MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Security Primer
March 2019 • SP2019-0510

TrickBot

TrickBot is a modular banking trojan that targets user financial information and acts as a dropper for other malware. It uses man-in-the-browser attacks to steal financial information, such as login credentials for online banking sessions. The malware authors are continuously releasing new modules and versions of TrickBot. TrickBot is disseminated via malspam campaigns. These campaigns send unsolicited emails that direct users to download malware from malicious websites or trick the user into opening malware through an attachment. TrickBot is also dropped as a secondary payload by other malware, most notably by Emotet. Some of TrickBot's modules abuse the Server Message Block (SMB) Protocol to spread the malware laterally across a network.

The malspam campaigns that deliver TrickBot use third party branding familiar to the recipient, such as invoices from accounting and financial firms. The emails typically include an attachment, such as a Microsoft Word or Excel document. The opened attachment will prompt the user to enable macros, which executes a VBScript to run a PowerShell script to download the malware. TrickBot runs checks to ensure it is not in a sandbox environment and then attempts to disable antivirus programs, such as Microsoft's Windows Defender. Once executed, TrickBot redeploys itself in the "%AppData%" folder and creates a scheduled task that provides persistence.

TrickBot sends HTTP requests to the following websites to collect the infected host's public IP address:

- hxxp://myexternalip.com/raw
- hxxp://api.ipify.org
- hxxp://icanhazip.com
- hxxp://bot.whatismyipaddress.com
- hxxp://ip.anysrc.net/plain/clientip

At this point, TrickBot starts receiving instructions from the command-and-control (C2) server and is ready to download modules, which are sent with a configuration file. The modules are delivered as Dynamic Link Libraries (DLLs). After receiving the infected host's system information, the initial TrickBot C2 sends an expiration time and a new IP address that will be used to download further modules. The C2 servers constantly change and the TrickBot infection is updated with this new information. TrickBot uses HTTP/HTTPS GET and POST requests to download modules and report stolen information/credentials to the C2 server.

TrickBot uses two types of web injects, 'redirection attacks' and 'server side injections', to steal financial information from online banking sessions to defraud its victims.

- **Redirection attacks** send victims to fraudulent banking site replicas when they navigate to certain banking websites. This fake website is hosted on the cyber threat actor's (CTA) malicious server and harvests the victim's login information.
- A **server side injection** intercepts the response from a bank's server, injects additional client-side code into the webpage, and can steal the victim's banking credentials through

form grabbing. Form grabbing records sensitive information typed into HTML forms, rather than capturing all keystrokes as with a keylogger.

TrickBot's distributors are using group tags (gtags) to uniquely identify specific TrickBot campaigns. The gtag and a unique bot identifier are included in the Uniform Resource Identifiers (URIs) when TrickBot communicates with its C2 servers.

TrickBot's modules perform tasks for stealing banking information, system/network reconnaissance, credential harvesting, and network propagation. The following is an overview of common TrickBot modules and configuration files, but this is not an exhaustive list since TrickBot is constantly adding new features.

Banking Information Stealers

- **LoaderDll/InjectDll –** Monitors for banking website activity and uses web injects (e.g. pop ups and extra fields) to steal financial information.
- **Sinj –** This file contains information on the online banks targeted by TrickBot. It uses redirection attacks (also known as web fake injections). Redirection attacks send victims to fraudulent banking site replicas when they navigate to certain banking websites. This fake website is hosted on the CTA's malicious server and harvests the victim's login information.
- **Dinj –** This file also contains information on the online banks targeted by TrickBot. It uses server side web injections. A server side web injection intercepts the response from a bank's server, injects additional client-side code into the webpage, and can steal the victim's banking credentials through form grabbing. Form grabbing records sensitive information typed into HTML forms, rather than capturing all keystrokes as with a keylogger.
- **Dpost –** Includes an IP address and port for stolen banking information. If the user enters banking information for one of the listed banks, the information is sent to the dpost IP address. Most of the data exfiltrated by TrickBot is sent to the dpost IP address.

System/Network Reconnaissance

- **Systeminfo –** Harvests system information so that the attacker knows what is running on the affected system.
- **Mailsearcher –** Compares all files on the disk against a list of file extensions.
- **NetworkDll –** Collects more system information and maps out the network.

Credential and User Information Harvesting

- **ModuleDll/ImportDll –** Harvests browser data (e.g. cookies and browser configurations).
- **DomainDll –** Uses LDAP to harvest credentials and configuration data from domain controller by accessing shared SYSVOL files.
- **OutlookDll –** Harvests saved Microsoft Outlook credentials by querying several registry keys.
- **SqulDll –** Force-enables WDigest authentication and utilizes Mimikatz to scrape credentials from LSASS.exe. The worming modules use these credentials to spread TrickBot laterally across networks.
- **Pwgrab –** Steals credentials, autofill data, history, and other information from browsers as well as several software applications.

Network Propagation

- **WormDll and ShareDll** – These are worming modules that abuse Server Message Block (SMB) and Lightweight Directory Access Protocol (LDAP) to move laterally across networks.
- **TabDll –** Uses the EternalRomance exploit to spread via SMB.

RECOMMENDATIONS:

The MS-ISAC recommends organizations adhere to the following general best practices, to limit the effect of TrickBot and similar malspam in your organization.

- Use antivirus programs on clients and servers, with automatic updates of signatures and software.
- Disable all macros except those which are digitally signed.
- Apply appropriate patches and updates immediately after appropriate testing.
- Implement filters at the email gateway to filter out emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- If you do not have a policy regarding suspicious emails, consider creating one and specifying that all suspicious emails should be reported to the security and/or IT departments.
- Implement Domain-Based Message Authentication, Reporting & Conformance (DMARC), a validation system that minimizes spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures.
- Mark external emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails.
- Provide social engineering and phishing training to employees. Urge them to not open suspicious emails, click on links contained in such emails, post sensitive information online, and to never provide usernames, passwords and/or personal information to any unsolicited request. Teach users to hover over a link with their mouse to verify the destination prior to clicking on the link.
- Adhere to the principle of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators.
- Adhere to best practices, such as those described in the CIS Controls, which are part of the CIS SecureSuite.

If a user opened a malicious email or an infection is believed to exist, we recommend running an antivirus scan on the system and take action based on the results to isolate the infected computer. If multiple machines are infected:

- Identify, shutdown, and take the infected machines off the network.
- Do not login to infected systems using a domain or shared local admin accounts.
- Issue password resets for both domain and local credentials.
- As TrickBot scrapes additional credentials, consider password resets for other applications that may have had stored credentials on the compromised machine(s).
- Determine infection vector to see if there was a different primary infection, such as Emotet dropping TrickBot. A TrickBot infection could indicate that there is an active Emotet or other infection on the network and vice versa.

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well

as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.