Severity

High

Analysis Summary

TrickBot — a windows-based banking trojan — makes its first appearance in 2016. It targets sensitive data and serves as a distribution point for additional malware. Malspam operations are the most common way for Trickbot to propagate. These tactics send unsolicited emails that link consumers to harmful websites where they may download malware or deceive them into opening malware through an attachment. Other malware can potentially release TrickBot as a secondary payload. Trickbot is used in malspam operations that imitate recognizable brandings, such as invoices from accountancy and banking businesses. An attachment, such as a Microsoft Word or Excel document, is usually included in the emails. When the user opens the attachment, it will request them to activate macros, which will start a VBScript that will download the malware via a PowerShell script.

Impact

- Credential Theft
- Financial Loss
- Exposure of Sensitive Data

Indicators of Compromise

MD5

- 01dec476353280d4d5f1965a139fa4d8

SHA-256

- 018c2dcaaa95ae02fff25b303888b8f1059cbd6c6fd2879f8932d207fde061ad

SHA-1

- 8c4066be6d55c4eeb11b1bf6085d05f10875b0d4

Remediation

- Block all the threat indicators at your respective controls.
- Search for IOCs in your environment.