

24 September 2008

By: Lucian Constantin, Web News Editor



Maserati hacked and  
blackmailed  
Maserati Spa for the  
logo

## **Maserati Hacker Arrested**

*A man is accused of hacking into a Maserati database and blackmailing the company with information disclosure*

The police executed a bench warrant and arrested a 60-year-old man resident of Solana Beach, California. He is charged with computer intrusion and extortion and he is scheduled to appear in a federal court on October 31. Bruce Mengler is accused of hacking his way into a promotional website belonging to the US branch of car manufacturer Maserati and retrieving personal information about the company's potential customers.

The stolen personal data was gathered by Maserati as part of a promotion that was offering free gift certificates in exchange for participation in a test drive. The company distributed fliers to potential customers containing an invitation to test drive Maserati cars. The fliers contained a unique identification code intended to be used by the interested people on a promotional website in order to receive gift certificates usable at Omaha Steaks. Along with the code on the flier, people were asked on the website to also provide personal contact information.

The indictment does not specify exactly how Mengler accessed the information, but it suggests that he successfully downloaded the entire database, then blackmailed Maserati by asking money in return for his silence. He is supposed to have sent several letters from a "sol.beach@gmail.com" email address threatening to disclose the information and the incident publicly if he was not paid. To prove the authenticity of his claims, he included samples of the stolen information.

The company's losses are estimated at around \$5,000, but the most important aspect of this incident is represented by the security policies adopted by companies in regard to customers' personal data. 2008 has already been tagged by security researchers as "the data loss year" due to the increased number of cases where sensitive data was lost by employees, stolen by hackers or leaked through website security holes.

[Graham Cluley](#), Senior Technology Consultant for security vendor Sophos, noted on his blog referring to the case that "if a hacker was able to gain access to customer information via the promotional website then there is a clear warning here to all companies that they need to properly secure their public websites". Undergoing such marketing campaigns where sensitive customer info is gathered is fine as long as they are performed in accordance to responsible security practices. "It's all very well asking for potential customers to enter their names and addresses in exchange for free steaks, but you'll be dealing with higher stakes (groan) if your website is not properly defended," Mr. Cluley adds.