya, the researchers found a server in an address block registered to a user identified as "National Security Intelligence"—an old version of the name for the country's National Intelligence Service. Both organizations have been implicated in human rights violations including disappearances and torture.

Bangladesh's Directorate General of Forces Intelligence did not return messages seeking comment. Kenyan officials also didn't return messages. Cpt. Amilcar Vera, the spokesman for Paraguay's anti-terror and anti-drugs task force, said he could neither confirm nor deny his country's use of FinFisher. In Macedonia, Interior Ministry spokesman Ivo Kotevski said the brand of spyware used by his country's spies was "classified information."

More information: Citizen Lab's report: citizenlab.org/2015/10/mapping … nuing-proliferation/

Privacy International's report: privacyinternational.org/node/656