GozNym Banking Trojan Targeting German Banks

By Chris Brook

Published: 2016-08-23 · Archived: 2026-04-02 11:40:41 UTC

Fresh from targeting banks in Poland, the banking Trojan GozNym has begun taking aim at banks in Germany.

GozNym's Euro trip rolls on. Fresh from targeting banks in Poland, the banking Trojan has reportedly begun taking aim at banks in Germany.

For many, August marks the long, dog days of summer but developers behind GozNym appear to be working hard. According to numbers published by IBM's X-Force team this week, researchers have seen a 3,550 percent hike in the Trojan this month over numbers it saw in July. The surge marks a 526 percent rise when compared to the total number of attacks since the Trojan's iteration.

The Trojan, a hybrid of Nymaim and Gozi malware, initially formed in April and thrives on carrying out redirection attacks via DNS poisoning. In the attacks, unsuspecting bank customers are redirected to a seemingly legitimate replica of their bank's site and then tricked into giving up their login information.

Now GozNym is now targeting 13 banks and subsidiaries in Germany, Limor Kessem, Executive Security Advisor at IBM, said Tuesday. The Trojan's usual redirection attacks are being complemented with web injection-based attacks that cater to the banks as well.

Kessem told Threatpost on Tuesday that unlike the redirection attacks, which are designed to show victims a completely fake page, the injections rely heavily on social engineering visuals. The injections, which can come in the form of modifications to the bank's page, or pop-ups throughout a session, mean a victim may not notice them.

The ability to use of both redirection and injection attacks gives the malware more customization, experts say.

"Almost all targets of the injection attacks are also on the redirection attack list, which means that the malware can choose a preferred path for each case (which we've seen in other redirection attacks, like Dyre and Dridex)," Kessem said, "the 'decision,' if you will, is taken on the server side by the attacker, and does not seem to rely on a built-in logic."

In April, shortly after the Trojan's discovery, researchers observed a massive GozNym campaign targeting 24 North American banks. Attackers used that campaign to steal $4 million over the course of two weeks before they expanded GozNym's scope to include corporate, SMB, investment banking and consumer bank accounts in Poland.

By the end of April, GozNym had redirection instructions for 17 Polish banks in its repertoire, along with an extra 230 URLs designed to assist attackers in targeting community banks and email service providers in the Eastern European country.

When we last heard from the Trojan, its operators were seen launching redirection attacks on four large, U.S. banks in June.

The fact that the cybercriminals behind GozNym have already adapted the Trojan for three different languages and in countries which have different banking systems is unique, according to Kessem. Attackers behind Dyre have used similar tactics in the past but have only deployed their attacks in English speaking countries and Spain.

“Looking at GozNym’s timeline, it is evident that the gang operating the malware has the resources and savvy to deploy sophisticated cybercrime tactics against banks,” Kessem said Tuesday, “The project is very active and evolving rapidly, making it likely to spread to additional countries over time.”
