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

- b85405fc1d3a4473826d7ebd31111a50
- 66ac9a127ebb19f915987c31cf67d8d3
- ba33bff302fdecf939ed96296d93593f
- 1b22f613a65698007fe993b30d43ab5e
- b888083ff853d4f150acb307906fb38d

SHA-256

- 26af00a279ce082c2bb1db2cb50d2d590623e3f20e6c260d77ca77bf72b51797
- 94c0cedd61450d24b1195538edcd623b734749553680a42b5b64bc6194c2126a
- 55f53b1d9dac903d695b48f52894117a87acd81c1c10fc6eafb6dad5d6bc28b4
- 48d3a64c501f161c1436933c5f98dea6911f88a48ec445eada05f67e87c1d78d
- 9619a55c49642d423d9244bfe2e50b5027c395386056f82bbd10b7134b3d854e

SHA-1

- 4b62c6e56be21a0dc8f285a23ca62a055a768956
- b90e008f65d129cd9ade9aa24a9e046d727ff3f6
- f422c218c50549a380234e6c57231e95a5774371
- 7bb2291535ce8e20094d762e9535e4dc68db469f
- 2820b43315c4792515bff6b6cf96e1021c711b4f

Remediation

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