# The Banking Malware Offspring of Gozi ISFB and Nymaim

**securityintelligence.com**/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/

April 14, 2016

Home&nbsp/ Malware

Meet GozNym: The Banking Malware Offspring of Gozi ISFB and Nymaim

Malware April 14, 2016

By Limor Kessem co-authored by Lior Keshet 5 min read

IBM X-Force Research uncovered a Trojan hybrid spawned from the Nymaim and Gozi ISFB malware. It appears that the operators of Nymaim have recompiled its source code with part of the Gozi ISFB source code, creating a combination that is being actively used in attacks against more than 24 U.S. and Canadian banks, stealing millions of dollars so far. X-Force named this new hybrid GozNym.

The new GozNym hybrid takes the best of both the Nymaim and Gozi ISFB malware to create a powerful Trojan. From the Nymaim malware, it leverages the dropper's stealth and persistence; the Gozi ISFB parts add the banking Trojan's capabilities to facilitate fraud via infected Internet browsers. The end result is a new banking Trojan in the wild.

Internally, GozNym works like a double-headed beast, where the two codes rely on one another to carry out the malware's internal operations. More information about the hybrid's intertwined operation appears in the technical section of this blog.

## Targeting North America

In terms of its current targets, X-Force noted that the GozNym hybrid's configuration is presently focused on the U.S., targeting 22 banks, credit unions and popular e-commerce platforms. Two financial institutions based in Canada are also on the list. GozNym's operators' top target is business accounts.

## When Source Codes Collide

How was this hybrid created? GozNym's source code is composed of two known malware codes, one of which is Gozi ISFB, which leaked in 2010. Gozi ISFB was actually leaked more than once: A second disclosure took place in late 2015, when a modified ISFB code was rumored to have been compromised yet again.

On the Nymaim side, the only group known to possess its source code is the original development team. The most likely scenario is that the Nymaim team obtained the leaked Gozi ISFB code and successfully incorporated it into their own malware to create a combination Trojan for financial fraud attacks.

## From Nymaim to GozNym

Nymaim is a two-stage malware dropper. It usually infiltrates computers through exploit kits and then executes the second stage of its payload once it is on the machine, effectively using two executables for the infection routine.

On its own, the Nymaim Trojan is a stealthy, persistent dropper that uses evasion techniques such as encryption, anti-VM, anti-debugging and control flow obfuscation. Although it has dabbled with other banking Trojans in the past, its first tight connection with banking malware began in November 2015; up until then, Nymaim was almost exclusively used as a ransomware dropper.

Nymaim is believed to be operated by a closed group and developed on an ongoing basis by what appears to be the same developer(s). The Trojan has a global reach and launched an untold number of ransomware attacks using its own generic locker on users in Europe, North America and South America, PCWorld reported.

Campaigns linked with the malware were not all documented. However, related data from an independent blogger cited over 2.5 million infections via the Blackhole Exploit Kit (BHEK) in late 2013.

*Source: Malware don't need Coffee*

X-Force researchers noticed that Nymaim started fetching a Gozi ISFB module, a webinjection dynamic link library (DLL), and using it to launch online banking attacks in late 2015.

As for the infection vector, some recent cases from 2016 revealed that the Pony loader executed Nymaim, which then fetched Gozi ISFB as a third step in the infection flow. The resulting online banking fraud attempts were detected as Gozi ISFB attacks, even though they originated with Nymaim.

The first merged variant, GozNym, was detected in early April 2016, when new Nymaim samples came embedded with Gozi ISFB code and were recompiled into one malware. In the hybrid form, Nymaim is the first executable launched. It then launches the Gozi ISFB component as the second stage of the malware deployment.

## Some Technical Details

Before merging into an actual hybrid, earlier versions of Nymaim used to fetch and inject Gozi ISFB's financial module as a complete DLL into the infected victim's browser to enable webinjections on online banking sites. That DLL is about 150 KB and was a valid Portable Executable (PE) file.

More recent versions of Nymaim include altered Gozi ISFB code. Instead of the 150 KB DLL, it now injects a 40 KB buffer into the browser. This buffer still performs Gozi ISFB's functionality. For example, when it comes to the Export Address Table (EAT), which contains the addresses of modules exposed for consumption by other applications and services, GozNym uses the same hook engine to perform webinjections.

However, there are some pointed differences. For one, the new buffer is not a valid PE file — it has more of a shellcode structure. It constructs its own Import Address Table (IAT) and has no PE headers.

Another difference is that the new buffer is intertwined with Nymaim's code. We have at least two examples that demonstrate that interoperability: One is where Gozi ISFB calls Nymaim code to obtain strings; the other is where Gozi ISFB's buffer code needs to perform actions such as memory allocations.

This intertwined construction led us to the conclusion that Nymaim and Gozi ISFB were in fact compiled into one project.

## Analyzing the Gozi ISFB Code

To illustrate that, let's have a look at a comparison between the earlier Gozi ISFB DLL version and the new GozNym buffer code. Both pieces perform the same essential action and are taken from the ISFB hook engine.

Here is the original Gozi ISFB DLL that used to be fetched by Nymaim:

Here is the new GozNym buffer:

In this last figure, we see the new hybrid version's function jmp_nymaim_code:

This piece of code is called whenever Gozi ISFB requires Nymaim to perform an operation. In our example, it is calling HeapAlloc. The function prepares the required arguments, operation type, allocation size, etc. for Nymaim. Nymaim then performs the action and returns the result to the Gozi ISFB code.

### Relevant Sample MD5

The MD5 hash is 2A9093307E667CDB71884ECC1B480245.

## Detecting and Stopping GozNym Attacks

The merging of Nymaim and parts of Gozi ISFB has resulted in a new banking Trojan in the wild. This malware is as stealthy and persistent as the Nymaim loader while possessing the Gozi ISFB Trojan’s ability to manipulate Web sessions, resulting in advanced online banking fraud attacks.

IBM Security has studied the GozNym malware and its 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.

Read the white paper: Accelerating growth and digital adoption with seamless identity trust

*For technical details on this research and related indicators of compromise, see the X-Force Advisory on X-Force Exchange.*

Limor Kessem
Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...

Watch on demand →