

27 April 2009

By: Lucian Constantin, Web News Editor



NET Virtua subject to a DNS cache poisoning attack
NET Serviços de Comunicação

[DNS Poisoning Attack Against Major Brazilian ISP](#)

Banking Trojan served through fake Google Ads

The broadband Internet service of NET Serviços de Comunicação (NET Communications Services), called NET Virtua, was the target of unnamed attackers earlier this month. According to Brazilian media outlet [Globo.com](#), NET's DNS cache has been poisoned to serve a banking trojan to Virtua costumers, as well as to hijack their online banking details.

NET Virtua reported a number of over two million customers on the Brazilian market during the last trimester of 2008. The company plans to introduce broadband connection at speeds of 60 Mbps across Brazil during this year. A company spokesperson told Globo that 1% of its customer base was affected by this attack.

The Domain Name System (DNS) is one of the vital components of the Internet. It is responsible for resolving domain names into IP addresses. DNS servers worldwide communicate with each other in order to keep DNS records in sync, ensuring that changes made to them propagate across the entire Internet. In order to decrease the bandwidth load, DNS servers maintain a cache of records, which they serve to the clients querying them.

Due to an underlying flaw in the architecture of DNS discovered by security researcher Dan Kaminsky, it is possible for an attacker to inject fake records into the cache of a DNS server. This technique is called DNS poisoning and can facilitate highly complex attacks.

According to the available information, in the NET Virtua incident, the attackers hijacked two DNS records: one for the domain name used to serve advertisements from Google AdSense, and one for the domain name of Bradesco, one of the largest Brazilian financial institutions.

By changing the corresponding IP address, attackers forced websites that were loading ads from Google to unknowingly serve a banking trojan to their visitors instead. Meanwhile, Bradesco customers attempting to reach the company's website were being directed to a cloned version, which was instructing them to input their banking details.

The attack reportedly lasted for about four hours, but it is yet unclear how many users actually fell victims to it. Ronaldo Castro de Vasconcellos, a Brazilian IT security professional who monitored the attack, told [Security Fix](#) that the server hosting the cloned Bradesco page was located in South Korea.

A similar subtle attack [targeted](#) one of the biggest ISPs in China, during August last year. In that incident, customers of China Netcom who were typing any inexistent domain name into their address bars were being directed to a malicious Web page that was loading various exploits.

More recently, the DNS records of CheckFree, a large online bill-payment service, have been [hijacked](#) and set to direct users to a malware-distribution service. The attack has allegedly [affected](#) an estimated 160,000 CheckFree customers, but has been the result of the domain account password being stolen.