## Severity

High

## Analysis Summary

IcedID, aka BokBot — a banking trojan — first appeared in 2017. The threat actor behind IcedID is Lunar Spider. The main purpose of this trojan is to steal financial information but aside from this, it is also a passage for a RAT. Initially, it was delivered as a later-stage payload from multiple threats including Emotet, TrickBot, and Hancitor. Recently, it is observed that its threat actors are using several new techniques to avoid detection by the sandbox and endpoint security. This trojan has capabilities similar to Zeus, Dridex, and Gozi (financial threats). IcedID can download different additional modules and a configuration file from C2. It performs its task of stealing information by deploying a man-in-the-browser attack which assists in gaining banking credentials.

## Impact

- Financial Loss
- Exposure of Sensitive Data

## Indicators of Compromise

### MD5

- 3aa6bf4ed8c485717d767013d43f7cdb
- 89a0e6601d22c145a7dd5f5dd65b1f04

### SHA-256

- 08d30d6646117cd96320447042fb3857b4f82d80a92f31ee91b16044b87929c0
- 55df2954add86715fc3d728459d79a6d2b88d34d9f23fafe9c5a573bb773d9e9

### SHA-1

- 83ea9a8627819a7ba2ecad058f22e7f697256bc0
- 0f964caafc104b44d371a71809f01ceca7a39128

## Remediation

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