Trickbot RFI Response

Summary

Trickbot, a malware developed by the Wizard Spider group, was first discovered in 2016 as a Windows-based Trojan that steals banking credentials. It has since evolved into modular crimeware platform that can also infect Linux systems, capable of self-propagation, bypassing security software, credential harvesting, creating backdoor persistence, and dropping additional malwares.

Trickbot primarily spreads and infects systems through spearphishing and malspam using emails with malicious macro-embedded Office documents. Recently, the group has been found to have partnered with other malicious actors to diversify the delivery method. Hijacked email threads, fake customer response forms, and fake call centers are all possible ways for Trickbot to gain a foothold on a machine.

Once a machine is infected, the Trickbot operators install keyloggers and harvest credentials on the compromised machine to attempt to move laterally in the network. They gather and exfiltrate information from each system they have access as well as install a ransomware. Once they have accessed and exfiltrated everything they can, they trigger the ransomware to demand payment from the victim.

Threat to Institution

Given that the Trickbot started as a banking Trojan, if the operators manage to harvest banking credentials from the institution's clients, they will most likely attempt to access the online bank accounts to perform wire fraud and bank fraud. Even without banking credentials, if they obtain personal information, they can attempt identity fraud or sell the information online. This would have a significant impact in the privacy of the firm's clients, causing clients to not trust the firm's ability to protect their information and damaging the firm's reputation.

Furthermore, the installation of the ransomware means immediate financial consequence. Once the ransomware encrypts the files on the network, the only way to regain access is to either pay the ransom or rebuild, neither being a cheap solution. Either way, the loss of access to the encrypted data will disrupt the firm's operations and impact revenue.

Indicators of Compromise

There are over a hundred variations of Trickbot and there are numerous different possible indicators of compromise. Below are some indicators and what they might entail.

hxxp[:]//mulenoras[.]space/333g100/index.php

It is likely that Trickbot partnered with Hive0107 for this attack, with the link delivered via the organization's online contact form claiming either a copyright infringement by the firm or that the firm has been performing a denial-of-service attack against them. There is a good chance that the malwares BazarLoader, Cobalt Strike, and Trickbot are all on the compromised machine and ultimately the malicious actors will launch a ransomware attack.

hxxp[:]ds1.devicevm[.]com/

The URL is associated with Splashtop Streamer, which is a software that allows another device to remotely access the machine. The machine that hit the endpoint is compromised and most likely is being used as a foothold for lateral movement.

185[.]234[.]15[.]183

This IP is in a PasteBin list of IPs associated with TrickBot posted in 2018. It is possible that Trickbot is using this IP address again.

212[.]192[.]246[.]14

This IP has been known to send spam as well as display irregular SMTP client behaviors. Any host attempting to reach this IP is most likely compromised.