Severity

Medium

Analysis Summary

NjRat is a Remote Access Trojan, which is found leveraging Pastebin to deliver a second-stage payload after initial infection. There are multiple versions of the secondary payload used, ranging from base64 encoded version, hexadecimal, JSON data format, compressed blobs, and also plain text data with malicious URLs embedded within. This is done in order to evade detection by security products and increase the possibility of operating unnoticed. njRat is developed in .NET framework and is able to hijack the functions of a compromised machine remotely, including taking screenshots, exfiltrating data, keylogging, and killing processes such as antivirus programs, while also connecting the machine to a botnet. RAT was also found abusing Windows API functions such as Windows API calls such as GetKeyboardState(), GetAsynckeyState(), MapVirtualKey() for keylogging, and data theft. It was also discovered downloading web scraping tools such as “proxy scrapper” in order to extract large amounts of data via proxies

Impact

- Unauthorized Access

Indicators of Compromise

MD5

- ce82e60feca483c7d181aab8137196ba

SHA-256

- 38f491f1d99b9adb8f73c9f28a97969c6309fcc285d1a2c3c669300c19959ae8

SHA-1

- ff4e4a96011293e7e589d403bd69fc91553c2557

Remediation

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