Leading Egyptian opposition politician targeted with spyware, researchers find

September 24 2023, by Frank Bajak

Credit: CC0 Public Domain

A leading Egyptian opposition politician was targeted with spyware multiple times after announcing a presidential bid—including with malware that automatically infects smartphones, security researchers

have found. They say Egyptian authorities were likely behind the attempted hacks.

Discovery of the malware last week by researchers at Citizen Lab and Google's Threat Analysis Group prompted Apple to rush out operating system updates for iPhones, iPads, Mac computers and Apple Watches to patch the associated vulnerabilities.

Citizen Lab said in a blog post that attempts beginning in August to hack former Egpytian lawmaker Ahmed Altantawy involved configuring his phone's connection to the Vodaphone Egypt mobile network to automatically infect it with Predator spyware if he visited certain websites not using the secure HTTPS protocol.

Citizen Lab said the effort likely failed because Altantawy had his phone in "lockdown mode," which Apple recommends for iPhone users at high risk, including rights activists, journalists and political dissidents in countries like Egypt.

Prior to that, Citizen Lab said, attempts were made beginning in May to hack Altantawy's phone with Predator via links in SMS and WhatsApp messages that he would have had to click on to become infected.

Once infected, the Predator spyware turns a smartphone into a remote eavesdropping device and lets the attacker siphon off data.

Given that Egypt is a known customer of Predator's maker, Cytrox, and the spyware was delivered via network injection from Egyptian soil, Citizen Lab said it had "high confidence" Egypt's government was behind the attack.

Bill Marczak of the University of Toronto-based internet watchdog obtained the exploit chain with Google researcher Maddie Stone.

"It's scary the fact that the government can essentially select anyone on Vodafone Egypt's network and perhaps other networks for infections and they just flip a switch" and select them for targeting, he said. Marczak said "the most likely scenario here is that, yes, there is this cooperation from from Vodafone."

In a separate incident in 2021, Citizen Lab determined that Altantawy—who announced his candidacy in March—was successfully hacked with Predator.

Egyptian officials did not respond Saturday to requests for comment.

Altantawy, a former journalist and lawmaker, announced in March his bid to challenge incumbent President Abdel Fatah el-Sissi in 2024, who has overseen a sharp crackdown on political opposition. Rights groups accuse el-Sissi's administration of targeting dissent with brutal tactics—forced disappearances, torture and long-term detentions without trial.

Altantawy, family members and supporters have complained of being harrassed, which led him to ask Citizen Lab researchers to analyze his phone for potential spyware infection.

Altantawy said Saturday in written responses to questions relayed by a trusted intermediary who requested anonymity for personal security that he contacted Citizen Lab after receiving a serious of suspicious and anonymous messages embedded with links he suspected were malicious.

He said he believed the hacking attempts were "inextricably linked to my political candidacy and my opposition role" and sought "not only to surveil, but perhaps also to find compromising material that could be used to discredit or defame me."

Altantawy also said the incident raises questions about whether telecommunications companies operating in Egypt might be complicit.

Previously, Citizen Lab documented Predator infections affecting two exiled Egyptians, and in a joint probe with Facebook determined that Cytrox had customers in countries including Armenia, Greece, Indonesia, Madagascar, Oman, Saudi Arabia and Serbia.

In July, the U.S. added Predator's maker, Cytrox, to its blacklist for developing surveillance tools deemed to have threatened U.S. national security as well as individuals and organizations worldwide. That makes it illegal for U.S. companies to do business with them. Israel NSO Group, maker of the Pegasus spyware, was similarly sanctions in November 2021. The reported use of Predator in Greece helped precipitate the resignation last year of two top government officials, including the national intelligence director.

The latest discovery brings to five the number of zero-day vulnerabilities to Apple software for which patches have been released this month.