Trickbot Gang Evolves, Incorporates Account Checking Into Hybrid Attack Model

flashpoint-intel.com/blog/trickbot-account-checking-hybrid-attack-model/

November 22, 2017

Blogs

Blog

Individuals who reuse login credentials across multiple sites are more susceptible to account checking attacks, which occur when threat actors use credentials stolen from past database breaches or compromises to gain unauthorized access to other accounts belonging to the same victims. However, the process of mining compromised data for correct username and password combinations requires significant computer processing power and proxy pool lists to be successful — a capability that is now exhibited by the Trickbot gang.

Individuals who reuse login credentials across multiple sites are more susceptible to account checking attacks, which occur when threat actors use credentials stolen from past database breaches or compromises to gain unauthorized access to other accounts belonging to the same victims. However, the process of mining compromised data for correct username and password combinations requires significant computer processing power and proxy pool lists to be successful — a capability that is now exhibited by the Trickbot gang.

Considered to be the successor of the formidable Dyre banking Trojan gang, the Trickbot banking Trojan gang continues to evolve by adopting new attack methods and targeting various industries. While Trickbot predominantly targeted the financial industry, it has now expanded its targeting of other industries via its account checking activities; these are perpetrated through the backconnect SOCKS5 module enlisting victims as proxies. Enlisting victims as its proxies allows the gang to perform account checking activity with the same IP as its victims. The gang account checking operation requires a steady stream of new and “clean” proxies to make sure their activities wouldn’t get automatically blocked by companies’ automatic IP origin anti-fraud systems. Therefore, their existing infections are turned into account checking proxies.

***Image 1:** The process of Trickbot’s backconnect proxy account checking activity. In the first step, the Trickbot gang distributes email spam. In the second step, the victim opens the spam attachment. In the third step, Trickbot downloads and executes the payload from the payload server on the compromised machine. In the fourth step, the victim machine downloads the backconnect SOCKS5 proxy module from the module server. Then, the victim connects to the preconfigured gang’s backconnect server. Finally, the Trickbot gang connects to the victim enlisting their machine’s IP as its proxy for account checking activities via its backconnect SOCKS5 module.*

The Trickbot gang continues to search for ways to monetize infections by adopting a hybrid attack model, which utilizes both Trickbot modular payloads and knowledgeable fraud operators. The Trickbot gang has also extended its operations to include account checking activity; such attacks are a combination of malware expertise and knowledgeable human operators. This hybrid approach allows Trickbot operators to launch account checking attacks leveraging infected victims as proxies.

Distributed through malicious Microsoft Office documents via email spam campaigns, Trickbot is notable for loading its backconnect SOCKS5 module bcClientDllTest onto compromised machines. This module is used extensively by the gang for account checking activity.

From Aug. 17 to the present, analysts observed close to 6,000 unique compromised machines associated with Trickbot SOCKS5 proxy module activities. Of these machines, more than 200 of them were actively enlisted for account checking fraud activities at any one time.

***Image 2:** The Trickbot SOCKS5 backconnect module contains authorization backconnect logic to check in to the backend.*

Trickbot utilizes a backconnect communication protocol maintaining the following commands, which are used for client-server communications initially with the command prefix “c”:

- disconnect: Terminate the backconnect server connection
- idle: Maintain the client-server connection
- connect: connect to the backconnect server. The command must consist of the following

parameters:

○ ip: Backconnect server’s IP address
○ auth_swith: Use authorization flag. If the value is set to “1”, the Trojan receives the auth_login and auth_pass parameters. If the value is “0”, the Trojan gets the auth_ip parameter. Otherwise, the connection will not be established.
○ auth_ip: Authentication IP address
○ auth_login: Authentication login
○ auth_pass: Authentication password

Image 3: *A Trickbot victim connects to the Trickbot backconnect server.*
There are three main Trickbot SOCKS5 server-client commands:

- c=idle
- c=disconnect
- c=connect

Trickbot victims create a sequence of GET requests to the server on gate[.]php:

- client_id=&connected=&server_port=&debug=

The server responds with a POST request with the following parameters if the connection needs to be established:

- c=connect&ip=&auth_swith=&auth_ip=&auth_login=&auth_pass=

If the connection needs to be terminated, the server will respond with c=disconnect.

Image 4: *The Trickbot machine actively pings the server every 100 seconds.*
Most notably, once compromised, Trickbot targets customers of financial institutions via webinjects and redirection attacks. The Trojan also uses victim IPs as proxies to leverage username and password combinations for account checking activity. The observed account checking activity mainly targets customers of companies in nine industries, most of those in gaming. Notably, some of the targets appear to be Russia-based companies.

Image 5: *Trickbot account checking activities mainly target customers in nine industries.*
Trickbot account checking activity is mainly directed to customers of U.S.- and Russia-based companies operating in the following industries:

- Gaming
- Technology
- Financial
- Entertainment
- Adult
- Social Media

- Retail
- Rewards
- Cryptocurrency

Likely leveraging commercial account checker tools, the Trickbot gang and its associates heavily utilize its victims' IPs as proxies for account checking activity that imitates mobile device-based account logins. Their attacks leave various web applications artifacts such as spoofed user agent information and device information, indicating as if the activity was being performed leveraging mobile devices. Such mobile logins are meant to bypass traditional anti-fraud controls that are largely implemented to address web-based logins. In cybercriminals' pursuit of targets, their attempts at evading anti-fraud systems are thus dictated by a company's anti-fraud controls, which are in turn influenced by cybercriminal tactics, techniques, and procedures (TTPs). Analysts assess with moderate confidence the Trickbot operators will likely continue to monetize infections by turning victims' IPs into proxies that subsequently fuel account checking activities.Block has been deleted or is unavailable.