Venezuelan military under cyber spies attack

Caracas, August 7 (RHC)-- A cyber-espionage group dubbed as Machete has been stealing files from the Venezuelan army, according to a report published Monday by IT security company, ESET.

ESET said it observed no less than 50 hacked computers between March and May within Venezuela, Nicaragua, Ecuador and Colombia, but 75 percent of the computers infected by Machete servers were based in Venezuela.

The group has been active for nine years now and has pursued many different targets worldwide. However, the ESET report said that from the start of this year, those who control Machete have centered their attention and efforts on Venezuela.

Around three-quarters of the infections were located in Venezuela, and more than half of the victimized computers pertained to the Venezuelan military. The central interest of the hackers was Venezuelan military grids, positioning, and navigation routes.

"The attackers exfiltrate specialized file types used by geographic information systems (GIS) software," said ESET security researcher Matias Porolli. "The group is specifically interested in files that describe navigation routes and positioning using military grids." The researchers reported that the hackers have been very successful, stealing gigabytes of confidential documents every week, while their campaign is

still active to this day.

In addition to Venezuela, the attackers also targeted other Latin American countries including Ecuador, Colombia, and Nicaragua, yet the vast majority of the attacks have taken place in Venezuela.

The group’s maneuvering is the one used by all cyber-espionage groups. It consists of sending phishing e-mails containing malicious attachments or links based on previous, genuine e-mails likely seen by those being hacked. A 'spy' infects the hard-drive and and runs indefinitely, copying and encrypting documents, takes screenshots and records passwords, says ESET.

It hasn't been revealed who is behind the Machete group. In 2014, cybersecurity and anti-virus provider Kaspersky said the group members seem to be Spanish-speaking individuals.

"Attribution is based on what we can actually observe," the ESET team told ZDNet. "Several hints and artifacts we saw during the course of our investigation lead us to support the claim that this is a Spanish-speaking group, as was said by other researchers in the past."

"Unfortunately, we cannot know if they are a state-sponsored group or if they are an independent group selling information to the highest bidder," ESET said.

---

https://www.radiohc.cu/en/noticias/internacionales/198327-venezuelan-military-under-cyber-spies-attack

Radio Habana Cuba