Trickbot: A primer

blog.talosintelligence.com/2020/03/trickbot-primer.html

By Chris Neal

Executive Summary

- Trickbot remains one of the most sophisticated banking trojans in the landscape while constantly evolving.
- Highly modular, Trickbot can adapt to different environments with the help of its various modules.
- The group behind Trickbot has expanded their activities beyond credential theft into leasing malware to APT groups.

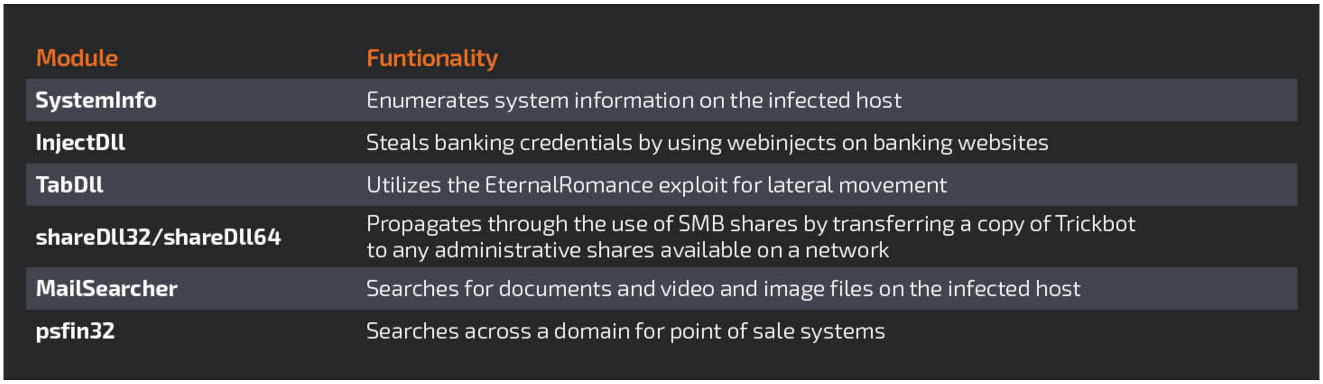
Overview

In recent years, the modular banking trojan known as Trickbot has evolved to become one of the most advanced trojans in the threat landscape. It has gone through a diverse set of changes since it was first discovered in 2016, including adding features that focus on Windows 10 and modules that target point of sale (POS) systems. Not only does it function as a standalone trojan, Trickbot is also commonly used as a dropper for other malware such as the Ryuk ransomware. The wide range of functionality allows this malware to adapt to different environments and maximize effectiveness in a compromised network.

Trickbot is typically delivered via a spam email containing a malicious document or malicious URL. In most cases, the subject of the emails will contain wording that is intended to alarm the person who received it, such as an issue with a credit or debit card, and in recent examples preying on fears of the COVID-19 virus. Once this document has been opened, a macro will execute and download the next stage of the infection process. In some cases, the second stage of this infection chain is a loader like Emotet which in turn drops Trickbot. In a reverse of roles, Trickbot has also been commonly observed to drop other malware families.

Functionality

A successor to the Dyre trojan, Trickbot was originally designed to steal and exfiltrate sensitive information from a compromised host through stealing cookies from browsers or performing webinjects on banking or cryptocurrency trading sites. Over the years, Trickbot has not only expanded that functionality, but also added new features such as the ability to be used as a dropper for other malware. Trickbot is highly modular and can be configured by the threat actor depending on the environment being targeted. Trickbot has a wide range of capabilities enabled by the different modules that can be installed remotely. Here's a rundown of a few of the modules:



Module	Funtionality
SystemInfo	Enumerates system information on the infected host
InjectDll	Steals banking credentials by using webinjects on banking websites
TabDll	Utilizes the EternalRomance exploit for lateral movement
shareDll32/shareDll64	Propagates through the use of SMB shares by transferring a copy of Trickbot to any administrative shares available on a network
MailSearcher	Searches for documents and video and image files on the infected host
psfin32	Searches across a domain for point of sale systems

A recent addition to the Trickbot arsenal of modules is "rdpScanDll" which allows the malware to brute-force Remote Desktop Protocol (RDP) credentials. The list of available modules for Trickbot is growing larger with time which shows that the authors are actively looking for new ways to use it for financial gain. The creators have shown repeatedly that they are persistent in regards to improving the functionality of Trickbot and its modules, and should be considered as a significant threat.

Trickbot employs several different techniques for obfuscation and evasion. TLS is used for command and control (C2) communications and while downloading the various modules for installation. C2 typically happens on the standard TLS port 443 but has also been observed to use port 449 on occasion. TLS is not the only form of encryption used by Trickbot. While exfiltrating sensitive information from a compromised host, the Microsoft CryptoAPI is used to encrypt the data as an extra layer of obfuscation.

There are several different obfuscation and evasion techniques that Trickbot has used throughout its lifetime including process hollowing, Heaven's Gate, custom base64 encoding and bypassing UAC. Trickbot has added functionality that is tailored specifically to Windows 10 after Microsoft dropped extended support for Windows 7 in early 2020. Earlier this year, a new feature was added which allowed fileless UAC bypass through the use of "WSReset.exe," a Microsoft signed binary used to reset Windows Store settings.

Trickbot Gang

The actors behind Trickbot are commonly referred to as the "Trickbot Gang." Financial gain is the primary motive for this group's actions. The group's operations have grown along with the malware itself. At the time of this writing, the group has ventured into pushing a malicious Android application to victims whose Windows machines have been infected with Trickbot. The intent is to convince the user to install the application on their Android phone, which steals one-time codes that banks send as part of a 2FA sequence. Currently, this attack has only been observed in Germany, but it is likely the use of this technique will increase if it proves to be effective.

Trickbot Gang also rents a Trickbot variant to state-sponsored APT groups. Not only are they supplying the malware, but they are also selling the access they have gained to high profile networks across the globe. This cooperation reflects the trend in recent years of state-sponsored cyber espionage groups interacting with cyber criminal organizations.

One of the most devastating threats that Trickbot poses is the delivery of the Ryuk ransomware with the help of Emotet. This has proven to be a dangerously effective combination, generating millions of dollars of income in 2019 alone. The reason for this combination of malware is that the Trickbot modules for lateral movement are an efficient means to propagate across a network before deploying Ryuk.

How to defend against Trickbot

To defend against Trickbot it is important to ensure a well organized, multi-layered cybersecurity program is in place within your organization.

1. Email and spam filters are critical in the case of Trickbot as this is the initial infection vector.
2. Perform regular updates and system hardening as Trickbot uses known Windows SMB exploits for propagation.
3. Give employees regular phishing training and conduct regular awareness programs.
4. Employ strong password policies and use multi-factor authentication, such as Duo.
5. Ensure updated endpoint security software, such as Cisco's AMP Endpoint, is deployed across your network.

Practical security hygiene is critical in any given scenario but in the case of defending against Trickbot — it is even more important to maintain a strong security posture. Due to the modular nature of Trickbot, it is impossible to predict how it will behave once it has an initial foothold, hence the importance of preventative security measures.