US officials: Kaspersky “Slingshot” report burned anti-terror operation

Joint Special Operations Command ran campaign against ISIS, Al Qaeda for at least 6 years.

Enlarge / US Navy SEALs conducting special reconnaissance of Al Qaeda operations in Afghanistan in 2002. JSOC added malware to Special Operations units' bag of tricks, and it may have been exposed by Kaspersky.

163

A malware campaign discovered by researchers for Kaspersky Lab this month was in fact a US military

operation, according to a report by CyberScoop's Chris Bing and Patrick Howell O'Neill. Unnamed US intelligence officials told CyberScoop that Kaspersky's report had exposed a long-running Joint Special Operations Command (JSOC) operation targeting the Islamic State and Al Qaeda.

RTHER READING
ent malware that hid for six years
ead through routers

The malware used in the campaign, according to the officials, was used to target computers in Internet cafés where it was believed individuals associated with the Islamic State and Al Qaeda would communicate with their organizations' leadership. Kaspersky's report showed Slingshot had targeted computers in

countries where ISIS, Al Qaeda, and other radical Islamic terrorist groups have a presence or recruit: Afghanistan, Yemen, Iraq, Jordan, Turkey, Libya, Sudan, Somalia, Kenya, Tanzania, and the Democratic Republic of Congo.

The publication of the report, the officials contended, likely caused JSOC to abandon the operation and may have put the lives of soldiers fighting ISIS and Al Qaeda in danger. One former intelligence official told CyberScoop that it was standard operating procedure "to kill it all with fire once you get caught... It happens sometimes and we're accustomed to dealing with it. But it still sucks. I can tell you this didn't help anyone."

JSOC is part of the US Special Operations

Command (SOCOM) and has in the past incorporated electronic warfare and signals intelligence units in its operations as part of its "special reconnaissance" mission. US Navy SEALs, Army Special Forces and Rangers, and other special operations units have worked in tandem in the past; a JSOC unit called the Computer Network Operations Squadron (CNOS) was formed in 2007, prior to the formation of US Cyber Command. CNOS operated from Fort Meade (where US Cyber Command and the National Security Agency are headquartered) and at CIA's headquarters in Langley, Virginia.

In his 2015 book *Relentless Strike: The Secret History of Joint Special Operations*

Command, *Army Times* journalist Sean Naylor described one example of how special operations teams used malware in Iraq, using "Mohawks"—Iraqis recruited by US Special Forces to serve as a counter-intelligence team—to install spyware onto targeted computers:

> Mohawks would enter the Internet café without arousing suspicion and upload software onto the computers. Sometimes the software was of the keystroke recognition type, at other times it would covertly activate a webcam if the computer had one, allowing

> the task force to positively identify a target... The insurgents often thought they were exercising good communications security by sharing one account with a single password and writing messages to each other that they saved as drafts rather than sending... But the keystroke tracking software meant JSOC personnel in the United States were reading every word.

Kaspersky's exposure of the program will likely not win the company any points in its

battle to get off a US federal government blacklist.

SEAN GALLAGHER

Sean is Ars Technica's IT and National Security Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

EMAIL sean.gallagher@arstechnica.com // **TWITTER** @thepacketrat