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

- 72b606cd09306e774d3944e046e0ca0f

SHA-256

- 4126376549609c61fa89d456f6b910ffd3ae57c9a6ce012094d2ccd6e59d3578

SHA-1

- cff9fcc6fb5c3b371e19d7e4e64ce8b17fe47a9a

Remediation

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