South America hacker team targets dissidents, journalists

December 9 2015, byFrank Bajak

Ecuadorian journalist Janet Hinostroza poses for a photo at the Teleamazonas tv station in Quito, Ecuador, Monday, Dec. 7, 2015. Hinostroza, who won a 2013 press freedom award from the New York-based Committee to Protect Journalists, said she was hacked in January and then again in August, a month after the interior minister claimed she was involved in a plot to overthrow the government. (AP Photo/Dolores Ochoa)

A shadowy cyber-espionage group that sent malware to the prosecutor

whose mysterious death transfixed Argentina early this year has been hitting targets in left-leaning nations across South America, the Internet watchdog group Citizen Lab reported Wednesday.

The breadth and brazenness of the hackers' activity bear the hallmarks of state sponsorship, the researchers found. So do its targets.

The group has been attacking opposition figures and independent journalists in Ecuador with spyware. It also ran dummy websites. The most elaborate, geared toward Venezuela, was a constantly updated news site featuring dubiously sourced "scoops" on purported corruption among that country's ruling socialists. In Ecuador, a similarly bogus site seemed tailored to attract disgruntled police officers.

The researchers launched the three-month probe after determining that spyware found on the smartphone of Argentine prosecutor Alberto Nisman was written to send pilfered data to the same command-and-control structure as malware sent to targets infected in Ecuador. They said the hackers had a "keen and systematic interest in the political opposition and the independent press" in the three nations, all of which have been run by allied left-wing governments. That suggests it may have operated on behalf of one or more of those governments, the report said.

In September, the hackers threatened a Citizen Lab researcher as he poked around in a U.S.-based machine the group had infected.

"We're going to analyze your brain with a bullet—and your family's, too," read a message that popped up on his computer screen. "You like playing the spy and going where you shouldn't, well you should know that it has a cost—your life!"

That's rare behavior among professional hackers, perhaps indicating little fear of criminal prosecution, said Morgan Marquis-Boire, one of

the researchers.

In November, the group attempted to infect the computer of an Associated Press reporter with a phishing attack aimed at stealing his Google password.

The researchers identified the group through intertwined Internet domains and tell-tale digital signatures on emails sent to infect computers. They said it had been active for seven years, finding it to have used hosting services in Brazil since at least 2008.

Determining who is behind the hacking, however, may be possible only with court orders due to Internet hosting companies' privacy policies.

In two examples, targets received an email from a phony organization purporting to oppose President Rafael Correa of Ecuador. Others received a message falsely signed by an opposition leader claiming to reveal names of people investigated by Ecuador's espionage agency.

Those who clicked on embedded links had their computers infected with spyware that secretly culled information from users' machines and sent it to servers run by the group, which researchers dubbed "Packrat."

"We believe this is a highly targeted operation," said John Scott-Railton, lead researcher on The Citizen Lab team at the University of Toronto's Munk School for Global Affairs. "Packrat seems to carefully choose and then relentlessly go after its targets."

The group has used the same Internet domains for years despite some exposure, a technical convenience that would be shunned by garden-variety cybercriminals wary of being identified by law enforcement agencies.

The researchers found at least 35 different types of booby-trapped files, and operated from domains hosted by companies based in Argentina, Brazil, France, Spain, Sweden, Uruguay and the United States.

For much of the past two years, about two dozen "seeding" sites resided at one time or other on servers owned by U.S.-based GoDaddy.com LLC, a web hosting company. The domain names that GoDaddy hosted included soporte-yahoo.com, update-outlook.com, mgoogle.us and login-office365.com.

The researchers notified most of the providers Friday, asking that Packrat's known infrastructure be shuttered.

GoDaddy spokesman Nick Fuller said the company takes immediate action when it identifies a problem website but did not elaborate.

Citizen Lab labeled the operation Packrat because the hackers use commercially available packages of remote access trojans—or RATs—that infect computers and smartphones, allowing hackers to capture keystrokes, emails and text messages. The software could even hijack microphones and webcams.

The malware was skillfully packaged to avoid detection by anti-virus programs, the researchers found.

The investigation was begun after it was determined that Packrat had targeted Nisman, the Argentine special prosecutor found dead of a gunshot wound last January while trying—unsuccessfully—to bring criminal charges against Argentina's president.

Researchers said Packrat sent a top Argentine journalist, Jorge Lanata, the identical virus that Nisman received a month before his death.

The virus' digital fingerprints showed it was built to communicate with the same Internet domains being used to spy on Ecuadorean opposition figures, who identified Packrat malware in their email with search scripts written by the researchers.

Most of the targets identified were in Ecuador, though researcher Scott-Railton cautioned that they likely represent a sliver of the group's activity.

"I doubt their Brazil-centric operations have stopped," he said. "We don't want Ecuador to overshadow the fact that we are looking at a campaign all over the place."

In Ecuador, Packrat targeted reporters, environmental activists and even the satirist known as Crudo Ecuador, whose lampoons infuriated the president. It also set up a website designed to mirror the email web interface of Ecuador's National Assembly in an apparent attempt to harvest lawmakers' usernames and passwords and break into their accounts, the investigation found.

Journalist Janet Hinostroza, who won a 2013 press freedom award from the New York-based Committee to Protect Journalists, said she was hacked in January and then again in August, a month after the interior minister claimed she was involved in a plot to overthrow the government.

"My computer has been contaminated for so long that I imagine they've got access to all my information," said Hinostroza.

She still can't access contacts and other data on her Apple iCloud because hackers changed her password and security questions.

Other prominent alleged Packrat targets in Ecuador include Martha

Roldos, an environmental activist, and Cesar Ricuarte, director of the press freedom watchdog Fundamedios. Roldos got a total of 34 malicious emails from Packrat, Citizen Lab found.

One website created by Packrat, called "justicia-desvinculados.com," tried to attract Ecuadorean police officers fired after a September 2010 revolt over benefits that badly shook Correa. Now removed, it included an affiliated Twitter account.

The group's most elaborate spurious website appears to be Pancaliente.info, the Venezuelan compendium of opposition-friendly news including plagiarized articles and inaccurate "scoops."

Taken offline Tuesday, the site displayed no contact information about itself.

But it did ask readers to enter their email addresses.

More information: Citizen Lab report: citizenlab.org/2015/12/packrat-report/