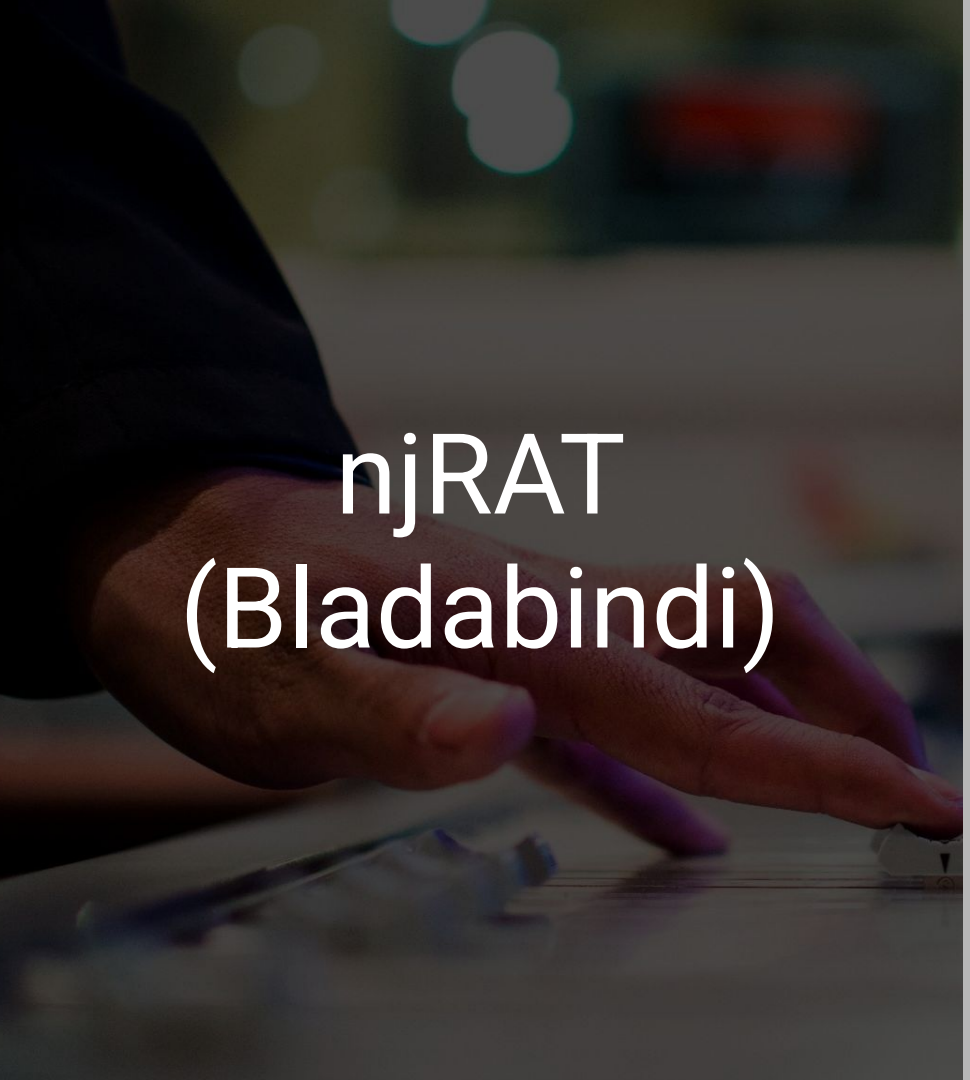
Informe de análisis estático del malware njRAT

Javier Alvarez
Malware Analysis
12-09-2025



njRAT (Bladabindi)

Introducción

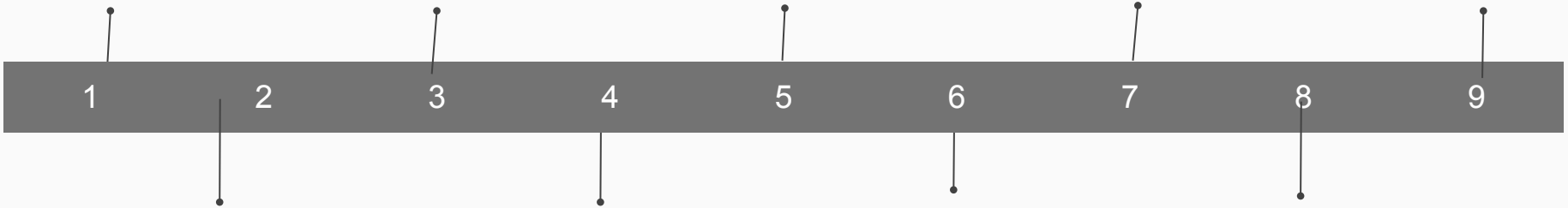
Información general

Metodología

Análisis estático

Referencias

Fases del Análisis Estático de Malware



1. Selección de la muestra
2. Recopilacion Información
3. Análisis de Cabeceras
4. Extracción cadenas Strings
5. Revision funciones importantes
6. Evaluación Entropía y Ofuscación
7. Análisis Ingenieria Inversa
8. Consulta en motores AV
9. Documentación y conclusiones

Introducción

Objetivo del estudio:
Analizar la muestra de malware njRAT para comprender su estructura, funciones maliciosas y técnicas de evasión.

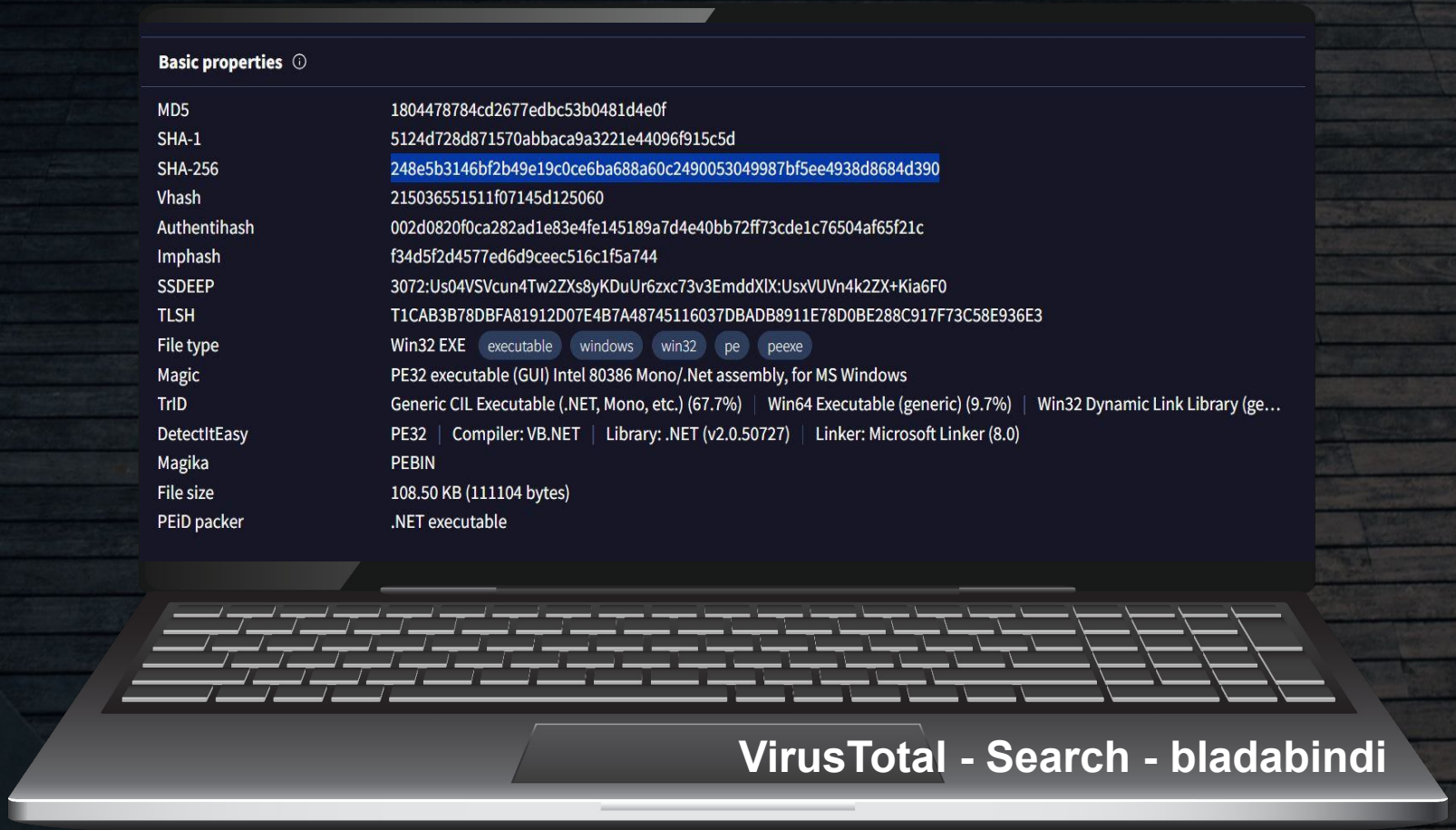
Objetivos
Identificar indicadores de compromiso IoCs
Detectar funciones clave del malware
Evaluar su capacidad de persistencia y comunicación con C2

Metodología
Análisis estático sin ejecución, utilizando ingeniería inversa, extracción de cadenas, revisión de cabeceras PE y análisis de secciones.

Introducción

Herramientas Utilizadas
PEStudio
Strings / BinText
Detect It Easy (DIE)
HxD
Ghidra o IDA free
VirusTotal

Información de la muestra
Nombre del archivo njrat_sample.exe
MD5 1804478784cd2677edbc53b0481d4e0f
Hash SHA256:
248e5b3146bf2b49e19c0ce6ba688a60c2490053049987bf5ee4938d8684d390
Tamaño 108.50 Kb (111104 bytes)
Tipo PE32 ejecutable para windows Win32 EXE



VirusTotal - Search - bladabindi

Análisis Estático njRAT

Cabeceras PE, estructuras internas de los archivos ejecutables en Windows (.exe, .dll) que contiene información esencial para que el sistema operativo cargue y ejecute el programa. Tipo de archivo, dirección de entrada, secciones de código, tabla de importación, timestamp de compilación etc.

- *Tipo de archivo: PE32 ejecutable para windows (Win32 EXE)*
- *Compilador: .NET*
- *Tamaño 108.50 KB*
- *Timestamp: Puede ser falsificado para evadir detección*
- *Secciones pRESENTES: .TEXT, .RSRC, .DATA*
- *Import Tabl funciones como CreateProcess, WriteFile, InternetOpen, GetAsyncKeyState*
- *Entropía: Alta en algunas secciones, lo que sugiere posible ofuscación o cifrado*
- *Firma Digital: inexistente o invalida*
- *Entry Point: Apunta a una rutina de iniciación que puede incluir persistencia o conexión con el C2*

Conclusiones

- *njRAT es un Remote Access Trojan altamente funcional; captura de teclado (GetAsyncKeyState), ejecución remota (CreateProcess), comunicación con servidores C2 (InternetOpen), persistencia mediante tareas programadas.*
- *El malware presenta alta entropía lo que sugiere técnicas de ofuscación o cifrado.*
- *No posee firma digital válida.*
- *El análisis estático permite identificar funciones clave sin necesidad de ejecutar el binario.*

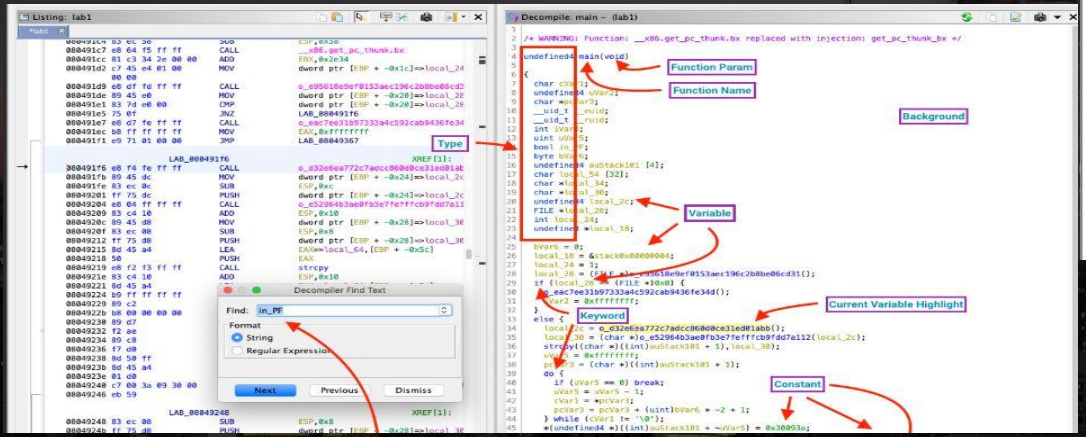
Paliativos y Recomendaciones

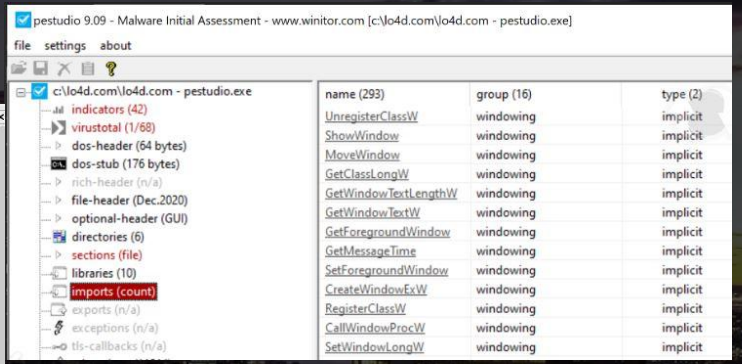
- *Segmentación de red para evitar propagación lateral.*
- *Monitorización de procesos, detectar ejecuciones sospechosas como njrat_sample.exe o procesos sin firma.*
- *Reglas YARA personalizadas basadas en funciones detectadas en el análisis, son filtros de búsqueda de amenazas en características observables, sin necesidad de ejecutar el archivo.*
- *Educación al usuario. Evitar ejecución de archivos desconocidos o adjuntos.*
- *Uso de sandbox y entornos controlados para el análisis dinámico.*

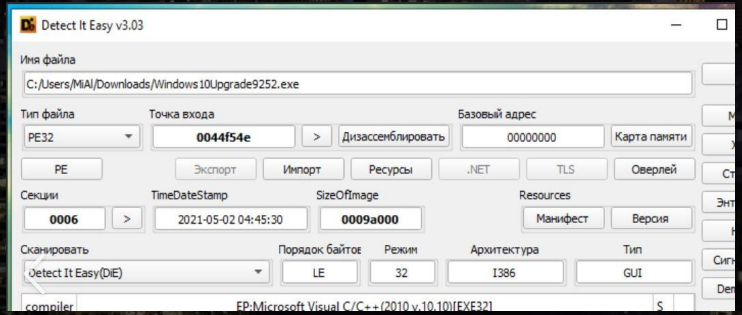
Herramientas Utilizadas en el Análisis Estático

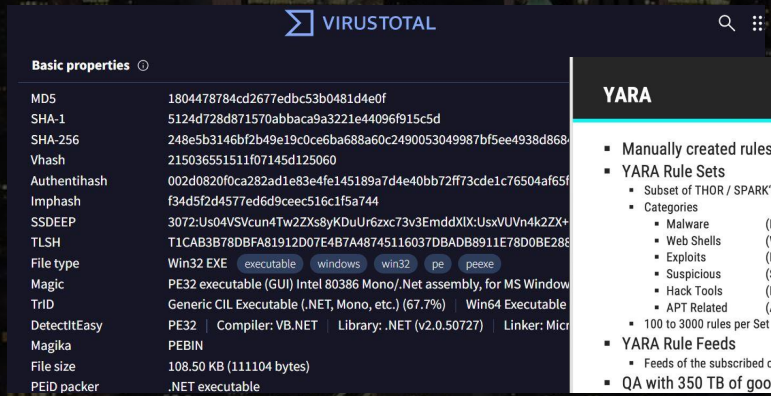
STRINGS. ***Identificación de URLs, comandos, funciones sospechosas incrustadas en el binario.***
PEStudio. Revisión de cabeceras PE, secciones, funciones importantes, firmas digitales y detecciones AV.
DETECT IS EASY. (DIE). Detección de compilador, tipo de archivo y posibles técnicas de ofuscación.
GHIDRA. Desensamblado y analisis de flujo de ejecución, funciones maliciosas y persistencia.
VIRUS TOTAL. Comprobación de detecciones por motores antivirus y análisis del comportamiento.
OTRAS. Process Hacker, Process Explorer, Resource Hacker, CFF Explorer, PEBear, RegShot, Autoruns.

Herramientas Utilizadas en el Análisis Estático





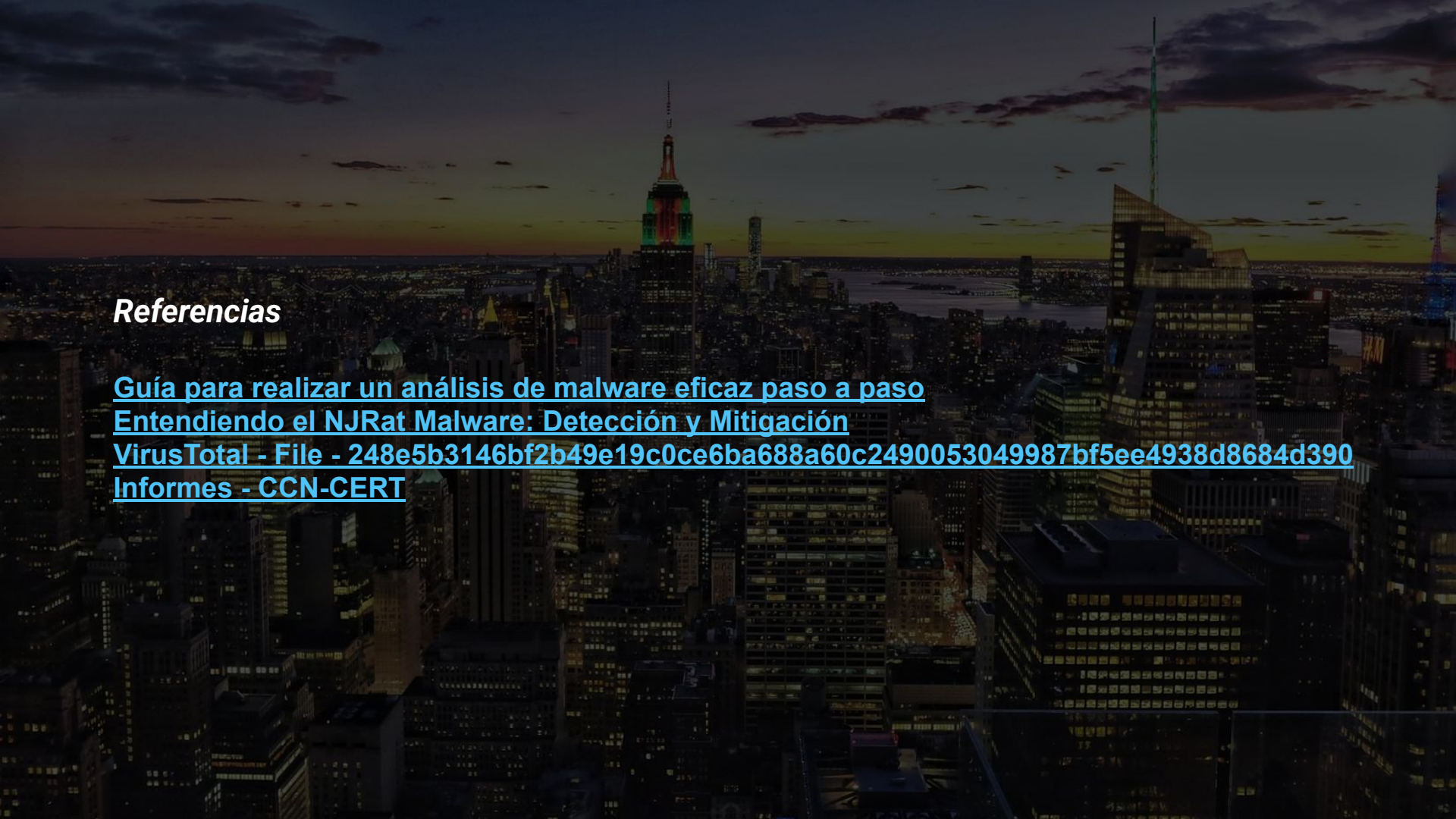




YARA

- Manually created rules for hunting or classification purposes
- YARA Rule Sets
  - Subset of THOR / SPARK's rule base
  - Categories
    - Malware (MAL_*)
    - Web Shells (Webshell_*)
    - Exploits (EXP_*)
    - Suspicious (SUSP_*)
    - Hack Tools (HKTL_*)
    - APT Related (APT_*)
  - 100 to 3000 rules per Set
- YARA Rule Feeds
  - Feeds of the subscribed categories
- QA with 350 TB of goodware data

```
┌──(javi㉿kali)-[~]
└─$ strings -n 20 netcheck.ps1
[Byte[]] $buf = 0×db,0×dc,0×d9,0×74,0×24,0×f4,0×bb,0×b2,0×c6,0×ad,0×c1,0×5a,0×2b,0
8,0×3d,0×46,0×26,0×a3,0×be,0×96,0×59,0×2d,0×5b,0×a7,0×4b,0×49,0×2f,0×95,0×5b,0×19,
4d,0×ec,0×86,0×83,0×b1,0×6f,0×7b,0×de,0×e5,0×4f,0×42,0×11,0×f8,0×8e,0×83,0×e7,0×77
x8,0×2f,0×f,0×3b,0×a4,0×2e,0×5f,0×94,0×bf,0×69,0×7f,0×9e,0×88,0×91,0×7e,0×73,0×8d,
58,0×d0,0×f1,0×e5,0×a1,0×14,0×35,0×16,0×d4,0×6e,0×45,0×ab,0×ee,0×b4,0×37,0×77,0×7b
```



Referencias

[Guía para realizar un análisis de malware eficaz paso a paso]

[Entendiendo el NJRat Malware: Detección y Mitigación]

[VirusTotal - File - 248e5b3146bf2b49e19c0ce6ba688a60c2490053049987bf5ee4938d8684d390]

[Informes - CCN-CERT]