Lapsus$ Attacks Localiza, Redirects Users to Porn Site

By Soumik Ghosh

Archived: 2026-04-05 15:51:35 UTC

Cybercrime , Cybercrime as-a-service , Fraud Management & Cybercrime

Brazilian Car Rental Firm Partially Restores Website • January 11, 2022

Snapshot from Localiza's Facebook page

The Lapsus$ ransomware group's latest victim is Brazilian car rental firm Localiza.

See Also: AI Pushes Cyberattacks to New Speed Levels

"We announce Localiza as a victim, this was one of the largest car rental(s) in Latin America/the world. Now it's a porn site," according to a message on the ransomware group's Telegram account, accessed by Information Security Media Group.

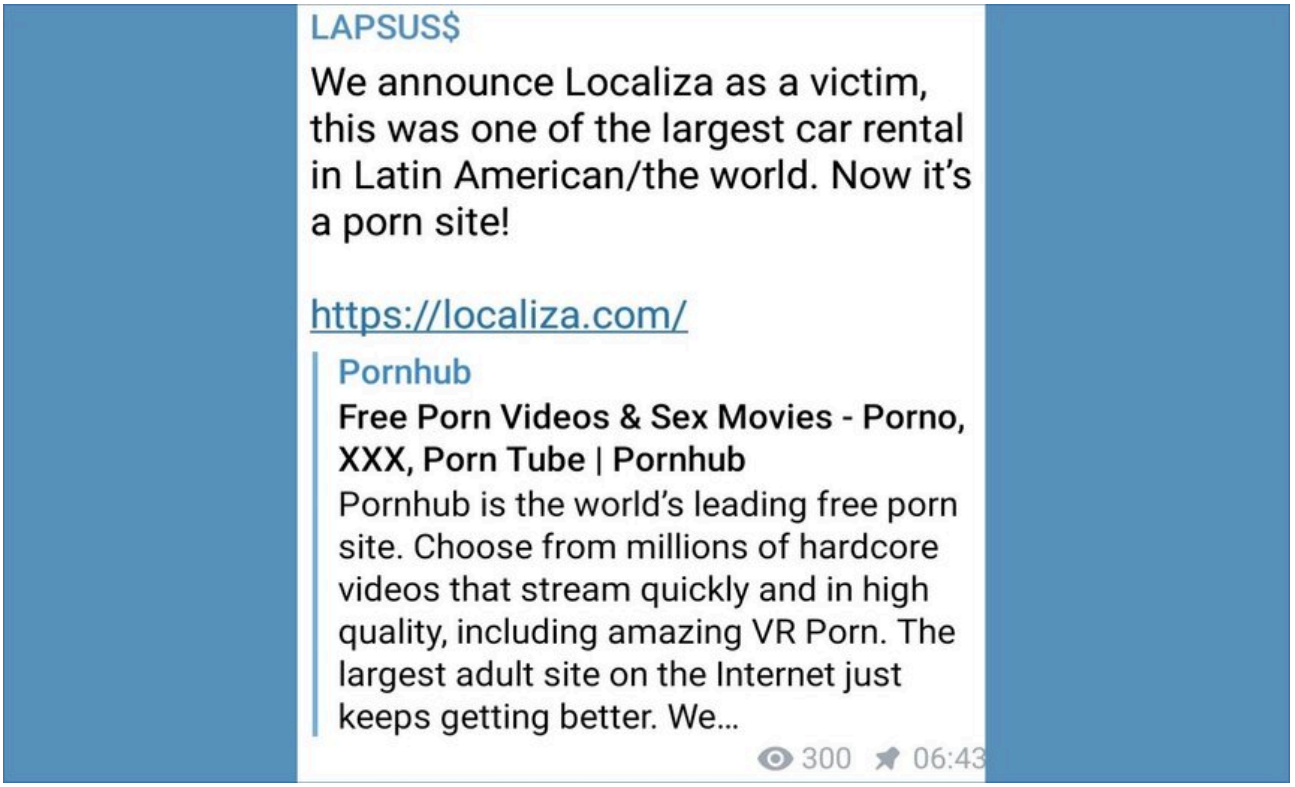
Anyone visiting the website of Localiza was redirected to a porn site between 2:30 a.m. and 4:00 a.m. Brazil time on Tuesday. The company appears to have restored user access to localiza.com's home page after 4:00 a.m. Brazil time the same day, although other functionality on the website remain inaccessible, with an error message: "Inaccessible due to a DNS error."

Localiza, which was reportedly set to acquire the second-largest car rental and leasing company in the market, Unidas, did not respond to ISMG's request for technical details of the cyberattack and ransomware demands.

Last week, the Lapsus$ ransomware group's cyberattack on Portugal-based news publication Expresso and TV channel SIC knocked out the media outlets' websites for more than three days. Expresso and SIC are owned by Impresa Sociedade Gestora de Participacoes Sociais SA, Portugal's largest media conglomerate.

On Saturday, following the attack, the Lapsus$ group said on its Telegram page: "News coming soon. Busy Days."

Three days later, the group struck Localiza.



Snapshot of Lapsus$ group's Telegram post from group's Telegram account)

With the attack on Localiza, the Lapsus$ ransomware group appears to be on a streak of successfully targeting major Portuguese-speaking companies. Portugal-based Expresso and SIC catered to the Portuguese-speaking populace in Portugal and Brazil.

Based on analysis of the Lapsus$ group's website and Telegram page, the threat actor is financially motivated and does not target a specific sector, Avkash Kathiriya, vice president of research and innovation at cybersecurity firm Cyware, told ISMG in the aftermath of the ransomware attack against Expresso and SIC.

A fairly unknown bad actor until recently, the Lapsus$ group's recent attack streak started in December 2021, when it targeted Brazil's Ministry of Health and stole close to 50 TB of data, according to Kathiriya.

It next hit Claro, a telecom company based in Brazil, and stole 10,000 TB of data, Kathiriya tells ISMG.

Localiza Incident Likely a DNS Attack

While the Localiza attack does not appear to be a denial of service attack that typically aims to overwhelm a company's systems, causing them to crash, rerouting traffic to PornHub likely indicates a DNS spoofing attack. In

the latter type of attack, hackers reroute traffic away from the real DNS servers and redirect them to a "pirate" server.

Security researcher and threat hunter Marc Reuf tells ISMG that although it's difficult to analyze the incident with the information available, he assumes that a break-in on the web server was possible, which would have allowed the attackers to redirect requests to the service.

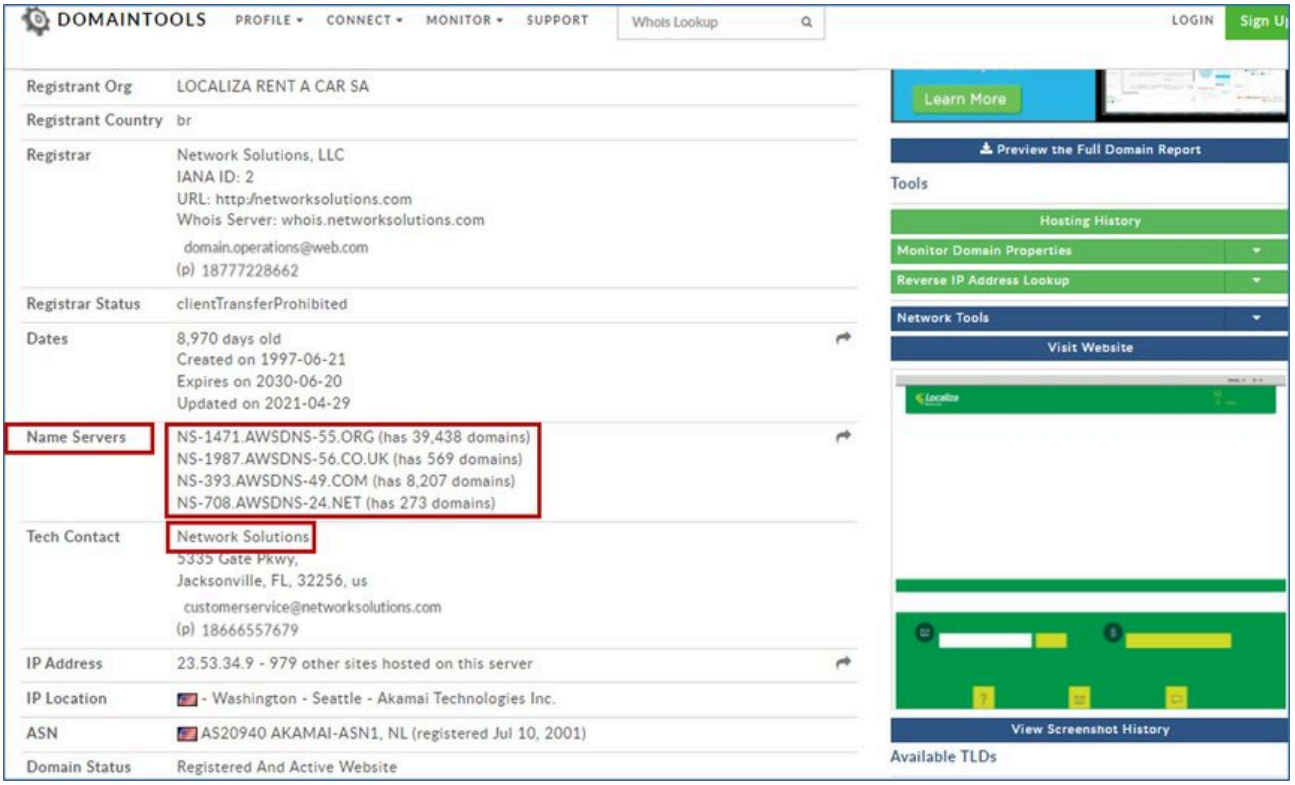
"In most cases, such attacks are realized due to weaknesses in web applications. But it may also have been a problem of the web server itself," Reuf says.

How Hackers Carry Out a DNS Attack

Jorge Orchilles, chief technology officer at Arlington-based cybersecurity firm SCYTHE and an instructor and author at the SANS Institute, tells ISMG that a domain such as http://localiza.com may be redirected to another site through the DNS.

Orchilles says that a hacker can use a website such as whois.domaintools.com to find out the domain registrar of an organization. In Localiza's case, the domain registrar is Network Solutions.

"A malicious actor may then gain administrative privileges to the account and make the change there," he says.



Source: whois.domaintools

Another option for hackers would be to make the change in the DNS server themselves. For Localiza, the "whois lookup" can tell hackers that there are four DNS servers for localiza.com. It also lists the number of domains under each of these servers, which is indicated in the red box in the above image.

Orchilles says that attacks on DNS redirection are not very common. He also says that the Lapsus$ group seems to be focused on ransomware, and this behavior is not consistent with its previous attacks, although the group remains focused on Portuguese-speaking targets.
