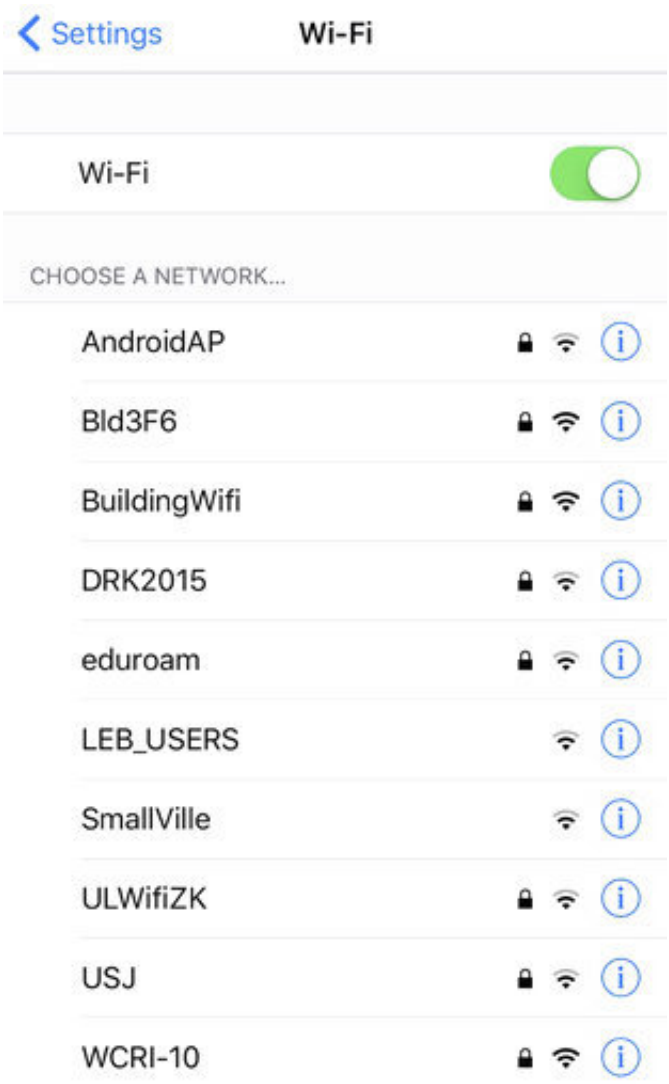
Report links hacking campaign to Lebanese security agency

January 18 2018, by Raphael Satter



A smartphone screenshot taken Wednesday, Jan. 18, 2017 shows the WiFi networks active at the corner of Pierre Gemayel and Damascus Streets in Beirut. A report being published Thursday identifies the second WiFi network from the

top as being associated with Lebanon's General Directorate of General Security, which is at the same address. (AP Photo)

A major hacking operation tied to one of the most powerful security and intelligence agencies in Lebanon has been exposed after careless spies left hundreds of gigabytes of intercepted data exposed to the open internet, according to a report published Thursday.

Mobile security firm Lookout, Inc. and the Electronic Frontier Foundation, a digital rights group, said the haul, which includes nearly half a million intercepted text messages, had simply been left online by hackers linked to Lebanon's General Directorate of General Security.

"It's almost like thieves robbed the bank and forgot to lock the door where they stashed the money," said Mike Murray, Lookout's head of intelligence. Lookout security researcher Michael Flossman said the trove ran the gamut, from Syrian battlefield photos to private phone conversations, passwords and pictures of children's birthday parties.

"It was everything. Literally everything," Flossman said.

Discoveries of state-sponsored cyberespionage campaigns have become commonplace as countries in the Middle East and Asia scramble to match the digital prowess of the United States, China, Russia and other major powers. But Lookout and EFF's report is unusual for the amount of data uncovered about the spying campaign's victims and its operators.

Notably, their report drew on data generated by suspected test devices—a set of similarly configured phones that appear to have been used to try out the spy software—to potentially pinpoint the hackers' exact address.

The report said the suspected test devices all seemed to have connected to a WiFi network active at the intersection of Beirut's Pierre Gemayel and Damascus Streets, the location of the bulky, sandstone-colored high-rise that houses Lebanon's General Directorate of General Security. The Associated Press was able to at least partially verify that finding, sending a reporter to the area around the heavily guarded, antennae-crowned building Wednesday to confirm that the same WiFi network was still broadcasting there. Other data also points to the intelligence agency: the report said the internet protocol addresses of the spyware's control panels mapped to an area just south of the GDGS building.

Electronic Frontier Foundation Director of Cybersecurity Eva Galperin said the find was remarkable, explaining that she could think of only one other example where researchers were able to pin state-backed hackers to a specific building.

"We were able to take advantage of extraordinarily poor operational security," she said.

The GDGS did not immediately comment on the report.

The 49-page document lays out how spies used a network of bogus websites and malicious smartphone apps—such as WhatsApp, Telegram, Threema and Signal—to steal passwords or pry into communications, eavesdropping on conversations and capturing at least 486,000 text messages. Some victims were tricked into visiting the websites or downloading the rogue apps by booby trapped messages sent over WhatsApp, the report said. Others may have had malicious programs installed physically when they were away from their phones. Still more may have been lured into compromising their devices by a set of apparently fake Facebook profiles set up to look like attractive young Lebanese women.

EFF and Lookout said the spying stretched over 21 different countries, including the United States and several European nations, but they declined to identify any of the victims except in general terms, saying that there were thousands of them and that in many cases it wasn't always obvious who they were.

Murray said relevant authorities had been notified of the spying but declined to go into further detail.

Lebanon has historically been a hub for espionage and Lebanese spies have a documented interest in surveillance software. In 2015, for example, the internet watchdog group Citizen Lab published evidence that GDGS had tapped FinFisher, a spyware merchant whose tools have been used to hack into the computers of several African and Middle Eastern dissidents.

The hacking campaign exposed Thursday by EFF and Lookout—which they dub "Dark Caracal"—was discovered in the wake of an entirely different cyberespionage campaign targeting Kazakh journalists and lawyers.

An EFF report on the Kazakh campaign published in 2016 caught the attention of researchers at Lookout, who swept through the company's vast store of smartphone data to find a sample of the smartphone surveillance software mentioned in the write-up. It was while pulling on that string that investigators stumbled across the open server full of photos, conversations and intercepted text messages—as well as the link to Lebanon.

Galperin and Murray both said researchers were marshalling more evidence and that more revelations were coming.

"Stay tuned," Murray said.

More information: EFF and Lookout's report: www.lookout.com/info/ds-dark-caracal-ty