The NukeBot Trojan, a Bruised Ego and a Surprising Source Code Leak

securityintelligence.com/the-nukebot-trojan-a-bruised-ego-and-a-surprising-source-code-leak/

March 28, 2017

Home / Banking & Finance

The NukeBot Trojan, a Bruised Ego and a Surprising Source Code Leak

Banking & Finance March 28, 2017
By Limor Kessem co-authored by Ilya Kolmanovich 4 min read

An Uncommon Tale of a Failed Banking Trojan Vendor

In early December 2016, IBM X-Force researchers noticed the emergence of a new banking malware advertised for sale in a few underground boards. The malware's vendor, who went by the online moniker Gosya, was a Russian-speaking member who introduced himself as the developer of Nuclear Bot, or NukeBot, a modular banking Trojan.

Considering the demand for commercially available malware in the cybercrime community, this malware should have been accepted very eagerly. But instead, its developer's user account was banned from multiple forums. In March 2017, the source code was leaked, apparently by the developer himself.

What led to this leak, and what impact can we expect as a result?

Gosya Comes to Town

In cybercrime forums, and especially in the more closed and Russian-speaking communities, members earn credibility by following certain customary steps. To begin, they must be introduced by a known member and vetted by the community according to what they can offer. Most importantly, they must gain the trust of the administrators running the board.

When Gosya joined underground communities, he apparently did not follow all the customary steps. He was introduced by a known member but took some wrong turns from there.

Immediately upon joining, Gosya began advertising a new banking malware for sale. According to X-Force research observations, he did not have the malware tested and certified by forum admins, nor did he provide any test versions to members. At the same time, he was attacked by existing competition, namely the FlokiBot vendor, who wanted to get down to the technical nitty gritty with him and find out if Gosya's claims about his malware's capabilities were indeed viable.

In posts where he replied to challenging questions, Gosya got nervous and defensive, raising suspicion among other forum members. This was likely a simple case of inexperience, but it cost him the trust of potential buyers.

For his next wrong move, Gosya started selling on additional forums under multiple monikers. When fraudsters realized that the same person was trying to vend under different names, they got even more suspicious that he was a ripper, misrepresenting or selling a product he does not possess. The issue got worse when Gosya changed the malware's name to Micro Banking Trojan in one last attempt to buy it a new life.

That was the point when Gosya was banned in the forums where he was attempting to sell his bot.

Was NukeBot Ever Real?

The notable part of this case is that NukeBot is an actual banking malware. It is a functional, modular Trojan that comes with a web-based admin panel to control infected endpoints. The malware is capable of webinjections and does not fall short of other, similar code by much.

Figure 1 NukeBot's Web-Based Admin Panel

When NukeBot had a test server up, it was captured and analyzed by Arbor Networks, which blogged about it in December 2016. Based on this analysis, the malware was a functional and viable code from the get go.

IBM X-Force researchers also analyzed NukeBot, specifically because Gosya claimed it was able to circumvent IBM Security's antifraud protection product, Trusteer Rapport. These claims were dispelled by X-Force, which determined that NukeBot did not affect Rapport at any point in its development. X-Force researchers also concluded that NukeBot was not a fake product and that its developer was not being taken seriously due to the way he introduced the malware, not because it was a hoax.

A Bruised Ego and a Malware Code Leak

Banned from the underground venues where he planned to sell NukeBot and distrusted by members of the cybercrime community, NukeBot's developer was likely struggling to come to terms with months of hard work amounting to nothing.

In mid-March 2017, X-Force researchers noticed that NukeBot's code was leaked in a web-based source code management platform and made available for anyone to pick it up. This move appears to have been the action of the developer, not an intentional leak by another party.

What could this mean? An educated guess would be that Gosya was disappointed with the distrust he faced in the underground and decided to release the main module of the malware for others to test and attest to.

In Gosya's arguments with the FlokiBot developer, the latter boasted the number of Google results that appear when one searches the FlockiBot value. Gosya may think the malware will get picked up by more experienced operators and start appearing in attacks in the wild — and in additional security blogs.

With yet another malware source code out in the open, the most likely scenario is that NukeBot code will be recompiled and used by botnet operators. Parts of it may be embedded into other malware codes, and we are likely to see actual NukeBot fraud attacks in the wild in the coming months.

It's also possible that Gosya will be readmitted to the same forums from which he was banned, this time as an authorized vendor. He may even deliver on previous promises to supply new modules for the malware.

Code Leaks Mean More Malware

We know from previous incidents, such as the Zeus, Gozi and Carberp leaks, that publicly available source code makes for more malware. This is often incorporated into existing projects. X-Force researchers noted that NukeBot is likely to see the same process take place in the wild, especially since its code is not copied from other leaked malware, per the developer's claims.

At this time, NukeBot has not been detected in real-world attacks and does not have defined target lists. This situation is likely to change in the near future.

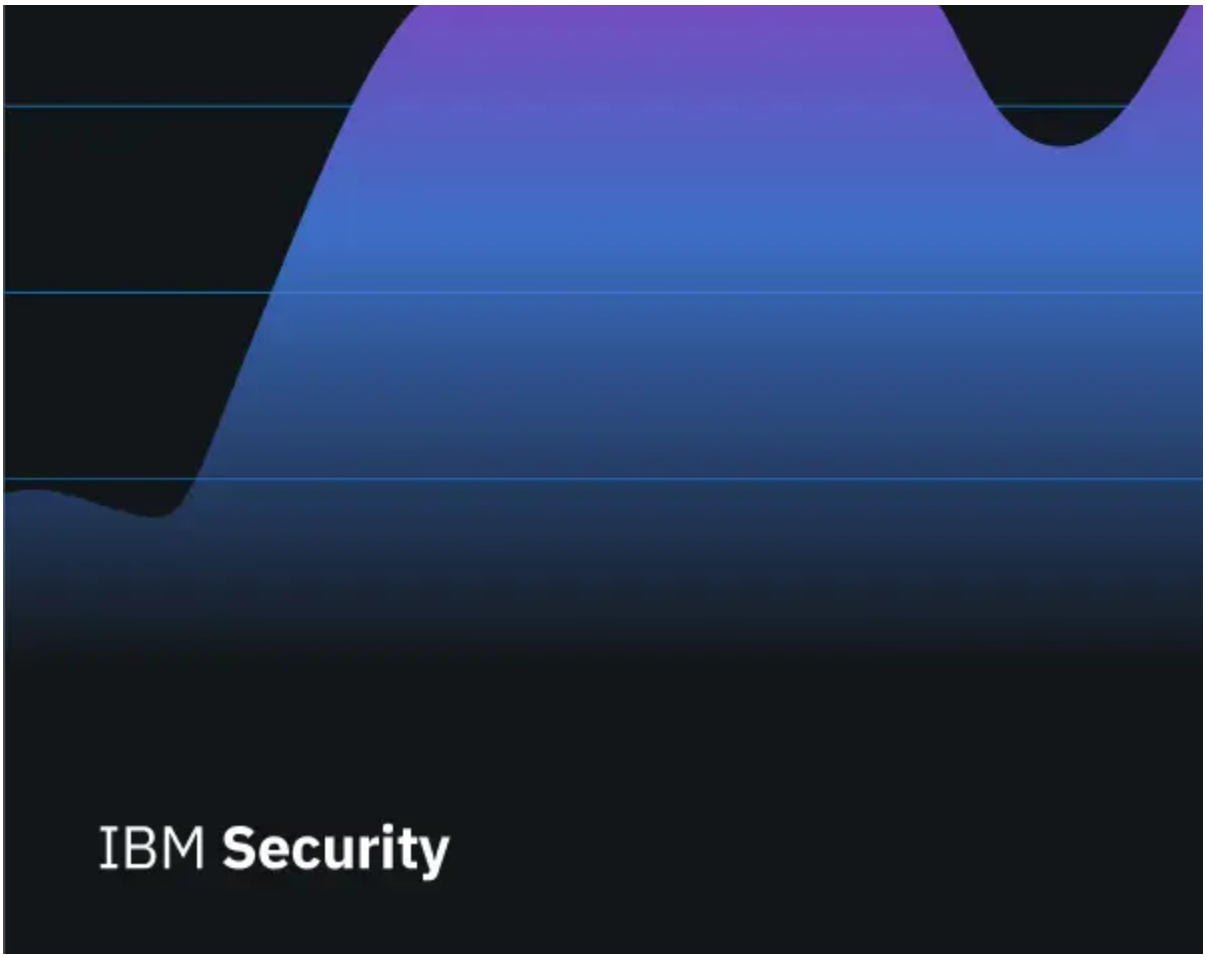
To help stop threats such as NukeBot before they ever cause damage, banks and service providers can use adaptive solutions to detect infections and protect customer endpoints. Fighting evolving malware threats can be made easier with the right malware detection solutions. With protection layers designed to address the ever-changing threat landscape, financial organizations can benefit from malware intelligence that provides real-time insight into fraudster techniques and capabilities.

Consumers wishing to protect themselves from malware infections on endpoints and mobile devices are invited to read our best practices page.

Read the white paper: Shifting the balance of power with cognitive fraud prevention

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 Security