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

- 422030b616989ef7bf2f56a2f266068f

SHA-256

- 6f1c23f3d7e471cf0c4a91f59c94853128413b84065ef42ad2065337b973beab

SHA-1

- 04ec47e9f08ed7e4861c6f252a381faee4283bf9

Remediation

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