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

- 88336c0d88bde767514b8355bfc6fad8

SHA-256

- 08bef391a284647a7f6f3933a0f264ac53ac23e4f288790996c86c0eeb89c8b1

SHA-1

- 72a6f71e78f423928209ac5954aaa58f23383b00

Remediation

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