# GozNym's Euro Trip – Launching Redirection Attacks in Germany

The GozNym banking malware, a Trojan hybrid discovered by IBM X-Force in early April, continues to increase its activity against banks in Europe. And the latest from the GozNym gang, as discovered by X-Force Research: redirection attacks launched in Germany, targeting 13 banks and their local subsidiaries. The new redirection schemes come in addition to web injection based attacks for all the targeted brands, showing GozNym's investment in German-language attack capabilities.

GozNym's Europe-attacking faction has been intensifying its activity across the region, showing a very sharp peak in activity in August 2016. In numbers, this peak accounts for a 3550% hike since July 2016, and a 526% rise compared to the total number of attacks to date since the rise of the GozNym hybrid (April to July 2016).

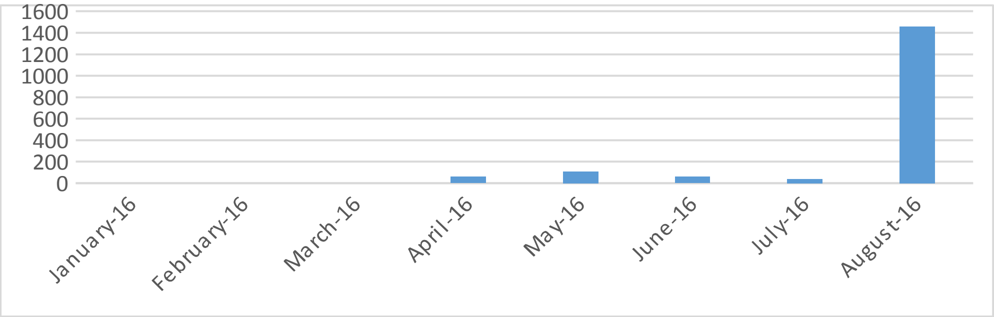

FIGURE 1: GOZNYM TROJAN'S ATTACK ACTIVITY TIMELINE | SOURCE: IBM SECURITY

The GozNym hybrid emerged in April 2016, launching an aggressive attack campaign on 24 banks in North America. Per X-Force Research, two weeks after the initial discovery, GozNym's operators began spreading a new configuration designed to target corporate, small to medium businesses banking, investment banking, and consumer accounts held with major Polish banks. That was also the time its operators began using **redirection attacks** for the first time – a rare capability in the cybercrime landscape.

By June 2016, GozNym redirection attacks started appearing in the U.S., and now, two months later, redirection attacks are coming to Germany.

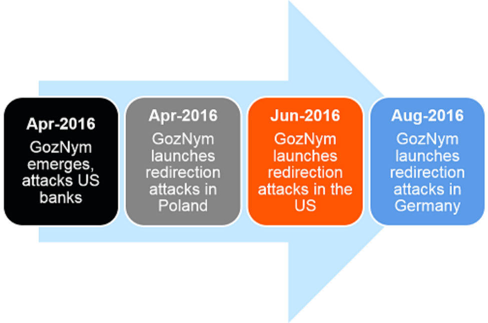
Apr-2016
GozNym emerges, attacks US banks
Apr-2016
GozNym launches redirection attacks in Poland
Jun-2016
GozNym launches redirection attacks in the US
Aug-2016
GozNym launches redirection attacks in Germany

**Figure 2:** GozNym Trojan's Attack Activity Timeline | Source: IBM Security

Looking at GozNym's timeline which has advanced into three geographies with redirection attacks within a mere 4 months, it is evident that the gang operating the malware has the resources and savvy to deploy sophisticated cybercrime tactics against banks. The project is very active and evolving rapidly, making it likely to spread to additional countries over time. Notably, the Dyre gang, the original contriver of malware redirection attacks, only managed to deploy them in English speaking countries, and in Spain. GozNym's operators already have three distinct geographies under attack, in three different languages, in countries that have different banking systems.

## Redirection Attacks – a Cybergang's Blueprint

"Redirection attacks" are successful because they bypass bank security measures by hijacking the victim to a malicious website before the victim ever reaches the bank's site. The malicious website provides a replica of the bank's website, so victims usually don't realize they arrived at the attacker's website rather than their bank's site.

By keeping the victim away from the bank's site, the fraudster can deceive them into divulging critical authentication codes on the replica site, without the bank knowing that the customer's session has been compromised.

Redirection attacks are most often associated with the resources and capabilities of organized cybergangs that have developers on the team, because of the extra setup required to pull it off, like the unique site replicas maintained for each target. The technique first surfaced in 2014, when the Dyre gang started using it to target banks, primarily in the UK, United States, Australia, and Spain.

Projects of this technical level are the domain of very few, major cybercrime gangs active in the world nowadays. Seamless redirection attacks are a resource-intensive endeavor, requiring their operators to invest heavily into creating website replicas of individual targeted banks. The Nymaim gang stands out as one of only two known groups to have this capability, with the only other known malware actively using redirection attacks being the Dridex Trojan.

## Cybercrime in Germany

IBM X-Force threat intelligence analysts looked into current underground trends focused on the German financial sector and have found that the topic is rather trendy.

Fraudsters target Germany in the same ways that they target other geographies: looking for bank account credentials, SMS interception schemes, and accomplices to work with on the cash-out of stolen funds. The overall chatter is quite indicative of the fact that cybercriminals have the same interest in German banks as they do in other parts of Europe, adapting their schemes to the local banking systems in order to avoid detection and failed fraud attempts.

## About GozNym

GozNym is a hybrid banking Trojan believed to be created by the cybergang that operates the Nymaim dropper. The original group has been active since 2013, using their malware to launch vast ransomware campaigns that resulted in millions of infected endpoints around the globe.

With the new GozNym Trojan and the attack schemes added to the malware in the past few months, it is clear GozNym attacks are evolving quickly, turning GozNym into a serious player in the financial threat landscape. IBM X-Force Research expects to see further rises in GozNym attacks in the coming weeks, and the expansion of redirection attacks to additional banks in the near future.

From a global perspective, GozNym attack volumes, as monitored by IBM Security anti-fraud solutions, have been rising. The malware already ranks 8th on the top 10 most active financial Trojans list, adjacent to longer standing malware gangs like Tinba, Rovnix, and GootKit.

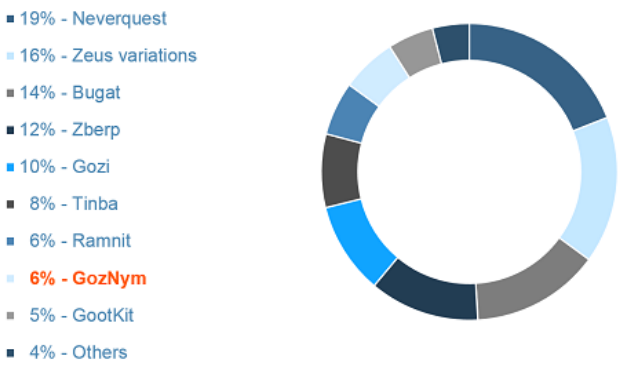

**Figure 3:** Most Active Financial Malware Globally Aug-2016 YTD | Source: IBM Security

## Detecting and Stopping GozNym Attacks

The GozNym hybrid is a powerful banking Trojan, as stealthy and persistent as the Nymaim loader while possessing the Gozi ISFB Trojan's ability to manipulate Web sessions and perform online banking fraud attacks.

IBM Security has studied the GozNym malware and its various attack schemes, and can help banks and other targeted organizations learn more about this high-risk threat. To help stop threats like GozNym, banks and service providers can use adaptive malware detection solutions and protect customer endpoints with malware intelligence that provides real-time insight into fraudster techniques and capabilities, designed to address the relentless evolution of the threat landscape.

Users looking to prevent malware infections on their endpoints must keep their operating system up to date at all times, update frequently used programs, and delete those they no longer use. Browsing hygiene for the prevention of Trojan infection includes disabling ads, and avoiding sites typically used as infection hubs, sites such as adult content, torrents, and free gaming. Also critically important is to never click on links or attachments in unsolicited email.

Most cases of malware infections, including GozNym's, begin with a malware-laden spam email that lures victims into opening an attachment by indicating it is an invoice or another important document. If users are not expecting this document, their best bet is to delete the email immediately, and then directly check their accounts or contact their service provider to check into the matter.

Those who frequently bank away from home are advised to never access any of their personal accounts from public computers in libraries, coffee shops, or locales offering Internet access. Online banking should be carried out from trusted devices which are protected by the adequate security solutions and limited as much as possible to the use of the account owner.