Trickbot: U.S. Court Order Hits Botnet's Infrastructure

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption

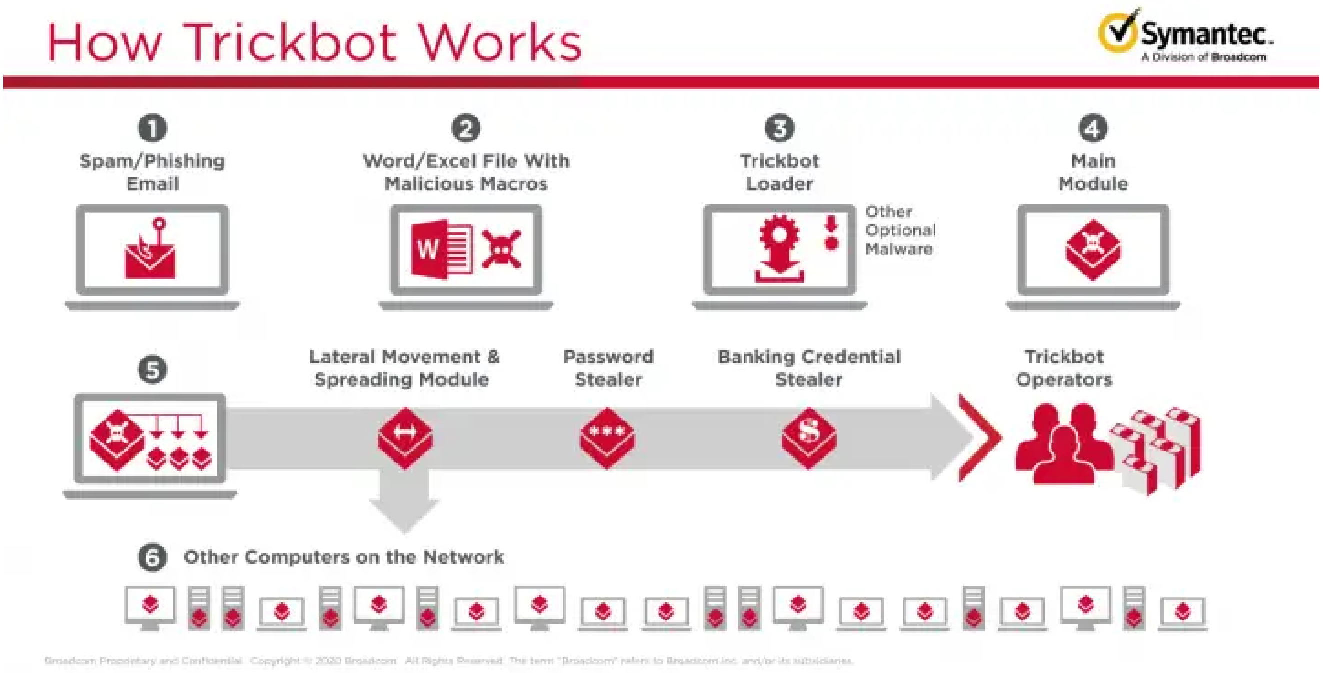
How Trickbot Works
Symantec. A Division of Broadcom
1 Spam/Phishing Email
2 Word/Excel File With Malicious Macros
3 Trickbot Loader
Other Optional Malware
4 Main Module
5
Lateral Movement & Spreading Module
Password Stealer
Banking Credential Stealer
Trickbot Operators
6 Other Computers on the Network
Broadcom Proprietary and Confidential. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Figure. How the Trickbot botnet works

What is Trickbot?

Trickbot is a major botnet consisting of computers that have been infected with the Trickbot Trojan (Trojan.Trickybot). The Trojan is modular in nature, meaning it can easily be customized with one or more of an array of custom components designed to carry out a range of malicious activities on infected computers. To date, it has mainly been used for two main purposes: stealing credentials from infected computers and acting as a distribution channel for other malware. Symantec believes that Trickbot's operators earn most of their revenue from selling stolen credentials on the cyber underground and leasing out the botnet as a distribution channel for other malware authors.

Trickbot is spread through spam and phishing email campaigns which usually bear a Microsoft Word attachment containing malicious macros. If the document is opened by the unsuspecting user, Trickbot will be installed on the victim's computer. In some cases, other malware, particularly ransomware, is also installed on the victim's computer.

Trickbot will also attempt to leverage known software vulnerabilities to move across the victim's network and install itself on other computers.

How Trickbot works

Trickbot is modular malware, capable of performing a range of different malicious activities. The first module to be installed on the victim's computer is the loader, which contains an encrypted list of IP addresses from which it can download its main module.

Once downloaded, the main module will check the architecture of the victim computer and save this along with the bot's own information. The main component then prepares a framework for additional modules and initiates a connection to one of a pre-configured list of command and control (C&C) servers.

The main module downloads one or more additional modules. Known modules include:

- Banking credential stealer (injectDll): For injecting malicious content into browser windows displaying banking websites in order to steal credentials
- Reconnaissance module (networkDll): For gathering system information and network/domain topology to determine whether the device can be infected with ransomware
- Data stealer (importDll): For stealing data from a web browser
- Password grabber (Pwgrab: For stealing passwords from various locations
- Cookie stealer (cookiesDll): For stealing cookies from the infected computer
- Information stealer (mailsearcher): For searching all files in all drives in the system looking for specific information
- Point-of-Sale recon (psfin): Reconnaissance module to determine if there are any Point-of-Sale (POS) devices connected
- Remote control module (vncDll): Virtual Network Computing (VNC) module

- SMB spreader (tabDll): For spreading over Server Message Block (SMB) using the EternalRomance exploit and other vulnerabilities patched by Microsoft in March 2017 (MS17-010)
- Outlook stealer (outlookDll): For stealing data saved by Microsoft Outlook
- Lateral movement module (shareDll): For lateral movement/enumeration via Lightweight Directory Access Protocol (LDAP) and SMB exploitation
- Lateral movement module (wormDll): For lateral movement/enumeration via LDAP and SMB exploitation. The shareDll and wormDll modules work in cooperation.
- RDP brute-force module (rdpScanDll): A new module that uses brute-forces the Remote Desktop Protocol (RDP) for a specific list of victims

Stealthy threat

Trickbot includes a number of features designed to minimize the risk of detection by security software. For example, the main module is designed to evade execution within “sandboxes,” which are controlled environments used by security companies to analyze malware.

This module will also check the current user’s privileges and, if they have low privileges, it will elevate them using User Access Control (UAC) bypass, a technique that allows execution of programs with elevated privileges without the user being prompted.

When it obtains elevated privileges, Trickbot will attempt to identify any security software that is installed on the computer and attempt to stop it and end any related services.

Credential theft

One of the main threats for Trickbot victims is credential theft. This is carried out by a module that monitors for browser visits to a pre-configured list of banking websites. If the user visits any of these websites, the module intercepts and alters network traffic between the computer and the website, allowing the attackers to steal the victim’s banking credentials after they are input by the user.

Trickbot will also attempt to steal other credentials from Chrome and Internet Explorer’s password storage features, from various RDP and SSH related services, and from other password managers.

Immediate threat

While infected computers are added to the Trickbot botnet, they yield the most value to attackers immediately after infection. Other malware families are usually delivered at the point of initial infection. Credential theft happens immediately after infection, while banking credentials are stolen the first time the victim attempts to log into their bank. Even if the malware is subsequently detected and the computer is removed from the botnet, much of the damage will have been done at this point, with stolen credentials exfiltrated by the attackers and likely sold to other cyber criminals.

Ongoing battle

By pooling resources and intelligence and utilizing available legal avenues, the information security and financial sectors hope to strike a major blow against Trickbot. Symantec is grateful for the leadership of Microsoft and FS-ISAC and the support of ESET, NTT, and Lumen Technologies. This latest action, however, is just one step in an ongoing campaign. Complete eradication of this botnet will likely require additional actions from government partners in multiple jurisdictions. However, this action proves that successful private industry collaboration can be effective in countering cyber-crime and we hope that this set a new precedent for further initiatives.

Protection

The following protections are in place to protect customers against Trickbot activity:

- Trojan.Trickybot
- SONAR.Trickybot
- Trojan.Trickybot!g7
- Trojan.Trickybot!g8
- Trojan.Trickybot!g11
- Trojan.Trickybot!g13
- Trojan.Trickybot!g16
- Trojan.Trickybot!gen2
- Trojan.Trickybot!gen5
- Trojan.Trickybot!gm

Mitigation

Symantec recommends users observe the following best practices to protect against Trickbot attacks:

- **Enable 2FA** to prevent compromise of credentials.
- **Harden security architecture around email systems** to minimize the amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.
- **Restrict access to RDP Services:** Only allow RDP from specific known IP addresses and ensure you are using multi-factor authentication.

- **Implement proper audit and control of administrative account usage:** You could also implement one-time credentials for administrative work to help prevent theft and usage of admin credentials.
- **Create profiles of usage for admin tools:** Many of these tools are used by ransomware attackers to move laterally undetected through a network. A user account that has a history of running as admin using PsInfo/PsExec on a small number of systems is probably fine, but a service account running PsInfo/PsExec on all systems is suspicious.