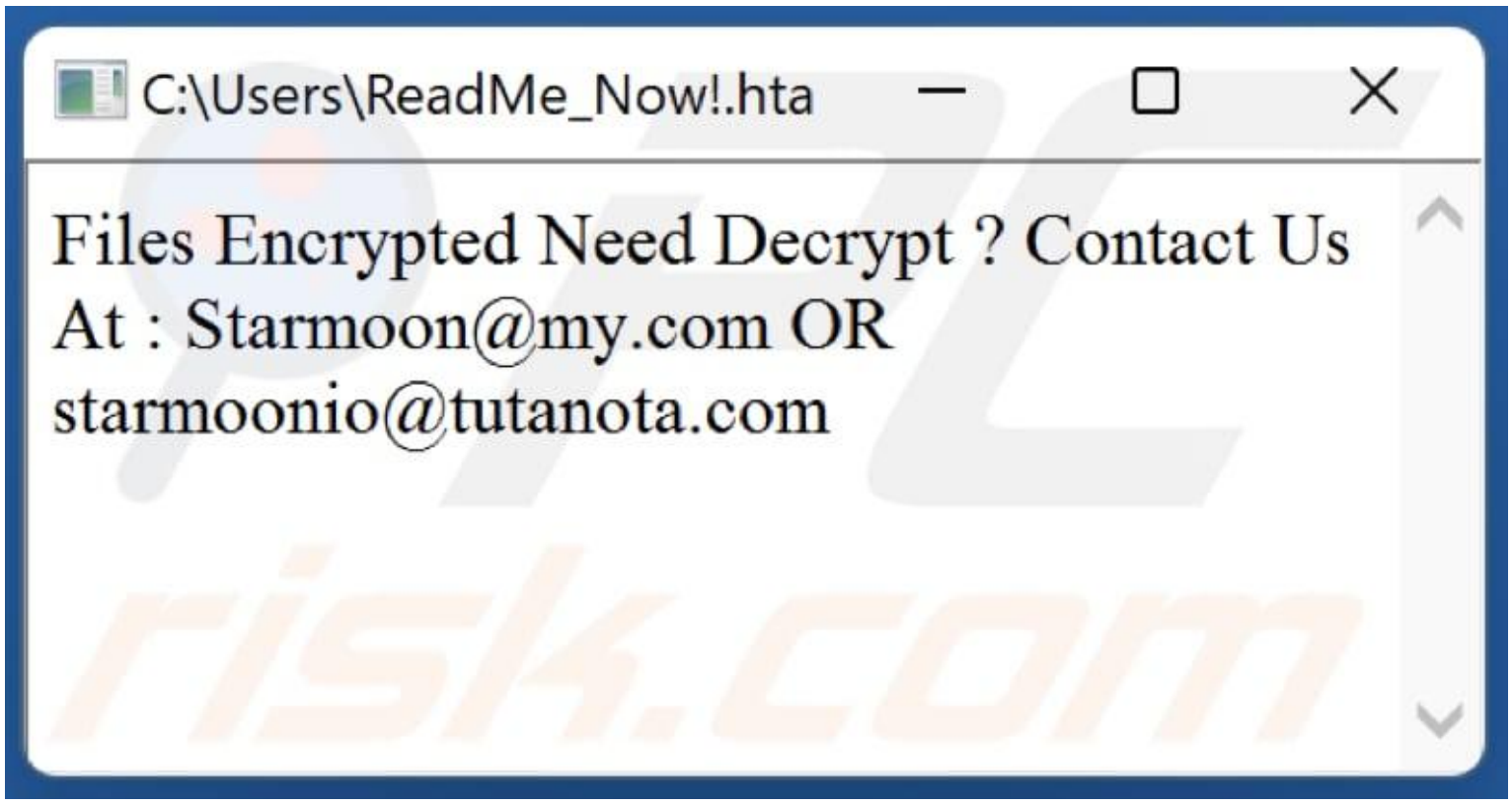
Severity

High

Analysis Summary

Starmoon ransomware is newly discovered ransomware called starmoon.It was found on virustotal while analyzing the malware samples.Starmoon ransomware is part of the spora ransomware family.It can encrypt the whole system files and appends the victims ID (starmoon@my.com) email address.



Impact

- Information Theft
- Files Encryption

Indicators of Compromise

MD5

- a56644a519d6fce5f20a744ae3820af2

SHA-256

- 563daaab9f9d7be02f037c540d561c424aa3e5efc6a9a5c8d58858d98e2aae3c

SHA-1

- 93acd978da4a602c9ea1a23b6a97d74ced436e56

Remediation

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