COMPROMISED INSTAGRAM ACCOUNT AND IMPERSONATED WEB SITE WERE ABOUT TO CAUSE CREDENTIAL THEFT

A bank based in the Gulf region was affected by an **Instagram hack.** An influential Instagram account dedicated to share daily financial news, stock market insights and investment journals fell victim to **cyber intrusions** by a malicious actor. The attackers manipulated the account to disseminate **fraudulent advertisements** which were designed to deceive users **by impersonating the bank's website** with a fake domain. The fraudulent ads featured images of the organization's **high-level executives,** directing users to a fake landing page with the intent of obtaining their credentials.

REGION
Gulf

INDUSTRY
Finance & Banking

CHALLENGE
Malvertisement, phishing and impersonation of social media accounts

SOLUTION
Phishing detection, take down, malicious link prevention

Upon discovering the ads and the impersonated domain, the bank demanded their **removal.** SOCRadar conducted an investigation of the impersonated website and although no malicious downloads on the user's side were detected, it was evident that the website was obviously **designed for credential harvesting**. SOCRadar analysts amplified the depth of their investigation, unearthing that the social media account was not merely **hijacked,** but was in fact **stolen** and subsequently underwent a name change.

In the end, the ads and the impersonated domains were successfully **taken down** after all these findings were presented to the customer in a way that the customer utilized them as evidence in a **legal case.**

Why is this important?

Phishing and fraudulent ads are both combined under **malvertisements** which is one of the practices of disseminating malware through web adverts and generally appearing as conventional banner ads, pop-up windows, or other types of online advertising on trustworthy websites. When a person clicks on a malicious advertisement, they could be taken to a malicious website or asked to download a file with dangerous code. Malware can include viruses, ransomware, spyware, keyloggers, and other malicious software with the goal of infiltrating the user's system or stealing personal data.

The victims of malvertising can inadvertently pose a **significant risk to the organizations** they are associated with. A single **compromised computer** within an enterprise network can serve as a **gateway for cybercriminals,** allowing them to spread malware or gain access to sensitive company information. In such instances, personal **data breaches** can quickly escalate into corporate data leaks, with devastating implications for operational integrity, customer trust, and legal compliance. Furthermore, if the victim's machine is used for critical functions, malware can cause disruptive system failures or even become a launch pad for further attacks.

SOCRadar®
Your Eyes Beyond

CHALLENGE
Phishing via Malvertisement

SOLUTION
Detection
Takedown

CUSTOMER STORIES

1 Threat actors redirected users to a fake domain name that impersonated the website of a bank, a customer of SOCRadar, by disseminating fake adverts from a compromised influential Instagram account.

2 After an investigation into the impersonated website, designed for credential harvesting, SOCRadar analysts discovered some details, such as a clear connection to the compromised social media account.

3 The fake ads and the impersonated domain were successfully taken down. Meanwhile, all the investigation outputs were presented to the customer for his disposal to initiate a legal case.