**A logo with colorful ribbons

Description automatically generated**

**Austria, Gian Carlo**

**Maddela, Aireen**

**Taule, Love**

**Southern Alberta Institute of Technology**

**Spring 2025 Malware Analysis (ITSC-303-SA1)**

**Project – Weekly Report 1**

**Ritika**

**July 15, 2025**

**Malware Analysis Report**

# Selection and Justification of Malware Sample

**a. Why We Chose This Sample**

We selected njRAT for our malware analysis project because it aligns with the learning outcomes of our course on malware analysis. This sample is widely documented and commonly used in educational labs, making it suitable and relatively safe for student-level analysis when proper precautions are in place.

We aimed to:

* Understand the behavior and characteristics of Remote Access Trojans (RATs)
* Explore both static and dynamic analysis techniques in a controlled lab environment
* Enhance our detection and reverse engineering skills

**b. Malware Sample Details**

* Sample Name: EnkSAr\_HaCKeR.exe
* Hash: fd62a4aa205517580e83fad7ac4ce4d64863c95ef62b34ac72647b1974a52822199
* File Type: .exe (Windows executable)
* File Size: 959.00 KB
* Source: theZoo GitHub Repository
* VirusTotal Analysis:
  + Detected by 62/71 antivirus engines.
  + Labels include: Trojan, Backdoor, MSIL/Bladabindi, MSIL/Perseus, and NJrat.
  + Identified threat categories: trojan, dropper.

**c. Main Features Observed in Research**

According to both our VirusTotal scan and external research sources njrat may have:

* Remote Control Capabilities: Full remote access to the victim's system via GUI
* Surveillance Functions: Keylogging, webcam access, screenshot capture
* Persistence Mechanisms: Registry modification, startup folder addition
* Command & Control: Communicates with C2 servers to receive commands
* Propagation Methods: USB spreading, phishing, drive-by downloads
* Data Theft: Extracts browser credentials, file data, and system information
* Malware Deployment: Can download and execute additional malicious payloads

# Security Measures for Handling and Analysis

To safely handle and analyze the njRAT sample, we implemented the following precautions:

|  |  |
| --- | --- |
| **Category** | **Measure** |
| **Isolated Environment** | The malware will be executed strictly within a sandboxed virtual environment that is fully isolated from the host system to prevent any accidental infection or data leakage. |
| **No Network Access** | A Host-Only or Internal Network setup was used. If Command and Control (C2) behavior needed to be observed, traffic was contained within the virtual lab environment without internet access. |
| **Snapshots** | Virtual machine snapshots will be taken before execution to allow quick rollback and full system restoration after malware analysis or in case of unintended behavior. |
| **Read-only Sample Handling** | The malware sample was stored and accessed in read-only mode to ensure it remains unaltered during the analysis, maintaining sample integrity and consistency. |
| **No Personal Data** | All virtual machines used in the lab were free from personal or sensitive data to avoid accidental exposure or theft by the malware. |
| **Evidence Preservation** | Throughout the analysis process, screenshots, logs, and other artifacts were captured and preserved immediately to maintain accurate and timely documentation. |
| **Security Tools used** | Tools such as Process Monitor, Wireshark, HxD/Hiew, Ghidra, and others will be used as needed during the progression of static and dynamic analysis. These tools helped monitor behavior, analyze binaries, and trace network activity. |

# Network Diagram

This diagram illustrates an isolated virtual environment used for analyzing malware like njRAT. The infected Windows VM and the Virtual C2 Server are both connected via an internal virtual network, enabling safe observation of C2 communications without exposing the host machine or internet. The host machine manages the virtual machines but remains isolated from the internal network to prevent contamination or leakage.

A diagram of a computer network

AI-generated content may be incorrect.

# Reference

Samsar4. (n.d.). Using njRAT [Webpage]. Ethical Hacking Labs. GitHub. <https://github.com/Samsar4/Ethical-Hacking-Labs/blob/master/6-Malware/1-Using-njRAT.md>

ytisf. (n.d.). *theZoo/malware/Binaries/njRAT-v0.6.4* [Repository]. GitHub. <https://github.com/ytisf/theZoo/tree/master/malware/Binaries/njRAT-v0.6.4>