| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2023-02 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTA DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 13-ene-2023 | **Linux Shc downloader malware** | Versión 1.1 |

## I. DATOS GENERALES:

**Clase de alerta:** Malware
**Tipo de incidente:** Downloader
**Nivel de riesgo:** Alto

## II. ALERTA

Atacantes han creado un malware basado en el módulo Shc de Linux. El malware está enfocado en instalar aplicaciones de minera de cripto monedas y bots utilizados para ataques de denegación de servicio DDoS.

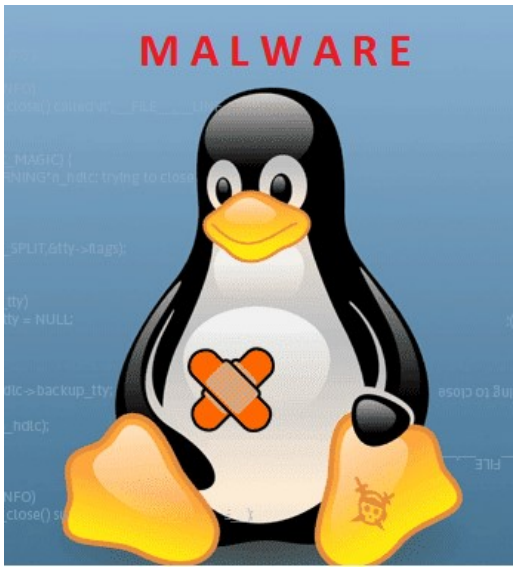


**Figura 1.** Icono de Linux anunciando malware
**Fuente:** EcuCERT

## III. INTRODUCCIÓN

Shc Shell Script Compiler, (Compilador de Scripts para shells de Linux) es una herramienta de Linux que permite la conversión del código de scripts de las bash shells al formato ELF Executable and Linkable Format, para las actividades típicas del sistema Linux.

Los componentes del malware detectado, consiste básicamente en los siguientes elementos:



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

1. Creación de un programa para descargas, utilizando el código del módulo Shc.
2. Instalación de una aplicación de minería para MONERO.
3. Instalación de una aplicación para formar parte de una BOTNET.

**Shc Downloader**

El código malicioso basado en el compilador Shc, a más de las funciones de compilación y transformación de scripts a ELF, define como actividades específicas de ejecución la descarga e instalación de las aplicaciones de minería de la criptomoneda Monero XMRig CoinMiner y un bot DDoS IRC Bot.

**XMRig CoinMiner**

La popularidad de la criptomoneda MONERO que genera un alto interés en masificar la moneda así como crear la infraestructura para su sostenibilidad, ha hecho que los ciber atacantes desarrollen aplicaciones maliciosos para la instalación de aplicaciones asociadas a esta cripto moneda. Las aplicaciones maliciosas se encuentran contenidas maliciosamente en otro tipo de aplicaciones populares para todo tipo de usuario, que son instaladas sin conocimiento del propietario del dispositivo en el que se instalan.

**DDoS IRC Bot**

El sistema infectado y una vez incluido en una red Botnet, se convierte en una herramienta permanente para que el ciber atacante ejecute ataques de denegación de servicio dirigidos hacia otros sistemas de información. En este escenario, las direcciones IP públicas del sistemas de información comprometido, son registradas en listas negras de direcciones IP, que son distribuidas mundialmente y que conlleva la mala reputación de la organización asociada a las direcciones iP registradas.

## IV. VECTOR DE ATAQUE:

Shc downloader puede emplear diferentes técnicas:

- **Sitios maliciosos de descarga**: A través de conexiones hacia sitios maliciosos no verificados ni filtrados, se ejecutan descargan para actualización del sistema operativo, archivos maliciosos.

| Nro. Alerta: | AL-2023-02 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTA DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 13-ene-2023 | **Linux Shc downloader malware** | Versión 1.1 |

- **Explotación de vulnerabilidades:** Credenciales inseguras de servidores SSH expuestos hacia el Internet.

## V. IMPACTO:

Los sistemas de información en los que se instalen el malware Shc downloader, serán utilizados para realizar ataques de denegación servicio y ejecutar actividades de minera de cripto monedas, lo cual tiene un impacto negativo de tipo alto respecto de la disponibilidad de la infraestructura para los fines lícitos con que fue desplegado el sistema.

## VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Actualizar las credenciales de administración de los servidores SSH.
- Implementar procesos de monitoreo de conexiones atípicas a fin de determinar posibles actividades maliciosas contra el sistema de información.
- Implementar controles de múltiple factor de autenticación para los procesos de actualización del sistema operativo y aplicaciones.

## VII. REFERENCIAS:

ASEC BLOG. (04 de 01 de 2023). *Shc Linux Malware Installing CoinMiner*: https://asec.ahnlab.com/en/45182/

Masterhacks Blog. (13 de 01 de 2023). *Detectan la implementacion de un malware de mineriaa de criptomoendas para Linux basado en shc*: https://blogs.masterhacks.net/noticias/hacking-y-ciberdelitos/detectan-la-implementacion-de-un-malware-de-mineria-de-criptomonedas-para-linux-basado-en-shc/

Toulas, B. (04 de 01 de 2023). *BleepingComputer*: https://www.bleepingcomputer.com/news/security/new-shc-compiled-linux-malware-installs-cryptominers-ddos-bots/



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec