UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00166

TRICKBOT ADD MAN-IN-THE-BROWSER CAPABILITIES

DATE ISSUED: 5th July 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Previously used exclusively as a precursor in delivering ransomware attacks, TrickBot has now added Man-in-the-Browser (MitB) capabilities for stealing credentials, similar to the Zeus banking trojan.

BREAKDOWN

Using a new module webinject, TrickBot is able to redirect unsuspecting users to malicious copycat websites in an effort to steal banking credentials. As victims attempt to visit a specifically targeted URL, in this case bank websites, the webinject package performs static or dynamic web injection to redirect users to an attacker-controlled fake site or by transmitting server responses to the Command and Control (C2) server before they are returned to the user, appearing as though returned requests came from a legitimate site. This evolution has been noted by Krytos Logic researchers as TrickBot becoming a first-stage multipurpose malware and no longer a one-trick pony.

REMEDIATION STEPS

- Monitor network traffic for unusual outbound traffic and any attempts to reach blacklisted IP addresses.
- Always enter URLs manually when visiting banking websites – never via hyperlink in emails.
- Check for HTTPS padlock in browser address bar to ensure websites are encrypted.
- Check URL is correct before entering any credentials – look for URL spoofing, typo squatting, and minor errors to indicate illegitimate sites.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/trickbot-banking-trojan-module/167521/
Malware Bytes	https://blog.malwarebytes.com/detections/trojan-trickbot/
CISA	https://us-cert.cisa.gov/ncas/alerts/aa21-076a
CIS	https://www.cisecurity.org/blog/trickbot-not-your-average-hat-trick-a-malware-with-multiple-hats/