Severity

Medium

Analysis Summary

The Ramnit malware has numerous variants, which may individually be categorized as trojans, viruses, or worms. The first ramnit malware discovered in 2010 were viruses that infected exe, .dll , and html files found on a computer. Later variants included the ability to steal confidential data from the infected machine. Depending on the variants, Ramnit-infected machines can also be enslaved in a botnet.

Impact

- Information Theft
- Exposure of Sensitive Data
- Credential Theft

Indicators of Compromise

MD5

- 37724dc81679260d059007e3c925b441
- ff5e1f27193ce51eec318714ef038bef
- 38c1e30d6fa5689e793c1e7bb77c2bfe

SHA-256

- 88d09be2c8976d0e47545751e4ca2ee3849013c9fe1be6e519449c0be013ed21
- fd6c69c345f1e32924f0a5bb7393e191b393a78d58e2c6413b03ced7482f2320
- 1469be1acebf503f3772925c29ce8047e2a2ede009ca97374992860fa35bb561

SHA-1

- 7b38916755905bf02639fc6839c3367296d43f54
- b4fa74a6f4dab3a7ba702b6c8c129f889db32ca6
- 857b3835f6f88f8d11aec161b9b2031cfafbd22c

Remediation

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