Trickbot (Worm Module)

Threat: **Information Stealer**

Author: **Jeffrey Farnan** Date Originally Published: **October 29th, 2021**

1. SUMMARY

- Trickbot is best known as a banking Trojan that steals sensitive information and also acts as a dropper for other malware. Trickbot can be best described as Hybrid Malware, it can be combination of Trojan, Ransomware or self-replicating worm all built into a single cyberattack package. Here we will focus on Trickbot's complex and stealthy worm module.

2. MALWARE FAMILY

- **Type** = Information Stealer.
- **Sub-type** = Worm.
- Traditionally the TrickBot malware was a banking Trojan, or information stealer, with its updated modular design, and with a wide range of plugins, it can perform a wide range of tasks. With modern Malware such as Trickbot an attack is carried out in stages, using modules to separate the code and can be loaded into memory when needed. One of the first stages of the attack is loading the worm module so it can get connected to network itself to spread to other hosts.

3. MALWARE CHARATERISTICS

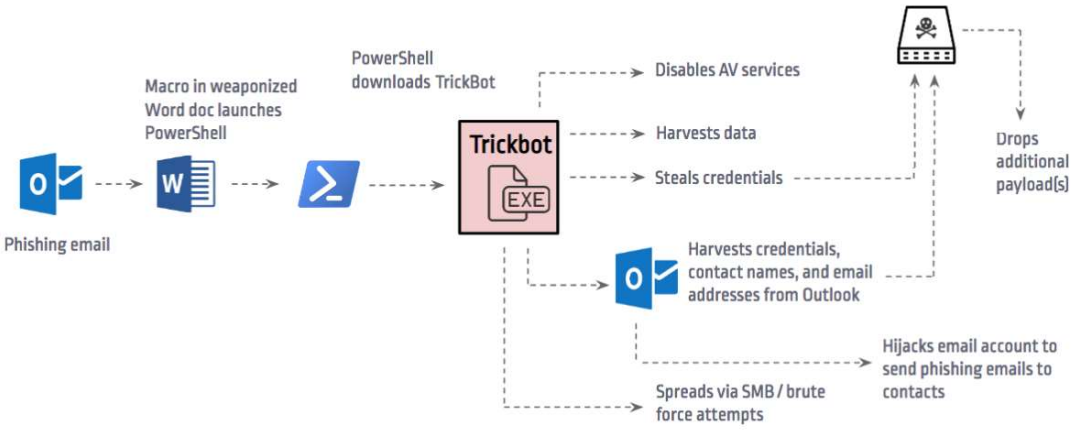
- **Suspected country of origin** = Russia.
- **First seen date/period** = October 2016.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = January 22th, 2020.

4. MALWARE HISTORY

- Trickbot was first discovered is 2016 and was primary know as a financial Trojan, targeting the customers of major banks. Trickbot is believed to have evolved from an earlier botnet known as Dyre or Dyreza. In Trickbot the worm is a separate module designed to spread throughout the network, download other malware and is under the command of the attacker. In the past a worm was defined as a malicious program which resides on a single computer, searchers for other clients and servers, replicates itself and spreads throughout the network. The past few years has seen the Trickbot worm module become more complex and stealthy.

5. MALWARE DESCRIPTION

- Trickbot is delivered via malspam campaigns, the emails are included with a Microsoft Word or Excel document. When the attachment is opened, you are prompted to enable macros, when confirmed executes a VBScript to run a Powershell script to download the malware. When Trickbot runs it checks to ensure it's not running in a sandbox environment. It disables Microsoft Defender and any other AV on the system. Modules are downloaded separately usually in dynamic link library (dll) files.



- Trickbot comes with an exe installer which loads the Dynamic Link Libraries (DLLs) files into memory. These are known as the modules and each module has a specific purpose:
    - **Disables Av services** - remain persistence and go undetected while carrying out its business.
    - **Harvests data** - collects all different types of data from system and network information, email accounts, tax information, etc.
    - **Steals credentials** - grab's credentials, is used to authenticate remote servers
    - **Spreads via SMB** - has a worm module which allows it to spread throughout the network
    - **Drops additional payloads** - additional payloads is easily implemented and download, an example is the Ryuk ransomware, which locks machines across the network.

- Modern malware is separated into components or modules each designed with a specific task. Trickbot's authors created the worm module after seeing the speed and effectiveness of the WannaCry worm and created its own worm spreading module which they called Mworm. This worm abuses the Server Message Block (SMB) and Lightweight Directory Access Protocol (LDAP) moving laterally across networks.

- An update to MWorm was seen by researches in April 2020, this new modular function is called Nworm. Nworm encrypts the Trickbot executable and launches the infection from memory, leaving behind no traces on the Hard Drive and harder for AV venders to detect it.

6. POTENTIAL CUSTOMER DEFENSE

Modern malware is changing all the time, to help protect your computer systems and networks here is some helpful tips:

- Have the latest version of the Windows10 and run the latest windows updates.
- Don't open any suspicious emails with attachments.
- Disable the use of SMBv1 the network communication protocol, and update to SMBv2.
- Use an Intrusion Detection System (IDS) system on your network, and keep up to date with the latest signatures.
- Keep up to date with the latest security news, learn about new TrickBot infections and how they are implemented.

Research Sources:

- https://www.cyclonis.com/trickbot-malware-new-tricks-coronavirus-themed-samples-fool-security-products-target-telecommunication-companies/
- https://kc.mcafee.com/corporate/index?page=content&id=KB92380
- https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-now-steals-rdp-vnc-and-putty-credentials/
- https://blog.f-secure.com/what-is-trickbot/
- https://www.greenviewdata.com/blog/trickbot-trojan-fake-bank-america-and-amazon-email
- https://www.cisecurity.org/white-papers/security-primer-trickbot/

Disclaimer: All opinions expressed in this article are the opinions solely of the author.