
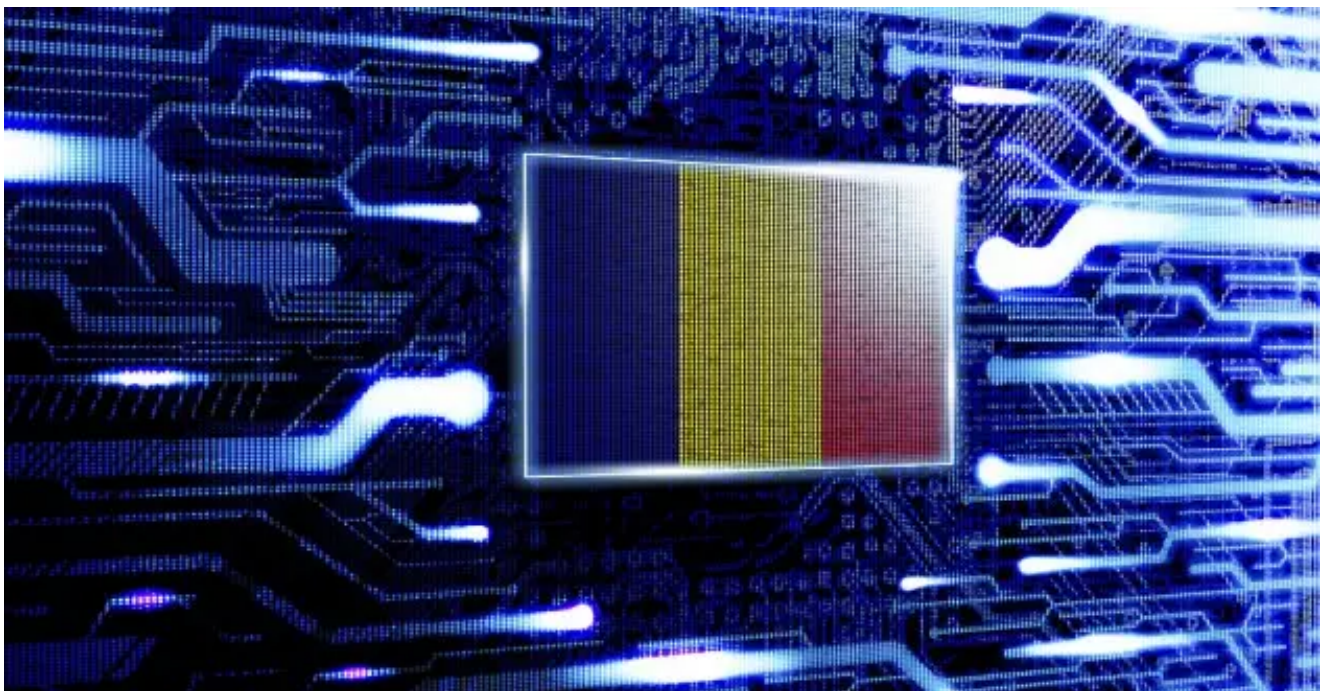
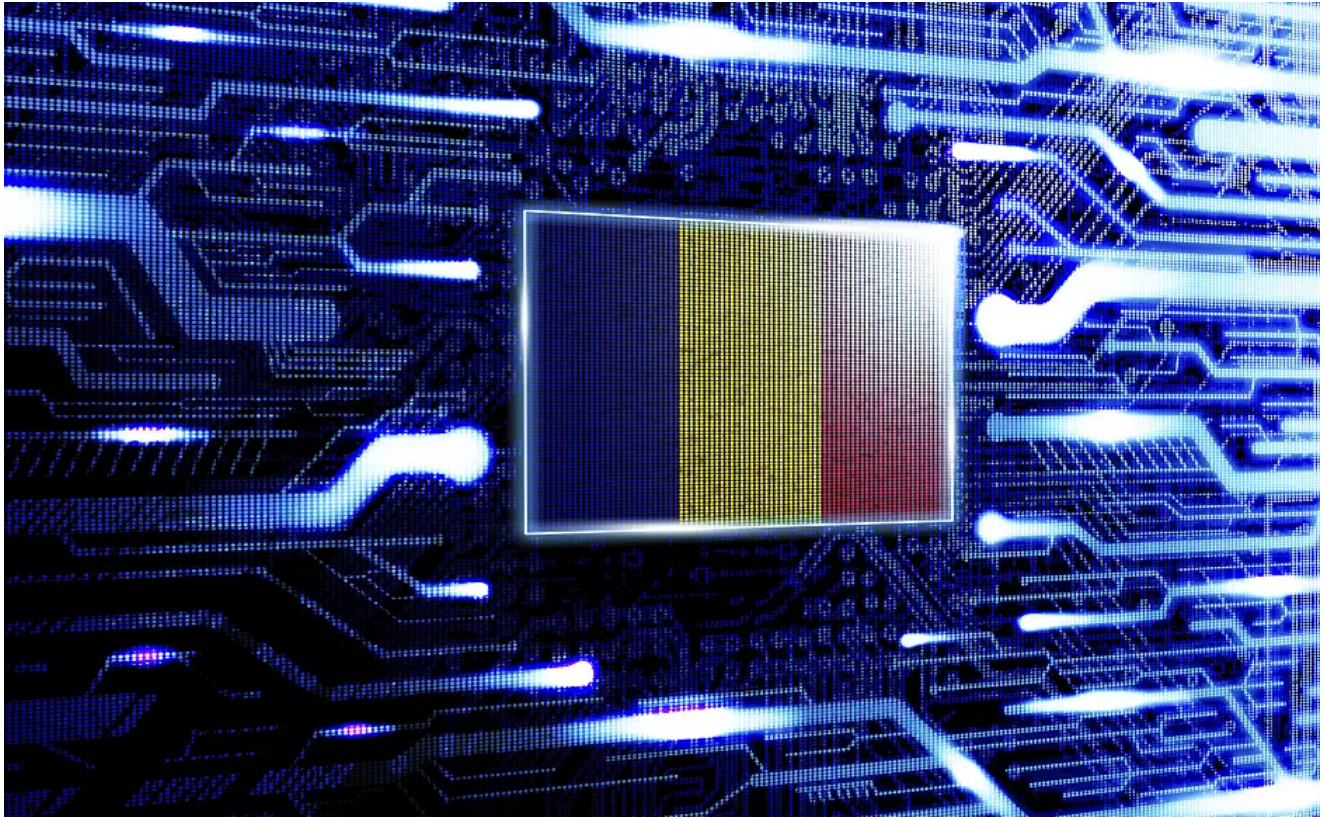


Tinba Trojan Sets Its Sights on Romania

 securityintelligence.com/tinba-trojan-sets-its-sights-on-romania/

August 12, 2015



Malware August 12, 2015

By Limor Kessel 4 min read

While Romania is widely suspected of being home to a large amount of cybercriminals – even with one city dubbed by some as “[Hackerville](#)” — we seldom see it targeted by those who attack Western countries.

In a recent finding, IBM Security X-Force researchers discovered an interesting Romania-focused configuration of the Tinba v3 Trojan, which exclusively targets 12 Romanian banks.

What’s New?

In late July 2015, [IBM Security X-Force](#) researchers analyzed a new Tinba v3 Trojan configuration file that is, according to our data, the first of its kind dedicated to Romanian banks. Previous versions of this malware attacked a number of European countries, but Romania wasn’t among them and is rarely a top target. Our analysis reveals that Tinba v3’s developers have expanded the capabilities and reach of the malware by updating its webinjections to match the new banks targeted in the Eastern European country.

The Tinba Bunch

The [Tinba Trojan](#) (also known as TinyBanker or Zusy) was first discovered in the wild in mid-2012. It was dubbed “tiny” due to its slim 20 KB file size, which included its configuration and webinjection kit. This malware initially acted like a classic banking Trojan, dedicated to grabbing user credentials and network traffic. The first Tinba release sported a form grabber to steal usernames and passwords and a webinjection mechanism for man-in-the-browser (MitB) attacks.

Although it started out as a tool used exclusively by its developers and their gang, its source code was leaked in mid-2014, and the project then began evolving in other directions. That code leak gave immediate rise to two more Tinba variations, which were taken up by different gangs, spawning Tinba v2 and Tinba v3. Each is a fully independent Trojan variation, clearly developed and updated by different individuals.

The most recent addition to the Tinba bunch is a fourth variation. Again, a new gang took the source code and revamped it to create a unique banking Trojan. In late June 2015, this gang lured in victims via a [malvertising campaign](#), which led users to an exclusive exploit kit called HanJuan. HanJuan then dropped Tinba 4, the actual banking malware.

Of all the Tinba variations, v3 appears to be the most active and possibly commercially available. It is more prolific and appears to be used by more than one group.

[Learn more about Staying ahead of threats with global threat intelligence](#)

Tinba v3 Extending Its Reach

The configuration that targets Romanian banks at this time is linked with Tinba v3. Right from its first release, this variation showed that the developer behind it put some work into new features designed to enhance the Trojan's evasion techniques, bypass automated security controls and "phone home," even when the original command-and-control (C&C) server is down.

Botmasters typically strive to protect their botnets from potential hijacking and takedowns, and Tinba v3's developer took extra care to ensure that its fallback mechanisms would secure the illicit business continuity.

In terms of its modus operandi, Tinba v3 relies on four principal fraud capabilities:

- A persistent user-mode rootkit;

- The ability to steal any set of credentials with a generic form grabber;

- MitB capabilities;

- Dynamic webinjection mechanisms.

Tinba v3 uses a few browser injection approaches. For example, the Trojan works with an automated transfer system (ATS) panel. ATS is fraudster lingo for a remote platform that Trojans access on the fly. The ATS contains transaction automation scripts, preprogrammed parameters and thresholds and mule account numbers that the malware relies on to complete illicit online transactions.

ATS was much more popular before two-factor authentication schemes came into the equation, but it is still effective in this case. The panels used by Tinba include dynamic social engineering designed to ask for the victim's one-time password and then plug it into the bank's page to complete the transaction.

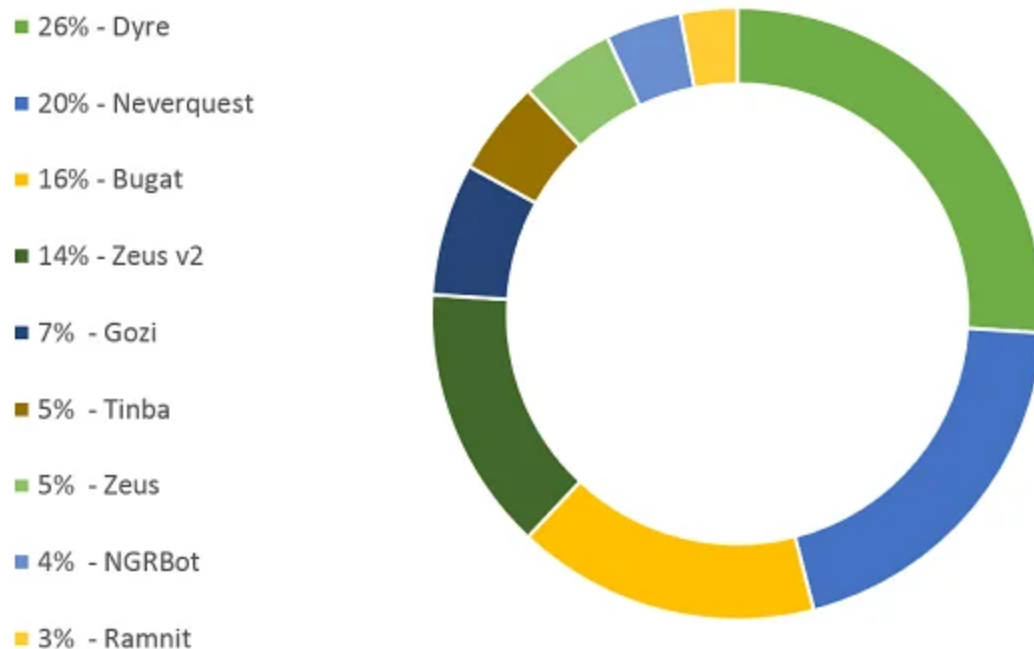
Another common webinjection approach Tinba v3 uses in its configurations is called FI-Grabber, short for full information grabber. This is lingo for an injection that asks the victim to key in a large amount of personally identifiable information (PII) and other private details about the account. These grabbers are accessed on a remote server and automatically match the most relevant injection to the bank the victim is browsing.

FI-Grabbers are actually a paid cybercrime service that promises effective injections leading to a successful transfer. This all happens in real time and without exposing the Trojan's actual injections inside the configuration file. Reaching out to an FI-Grabber is considered to be a more advanced means of manipulating Web sessions while still keeping the Trojan's secrets under wraps.

The malware's fraud scenario is similar to other Trojans of this grade: collect victims' credentials, grab PII and use social engineering to steal two-factor authentication codes. Actual illicit transactions generated from Tinba-infected users typically come from the victim's own device, which is indicative of the use of automation after the victim keys in the one-time password. Tinba-enabled illegitimate online banking operations take place via a remote transaction orchestration panel.

Threat Status

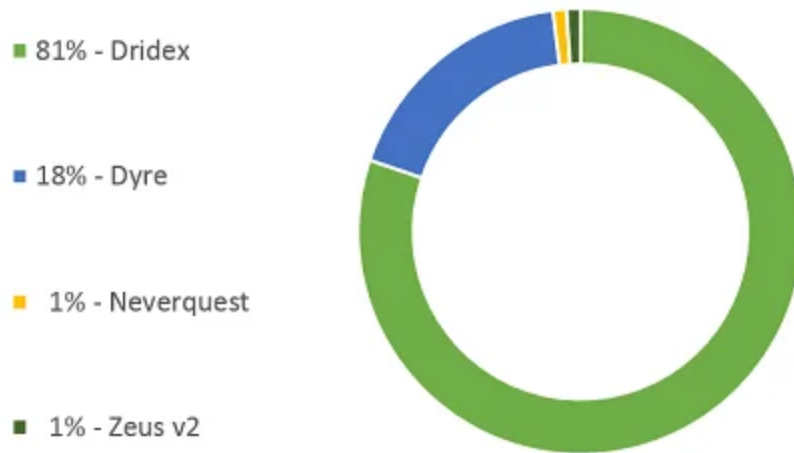
In terms of Tinba's proliferation this year, IBM Security data shows that this malware is ranked sixth in popularity. It is right behind Gozi, which is considered commercial malware.



Tinba v3 attacks online banking customers all over Europe, mainly targeting Poland, Italy, Germany and the Netherlands. Per IBM Security X-Force data, this is the very first time we identified any of the Tinba variations attacking in Romania.

What's Next for Romania?

Based on other Tinba v3 campaigns that IBM Security is familiar with, we expect to see more Tinba attacks in Romania going forward. The country may only be starting to face Tinba, but it is already plagued by the Dridex Trojan, Dyre, Neverquest and Zeus v2 variants. IBM Security data shows that, since the beginning of 2015, the most active Trojan in Romania is Dridex, but that could stand to change if Tinba accelerates its activity.



Since Tinba v3 webinjections are designed to harvest large amounts of personal information as well as two-factor authentication codes during the Web session, IBM Security recommends that banks alert their customers of the threat and refresh the online banking security education sections of their websites.

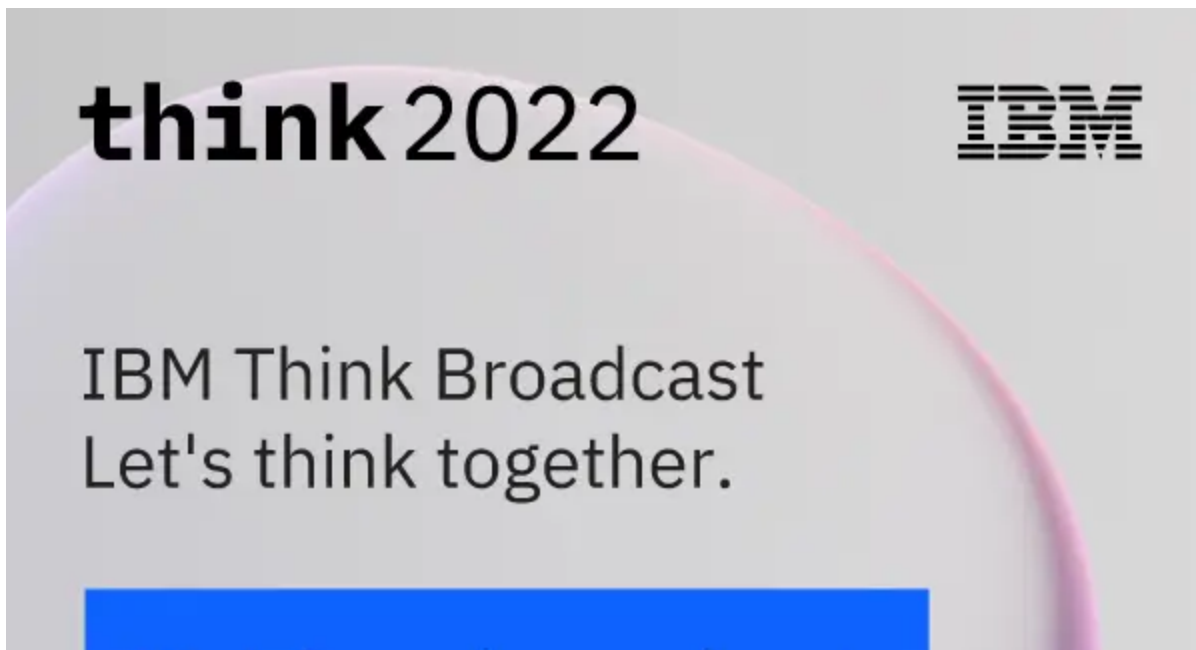
Romanian banks should ask customers to report suspicious emails. These financial institutions should also work closely with their antifraud provider to lower and contain risks as much as possible.

[Read the white paper: Staying ahead of threats with global threat intelligence](#)

[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 →