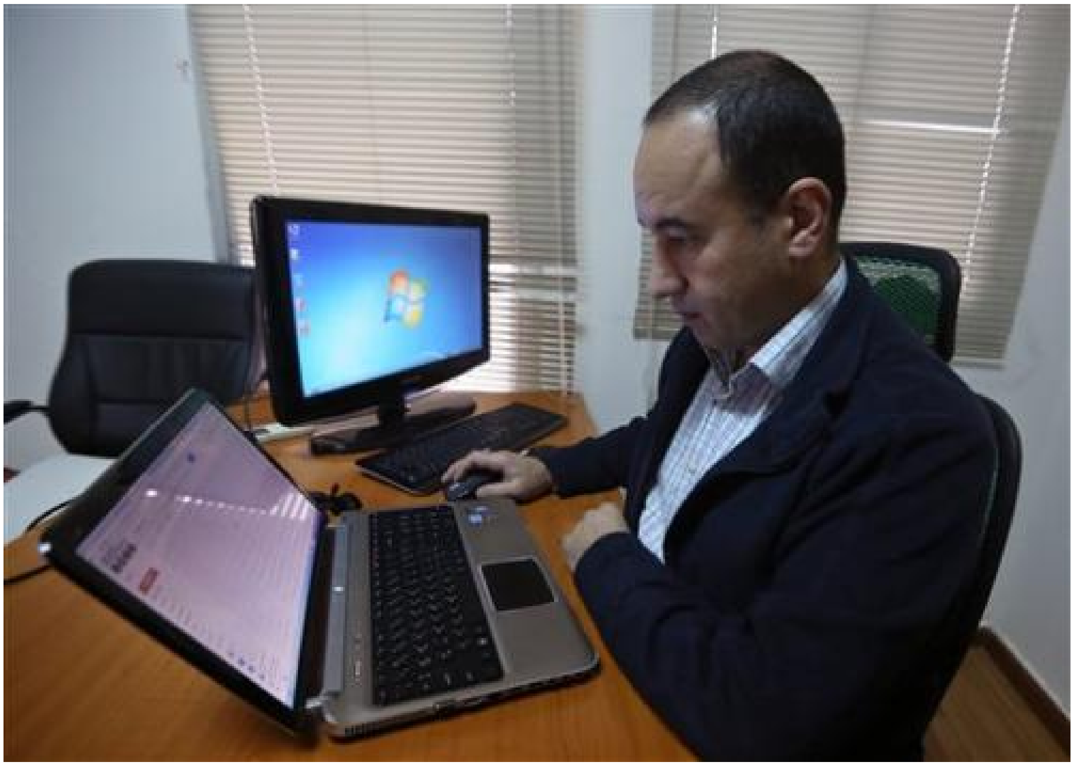
Botched cyberattack on Syria group blamed on IS

December 18 2014, byRaphael Satter



In this photo dated Wednesday, Dec. 17, 2014, Lebanese Bahaa Nasr of Cyber Arabs checks his email from his office in Beirut, Lebanon. Cyber Arabs is an online safety project run by the London-based Institute for War and Peace Reporting and Nasr is among those who recently helped uncover a botched cyberattack suspected of having been carried out by the Islamic State group. (AP Photo/Bilal Hussein)

A botched cyberattack aimed at unmasking Syrian dissidents has experts worried that the Islamic State group is adding malicious software to its arsenal.

Internet watchdog Citizen Lab says an attempt to hack into systems operated by dissidents within the self-styled caliphate could be the work of hackers affiliated with the Islamic State group.

Citizen Lab analyst John Scott-Railton said there is circumstantial evidence of the group's involvement, and cautioned that if the group has moved into cyberespionage, "the targets might not stop with the borders of Syria."

The Nov. 24 attack came in the form of a booby-trapped email sent to an activist collective in Raqqa, Syria, that documents human rights abuses in the Islamic State group's de-facto capital. The activist at the receiving end of the email wasn't fooled and forwarded the message to Bahaa Nasr of Cyber Arabs, a project which provides online security training.

"We are wanted—even just as corpses," the activist, whose name is being withheld to protect his safety, told Nasr. "This email has a virus; we want to know the source."

The message eventually found its way to Citizen Lab, based at the University of Toronto's Munk School of Global Affairs. There, Scott-Railton and malware researcher Seth Hardy determined that it could act as a kind of electronic homing beacon by revealing a victim's Internet Protocol address.

Citizen Lab regularly dissects rogue programs from the region, but Scott-Railton said this sample was different from previous attacks blamed on the Syrian government.

In this photo dated Wednesday, Dec. 17, 2014, Lebanese Bahaa Nasr of Cyber Arabs checks his email from his office in Beirut, Lebanon. Cyber Arabs is an online safety project run by the London-based Institute for War and Peace Reporting and Nasr is among those who recently helped uncover a botched cyberattack suspected of having been carried out by the Islamic State group. (AP Photo/Bilal Hussein)

"We think we are looking at a different actor," he said—an opinion echoed by malware scientist Thoufique Haq at California-based FireEye, who wasn't involved in the report.

The activists are convinced the "different actor" is the Islamic State group, whose supporters have publicly vowed to hunt the collective down.

Islamic State has previously expressed interest in electronic surveillance.

Last week, a post to a pro-Islamic State forum carried a proposal for a project named "Eye of the Caliphate" that would task a team of computer experts with hacking into the caliphate's enemies, according to the SITE Intelligence Group. British news media reported this year that Islamic State had recruited a British hacker.

Attempts to reach an Islamic State representative were unsuccessful. U.K. authorities have declined comment.

Scott-Railton said various bugs in the malware's code suggest an author "with basic skills, but perhaps without a lot of 'professionalism' ... or quality control."

Security consultant and former Scotland Yard detective Adrian Culley said that's no reason to write the hackers off.

"They will evolve and they will learn," he said.

More information: Citizen Lab's report: citizenlab.org/?p=24386

Cyber Arabs: www.cyber-arabs.com/

Citation: Botched cyberattack on Syria group blamed on IS (2014, December 18) retrieved 25 April 2024 from https://phys.org/news/2014-12-botched-cyberattack-syria-group.html