Daniel Ubalde

danielubaldelaguia@gmail.com

Descripción breve

Curso de especialización en ciberseguridad 2022

Detección de incidentes Caso de uso para dispositivos IoT



[1 Descripción 2](#_Toc128830508)

[2 Técnicas relacionadas MITRE 3](#_Toc128830509)

[2.1 T1566.001 Phishing: Spear Phishing 3](#_Toc128830510)

[2.2 T1110.003 Brute Force: Password Spraying 3](#_Toc128830511)

[2.3 T1110.004 Brute Force: Credential Stuffing 3](#_Toc128830512)

[2.4 T1190 Exploit Public-Facing Application 3](#_Toc128830513)

[2.5 T1557 Adversary-in-the-Middle 3](#_Toc128830514)

[3 Detección 4](#_Toc128830515)

[3.1 Página de login falsificada 4](#_Toc128830516)

[3.2 Cambio de configuración en cuentas 4](#_Toc128830517)

[3.3 Inicios de sesión fallidos 4](#_Toc128830518)

[3.4 Inicios de sesión sospechosos 4](#_Toc128830519)

[3.5 Conexiones sospechosas 4](#_Toc128830520)

[4 Fuentes de datos 5](#_Toc128830521)

[4.1 Registros de inicio de sesión 5](#_Toc128830522)

[4.2 Registros de eventos del sistema 5](#_Toc128830523)

[4.3 Registros de tráfico de red 5](#_Toc128830524)

[4.4 Monitorización de archivos 5](#_Toc128830525)

[4.5 Análisis de comportamiento 5](#_Toc128830526)

[4.6 Eventos de autenticación fallida 5](#_Toc128830527)

[5 Diagrama 6](#_Toc128830528)

# Descripción

Se plantea el caso de un robo de credenciales de usuario en el producto Home Assistant de Bionica Automations.

Home Assistant es un software de automatización del hogar de código abierto que permite controlar y monitorear una variedad de dispositivos y servicios en el hogar a través de una interfaz de usuario centralizada. Con Home Assistant, los usuarios pueden integrar dispositivos y servicios domésticos inteligentes de diferentes marcas y tecnologías en una sola plataforma, lo que les permite controlar y automatizar de manera eficiente las funciones de la casa, como la iluminación, la calefacción, la seguridad y los electrodomésticos.

Home Assistant se ejecuta en diferentes sistemas operativos, incluyendo Linux, y se puede instalar en diferentes tipos de hardware, desde dispositivos Raspberry Pi hasta servidores dedicados. La aplicación web de Home Assistant proporciona una interfaz de usuario fácil de usar para administrar la configuración y las automatizaciones de la casa, y también se pueden usar aplicaciones móviles para acceder a Home Assistant de forma remota.

El objetivo del caso de uso es identificar que impactos puede tener un robo de credenciales de acceso en Home Assistant y como detectarlo.

# Técnicas relacionadas MITRE

Han sido incluidas las tácticas aplicables al caso de uso.

El atacante en este caso de uso podría utilizar las siguientes técnicas de Mitre para robar las credenciales de Home Assistant:

## T1566.001 Phishing: Spear Phishing

El atacante podría enviar correos electrónicos diseñados para parecer legítimos a los usuarios de la aplicación, solicitando que ingresen sus credenciales de inicio de sesión en una página web falsa creada por el atacante simulado el portal de inicio de sesión de Home Assistant.

## T1110.003 Brute Force: Password Spraying

El atacante podría probar una lista de contraseñas comunes o débiles utilizando un ataque de diccionario contra la cuenta de inicio de sesión de Home Assistant hasta que se encuentre una contraseña válida.

## T1110.004 Brute Force: Credential Stuffing

Un atacante puede utilizar credenciales filtradas de otros sitios web para intentar iniciar sesión en Home Assistant.

## T1190 Exploit Public-Facing Application

Si Home Assistant tiene una vulnerabilidad conocida que permita la ejecución remota de código o la escalada de privilegios, el atacante podría explotarla para obtener acceso a la cuenta de inicio de sesión de Home Assistant.

## T1557 Adversary-in-the-Middle

Un atacante puede interceptar el tráfico de red entre el usuario y Home Assistant para capturar las credenciales de inicio de sesión, aunque es poco probable la extracción de información de estas comunicaciones ya que van cifradas con un certificado web de 3072 bits.

De igual forma utilizando una combinación de la técnica T1566.001 Phishing: Spear Phishing el atacante simularía una pagina de inicio de sesión igual a la de Home Assistant para así poder capturar las credenciales de usuario.

# Detección

La detección de robos de credenciales según la matriz de MITRE se puede realizar mediante la monitorización de los siguientes indicadores:

## Página de login falsificada

Mediante el análisis de correos electrónicos entrantes y salientes, registros DNS, registros de cortafuegos y registros de proxy web. Aunque esto queda fuera de las capacidades del dispositivo de Home Assistant ya que no hace dichas funciones.

## Cambio de configuración en cuentas

Como intentos de inicio de sesión con credenciales incorrectas, intentos de inicio de sesión desde ubicaciones inusuales, cambios en la configuración de la cuenta y actividades de redireccionamiento.

## Inicios de sesión fallidos

Como intentos repetidos de inicio de sesión con diferentes credenciales, que pueden indicar un intento de adivinación de contraseña.

## Inicios de sesión sospechosos

Los registros de eventos del sistema, como los registros de inicio de sesión, pueden indicar actividades sospechosas, como un inicio de sesión exitoso en una hora o ubicación inusual o el uso de credenciales de usuario que no coinciden con la información de la cuenta. La monitorización y análisis de los registros de eventos puede ayudar a identificar actividad malintencionada y potencialmente detectar el robo de credenciales.

Se deben analizar los registros de Home Assistant en busca de actividad inusual o sospechosa, como intentos de inicio de sesión repetidos o solicitudes inusuales a la API.

## Conexiones sospechosas

El tráfico de red relacionado con el robo de credenciales, como la transmisión de archivos de credenciales o la comunicación con servidores de comando y control, puede ser detectado mediante herramientas de análisis de tráfico de red como un NIDS. La monitorización de los patrones de tráfico inusual o no autorizado puede ayudar a detectar el robo de credenciales.

La actividad de la red debe ser monitoreada en busca de patrones inusuales, como tráfico proveniente de direcciones IP desconocidas o solicitudes de API inusuales.

# Fuentes de datos

## Registros de inicio de sesión

Los registros de inicio de sesión pueden proporcionar información detallada sobre quién intenta iniciar sesión en Home Assistant y cuándo.

## Registros de eventos del sistema

Los registros de eventos del sistema, como el registro de eventos de Windows, pueden mostrar intentos de inicio de sesión fallidos, intentos de inicio de sesión exitosos inesperados o cambios en la configuración del sistema que podrían indicar que se ha comprometido una cuenta de usuario.

## Registros de tráfico de red

La monitorización de la red, incluyendo la inspección profunda de paquetes, puede ayudar a detectar el tráfico de red anómalo que pueda estar relacionado con el robo de credenciales. Por ejemplo, si se detecta una gran cantidad de tráfico de inicio de sesión en una dirección IP desconocida, podría ser una indicación de que las credenciales han sido robadas.

## Monitorización de archivos

La monitorización de archivos, incluyendo el seguimiento de cambios en los archivos de credenciales del sistema, puede ayudar a detectar el robo de credenciales. Si se detecta un cambio inesperado en un archivo de credenciales, puede ser una señal de que se ha producido un robo de credenciales.

No solo los ficheros de almacenamiento de claves pueden ser un objetivo en este tipo de ataques, sino que también pueden modificar archivos del sistema para instalar software malicioso. También es poco probable debido a la naturaleza del producto ya que Home Assistant está basado en una arquitectura de contenedores.

## Análisis de comportamiento

El análisis de comportamiento puede ayudar a detectar el robo de credenciales. Por ejemplo, si una cuenta de usuario inicia sesión desde una ubicación geográfica inusual o en un momento inusual, podría ser una señal de que las credenciales han sido robadas y están siendo utilizadas por un atacante.

## Eventos de autenticación fallida

Si un adversario está intentando acceder a un sistema o servicio utilizando credenciales robadas, es posible que se produzcan varios intentos fallidos de inicio de sesión. El registro de eventos de autenticación fallida puede proporcionar información valiosa para detectar estos intentos.

# Diagrama