Lab Specification: Trickbot

The user views the state of the machine before infection. They then infect the machine with Trickbot and identify indicators of compromise.

Info

Quick Summary

Trickbot is a trojan, first discovered in September 2016 by Fidelis. It is a powerful tool used as part of multi-stage attacks.

Trickbot started life as an evolution to the Dyre banking trojan. Since then it has continuously expanded to become a powerful multi-faceted tool. Numerous attacks have been conducted using Trickbot including ransomware and login credential theft.

Compromise

Trickbot is usually delivered through a phishing email with a malicious attachment. It gains persistence through scheduling a task and connects to a hardcoded C2 server to await further instructions such as to download additional malware.

Once inside a network, Trickbot can spread laterally - sometimes using the EternalBlue exploit. For more information on EternalBlue, see the WannaCry lab.

Indicators of Compromise

In practice, analysing network logs is the best method for detecting widespread compromise across a network.

It can be difficult to notice infection on a sole machine. However, there are a few indicators:
- A task (such as 'Bot') will be scheduled that starts a file (such as 'Sweezy.exe').
- Files will be created in C:\Windows\User\AppData\Roaming.

Tasks

Set Up

A Windows machine without network connectivity and Microsoft Defender Disabled.

An infected Word document should be present on the desktop that contains a macro to start the predownloaded malware executable (as opposed to downloading the executable from a URL).

Tasks

1) The user counts the number of scheduled tasks on the machine prior to infection. This is the first token.
2) The user counts the number of folders in the AppData folder for the second token.

The user opens the infected Word document.
3) The user finds the name of or other information relating to the new task that has been scheduled.
4) The user finds the name of the new folder that has been created in the AppData folder.

References

Fidelis Original Article
Bleeping Computer Early Analysis
Malwarebytes Analysis
NCSC Advisory
CISA Fact Sheet: Trickbot Malware