Severity

High

Analysis Summary

BlackMoon, aka KRBanker, is a banking trojan it can steal financial and banking account information as well as other sensitive data. Blackmoon was discovered in 2014 by Fortinet researchers, and it is back again with a new campaign. Blackmoon used to attack the host with URLs, advertisements, and other web content. Once the host has been compromised it can open multiple pop-ups.

Impact

- Credential Theft
- Financial Theft
- Data Exfiltration

Indicators of Compromise

MD5

- 2acedd4b93a3baffdb2dce08ea56ad62

SHA-256

- 0d731dcee7ba0bd75e4d2a510311c3eb12b88e348d8c02b17081df54965f9d34

SHA-1

- 13215c247c2d03d9619a677b7b9b83a174927f8f

Remediation

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