njRAT, Software S0385 | MITRE ATT&CK®

Archived: 2026-04-05 16:17:24 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

njRAT has used HTTP for C2 communications.[3]

Enterprise T1010 Application Window Discovery

njRAT gathers information about opened windows during the initial infection.[1]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

njRAT has added persistence via the Registry key `HKCU\Software\Microsoft\CurrentVersion\Run\` and dropped a shortcut in `%STARTUP%`.[1][3]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

njRAT has executed PowerShell commands via auto-run registry key persistence.[3]

.003 Command and Scripting Interpreter: Windows Command Shell

njRAT can launch a command shell interface for executing commands.[1]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

njRAT has a module that steals passwords saved in victim web browsers.[1][3][4]

Enterprise T1132 .001 Data Encoding: Standard Encoding

njRAT uses Base64 encoding for C2 traffic.[1]

Enterprise T1005 Data from Local System

njRAT can collect data from a local system.[1]

Enterprise T1568 .001 Dynamic Resolution: Fast Flux DNS

njRAT has used a fast flux DNS for C2 IP resolution.[3]

Enterprise T1041 Exfiltration Over C2 Channel

njRAT has used HTTP to receive stolen information from the infected machine.[3]

Enterprise T1083 File and Directory Discovery

njRAT can browse file systems using a file manager module.[1]

Enterprise T1562 .004 Impair Defenses: Disable or Modify System Firewall

njRAT has modified the Windows firewall to allow itself to communicate through the firewall.[1][3]

Enterprise T1070 .004 Indicator Removal: File Deletion

njRAT is capable of deleting files.[1][3]

.009 Indicator Removal: Clear Persistence

njRAT is capable of manipulating and deleting registry keys, including those used for persistence.[3]

Enterprise T1105 Ingress Tool Transfer

njRAT can download files to the victim's machine.[1][3]

Enterprise T1056 .001 Input Capture: Keylogging

njRAT is capable of logging keystrokes.[1][3][4]

Enterprise T1112 Modify Registry

njRAT can create, delete, or modify a specified Registry key or value.[1][3]

Enterprise T1106 Native API

njRAT has used the ShellExecute() function within a script.[3]

Enterprise T1571 Non-Standard Port

njRAT has used port 1177 for HTTP C2 communications.[3]

Enterprise T1027 .004 Obfuscated Files or Information: Compile After Delivery

njRAT has used AutoIt to compile the payload and main script into a single executable after delivery.[3]

.013 Obfuscated Files or Information: Encrypted/Encoded File

njRAT has included a base64 encoded executable.[3]

Enterprise T1120 Peripheral Device Discovery

njRAT will attempt to detect if the victim system has a camera during the initial infection. njRAT can also detect any removable drives connected to the system.[1][3]

Enterprise T1057 Process Discovery

njRAT can search a list of running processes for Tr.exe.[3]

Enterprise T1012 Query Registry

njRAT can read specific registry values.[3]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

njRAT has a module for performing remote desktop access.[1]

Enterprise T1018 Remote System Discovery

njRAT can identify remote hosts on connected networks.[1]

Enterprise T1091 Replication Through Removable Media

njRAT can be configured to spread via removable drives.[1][3]

Enterprise T1113 Screen Capture

njRAT can capture screenshots of the victim’s machines.[3]

Enterprise T1082 System Information Discovery

njRAT enumerates the victim operating system and computer name during the initial infection.[1]

Enterprise T1033 System Owner/User Discovery

njRAT enumerates the current user during the initial infection.[1]

Enterprise T1125 Video Capture

njRAT can access the victim's webcam.[1][4]
