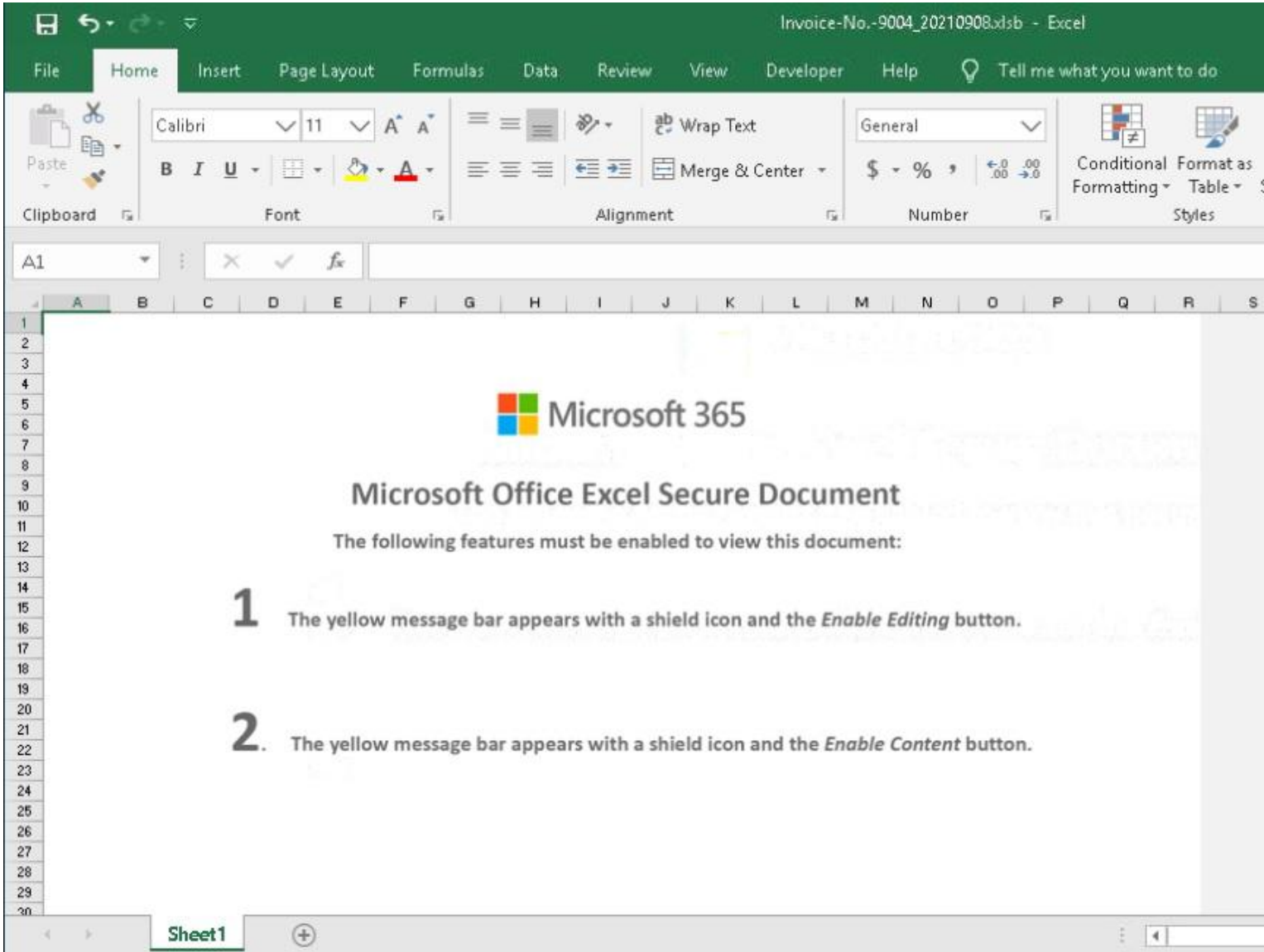


# Severity

High

# Analysis Summary

Dridex is a sophisticated strain of banking malware that targets the Windows platform, delivering spam campaigns to infect computers and steal banking credentials and other personal information to facilitate fraudulent money transfers. Through its history and development, Dridex has used several exploits and methods for execution, including modification of directory files, using system recovery to escalate privileges, and modification of firewall rules to facilitate peer-to-peer communication for extraction of data. The malware’s main use is to steal banking credentials and it has been attributed to the TA505 threat group (aka Evil Corp) known to have been active since at least Q3 2014.



# Impact

- Credential Theft
- Financial Loss
- Exposure of Sensitive Data

# Indicators of Compromise

## MD5

- fd10b3cc2659e901e12acdd6217b211c

## SHA-256

- 8db67274201786272d7be086f09c69dbbaefec34dc5763da408adb4cc734fd8b

## SHA-1

- ae82cda1cc1e56df59b6f012ee3d6bc1a679b3b8

# Remediation

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