The Intercept_

HACKING TEAM EMAILS EXPOSE PROPOSED DEATH SQUAD DEAL, SECRET U.K. SALES PUSH AND MUCH MORE

Ryan Gallagher

July 9 2015, 1:31 a.m.

Late Sunday, hackers dumped online a massive trove of emails and other documents obtained from the systems of Italian surveillance firm Hacking Team. The company's controversial technology is sold to governments around the world, enabling them to infect

smartphones and computers with malware to covertly record conversations and steal data.

For years, Hacking Team has been the subject of scrutiny from journalists and activists due to its suspected sales to despotic regimes. But the company has successfully managed to hide most of its dealings behind a wall of secrecy — until now.

For the last few days, I have been reading through the hacked files, which give remarkable insight into Hacking Team, its blasé attitude toward human rights concerns, and the extent of its spyware sales to government agencies on every continent. Adding to the work of my colleagues to analyze the 400 gigabyte trove of hacked data, here's a selection of the notable details I have found so far:

Demo for Bangladesh "death squad"

In May, a Hacking Team representative traveled to Dhaka, Bangladesh, to demonstrate the company's spy technology at the headquarters of a brutal paramilitary security agency that is known for torture and extrajudicial killings. The Rapid Action Battalion (pictured above) — described by Human Rights Watch as a "death squad" that has perpetrated systematic abuses over more than a decade — wanted to see "a practical demonstration" of Hacking Team's surveillance equipment "in the ground settings of Bangladesh," according to the company's emails. Last month, a reseller for Hacking Team in Bangladesh reported that he had submitted the bid papers for the deal and was "pushing RAB to select our offer through our personal relationship."

DEA mass surveillance in Colombia

Hacking Team supplies its technology to the DEA, which one email shows is apparently using the spyware to launch surveillance operations from the U.S. embassy in Bogota, Colombia. More notably, the email suggests that, in addition to the Hacking Team technology, the DEA is also using other spying equipment at the embassy in Colombia to perform dragnet Internet surveillance. Last month, a Hacking Team field engineer had a meeting with DEA agents in Cartagena and noted that he was told the agency had "bought another interception tool (something that will receive all the traffic for Colombian's [sic] ISPs)."

Impressing dictator's spies

In October 2014, in Doha, Qatar, Hacking Team demonstrated its technology for two officers from the Belarus intelligence agency Operations and Analysis Center, or OAC. The Belarus government is an authoritarian regime that been accused by Human Rights Watch of suppressing "virtually all forms of dissent," cracking down on journalists, activists, opposition politicians, and anyone else deemed to have deviated too far from the orthodoxy of despotic president Alexander Lukashenko, known as "Europe's last dictator." Nevertheless, these issues don't seem to have put off Hacking Team's attempts to make a sale. "The prospect confirms to be impressed by our solution," noted a Hacking Team employee after the meeting with the two officers. "They will evaluate to proceed with the Sales Department to arrange a dedicated meeting." It is unclear from the emails whether the sale went ahead or if efforts to finalize it are still ongoing.

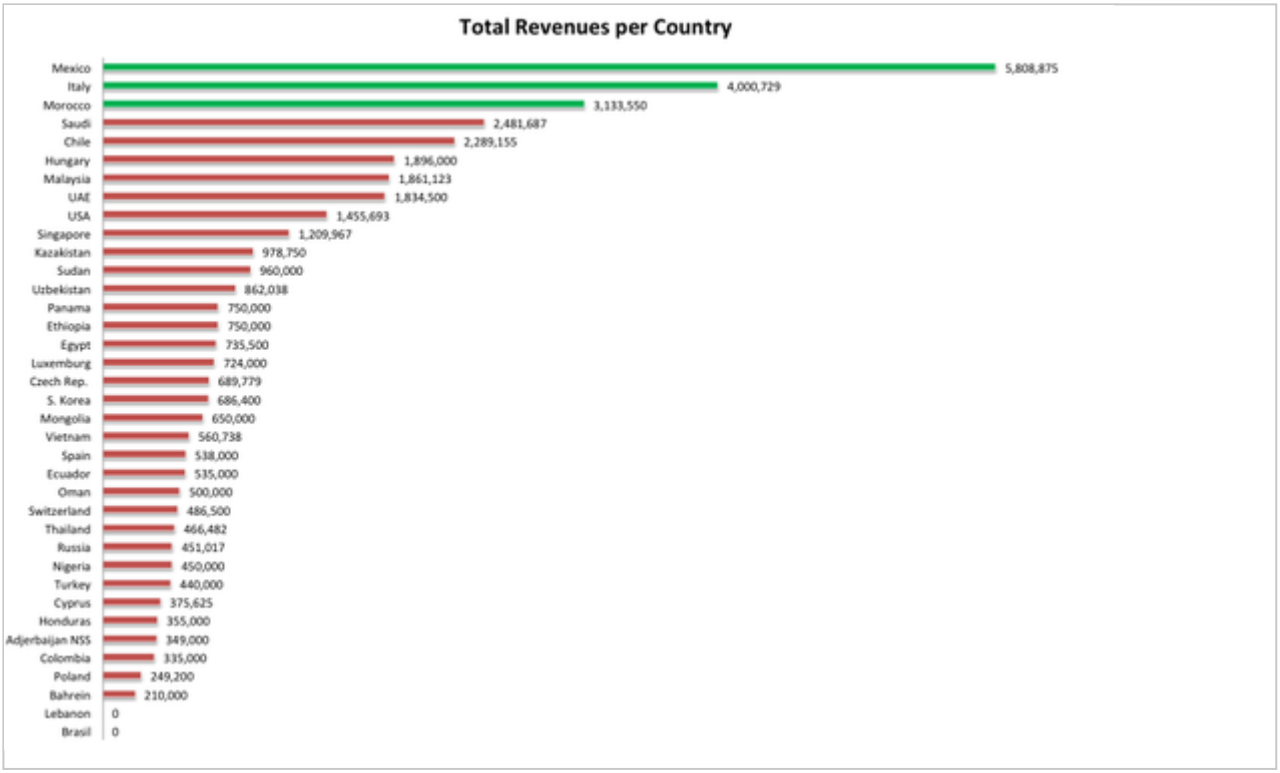
Sales through Israeli company

One of Hacking Team's key corporate partners is Nice Systems, an Israel-based company with close links to Israeli military and intelligence agencies. (CEO Barak Eilam, for instance, was formerly an officer with an "elite intelligence unit" in the Israeli Defense Forces, according to his biography. Eilam's LinkedIn profile links him to Unit 8200, Israel's signals intelligence corps.) The leaked Hacking Team documents show that Nice has been working on closing a large number of deals for the company across the world, winning contracts in Azerbaijan and Thailand and pushing for sales in Brazil, Colombia, Guatemala, Honduras, Israel, Kuwait, Finland, Georgia, Greece, India, Turkmenistan, Uzbekistan, Kirghistan and elsewhere.

Hacking Team had not responded to a request for comment on this story at time of publication. On Tuesday, a spokesperson for the company told the *International Business Times*: "We don't have anything to hide about what we are doing and we don't think that there is any evidence in this 400GB of data that we have violated any laws and I would even go so far as to argue that there is no evidence that we have behaved in anything but a completely ethical way."

Top clients

According to the hacked files, Hacking Team's top sales in recent years have come from governments and law enforcement agencies in these countries, in descending order of sales: Mexico, Italy, Morocco, Saudi Arabia, Chile, Hungary, Malaysia, UAE, the United States, 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.



Attempts to break U.K. market

Police agencies in the United Kingdom have trialed Hacking Team's technology, and have been attempting to purchase it for years, but have been hindered by apparent concerns about the legality of the technology.

In May 2011, through a U.K.-based corporate partner, Hacking Team arranged a secretive meeting with several interested British agencies. The company was told by the partner that attendees would possibly include London's Metropolitan Police, the government's Home Office, domestic intelligence agency MI5, customs officials, the Serious Organised Crime Agency and others.

After this meeting, in September 2013, the London police force told Hacking Team that it was "now ready to progress" with a trial of the spying tool. In December, the same year it then invited Hacking Team to formally submit a bid for a spy technology contract, a confidential document outlined that the force wanted to obtain "'Software' that can be covertly introduced to a third parties device and will allow us

to ‘Look, Listen and Follow’ the third party. The Authority will receive, record and playback the ‘Product’ retrieved from the third party on a ‘System’ that shall be scalable, using proven technology that has in-built security measures appropriate to this task.”

But the deal with the London cops, worth £385,000 ($591,000) to Hacking Team, was abruptly halted in in May 2014 following “internal reviews on how we wished to move this area of technology forward,” according to an email from the police, although the force left the door open for a future deal, adding: “Of course in the months/years to come this could change and if that is the case then we would welcome your organization’s participation.”

Since then, Hacking Team has continued to try to crack the U.K. market. It tried — and apparently failed — to set up a deal with Staffordshire Police after an officer contacted the company seeking technology to “access WiFi points to check users” and infect devices to covertly collect data.

Hacking Team discussed whether it could sell its technology disguised under a different name, “hiding” its full functionality.

And in January this year, it began negotiating a contract with the British National Crime Agency. The meeting was a success, with an officer for the agency telling Hacking Team that a demonstration of the covert surveillance technology “was extremely well received and proved to be a real eye opener for what can be achieved.”

In April, the same officer told Hacking Team he wanted a quote for basic spyware that would log keystrokes, noting that he could "then grow the system accordingly as we would then have the base platform." Hacking Team was interested in this proposal and discussed internally whether it could sell its technology disguised under a different name, "hiding" its full functionality. The deal appears to have since stalled, with the British agency telling Hacking Team in late May it was "unable to arrange" a meeting.

Plotting denials

Hacking Team's emails reveal its deceitful attempts to positively spin news reports that have exposed the company's technology being used against journalists and activists in repressive countries. In October 2012, for example, Bloomberg and Citizen Lab revealed the company's technology had apparently been used to target a pro-democracy activist in the United Arab Emirates, who was tracked down and beaten by suspected agents of the state. But instead of accepting responsibility and taking firm action against its customer, Hacking Team chose to issue a series of denials.

A technical analysis of the malware used against the activist showed it contained the acronym "RCS," a reference to Hacking Team's flagship spyware called Remote Control System. Hacking Team's public relations guru Eric Rabe scrambled to find a way to muddy the waters, suggesting to his colleagues that they could identify another software with RCS in its name and pin the blame on that. He proposed the company could announce that "The initials RCS are, of course, the initials of a Hacking Team product, Remote Control System, but are also commonly used in software code for the term (WHAT?) Frankly they could mean anything."

In other emails in the trove, Hacking Team employees appear to confirm that their spy tool did target the UAE activist. While

discussing a *Slate* piece I wrote on the incident in October 2012, Hacking Team developer Marco Valleri says that in the UAE case, malware was "downloaded" to infect the activist's device from "our old demo server." Moreover, as my colleague Lee Fang has reported, the hacked data shows Hacking Team's technology has been sold to the UAE since at least 2011. The pro-democracy activist was targeted by it in July 2012.

Enemies list

A presentation prepared by Hacking Team for a surveillance conference in South Africa later this month shows the company complaining about the "chilling effect" that it claims regulation of surveillance technology is having on the ability to fight crime.

The presentation singles out the organizations Hacking Team views as its main adversaries, noting that it is a "target" of groups such as Human Rights Watch and Privacy International and warning that "democracy advocates" are putting pressure on governments.

Separately, the company's emails show CEO David Vincenzetti's reaction to criticism from activist groups, who he says are "idiots" good at "manipulating things and demonizing companies and people."

In one email sent last month, Vincenzetti seems to have unwittingly foreseen the future, jokingly warning staff about the ramifications of the company's sensitive information leaking online.

"Imagine this: a leak on WikiLeaks showing YOU explaining the evilest technology on earth! :-)" he wrote. "You will be demonized by our dearest friends the activists, and normal people will point their fingers at you."

Photo: Munir Uz Zaman/AFP/Getty Images