Attackers Behind GozNym Trojan Set Sights on Europe

By Chris Brook

Published: 2016-04-25 · Archived: 2026-04-02 11:16:16 UTC

The banking malware GozNym has spread into Europe and begun plaguing banking customers in Poland with redirection attacks, IBM said.

The banking malware GozNym has legs; only a few weeks after the hybrid Trojan was discovered, it has reportedly spread into Europe and begun plaguing banking customers in Poland with redirection attacks.

The malware has started targeting corporate, SMB, investment banking and consumer accounts at banks, including some in Portugal and the U.S., in addition to Poland, according to researchers at IBM's X-Force team.

In the attacks, bank customers are redirected to a replica of their bank's actual page and tricked into giving up sensitive information such as credentials and authentication codes. With GozNym, attackers dupe users by showing them the actual bank's URL and SSL certificate. An overlay mask, facilitated by a Moscow-based server, covers the page, hiding any malicious content on the phishing page, something that makes it look normal to users and researchers alike.

Limor Kessem, a cybersecurity expert with IBM described the latest iteration of the malware Monday in a post on the company's Security Intelligence blog.

After a user is redirected to the malicious page, the overlay is removed and users are encouraged to enter their bank username and password. From there, the information is fired off to another server.

"After that initial fake login, the malware displays a delay screen via webinjection asking the victim to wait,"Kessem wrote on Monday, "While the victim is on hold, the fraudster queries the C&C server for additional webinjections to trick users to divulge further information about their accounts,"

According to Kessem the malware has redirection instructions for 17 banks, and features an additional 230 URLs to assist attackers in targeting community banks and email service providers in Poland.

The technique is similar to one used by the Dridex Trojan earlier this year. Attackers took a page from Dyre and peddled Dridex by launching redirection attacks focused on U.K. users in January.

The method, which technically redirects users through local DNS poisoning, requires a fair bit of work; recreating and maintaining fake bank sites can be an arduous task, but Kessem claims the group behind GozNym – Nymaim – appear up to the task.

"Convincing redirection attacks are a resource-intensive endeavor that require their operators to invest heavily in creating website replicas of individual targeted banks. The Nymaim gang stands out as one of very few groups with this capability," Kessem wrote.

The GozNym Trojan surfaced earlier this month after two other Trojans, Nymaim and Gozi, merged. Attackers went on to use the Trojan to steal $4 million from 24 banks, including 22 in the United States and two in Canada, in just two weeks. The malware is distributed primarily through laced spam emails that lure recipients into opening attachments.

Kessem warned the Trojan was a “very problematic threat” just 11 days ago when she spoke to Threatpost, calling the combination of the two Trojans a “double-headed beast,” adding that the number of attacks stemming from the malware the company observed were extremely high, especially given it had only existed for a few weeks at that point.
