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

- a3f865458a953459ba946b4ca4c29e7d
- a33b1b83050580b0e8f6de130cda1b31
- 153e79be9966927d988066f90c4a941d
- d611e4097540e840b6ffc2fad817bc7f
- e470e1f31915a6976b469978c21c2d27

SHA-256

- ef811f4e728f02a3d0b114d9876092ff0bb0aa9ddc6703567f3cb4374801c982
- 3493ec9e16e5a37a31e05914ebcf6548cc68497836aea2a35b9f0e1de5f3ce9f
- 932db39565ad2858a7a41df4a6651e47ae8076035fc32bbe094e626ca2664eed
- bb8feb596b3738d215beec88a943a5f1b4dee11c817de9ad8d366163501945e4
- 800ad98fb8f717bad7f295c373e8c0825765111d98e1d9195388d3e22d9cbc34

SHA-1

- d7695491e479b90f5f94d8ab65f3b4b7f2421654
- fb6eb7e488b69fef9a94e474fc9bf20b4439727e
- 5249ac7761cb6efa6ed04c928a3f91686e734cc5
- 9a4027108d62c071afbb3a944846d79cdd507583
- a304557a899554e4553268f9cd7361e9fa904b36

Remediation

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