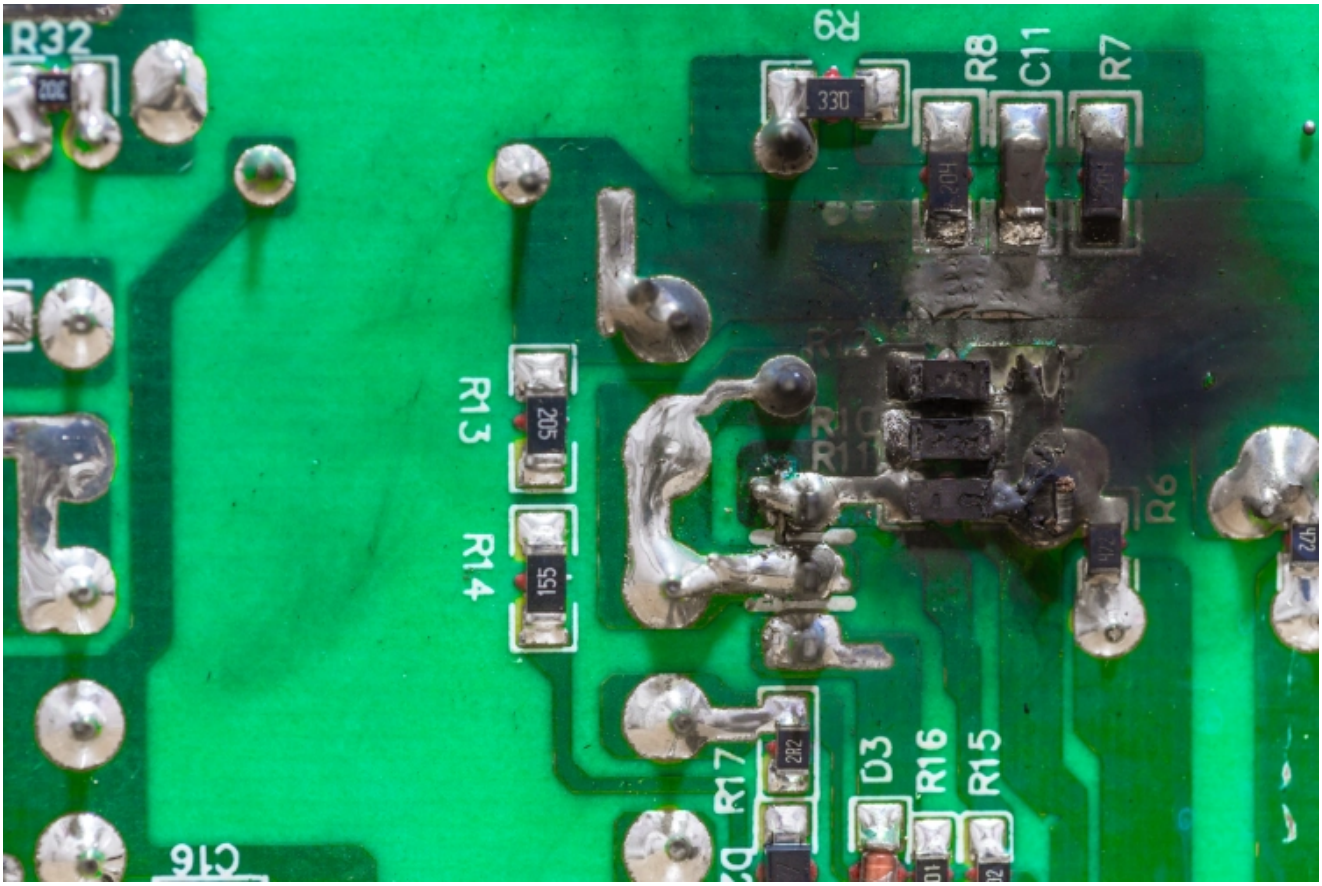
Related news

cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/

March 20, 2018



government

Kaspersky's 'Slingshot' report burned an ISIS-focused intelligence operation

(Getty)
Written by Chris Bing and Patrick Howell O'Neill
Mar 20, 2018 | CYBERSCOOP
The U.S. government and Russian cybersecurity giant Kaspersky Lab are currently in the throes of a nasty legal fight that comes on top of a long-running feud over how the company has conducted itself with regard to U.S. intelligence-gathering operations.

A recent Kaspersky discovery may keep the feud alive for years to come.

CyberScoop has learned that Kaspersky research recently exposed an active, U.S.-led counterterrorism cyber-espionage operation. According to current and former U.S. intelligence officials, the operation was used to target ISIS and al-Qaeda members.

On March 9, Kaspersky publicly announced a malware campaign dubbed "Slingshot." According to the company's researchers, the campaign compromised thousands of devices through breached routers in various African and Middle Eastern countries, including Afghanistan, Iraq, Kenya, Sudan, Somalia, Turkey and Yemen.

Kaspersky did not attribute Slingshot to any single country or government in its public report, describing it only as an advanced persistent threat (APT). But current and former U.S. intelligence officials tell CyberScoop that Slingshot represents a U.S. military program run out of Joint Special Operations Command (JSOC), a component of Special Operations Command (SOCOM).

The complex campaign, which researchers say was active for at least six years, allowed for the spread of highly intrusive malware that could siphon large amounts of data from infected devices.

Slingshot helped the military and intelligence community collect information about terrorists by infecting computers they commonly used, sources told CyberScoop. Often times, these targeted computers would be located within internet cafés in developing countries. ISIS and al-Qaeda targets would use internet cafés to send and receive messages, the sources said.

These officials, all of whom spoke on condition of anonymity to discuss a classified program, fear the exposure may cause the U.S. to lose access to a valuable, long-running surveillance program and put soldiers' lives at risk.

The disclosure comes at a difficult time for Kaspersky. The company is currently fighting the U.S. government in court after the government claimed that the Moscow-based company's software poses a national security risk due to the company's Russian government ties. Kaspersky has consistently denied any wrongdoing.

CyberScoop's reporting of JSOC's role in Slingshot provides the first known case of a SOCOM-led cyber-espionage operation. The command is better known for leading physical missions that place elite soldiers on the ground in hostile territories. Over the last decade, SOCOM has been instrumental in the Global War on Terror, having conducted many sensitive missions, including the one that killed former al-Qaeda leader Osama bin Laden.

Slingshot, CyberScoop has learned, is a complement to JSOC's physical missions.

A former intelligence official told CyberScoop that Kaspersky's findings had likely already caused the U.S. to abandon and "burn" some of the digital infrastructure that JSOC was using to manage the surveillance program.

"SOP [standard operating procedure] is to kill it all with fire once you get caught," said the former intelligence official. "It happens sometimes and we're accustomed to dealing with it. But it still sucks … I can tell you this didn't help anyone."

SOCOM has hackers?

While not an intelligence agency by nature, SOCOM has dabbled in cyber-operations — known inside the unit as "special reconnaissance" — for some time, according to multiple academics who have examined the use of offensive cyber tools within special operations units. Most of these operations would usually combine elements of human (HUMINT) and signals intelligence (SIGINT) in order to catch terrorists.

As the Global War on Terror grew, most combatant commands took visible steps and received considerable funding to build out their own espionage capabilities. One of the military organizations which benefited most from this explosive growth in resources was SOCOM, a unit that many describe as the "tip of the spear" when it comes to military operations.

"Many units within SOCOM possess independent cyber capabilities," a senior U.S. intelligence official told CyberScoop.

Throughout the past decade, SOCOM has used cyber operations in a very ad hoc manner. If cyberwarfare was used in an operation, SOCOM has either been given support from U.S. Cyber Command or reliant on smaller squadrons within various units.

For instance, a group of hackers organized under the name "Computer Network Operations Squadron" (CNOS), were known to operate within JSOC command circa 2007. Though headquartered in Northern Virginia, CNOS helped coordinate missions where on-the-ground agents in the Middle East — and sometimes undercover operatives — would infiltrate internet cafés and local telecommunications firms. The squadron was first written about in "Relentless Strike: The Secret History of Joint Special Operations Command," a book by journalist Sean Naylor.

Naylor wrote that CNOS staff could be stationed around the world, including at Fort Meade in Maryland and CIA's Langley, Virginia, headquarters. CNOS had close connections to CIA, blurring the already fuzzy line between U.S. intel and military organizations.

In one case mentioned by Naylor's book, CNOS infected a terrorist's computer with "keystroke recognition [software], at other times it would covertly activate a webcam if the computer had one, allowing the task force to positively identify a target."

The Slingshot program found by Kaspersky had similar capabilities.

SOCOM's exclusive structure provides an easy way to leverage long-standing intelligence programs, since it is permitted to quickly organize and deploy forces globally wherever defined rules of engagement exist. Teams like CNOS, as described by Naylor, are usually able to work closely with intelligence agencies in foreign, undefined war-zones after receiving approval from the appropriate regional combatant commands and Pentagon.

JSOC and CIA have a history of working together and when combined, meet a similar profile to how Slingshot would be utilized.

“The military kept CNOS in JSOC ‘because we want it to operate in areas that are not necessarily … where we’re currently at war’ … we want it to operate around the globe [pursuing] national objectives,” a passage in Naylor’s book, citing an unnamed military intelligence officer, reads. “[CNOS] was how the pesky networks were broken in Iraq.”

Slingshot’s ties to spies

One Kaspersky researcher involved with the Slingshot report said the malware campaign illustrated one of the most skilled and sophisticated hacking operations ever to be publicly documented. Its creators took numerous steps to hide their identity and purpose, making Slingshot extremely difficult to study, explained Kurt Baumgartner, a principal security researcher with Kaspersky.

Baumgartner, a U.S. citizen, did not author the Slingshot report. Instead, a team of four researchers based overseas, largely in Russia, are credited with writing it.

“It is one of the most technically sophisticated groups we’ve ever seen,” said Baumgartner. “Most of the code is entirely unique, meaning that no one has ever seen it before … the only overlap we’ve seen, and I think there are people already discussing it, is there’s some limited similarities maybe to Equation Grayfish and White Lambert.”

“Grayfish” is a software implant associated with the “Equation Group,” an entity that is widely attributed to the National Security Agency. The “Lamberts,” another group identified and first catalogued by Kaspersky, has been separately linked to the CIA.

Hacking tools tied to past Equation Group and Lambert-inspired operations were written in English, just like Slingshot. Akin to Grayfish and Lamberts, Slingshot used a distinct software driver abuse technique to install malicious code onto targeted systems. They are the only three documented APTs to use this exact same driver abuse method.

Broadly speaking, Kaspersky’s ability to identify even the most advanced malware variants is well-documented; especially within the highly competitive cybersecurity community. Most of these cases are handled by Kaspersky’s heralded Global Research & Analysis Team (GReAT) team. The Russian company is known for employing some of the best reverse malware engineers and analysts in the entire industry.

It also has a vast business presence in the Middle East. Slingshot was discovered through the company’s work in that region.

A source close to Kaspersky Lab told CyberScoop that while some researchers may have thought Slingshot was the work of a “Five Eyes” nation — a term used to describe an intelligence alliance between Australia, Canada, New Zealand, the United Kingdom and the

U.S. — they couldn't have known for sure. This source told CyberScoop that the Kaspersky researchers lacked context because there's "only so much that can be gleaned from technical evidence."

Questions sent to the Russian company regarding if they knew about Slingshot's U.S. military origin went unanswered.

Even so, a cursory review provides some tips that Slingshot be linked to U.S. spies.

The malware is comprised of individual modules, each carrying a different title, like "Gollum," "Cahnadr" or "NeedleWatch," according to Kaspersky. A leaked NSA memo released in 2015 describes Gollum as a "partner implant" used by another agency aside from NSA. The memo, circulated between Five Eyes nations, talks about the need to create an accessible data pipeline that pulls information from infected computers where an active implant is hidden.

In addition to "Gollum," the way Slingshot exploits routers made by Latvian company Mikrotik could perhaps be traced back to another spy agency: the CIA. Classified documents published by WikiLeaks as part of the so-called "Vault 7" dump show that the CIA has been interested in compromising Mikrotik equipment since at least 2015. Mikrotik products are popular in the Middle East and Southeast Asia.

Spokespeople for the Office of the Director of National Intelligence, NSA and Special Operations Command (SOCOM) all declined to comment.

Adding fuel to the fire

CyberScoop spoke with several U.S. cybersecurity researchers who said they weren't surprised or angered by the fact that Kaspersky had potentially publicized a U.S. cyber-espionage operation.

These experts, who asked for anonymity because they feared blowback for speaking publicly, said that it's only natural for Kaspersky to attempt to stop cyberattacks aimed at its clients. Others who spoke to CyberScoop, however, including current U.S. officials, said they were angry because publicly disclosing Slingshot may put lives in danger.

Complicating the matter is the lawsuit Kaspersky has filed against the U.S. government. The 2018 National Defense Authorization Act banned the use of Kaspersky products across the federal government. Kaspersky charges that ban is unconstitutional.

The ban comes after numerous reports that the company's anti-virus engine was leveraged by Russian spies to remotely pilfer secret U.S. documents on systems where the software was installed. In response, Kaspersky launched a transparency effort in October 2017, which it says proves its products are not malicious.

At the moment, it's not clear if the Russian company expected that its focus on Slingshot would eventually expose a sensitive U.S. counterterrorism initiative.

A senior U.S. intelligence official claimed that it would be hard to believe that Kaspersky was totally unaware of what it was handling.

"It's clear by the way they wrote about this that they knew what it was being used for," said the senior official. "GReAT is extremely adept at understanding the information needs of different actors out there on the internet. They take into considering the geopolitical circumstances, they've shown that time and time again. It would be a stretch for me to believe they didn't know what they're dealing with here."

Greg Otto contributed to this report.