THREAT BRIEF

TrickBot (Malware)

The Malleable Bot That's Tough to Spot • Winter 2020

Gartner COOL VENDOR 2020™

TrickBot is a trojan, a type of malware that looks harmless with the aim of deceiving you into installing it yourself and releasing a payload that can easily take control of a computer. While TrickBot is designed to exfiltrate sensitive banking information, its modular framework can also deploy other malware to spread throughout your network and leverage other known exploits, such as EternalBlue and Mimikatz. Over time, TrickBot has evolved dramatically, including variations in delivery mechanisms and purpose.

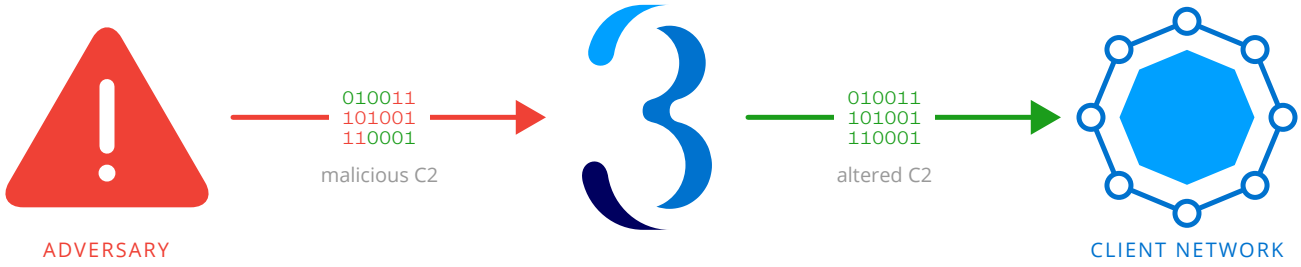
The most common way TrickBot spreads is through spearphishing campaigns. These campaigns send unsolicited emails that direct users to download malware from malicious websites or open it through an attachment. TrickBot can also be distributed as a secondary payload within other well-known malware families, such as Emotet.

Once a computer is infected, TrickBot exfiltrates sensitive information—like financial records, login credentials, network data, and more—and can connect other infected devices to create its own network of infected systems (a botnet). Left untouched to spread laterally and infect the entire network, TrickBot will download additional malicious files such as Remote Access Trojans (RATs), persistent data exfiltration tools, and even final stage ransomware that can bring business operations to a halt.

Trinity Cyber Stops TrickBot Cold

Trinity Cyber detects TrickBot in various stages, including recent module variants like "Anchor." While these variants of TrickBot binary payloads are exceptionally difficult to spot in transit, we don't depend on merely detecting them; we also focus on TrickBot Command & Control (C2) traffic on your network, in either direction. Our detection of TrickBot C2 happens within full session network traffic—using subtleties and characteristics that form unique patterns—enabling us to detect and act on TrickBot without relying on static indicators like IP, domain, or malware hash. Furthermore, this approach means that if you have an existing infection of TrickBot on your network, we can actively stop it from communicating with its C2 infrastructure.

Trinity Cyber detects and neutralizes TrickBot attacks without relying upon static indicators. We respond where necessary to every evolution in TrickBot campaigns with Formulas that render the attacks harmless. Our team is constantly keeping up with the pulse of TrickBot campaigns, so that we can better protect you from this pervasive threat.



sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber