

# 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

- e114951c5607c67a80be82c980bd720e
- 774efb94ed852690c35d3d794a511638
- 406f1692f3ef6f12b9e990bcf7242e1e
- 6856f81f431ee2b0bd20c5330253f324

## SHA-256

- 201c4d0070552d9dc06b76ee55479fc0a9dfacb6dbec6bbec5265e04644eebc9
- 82aeb5d0564557665ebff9d1ccefc066336111de1be149eca12275f05085a2cd7
- 608b6496c57aa61f059face6339a621382af4865bdf7e86800b8c7ecbbfa01ef
- ab1d4dc22088fdf0ebf5b57d3a9909ad7d159b69e1e79174ac5b29c8fb187a7a

## SHA-1

- 7b5a1cddc001844ef446d980813f0653659f850d
- e74e97ccf970176a86e1443d542a3558befc8f6f
- c8529cdb16556c5a0ae29e446c4a8aaf35a25f86
- d0a5a278a54fa6a4473791b3e40ed1a4b6542c48

# Remediation

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