GozNym Trojan targets business accounts at major U.S. banks

By Lucian Constantin

Published: 2016-06-23 · Archived: 2026-04-05 23:43:34 UTC

A hybrid Trojan program created for financial fraud has started redirecting users of four large U.S. banks to rogue websites in order to hijack their accounts.

GozNym is a relatively new threat, first discovered in April, and is based on the Nymaim malware dropper and the Gozi banking Trojan. Like most banking Trojans, GozNym can inject rogue code into banking websites displayed in local browsers to steal credentials and other sensitive information.

However, in addition to this old technique, the cybercrime gang behind it has also built the necessary infrastructure to host rogue copies of banking websites, and they've started to redirect victims there.

GozNym used this redirection method two months ago against users of several banking websites from Poland. However, according to researchers from IBM's X-Force team, its authors have recently launched similar attacks against the online business banking services of four large U.S. banks.

First, the Trojan redirects the victim to the fake version of the site hosted on the attackers' infrastructure, and it then temporarily displays a white overlay over the page. This unusual masking trick might be intended to distract the users and to make them believe that the page is harmless.

The fake sites are perfect replicas of the real ones. The malware uses some technical tricks locally to keep the bank's real URL in the address bar and even the SSL certificate.

Once users input their credentials into the fake website, the credentials are tested in real-time against the bank's genuine website. If they work, the attackers initiate fraudulent money transfers out of the victim's account.

"Moreover, the victim is kept on the fake website, where the attacker can push social engineering notifications to them, making them divulge personally identifiable information and two-factor authentication elements," the IBM X-Force researchers said in a blog post.

Despite being new, GozNym is quickly gaining ground in the cybercrime arena, currently ranking fifth for banking Trojan activity in 2016. The IBM researchers expect that after this testing period, its creators will add more U.S. banking websites to the rogue redirection list. The researchers didn't name the original banks targeted.

In addition to the usual security recommendations of keeping software up to date, running an antivirus program and being wary of email attachments, employees in charge of finances inside companies should try to use dedicated computers to access bank accounts and operate financial transactions. These computers shouldn't be used for other tasks like general browsing and email.

Source: https://www.computerworld.com/article/3088102/goznym-trojan-targets-business-accounts-at-major-us-banks.html