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

Security Primer
September 2019 • SP2019-0962

TrickBot

TrickBot is a modular banking trojan that targets sensitive information and acts as a dropper for other malware. Since June 2019, the MS-ISAC is observing an increasingly close relationship between initial TrickBot infections and eventual Ryuk ransomware attacks. The malware authors are continuously releasing new modules and versions of TrickBot to expand and refine its capabilities. TrickBot uses man-in-the-browser attacks to steal financial information, such as login credentials for online banking sessions. Additionally, some of TrickBot's modules abuse the Server Message Block (SMB) Protocol to spread the malware laterally across a network.

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.

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 determine 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) server and harvests the victim's login information.

- A **server side injection** intercepts the response from a bank's server and redirects it to the CTA's server. The CTA's server injects additional code into the webpage before it is returned to the client. The CTA can then steal the victim's banking credentials through form grabbing. Form grabbing records sensitive information typed into HTML forms, such as usernames and passwords.

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 and it uses redirection attacks (also known as web fake injections).
- **Dinj –** This file contains information on the online banks targeted by TrickBot and it uses server side web injections.
- **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 (CVE-2017-0147) to spread via SMBv1.

RECOMMENDATIONS:

The MS-ISAC advises SLTT government entities to adhere to the following recommendations to prevent, detect, and remediate TrickBot infections:

To help prevent TrickBot infections:

- Provide social engineering and phishing training to employees.
- If you do not have a policy regarding suspicious emails, consider creating one and specify that all suspicious emails should be reported to the security and/or IT departments.
- Mark external emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails.
- Apply applicable patches and updates immediately after appropriate testing.
- Implement filters at the email gateway for emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- To lower the chance of spoofed or modified emails, implement Domain Message Authentication Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards. (CIS Subcontrol 7.8)
- Organizations should consider using application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets (CIS Subcontrol 2.7). Organizations should also ensure that the application whitelisting software only allows authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) to run on a system (CIS Subcontrol 2.9).
- Adhere to the principal of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators.
- Implement a centrally-managed, up-to-date anti-malware solution (CIS Subcontrol 8.2). In addition to valuable preventive and corrective capabilities, detective controls provided by anti-malware software are beneficial in providing awareness of any threats which may become active within the environment.
- If not already being done, consider implementing an Intrusion Detection System (IDS) to detect command and control (C2) activity and other potentially malicious network activity, such as the MS-ISAC's Albert system.
- Ensure that systems are hardened with industry-accepted guidelines, such as those provided by the CIS Benchmarks division. (https://www.cisecurity.org/cis-benchmarks/)
- Disable the use of SMBv1 across the network and require at least SMBv2 to harden systems against Network Propagation modules used by TrickBot.

If a TrickBot infection is identified:

- Disable Internet access at the affected site to help minimize the extent of exfiltration of credentials associated with external, third-party resources.
- Review impacted subnets to identify multi-homed systems which may adversely impact containment efforts. Also, consider temporarily taking the network offline to perform identification, prevent reinfections, and stop the spread of the malware.
- Identify, shutdown, and take the infected machines off the network.
- Heighten monitoring of SMB communication or outright block it between workstations, and configure firewall rules to only allow access from known administrative servers.

- Assess the need to have ports 445 (SMB) open on systems and, if required, consider limiting connections to only specific, trusted hosts.
- Start with remediation of multi-homed systems (e.g. Domain Controller, File Server) as these can communicate across Virtual Local Area Networks (VLANs) and can be a potential means for spreading malware.
- Create clean VLANs that do not have access to infected VLANs. After the systems have been reimaged or restored from a known good backup, place them on the clean VLAN.
- Do not login to infected systems with domain or shared local administrator accounts. This is the best remediation strategy since TrickBot has several ways of gaining access to credentials.
- As TrickBot is known for scraping both domain and local credentials, it is recommended that a network-wide password reset take place. This is best done after the systems have been cleaned and moved to the new VLAN. This is recommended so new passwords are not scraped by the malware.
- Apply host-based isolation via Windows Firewall Group Policy Objects (GPOs), host-based intrusion detection system/network intrusion detection system (HIDS/NIDS) products, a Private Virtual Local Area Network (pVLAN), or similar means to help mitigate propagation.
- Determine the infection vector (patient zero) to determine the root cause of the incident.

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.