| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°194 | Fecha: 18-08-2023 |
|---|---|---|
| | | Página: 8 de 32 |

| | | | |
|---|---|---|---|
| Componente que reporta | **CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ** | | |
| Nombre de la alerta | Conoce los Peligros Ocultos de las Actualizaciones Fraudulentas en Chrome | | |
| Tipo de Ataque | Malware | Abreviatura | Malware |
| Medios de propagación | USB, Disco, Red, Correo, Navegación de Internet | | |
| Código de familia | C | Código de Sub familia | C02 |
| Clasificación temática familia | Código Malicioso | | |

Descripción

**1. ANTECEDENTES:**

El 14 de agosto del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tiene conocimiento que hay un plan en marcha para engañar a las personas y hacer que instalen una herramienta de control remoto llamada NetSupport Manager. Estas actualizaciones Se logran mediante la distribución de supuestas actualizaciones fraudulentas del navegador Chrome, con el propósito de atraer a las personas y hacer que instalen esta herramienta sin que sean conscientes de ello.

**2. DETALLES:**

Los actores de amenazas utilizan este software de administración remota como un ladrón de información y para tomar el control de las computadoras de la víctima. Las investigaciones apuntan a una supuesta campaña de SocGholish que anteriormente fue realizada por un actor de amenazas ruso, pero que aún no es concluyente.

**A. Investigaron los siguientes ataques:**

NetSupport Manager es un software de administración remota utilizado para controlar y gestionar ordenadores de forma remota. Sin embargo, ha habido casos en los que los ciberdelincuentes han utilizado tácticas de ingeniería social para engañar a los usuarios para que instalen software malicioso, como NetSupport Manager, haciéndolo pasar por actualizaciones falsas de navegadores como Chrome. Aquí hay algunos posibles riesgos y ataques asociados con esta situación:

- Malware y software malicioso: Los atacantes pueden distribuir versiones falsas de NetSupport Manager junto con supuestas actualizaciones del navegador Chrome. Al instalar esta versión maliciosa, los usuarios pueden exponer sus sistemas a malware y software malicioso que podría permitir a los atacantes tomar el control remoto de sus computadoras, robar información confidencial, o realizar otros tipos de ataques.
- Control remoto no autorizado: Si un usuario instala una versión falsa de NetSupport Manager creyendo que es una actualización legítima de Chrome, los atacantes podrían obtener un acceso remoto no autorizado a la computadora. Esto les permitiría controlar el sistema, ejecutar comandos, acceder a archivos y realizar actividades maliciosas en el dispositivo comprometido.
- Robo de datos y credenciales: Con el control remoto de la computadora, los atacantes podrían acceder a información confidencial, como contraseñas, datos bancarios y otros detalles personales almacenados en la máquina. Esto podría llevar al robo de identidad ya otros tipos de fraudes.

**B. Indicadores de compromiso**

hxxps://altiordp[.]com/cdn/www.php
hxxps://cheetahsnv[.]com/cdn-js/wds.min.php

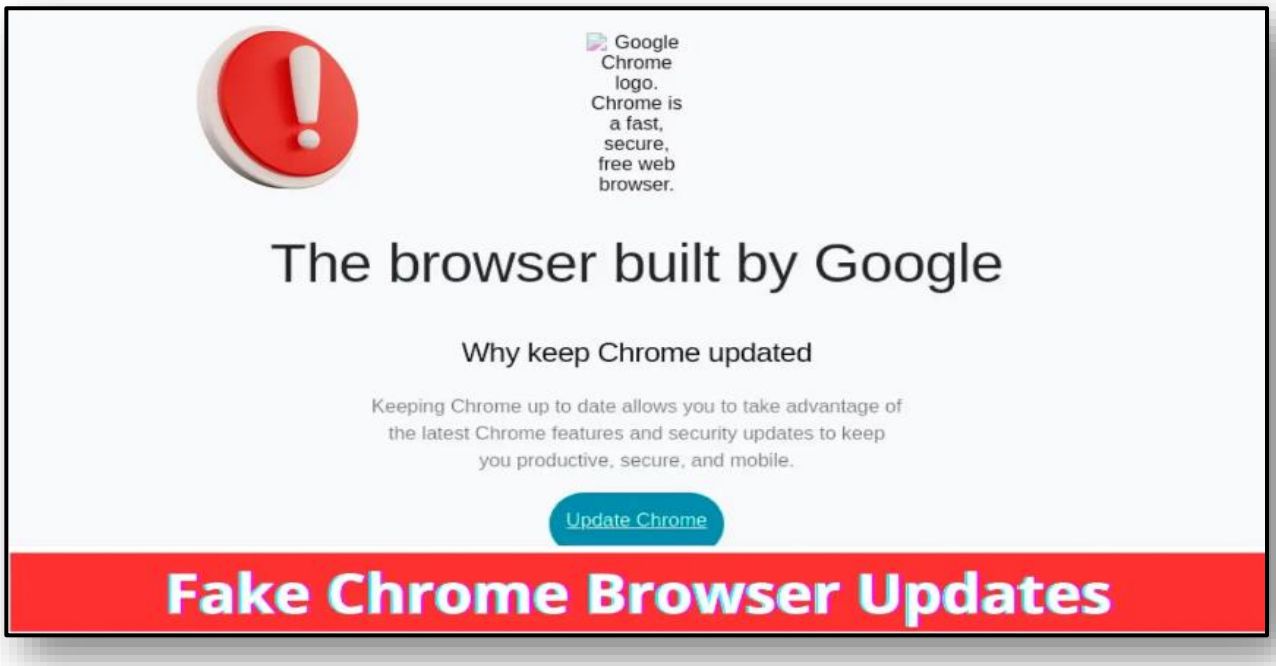
hxxps://ponraj[.]com/05e2f56dd5d8c33a6c402a19629be61c__9336ebf25087d91c818ee6e9ec29f8c1/1.bat? 964084

hxxps://ponraj[.]com/05e2f56dd5d8c33a6c402a19629be61c__9336ebf25087d91c818ee6e9ec29f8c1/tempy.7z

hxxps://ponraj[.]com/

05e2f56dd5d8c33a6c402a19629be 61c__9336ebf25087d91c818ee6e9ec29f8c1/7zz.exe
hxxps://ponraj[.]com

/05e2f56dd5d8c33a6c402a19629be61c__9336ebf25087d91c818ee6e9ec29f8c1/2.bat




**3. RECOMENDACIONES:**

- **Descargar solo desde fuentes confiables:** Descargar software y actualizaciones únicamente desde fuentes oficiales y confiables.
- **No hacer clic en enlaces sospechosos:** Evitar hacer clic en enlaces de sitios web desconocidos o en mensajes de correos electrónicos no solicitados que ofrezcan actualizaciones de software. Es preferible acceder directamente al sitio oficial del software desde el navegador.
- **Configurar Chrome para que se actualice automáticamente:** De esta manera, se recibirá las actualizaciones legítimas directamente del navegador sin necesidad de interactuar con mensajes emergentes.
- **Verificar la URL del sitio web:** Antes de descargar cualquier actualización, verifica la URL del sitio web para asegurarte de que estás en el sitio oficial. Los ciberdelincuentes crean a menudo sitios web falsos con nombres similares para engañar a los usuarios.
- **Mantener el software actualizado:** Además de mantener Chrome actualizado, asegúrese de que su sistema operativo y otros programas también estén actualizados. Los parches de seguridad y las actualizaciones pueden corregir vulnerabilidades que los atacantes podrían aprovechar.

| | |
|---|---|
| Fuente de Información: | • hxxps://gbhackers.com/papercut-flaw-windows-servers/ |