CLEVER Solutions Empowering Global Enterprises

How did John lose all of his crypto currency?

ethereum

When John (not his real name) visited MyEtherWallet's website in the morning of 4/24/18, his browser displayed a warning about the site's unsigned SSL certificate, but he didn't pay much attention and still clicked through the warning. Unbeknownst to him, John was actually logging on to a malicious site in Russia, which proceeded to empty his digital wallet.

John was a victim of a sophisticated attack on Amazon's Route 53 Internet Domain Name Service (DNS). DNS has been called "the phone book of the Internet." It is one of the most critical Internet services. The goal of hijacking a DNS service is to change the domain binding, so the resolver would return the spoofed IP address of a malicious site. In this case the DNS hijack lasted for over 2 hours before it was detected, resulting in substantial financial losses for MyEtherWallet's customers.

How do you prevent such attacks on your corporate DNS service? One way is to monitor your key DNS records in real-time to compare against the baseline that contains valid data. This kind of monitoring should cover not only the "A" records for domains, but also the "MX" records for email servers, the "SRV" records for services, and the "PTR" records for reverse lookup, etc. Any mismatch indicates a potential DNS attack or some misconfiguration due to update or migration.

CLEVERDetect® for DNS offers state of the art monitoring of your **DNS service** for availability and performance. It also provides real-time **DNSDiff™** to ensure data integrity in your DNS system.

For more information, please visit the link below.

Get More Information on CLEVERDetect for DNS

STAY CONNECTED:



1-650-617-2400

AES | Copyright | 650-617-2400 | Email | Website

AES - Applied Expert Systems, Inc., P.O. Box 50927, Palo Alto, CA 94303