|  |  |  |
| --- | --- | --- |
| ipn-1 |  | **Instituto Politécnico Nacional**  **Centro de Investigación en Computación** |

Análisis y Detección de Malware

Familia de Malware

Rootkit

**Autor (es)**

Nombre Ap\_paterno Ap\_materno

**Versión 1.0**

**15 de marzo del 2022**

# Control de versiones del documento

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha | **Ver.** | **Comentarios** | **Autor (es)** |
| 15/mzo./2023 | 1.0 | Versión inicial (estructura del documento). | Profr. Raúl Acosta Bermejo  (RAB) |
|  | 1.1 | Redacción del contenido | Lista de alumnos e iniciales. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  | **Versión final** |  |

Tabla de Contenido

[1 Control de versiones del documento 2](#_Toc182170944)

[2 Tabla de Figuras 3](#_Toc182170945)

[3 Descripción General 4](#_Toc182170946)

[3.1 Nombre 4](#_Toc182170947)

[3.2 Descripción del malware 4](#_Toc182170948)

[3.3 Linea del tiempo 4](#_Toc182170949)

[4 Descripción técnica 4](#_Toc182170950)

[4.1 Mecanismos de infección 4](#_Toc182170951)

[4.2 Comportamientos que puede tener 5](#_Toc182170952)

[5 Lista de las muestras de malware 5](#_Toc182170953)

[6 Referencias 5](#_Toc182170954)

# Tabla de Figuras

[**Figura 1**.- Gráfica de la evolución. **Fuente**. Propia. 4](#_Toc129623942)

# Descripción General

## Nombre

1. Nombre
   1. El nombre será el más común utilizado por varias empresas de ciberseguridad.
   2. Lista de sinonímos.
2. Fecha de la 1ª aparición o detección.
3. Lugar del ataque
4. Origen de la muestra
   1. Quien o en que lugar se creo.
5. Variantes
   1. Nombres asignados.
   2. Descripción de los nuevos comportamientos.

## Descripción del malware

Es una descripción no técnica del comportamiento.

## Linea del tiempo

De la evolución del malware y sus variantes.

**Figura 1**.- Gráfica de la evolución. **Fuente**. Propia.

# Descripción técnica

Esta sección explica .

## Mecanismos de infección

## Comportamientos que puede tener

# Lista de las muestras de malware

1. Referencias al repositorio MAREA.
2. Debe incluir los valores hash.

# Referencias

Usar la notación de la IEEE y la funcionalidad de Word.

1. Libros, sitios web (blogs, fichas descriptivas de empresas de ciberseguridad, etc), artículos científicos, etc.
2. Trate de poner las referencias más serias.

====================== ESTA ES LA ÚLTIMA PÁGINA ======================