Malware - TrickBot(TrickLoader)

Introduction :

TrickBot, AKA TrickLoader, is a banking trojan – a malware designed to steal banking credentials. It is aimed at corporate and private victims and utilizes techniques such as redirection attacks. It manipulates what the victim sees in the browser and redirects to a bank cabinet webpage forged by the hackers.

Reportedly, TrickBot tries to follow ransomware and has already stolen millions of dollars from banks in the United States of America, England, Australia, New Zealand, Canada, and Germany.

The first versions of this trojan used to target mostly corporate bank accounts, the same as ransomware, aiming at a specific regional banking platform used by American banks.

The malware is thought to be created by the same team of criminals known for developing another dangerous trojan – Dyre, which has been active until 2015 and reportedly successfully stolen millions of dollars for the Ryanair airline. Dyre rapidly stopped operating in 2015 after Russian authorities seized a group of hackers. However, this connection has never been proven definitively.

It’s speculated that some hackers from the group managed to avoid Russian authorities and came together to create Dyre's successor – TrickBot. This version is supported by the fact that TrickBot’s source code appears to be a rewrite of Dyre, albeit upgraded and refined utilizing C++ instead of Dyre, which mostly utilized C.

Through its lifespan, TrickBot malware developers have upgraded the functionality of the virus multiple times, adding new features and improving the banking trojan, and changing target banks, making their attacks highly unpredictable. Among other updates, TrickBot received support for the EternalBlue exploit, thus allowing it to spread over corporate networks. By August 2016, the malware gained email and browser history theft functionality. In September 2016, the virus learned to steal cryptocurrency by interjecting the normal payment process and stealing the coins when the user fills in personal and payment information on a payment gateway, grabbing the valuable tokens and redirecting them to a wallet that belongs to the hackers.

Impact :

TrickBot is an advanced banking trojan that attackers can use to steal payment credentials from the victims. It can redirect the victim to a fake banking cabinet and retrieve credentials typed in on the webpage.

Working :

The virus utilizes a sophisticated method for infections which allows it to stay undetected by antivirus software. Instead of keeping configuration files locally on the user's machine, TrickBot is able to receive this data from C2 in real-time. Particularly, when a victim heads to one of the target web pages, TrickBot intersects the HTTP response of the website while sending the following information to C2:

* A complete URL of the target bank website that the user navigates to
* A whole HTTP query
* HTML code of the webpage that the victim is trying to view

The C2 server then sends a new HTML markup that includes the malicious parts to the user, and instead of visiting a bank account, the user ends up on a forged page.

Distribution of this Malware :

TrickBot trojan is distributed with malspam and phishing campaigns but unlike ransomware, it is powered by the Necurs botnet, which has become extremely popular among attackers who utilize the malware-as-a-service business model.

Attackers will usually try to threaten and scare the victim to make the victim read the email and download any attached files. Finally, the trojan itself manages to get on a victim's machine through an Excel document that contains a macro programmed to download and start the execution of the banking trojan. However, In some of the more recent campaigns, HTML attachments have been included in the emails. Programmed to download Microsoft Office documents, the use of HTML attachments helps to avoid detection by antivirus software. What’s more, In the very last distribution campaigns, the attackers have started utilizing eFax ploys, tricking victims into clicking on VBS extensions that contain the virus.

How to defend from Trickbot :

Since the virus is often distributed in Microsoft Office files, it needs macros or the Microsoft Office's editing mode to be activated to enter an active phase. As long as both macros are deactivated, and the editing mode is switched off, the virus will pose no danger to a PC.