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

- 9d51ce10bc62e2ee50f6e96585bf9ee4

SHA-256

- a65b5662563a6a4d06c89c9340c5886a9afdb8992ac6ee19ef7a52a78efb84bf

SHA-1

- fc2f36e27e0f963d224b5aa14a833af04a13dc21

Remediation

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