Mysterious hacking group Careto was run by the Spanish government, sources say

techcrunch.com/2025/05/23/mysterious-hacking-group-careto-was-run-by-the-spanish-government-sources-say/

May 23, 2025

More than a decade ago, researchers at antivirus company Kaspersky identified suspicious internet traffic of what they thought was a known government-backed group, based on similar targeting and its phishing techniques. Soon, the researchers realized they had found a much more advanced hacking operation that was targeting the Cuban government, among others.

Eventually the researchers were able to attribute the network activity to a mysterious — and at the time completely unknown — Spanish-speaking hacking group that they called Careto, after the Spanish slang word (“ugly face” or “mask” in English), which they found buried within the malware’s code.

Careto was never publicly linked to a specific government. But TechCrunch has now learned that the researchers who first discovered the group were convinced that Spanish government hackers were behind Careto’s espionage operations.

When Kaspersky first revealed the existence of Careto in 2014, its researchers called the group “one of the most advanced threats at the moment,” with its stealthy malware capable of stealing highly sensitive data, including private conversations and keystrokes from the

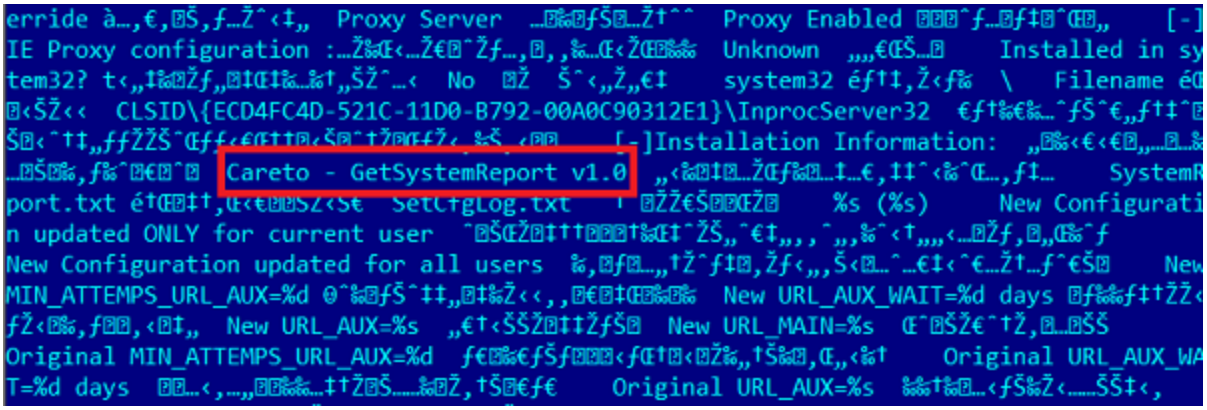
computers it compromised, much akin to powerful government spyware today. Careto's malware was used to hack into government institutions and private companies around the world.

Kaspersky avoided publicly blaming who it thought was behind Careto. But internally, according to several people who worked at Kaspersky at the time and had knowledge of the investigation, its researchers concluded that Careto was a hacking team working for the Spanish government.

"There was no doubt of that, at least no reasonable [doubt]," one of the former employees told TechCrunch, who like other sources in this story agreed to speak on condition of anonymity to discuss sensitive matters.

Careto is one of only a handful of Western government hacking groups that has ever been discussed in public, along with U.S. government units such as Equation Group, widely believed to be the U.S. National Security Agency; the Lamberts, believed to be the CIA; and the French government group known as Animal Farm, which was behind the Babar and Dino malware. In a rare admission, Bernard Barbier, former head of the French intelligence service DGSE, publicly confirmed the French government was indeed behind Babar.

The Spanish government now joins this small group of Western government hacking groups.



A screenshot of Careto's malware code, which inspired the name of the hacking group**Image Credits:**Kaspersky

Early in its investigation, Kaspersky discovered that the Careto hackers had targeted a particular government network and systems in Cuba, according to a second former Kaspersky employee.

It was this Cuban government victim that sparked Kaspersky's investigation into Careto, according to the people speaking with TechCrunch.

"It all started with a guy who worked for the Cuban government who got infected," the third former Kaspersky employee, with knowledge of the Careto investigation, told TechCrunch. The person, who referred to the Cuban government victim as "patient zero," said that it

appeared the Careto hackers were interested in Cuba because during that time there were members of the Basque terrorist organization ETA in the country.

Kaspersky researchers noted in a technical report published after their discovery that Cuba had by far the most number of victims per country at the time of the investigation into Careto's activities, specifically one unnamed Cuban government institution, which the report said showed "the current interest of the attackers."

This Cuban government victim would prove key to link Careto to Spain, according to the former Kaspersky employees.

"Internally we knew who did it," the third former Kaspersky employee said, adding that they had "high confidence" it was the Spanish government. Two other former Kaspersky employees, who also had knowledge of the investigation, said the researchers likewise concluded Spain was behind the attacks.

The company, however, decided not to disclose it. "It wasn't broadcast because I think they didn't want to out a government like that," a fourth former Kaspersky researcher said. "We had a strict 'no attribution' policy at Kaspersky. Sometimes that policy was stretched but never broken."

Apart from Cuba, other Careto targets also pointed to Spain. The espionage operation affected hundreds of victims in Brazil, Morocco, Spain itself and — perhaps tellingly — Gibraltar, the disputed British enclave on the Iberian peninsula that Spain has long claimed as its own territory.

Kaspersky declined to answer questions about its researchers' conclusions.

"We don't engage in any formal attribution," Kaspersky spokesperson Mai Al Akkad told TechCrunch in an email.

The Spanish Ministry of Defense declined to comment. The Cuban government did not respond to emails sent to its Ministry of Foreign Affairs.

The discovery of Careto

After Kaspersky discovered the group's malware in 2014 and, as a result, learned how to identify other computers compromised by it, the researchers found evidence of Careto infections all over the world, compromising victims in 31 countries spanning several continents.

In Africa, the group's malware was found in Algeria, Morocco, and Libya; in Europe, it targeted victims in France, Spain, and the United Kingdom. In Latin America, there were victims in Brazil, Colombia, Cuba, and Venezuela.

In its technical report, Kaspersky said that Cuba had the most victims that were being targeted, with "all belonging to the same institution," which the researchers perceived as of significance to the hackers at that point in time.

Spain had its own particular interest in Cuba in the preceding years. As an exiled Cuban government official told the Spanish daily El Pais at the end of 2013, there were around 15 members of the terror group ETA who lived in Cuba with the approval of the local government. In 2014, a leaked U.S. diplomatic cable noted that Cuba had given refuge to ETA terrorists for years. Earlier in 2010, a Spanish judge ordered the arrest of ETA members living in Cuba.

When covering the news of the discovery of Careto, the Spanish online news outlet El Diario noted that targeting countries such as Brazil and Gibraltar would favor the Spanish government's "geostrategic interests." The Spanish government had been pushing for a consortium of government-owned and private companies to win a bid to build a high-speed railway in Brazil from Rio de Janeiro to São Paulo.

Aside from targeting government institutions, embassies, and diplomatic organizations, Kaspersky said the Careto group also targeted energy companies, research institutions, and activists.

Kaspersky researchers wrote that they were able to find evidence that the Careto malware existed as far back as 2007, and found subsequent versions of Careto capable of exploiting Windows PCs, Macs, and Linux computers. The researchers said they found possible evidence of code capable of targeting Android devices and iPhones.

While Kaspersky didn't make its internal attribution public, its researchers left clear hints that pointed to Spain.

First, the company researchers noted that they found a string in the malware code that was particularly interesting: "Caguen1aMar." That string is a contraction for the popular Spanish expletive, "me cago en la mar," which literally means "I sh–t in the sea," but roughly translates to "f—k," a phrase typically used in Spain, and not in other Spanish-speaking countries.

When Kaspersky announced its discovery of Careto in 2014, the company published a map showing all the countries that the hacking group had targeted. Along with the map, Kaspersky included an illustration of a mask with bull's horns and a nose ring (the bull is a national symbol of Spain), castanets or clackers (an instrument used in Spanish folk music), and the red and yellow colors of the Spanish flag.

A detail in the map revealed how important Cuba was for Careto. For certain countries, Kaspersky added icons specifying what type of targets it was able to identify. The map showed Cuba had a single hacked victim, marked as a government institution. Gibraltar,

Morocco — whose proximity and territorial disputes make it a strategic espionage target for Spain — and Switzerland were the only other territories with a government victim.

a map of careto's victims along with An illustration of a mask**Image Credits:**Kaspersky /

Kaspersky said in 2014 that the Careto group's malware was one of the "most advanced threats" of the time for its ability to grab highly sensitive data from a victim's computer. Kaspersky said the malware could also intercept internet traffic, Skype conversations, encryption (PGP) keys, and VPN configurations, take screenshots, and "fetch all information from Nokia devices."

The Careto group relied in large part on spearphishing emails that contained malicious links impersonating Spanish newspapers like El País, El Mundo, and Público, and videos about political subjects and food recipes. One of the former Kaspersky employees told TechCrunch that the phishing links also included references to ETA and Basque news, which Kaspersky's report omitted.

When clicking on these malicious links, the victim would get infected using an exploit that hacked the user's specific device, then redirected to a legitimate web page so as to not raise suspicions, according to Kaspersky's report.

The Careto operators also took advantage of a since-patched vulnerability in older versions of Kaspersky's antivirus software, which the company said in its 2014 published report was how it first discovered the malware.

The ubiquity of Kaspersky's software in Cuba effectively made it possible for Careto to target almost anyone on the island with an internet connection. (By 2018, the Russian antivirus company controlled some 90% of the island's internet security market, according to Cuba Standard, an independent news website.) The antivirus is so popular across the country that the company's name has become part of the local slang.

But soon after Kaspersky published its research, the Careto hackers shut down all of its operations discovered by the Russian firm, going as far as wiping its logs, which researchers noted was "not very common" and put Careto into the "elite" section of government hacking groups.

"You can't do that if you're not prepared," one of the former Kaspersky employees told TechCrunch. "They systematically, and in a quick manner, destroyed the whole thing, the whole infrastructure. Boom. It was just gone."

Careto gets caught again

After Careto went dark, neither Kaspersky nor any other cybersecurity company publicly reported detecting Careto again — until last year.

Kaspersky announced in May 2024 that it had found Careto's malware once again, saying it saw the group target an unnamed organization in Latin America that was "previously compromised" by the hacking group most recently in 2022, again in 2019, and on another occasion more than 10 years ago.

Careto also hacked a second unnamed organization, located in Central Africa, said Kaspersky.

In a blog post later in December 2024, Kaspersky's researchers attributed the new hacks to Careto "with medium to high confidence," based in part on filenames that were "alarmingly similar" to filenames found in Careto's activities from a decade ago, as well as overlapping tactics, techniques, and procedures, or TTPs, a cybersecurity expression that refers to the unique behaviors of a certain hacking group.

Kaspersky researchers Georgy Kucherin and Marc Rivero López, who wrote a paper and presented their research at the Virus Bulletin security conference in October 2024, said Careto "has always conducted cyber attacks with extreme caution," but still "managed to make small but fatal mistakes during their recent operations" that matched activity from Careto a decade earlier.

Despite that, Kucherin told TechCrunch that they don't know who, or which government, is behind the Careto hacking group.

“It’s likely a nation state,” said Kucherin. “But what entity it was, who developed the malware? From a technical perspective, it’s impossible to tell.”

Contact Us

Do you have more information about Careto (aka The Mask), or other government hacking groups and operations? From a non-work device and network, you can contact Lorenzo Franceschi-Bicchierai securely on Signal at +1 917 257 1382, or via Telegram and Keybase @lorenzofb, or email.

According to Kaspersky’s most recent report, this time the Careto hackers broke into the unnamed Latin American victim’s email server and then planted its malware.

In one of the hacked machines the researchers analyzed, Kaspersky found that Careto’s malware could surreptitiously switch on the computer’s microphone (while hiding the Windows icon that normally alerts the user that the mic is on), steal files, such as personal documents, session cookies that can allow access to accounts without needing a password, web browsing histories from several browsers, and more.

In the case of another victim, according to the report, Careto hackers used a set of implants that work as a backdoor, a keylogger, and a screenshot-taker.

Despite the fact that they got caught, and compared to what Kaspersky found more than a decade ago, Kucherin said that the Careto hackers are “still that good.”

Compared to the larger and more well-known government-backed hacking groups, like the North Korean Lazarus Group and China’s APT41, Kucherin said Careto is a “very small [advanced persistent threat] that surpasses all those large ones in complexity.”

“Their attacks are a masterpiece,” said Kucherin.

Topics

Lorenzo Franceschi-Bicchierai is a Senior Writer at TechCrunch, where he covers hacking, cybersecurity, surveillance, and privacy. You can contact Lorenzo securely on Signal at +1 917 257 1382, on Keybase/Telegram @lorenzofb, or via email at lorenzo@techcrunch.com.

View Bio