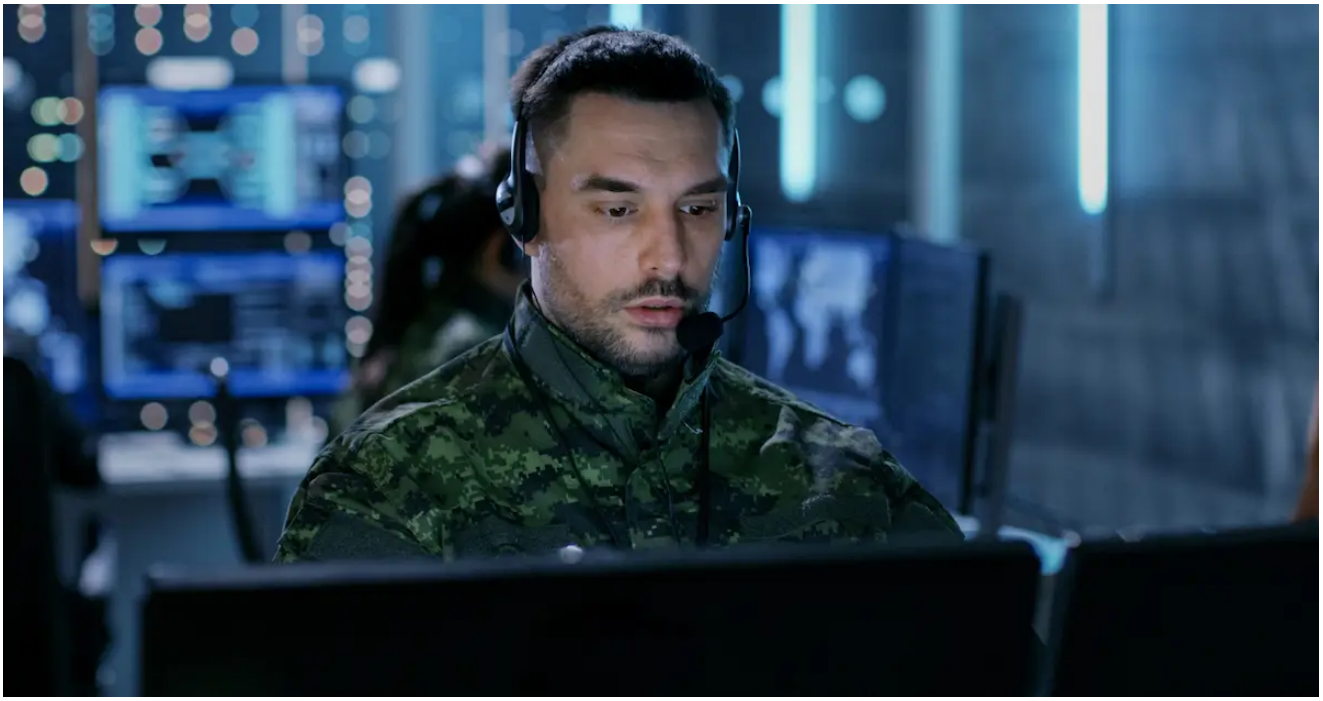
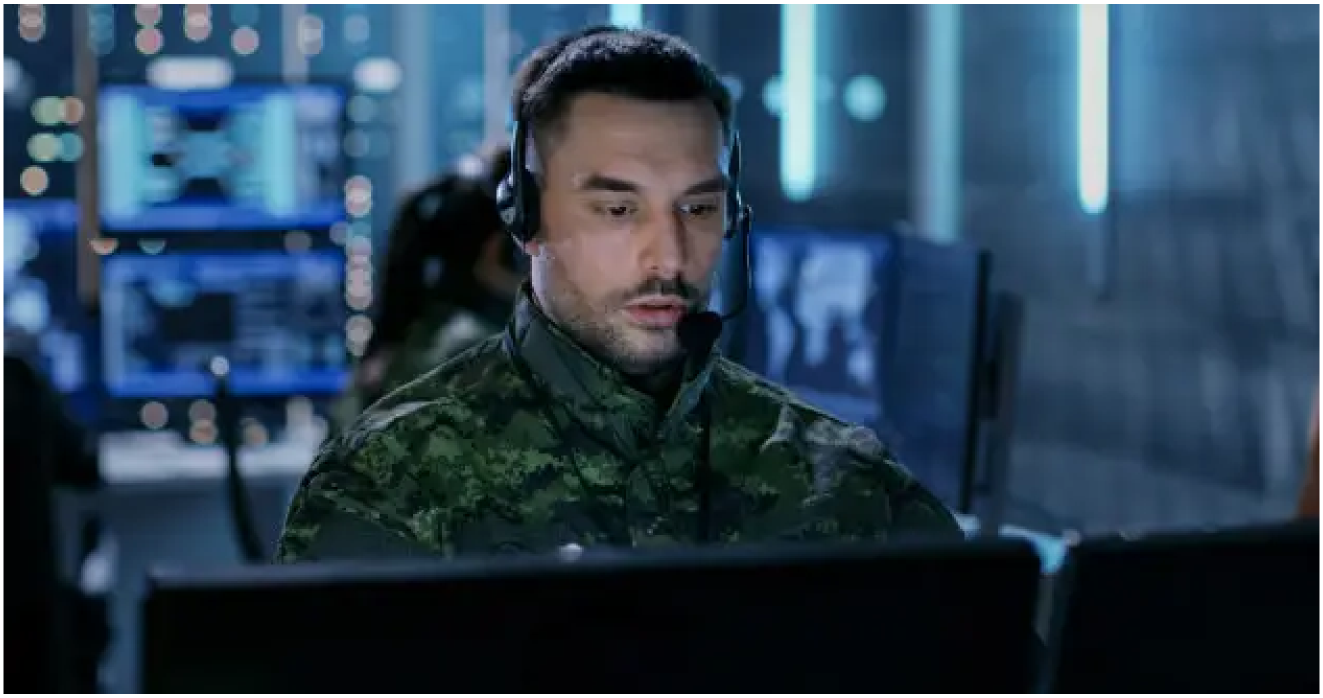
GozNym Closure Comes in the Shape of a Europol and DOJ Arrest Operation

securityintelligence.com/posts/goznym-closure-comes-in-the-shape-of-a-europol-and-doj-arrest-operation/



Home&nbsp/ Advanced Threats

GozNym Closure Comes in the Shape of a Europol and DOJ Arrest Operation



Advanced Threats May 16, 2019

By Limor Kessem 4 min read
Two and a half years after the initial arrest of a major member of the GozNym cybercrime gang, Europol and the U.S. Department of Justice (DOJ) joined forces to reach additional gang members who used the Trojan to pilfer large amounts of money from companies in the U.S. The operation was crowned “unprecedented,” having successfully dismantled what was left of the gang that attempted to steal well over $100 million.

A Two-Headed Beast Emerges

In April 2016, IBM X-Force researchers came across a new banking Trojan that seemed a little too familiar. After taking a closer look at what seemed to be a pretty sophisticated, modular code, our team announced that a Trojan hybrid was spawned from the Nymaim and Gozi ISFB malware.

X-Force named it GozNym, representing its two major components, having realized that the likely operators of Nymaim — a malware loader used mostly in ransomware attacks — recompiled its source code with part of the Gozi ISFB source code, creating a combination that they launched into attacks targeting the customers of more than 24 U.S. and Canadian banks. GozNym-facilitated fraud attacks amounted to over $4 million in losses within the first few days of its activity.

What was the purpose of this odd combination? It is likely that those behind the GozNym project aimed to marry the best of both Nymaim and Gozi ISFB to create a powerful new Trojan. GozNym leveraged the Nymaim dropper’s stealth and persistence and the Gozi ISFB parts added the banking Trojan’s modules and its capabilities to facilitate wire fraud on infected user devices.

Technical information about this hybrid was released by X-Force research in July 2016, when GozNym started spreading to additional geographies.

Takes the World by Storm

Very soon after activating their campaigns, GozNym’s operators were not waiting. They teamed up with the Avalanche botnet (Avalanche was taken down by Europol in late 2016, leading to the exposure of some of GozNym’s major operators) to spread the malware and link up with other elite cybercriminals, and started moving the project into additional countries.

Within no more than a week after launching aggressive attacks on online banking users in North America, GozNym was equipped with redirection attacks and set loose in Poland. Malware-facilitated redirection is a sophisticated way to hijack online banking users to an obscure replica of their bank’s website and there, away from their bank’s security controls, dupe them into divulging their account credentials, personal information and secondary authentication codes. In the background, a fraudster is initiating a fraudulent transaction and completes it using the freshly stolen data.

In June 2016, GozNym redirection attacks spread to the U.S., targeting the business banking customers of major financial institutions in the country. By August 2016, GozNym was off to a Euro-trip of sorts, launching redirection attacks on banks in Germany.

Spreading out this quickly and efficiently is no small feat. To begin, creating and maintaining redirection attacks is a resource-heavy endeavor. But going beyond that technical hurdle, spreading a banking Trojan to countries with a unique language, such as German or Polish, for example, where banking systems differ, entails people on the streets. It means that GozNym collaborators had the contacts to help them craft and spread quality malspam in those languages, work the redirection attacks simultaneously in different parts of the world, receive backing from local organized crime to facilitate cash-out, and move the money out quickly.

But as they stormed through different parts of the globe, GozNym's operators did not realize they had garnered a lot of attention from the security research industry and from global law enforcement agencies.

Wham Bam — GozNym's Down

With multiple operations across the globe, the GozNym crew was having a heyday. In November 2016, X-Force research was tracking campaigns in the U.S. and Germany, likely operated by two groups in tandem. In Germany, the malware continued to focus on business banking, and in the U.S., where the holiday season was in full swing, the group lined up the top electronics retailers, e-commerce sites, e-wallet providers, telecommunications vendors and payment card providers, adding them to spruced up configuration files in preparation of new infection campaigns.

But while all this activity was keeping GozNym operators busy, Europol was busy taking down the notorious Avalanche botnet, a major cybercrime infrastructure that served as a bulletproof hub for spreading some of the world's worst malware gangs. One of those gangs was GozNym.

The takedown was announced by Europol on Dec. 1, 2016. On Dec. 12, 2016, the DOJ released the notice about the arrest of one of GozNym's major players, a Bulgarian national named Krasimir Nikolov — the group's master account takeover specialist, versed in stealing money from compromised accounts. At the time, Nikolov was the sole defendant, but the GozNym team was very quick to react and disband. Campaigns immediately died out and GozNym attacks ceased, never to return again.

Pinning Down the Ghosts of the GozNym Operation

Was it the arrest of Nikolov that led to additional information on the remaining members of what used to be one of the most brazen and aggressive cybercrime gangs? Possibly. Either way, international law enforcement did not rest on its laurels after that first arrest, knowing all too well that a gang so prolific can bring many more people to justice.

Providing additional closure to this chapter in cybercrime history, Europol, in collaboration with the DOJ, have managed to reach and arrest gang members in Bulgaria, Georgia, Moldova and Ukraine and serve up criminal prosecutions in Georgia, Moldova, Ukraine and the U.S. — in total, 10 defendants in five countries, accounting for attacks on more than 41,000 victims, mostly businesses across North America and Europe.

This successful operation is a meaningful event. It underlines the evolving capabilities of law enforcement to collaborate on such complex operations to bring cybercriminals to justice, and serves as a warning to both existing and would-be criminals of the future.

It is also a reminder that the quick sharing and democratizing of threat intelligence is a critical part of fighting cybercrime. The IBM X-Force team is proud to have played its small role in getting the eyes of justice focused on GozNym.

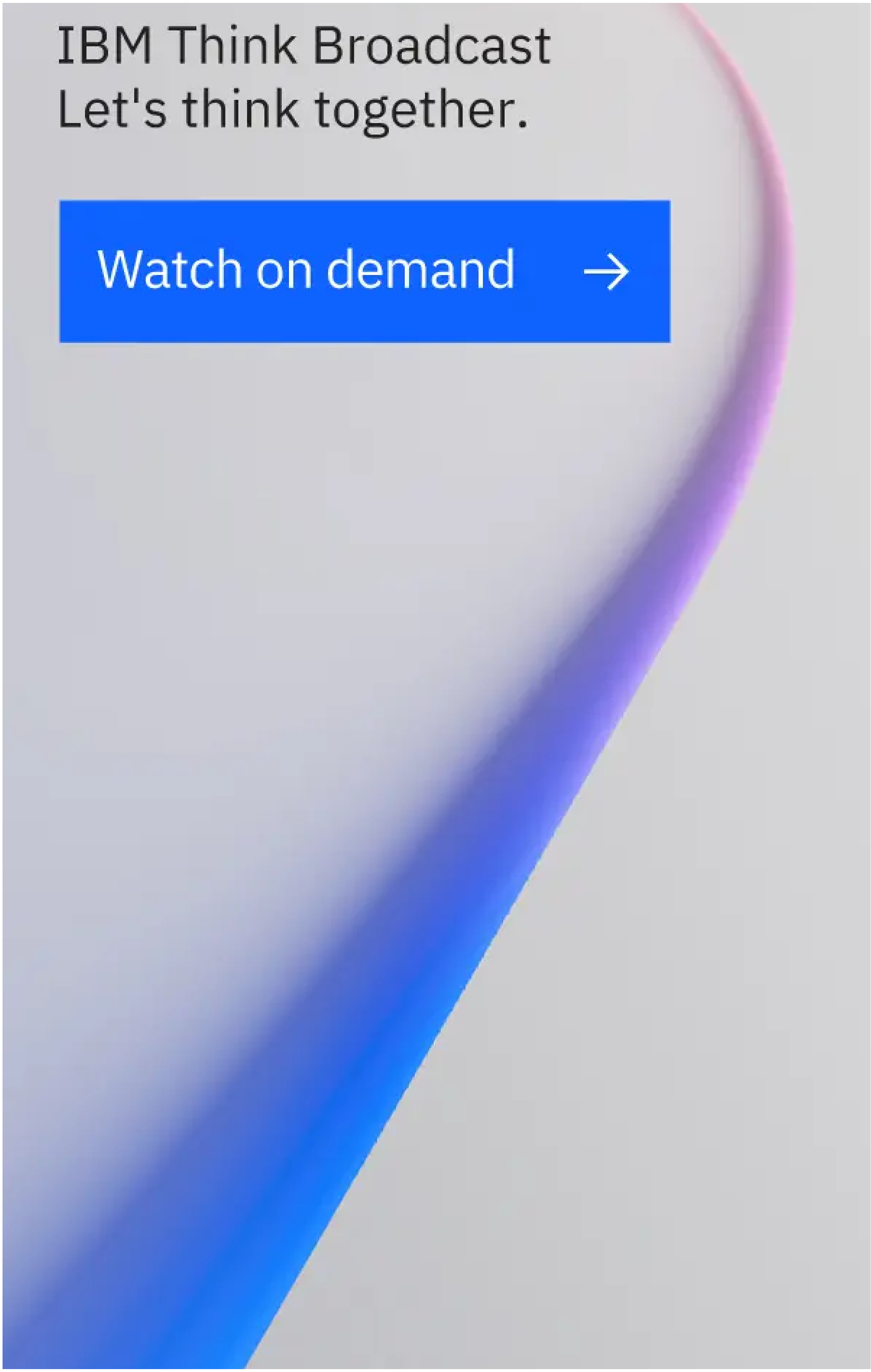
What’s Next for Cybercriminals Post-GozNym?

After GozNym departed the cybercrime arena, our team has seen the TrickBot malware fill that void, having emerged in 2016. In 2018, X-Force noted much tighter collaboration between the leading malware gangs, specifically TrickBot and IcedID, which was also discovered by IBM Security.

Over the course of 2018, IcedID took on more obfuscation techniques used by TrickBot, while TrickBot began to also drop IcedID malware on infected machines. It appears that intergang collaboration is still trending, and likely for the same reasons: criminals coming together to create something more powerful than what they have separately. Lest we forget, doing the same as defenders is what makes all the difference.

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...


IBM Think Broadcast
Let's think together.
Watch on demand →