NBC.com Hacked, Infected With Citadel Trojan

By Damon Poeter
ARTICLE DATE : February 21, 2013
pcmag.com

NBC said Thursday that it was working to resolve a problem on its website after security researchers began issuing warnings that NBC.com and related sites had been hacked and infected with malware that was redirecting visitors to malicious websites.

"We've identified the problem and are working to resolve it. No user information has been compromised," NBC said in a statement.

Malware on NBC.com and other sites associated with the TV network's entertainment portal was also detected and blocked by Internet browsers like Google's Chrome, NBC News reported. The network's NBC News Digital sites, including NBCNews.com and TODAY.com, were unaffected, according to NBC News.

Facebook also blocked NBC.com for a period of time after reports of the malware infection emerged, according to Reuters.

Security software developer Malwarebytes identified the malware infecting NBC.com and properties like the network's website for "Late Night with Jimmy Fallon" as the Citadel Trojan.

"This morning, NBC.com was hacked and embedded with malicious iframe code that spread the Citadel Trojan. It was detected as Backdoor.Agent.RS. ... The NBC web site was compromised for about 15 min and the actual iframe with the malicious redirect was embedded in a javascript file located on the NBC.com web server," a company spokesperson said in an emailed statement.

The Malwarebytes spokesperson said Citadel is a reproduction of the older Zeus Banker Trojan and "has the same capabilities of stealing financial information from users." The parties responsible used the RedKit exploit kit and vulnerabilities in Java and Adobe Reader to spread the Trojan on NBC's websites, she added.

While it appeared by late Thursday that NBC was successful in purging the infected code, anyone infected with the Citadel Trojan after visiting an NBC site earlier in the day may also have risked having the ransomware installed on their system, the spokesperson said.

Meanwhile, security researcher Dancho Danchev theorized that the group behind the NBC.com hack may be the same cybercriminals responsible for faked Facebook and Verizon emails that direct customers to infected Web pages.

The tactics of the NBC.com attack and sites infected users were redirected to mirrored the details of the earlier Facebook and Verizon campaigns, Danchev said on his security blog, adding, "Someone's multi-tasking. That's for sure."