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

- 8007b512062da01473f21e88d70277fa

SHA-256

- 9f9c85fef8b14244cf970f9b2486c622d120f3457df6475c733c0fbb6654f3dc

SHA-1

- ca0c519cffacd9a170424c933afce6948a5ebd09

Remediation

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