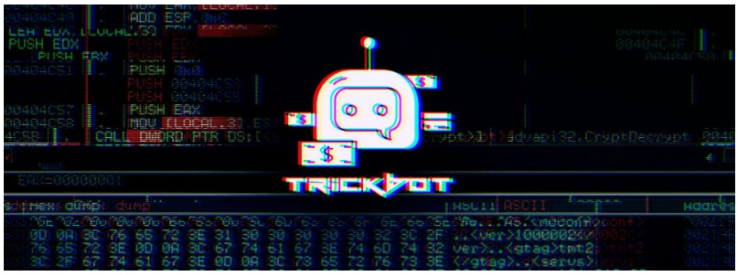
Global Campaign: Trickbot

TrickBot (also known as Trickster, TheTrick, and TrickLoader) is one of the most recent and popular bank trojans that have been used over these years. Is a modular trojan type malware originally designed to target and steal sensitive user information like bank accounts and email account passwords, but have been evolving through the years, being capable to make web injection (like server-side injections and redirection attacks), install malware (including ransomware) and steal a lot of information from the victims' machine. Such as cookies, Windows databases and even bitcoin wallets.



EVOLUTION AND UPDATES

Since its development in 2016, TrickBot has been changing its business model, and its growth has been based on major software updates. Initially, malicious actors carried out attacks directed at natural persons, where they took advantage of his operation as a sniffer to obtain information about the victim and proceeded to filter it through back doors. But over the years, its danger has dramatically increased. Thanks to a business model based on the three pillars of the industrial post-revolution (automation, decentralization and integration), TrickBot has become a completely flexible universal module of criminal solutions, reaching the point of being able to attack and hijack large information Corporations and banks.

Chronology:

• **(2016)** TrickBot is released. Its developers looked for ways to expand the borders of TrickBot, so they began adding functions and modules that allow transmission via email. (During this year, the initial victims of TrickBot were Australian banks, but at the end of November they increased, also threatening the banks of New Zealand, Great Britain, Germany and Canada).

• **(2017)** TrickBot is updated. The expansion of TrickBot was notorious thanks to the phishing campaigns carried out by its first version, but not enough, so a new version of TrickBot emerged, this time capable of spreading like a worm within the network after the initial infection. (The number of TrickBot targets increased, as it can now also collect data from electronic banking applications (such as PayPal), mail clients and web history in search of personal identifiers. In addition, it is also capable of stealing passwords and credentials of web browsers like Firefox, Chrome, MS-Edge and many others).

• **(2018)** TrickBot changes its structure. TrickBot now becomes a "malware solution", after all this "information gathering", developers began indexing stolen information and providing access to that information as a paid service. But this wasn't all its evolution, in addition, thanks to its new modular system, TrickBot became adaptable to any type of system (which made it much more infectious), reaching the point where it becomes a weapon that installs ransomware with its infections (using what is known today as "Ryuk" Ransomware).

• **(2019)** TrickBot "develops" an all-in-one attack framework known as "The Anchor", is a recompilation of tools that allows the actors (APTs) to leverage this framework against higher-profile victims. This structure was designed to secretly upload any kind of malware the attacker needs and clean up all of the evidence left on the attacked

machine.

INFECTION PROCESS

Like many existing banking Trojans, TrickBot is distributed through spam emails with malicious attachments (MS Office files or PDF files), which use the victim's naivety as a starting point to carry out its infection. Once the file is opened, the file implements a kind of macros that installs the Trojan and the infection begins.

WEB INJECTION

We cannot finish talking about TrickBot without first warning about one of the most dangerous uses that have been exploited by it. Since, as previously mentioned, within the modules that this malware possesses there is a specific one that very few people can correctly differentiate, this is web injection. Thanks to this module, TrickBot is capable of carrying out two types of attacks that are quite interesting to analyze: first, we have the ARP spoofing to web-fakes. And secondly, we have attacks from server-side injections (also known as Man-In-The-Browser).

Arp Spoofing to Web-Fakes

In this attack, TrickBot takes advantage of the victim's attempts to connect to his bank's website. How is this? Well, once the person enters the website address, the malware uses the computer's ARP table to redirect this request to a website that simulates the specific bank login page. This page is hosted by the malicious server (It is worth clarifying that the address in the browser of this website is the same as the original bank, only that it points to a different IP address, this is thanks to the redirection of ARP). Once the victim believes they are on their bank's website, they proceed to enter their login credentials, which allows the attacker to obtain them directly from the victim and can continue with the attack. After this, the infected user receives a waiting message while displaying the text "logging in" or "please wait" (this text can also change, depending on what the attacker wants to request from the user). While this happens, the attacker proceeds to log in to the bank of the affected party, where they can thoroughly analyze the victim's account and, if wish, can initiate an exfiltration of the victim's money.

Server-Side Injections

The server-side injection attack is a technique that TrickBot uses to hijack a victim's communications with a website. Unlike the previous attack, the malware allows the initial communication of the infected user with the original server of the website (e.g. banking). After this, the malware intercepts all Server-Client communications before these are processed in the browser and sends a response with malicious code to the infected client (this is achieved by injecting HTML or JavaScript elements into the browser).

Previous Topic
Mark Complete
Next Topic
Back to Lesson