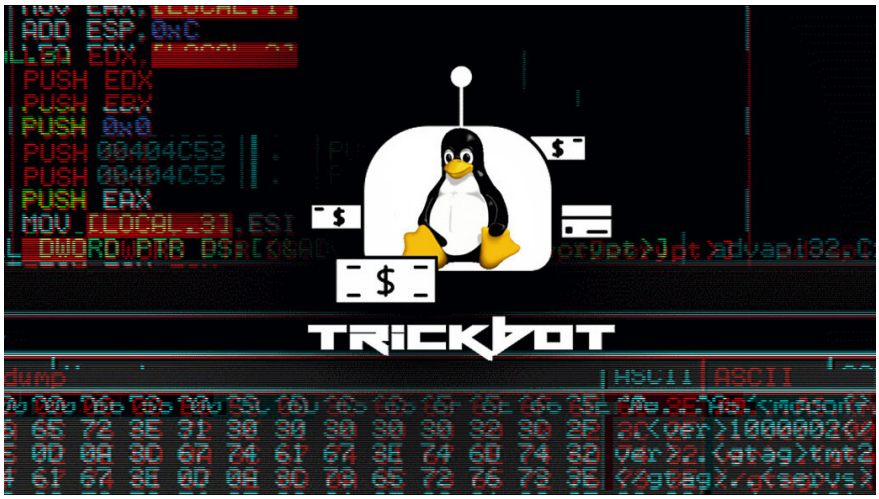
TrickBot Linux Variants Resurface Despite Removal

The coalition's efforts to take down TrickBot may have taken down much of the notorious botnet's critical infrastructure, but the cybercriminals behind the malware have refused to let their hard work go to waste.



According to ***TipsMake*** , efforts to take down TrickBot may have taken down much of the notorious botnet's critical infrastructure. However, the people behind the malware are not willing to let their work be taken down for good.

New shares from cybersecurity company Netscout, the authors behind TrickBot have ported their code to **Linux** . This is one of the efforts to expand their attack range to target more victims.

Appearing in 2016, TrickBot appears as a trojan and is a Windows-based crimeware solution that uses different modules to perform malicious actions on the victim's system such as: stealing credentials, conducting ransomware attacks.

However, over the past few weeks, the US Cyber ??Command and Microsoft have helped take down 94% of TrickBot's command and control (C2) servers. This includes both servers that were in use and new infrastructure that the TrickBot authors attempted to bring online to replace previously disabled servers.

Despite Microsoft's steps to stop it, TrickBot will likely find a way to restore its operations.

TrickBot's Anchor Module

In late 2019, a TrickBot backdoor framework called Anchor was discovered using the DNS protocol to surreptitiously communicate with C2 servers.

'This module allows actors — potential TrickBot customers — to leverage this framework against more advanced victims. At the same time, integrating APT attack capabilities into a monetization business model has seen the malware grow exponentially,' SentinelOne said.

According to the report by NTT researchers, the variant named 'Anchor_DNS' allows the infected client to use DNS tunneling to establish communication with the C2 server, which then transmits data with resolved IPs as responses.

Researcher Waylon Grange of Stage 2 Security discovered in July that Anchor_DNS had been ported to a new Linux backdoor called "Anchor_Linux."

How C2 Server Works Using Anchor

As Netscout's latest research has deciphered: How the bot and the C2 server communicate during the initial setup phase, the client sends "c2_command 0" to the server. Along with information about the compromised system and the bot ID. The server then responds with a "signal /1/" message to the bot.

To confirm, the bot will send a message to C2, then the server will issue a command to execute on the client. Finally, the bot will send the execution result back to the C2 server.

"Each communication with the C2 server follows a sequence of three different DNS queries," said Netscout security researcher Suweera De Souza.

List of IP addresses representing data corresponding to payload

The result of the third query is a list of IP addresses which are then parsed by the client to build the executable payload.

Corresponding to a command type, the final piece of data sent by the C2 server (numbered 0-14 in Windows, 0-4, 10-12 and 100 in Linux) executes the payload via cmd.exe or injects it into running processes such as Windows File Explorer, Notepad.

According to De Souza: "The complexity of Anchor's C2 communications and the payloads the bot carries reflect the formidable capabilities of the cybercriminals behind Trickbot. They also demonstrate a continued level of innovation and adaptability, with the fact that they quickly moved to a new platform."