Reuse of login credentials put more than 20M Alibaba accounts at risk

February 8, 2016 By Pierluigi Paganini

The reuse of login credentials on Taobao exposed more than 20 million accounts on Alibaba's websites to attacks.

According to the state media reports, hackers have targeted over 20 million active accounts on Alibaba Group's Taobao e-commerce website using Alibaba's own cloud computing service.

The Chinese Giant detected the attack in "the first instance" and responded requesting users to change their passwords.

According to a report published on a website managed by the Ministry of Public Security, hackers behind the attack obtained a database of 99 million usernames and passwords from a number of websites.

The hackers used the Alibaba's cloud computing platform in the attempt to use the stolen credentials with the Taobao platform.

Chinese Giant.

20.59 million represents about five percent of annual active buyers on Chinese retail marketplaces.

'A spokesman from Alibaba confirmed that hackers rented the cloud computing service to launch the attack, but highlighted that there are no security issues affecting the company's platform.

"Alibaba's system was never breached," the spokesman declared.

The hackers started to test the stolen credentials in mid-October and were discovered in November, when experts at Chinese company discovered the unauthorized accesses reported the case to police.

According to the ministry website, Alibaba discovered and blocked the majority of login attempts.

The experts discovered that the compromised accounts were used in various fraudulent activities. The hackers used them to raise Taobao sellers' rankings placing fake orders, a mechanism known as 'brushing'.

The incident once again raises the importance of a proper security posture for Internet users, the bad habit of sharing same login credentials among several web services is one of the main causes of security breaches.

Pierluigi Paganini

(**Security Affairs** – Taobao, hacking)

Share it please ...

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker

News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

Dyre crackdown, the biggest effort to date by Russian authorities against cybercrime

NEXT ARTICLE

Hackers leaked DHS staff records, 200GB of files are in their hands

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top