Daniel Ubalde

danielubaldelaguia@gmail.com

Descripción breve

Curso de especialización en ciberseguridad 2022

Detección de incidentes Caso de uso para dispositivos IoT



[1 Descripción 3](#_Toc128331780)

[1.1 Métodos comunes de robo de credenciales 3](#_Toc128331781)

[1.1.1 Phishing 3](#_Toc128331782)

[1.1.2 Keylogging 3](#_Toc128331783)

[1.1.3 Ingeniería social 3](#_Toc128331784)

[1.1.4 Malware 3](#_Toc128331785)

[1.1.5 Ataques de fuerza bruta 3](#_Toc128331786)

[2 Técnicas relacionadas MITRE 4](#_Toc128331787)

[2.1 T1557 Adversary-in-the-Middle 4](#_Toc128331788)

[2.2 T1110 Brute Force 4](#_Toc128331789)

[2.3 T1555 Credentials from Password Stores 5](#_Toc128331790)

[2.4 T1212 Exploitation for Credential Access 5](#_Toc128331791)

[2.5 T1621 Multi-Factor Authentication Request Generation 5](#_Toc128331792)

[2.6 T1528 Steal Application Access Token 6](#_Toc128331793)

[2.7 T1649 Steal or Forge Authentication Certificates 7](#_Toc128331794)

[2.8 T1539 Steal Web Session Cookie 8](#_Toc128331795)

[2.9 T1552 Unsecured Credentials 9](#_Toc128331796)

[3 Detección 10](#_Toc128331797)

[3.1 Detección de actividades de phishing o spear phishing 10](#_Toc128331798)

[3.2 Detección de actividad inusual en cuentas de usuario 10](#_Toc128331799)

[3.3 Detección de actividad de fuerza bruta 10](#_Toc128331800)

[3.4 Detección de credenciales en texto claro 10](#_Toc128331801)

[3.5 Monitoreo de registros 10](#_Toc128331802)

[3.6 Análisis de tráfico de red 10](#_Toc128331803)

[3.7 Monitorización de endpoints 10](#_Toc128331804)

[3.8 Monitoreo de cuentas de usuario 11](#_Toc128331805)

[4 Fuentes de datos 12](#_Toc128331806)

[4.1 Registros de eventos del sistema 12](#_Toc128331807)

[4.2 Monitorización de red 12](#_Toc128331808)

[4.3 Detección de malware 12](#_Toc128331809)

[4.4 Monitorización de archivos 12](#_Toc128331810)

[4.5 Análisis de comportamiento 12](#_Toc128331811)

[4.6 Eventos de autenticación fallida 12](#_Toc128331812)

[4.7 Análisis de actividad del sistema 13](#_Toc128331813)

[5 Diagrama 13](#_Toc128331814)

# Descripción

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

Home Assistant es un HUB inteligente de dispositivos IoT que posee una interfaz web por HTTPS a través de un proxy que puede estar expuesto a internet, un servidor SSH para mantenimiento, un servidor SNTP y NTP para los dispositivos IoT locales, un bróker MQTT y MQTTS. Los métodos de autenticación que admite el cliente web son: autenticación básica con usuario y contraseña con o sin MFA y autenticación con token con posibilidad de hacer llamadas a la API.

El objetivo del caso de uso es identificar como las credenciales de acceso puedes ser sustraídas de un sistema informático y prevenir que eso suceda.

## Métodos comunes de robo de credenciales

### Phishing

Este es uno de los métodos más utilizados para robar credenciales. Consiste en engañar al usuario para que proporcione sus credenciales a través de una página web falsa que se parece a la de un sitio web legítimo. Los atacantes pueden enviar correos electrónicos o mensajes de texto que parecen provenir de una fuente confiable, como una empresa o una institución financiera, para solicitar información de inicio de sesión.

### Keylogging

Este tipo de robo de credenciales implica la instalación de un software espía en el dispositivo del usuario para registrar todo lo que se escribe en el teclado, incluidas las credenciales de inicio de sesión.

### Ingeniería social

Este tipo de robo de credenciales involucra a un atacante que intenta engañar al usuario para que revele sus credenciales mediante el uso de la persuasión o la manipulación psicológica. Por ejemplo, un atacante puede hacerse pasar por un empleado de una empresa y llamar al usuario para pedirle sus credenciales de inicio de sesión.

### Malware

El malware es un software malicioso que puede instalarse en el dispositivo del usuario sin su conocimiento. Una vez instalado, el malware puede registrar las credenciales de inicio de sesión y enviarlas al atacante.

### Ataques de fuerza bruta

Este tipo de ataque implica a un atacante que intenta adivinar las credenciales de inicio de sesión mediante la prueba de diferentes combinaciones de nombres de usuario y contraseñas hasta que se encuentre la combinación correcta.

# Técnicas relacionadas MITRE

## T1557 Adversary-in-the-Middle

Los adversarios pueden intentar posicionarse entre dos o más dispositivos conectados en red utilizando una técnica de adversario-en-el-medio (AiTM) para llevar a cabo comportamientos secundarios como el Espionaje de Red o la Manipulación de Datos Transmitidos. Al abusar de las características de los protocolos de red comunes que pueden determinar el flujo del tráfico de red (por ejemplo, ARP, DNS, LLMNR, etc.), los adversarios pueden forzar a un dispositivo a comunicarse a través de un sistema controlado por un adversario para recopilar información o realizar acciones adicionales.

Por ejemplo, los adversarios pueden manipular la configuración DNS de la víctima para permitir otras actividades maliciosas, como evitar/redirigir a los usuarios para que no accedan a sitios legítimos y/o propagar malware adicional. Los adversarios también pueden manipular DNS y aprovechar su posición para interceptar credenciales de usuario y cookies de sesión. Los Ataques de Degradación también se pueden utilizar para establecer una posición AiTM, como al negociar una versión de protocolo de comunicación (SSL/TLS) o algoritmo de cifrado menos seguro, obsoleto o más débil.

Los adversarios también pueden aprovechar la posición AiTM para intentar monitorear y/o modificar el tráfico, como en la Manipulación de Datos Transmitidos. Los adversarios pueden establecer una posición similar a AiTM para evitar que el tráfico fluya hacia el destino adecuado, potencialmente para debilitar las defensas y/o en apoyo de un Ataque de Denegación de Servicio de Red.

## T1110 Brute Force

Los adversarios pueden utilizar técnicas de fuerza bruta para acceder a cuentas cuando las contraseñas son desconocidas o cuando se obtienen hashes de contraseñas. Sin conocimiento de la contraseña de una cuenta o conjunto de cuentas, un adversario puede adivinar sistemáticamente la contraseña utilizando un mecanismo repetitivo o iterativo. La fuerza bruta de contraseñas puede ocurrir mediante la interacción con un servicio que verificará la validez de esas credenciales o sin conexión con datos de credenciales previamente adquiridos, como hashes de contraseñas.

La fuerza bruta de credenciales puede ocurrir en varios puntos durante una brecha. Por ejemplo, los adversarios pueden intentar forzar el acceso a Cuentas Válidas dentro de un entorno víctima aprovechando el conocimiento recopilado de otros comportamientos posteriores al compromiso del sistema, como el volcado de credenciales del sistema operativo, el descubrimiento de cuentas o el descubrimiento de políticas de contraseñas. Los adversarios también pueden combinar la actividad de fuerza bruta con comportamientos como servicios remotos externos como parte del Acceso Inicial.

## T1555 Credentials from Password Stores

Los adversarios pueden buscar lugares comunes de almacenamiento de contraseñas para obtener las credenciales de usuario. Las contraseñas se almacenan en varios lugares en un sistema, dependiendo del sistema operativo o de la aplicación que mantenga las credenciales. También hay aplicaciones específicas que almacenan contraseñas para facilitar a los usuarios su gestión y mantenimiento. Una vez que se obtienen las credenciales, pueden utilizarse para realizar movimientos laterales y acceder a información restringida.

## T1212 Exploitation for Credential Access

Los adversarios pueden explotar vulnerabilidades de software para intentar recopilar credenciales. La explotación de una vulnerabilidad de software ocurre cuando un adversario aprovecha un error de programación en un programa, servicio, o dentro del sistema operativo o del kernel en sí, para ejecutar código controlado por el adversario. Los mecanismos de credenciales y autenticación pueden ser objetivos de explotación por parte de los adversarios como un medio para obtener acceso a credenciales útiles o para evitar el proceso de acceso a sistemas. Un ejemplo de esto es MS14-068, que apunta a Kerberos y se puede utilizar para forjar tickets de Kerberos utilizando permisos de usuario de dominio. La explotación para el acceso a credenciales también puede resultar en una escalada de privilegios, dependiendo del proceso objetivo o de las credenciales obtenidas.

## T1621 Multi-Factor Authentication Request Generation

Los adversarios pueden intentar evadir los mecanismos de autenticación multifactor (MFA) y obtener acceso a cuentas generando solicitudes de MFA enviadas a los usuarios.

Los adversarios en posesión de credenciales de Cuentas Válidas pueden ser incapaces de completar el proceso de inicio de sesión si carecen de acceso a los mecanismos de 2FA o MFA requeridos como un control de seguridad adicional. Para eludir esto, los adversarios pueden abusar de la generación automática de notificaciones push a servicios de MFA como Duo Push, Microsoft Authenticator, Okta o servicios similares para que el usuario conceda acceso a su cuenta.

En algunos casos, los adversarios pueden repetir continuamente los intentos de inicio de sesión para bombardear a los usuarios con notificaciones push de MFA, mensajes de texto y llamadas telefónicas, lo que potencialmente resulta en que el usuario finalmente acepte la solicitud de autenticación en respuesta a la "fatiga de MFA".

## T1528 Steal Application Access Token

Los adversarios pueden robar tokens de acceso de aplicaciones como medio para adquirir credenciales y acceder a sistemas y recursos remotos.

Los tokens de acceso de aplicaciones se utilizan para realizar solicitudes de API autorizadas en nombre de un usuario o servicio y se utilizan comúnmente como una forma de acceder a recursos en aplicaciones basadas en la nube, contenedores y software como servicio (SaaS). OAuth es un marco comúnmente implementado que emite tokens a los usuarios para acceder a sistemas. Los adversarios que roban tokens de API de cuentas en entornos en la nube y contenerizados pueden acceder a datos y realizar acciones con los permisos de estas cuentas, lo que puede llevar a una escalada de privilegios y una mayor compromiso del entorno.

En entornos de Kubernetes, los procesos que se ejecutan dentro de un contenedor se comunican con el servidor de API de Kubernetes utilizando tokens de cuenta de servicio. Si se compromete un contenedor, un atacante puede robar el token del contenedor y, por lo tanto, obtener acceso a los comandos de API de Kubernetes.

El robo de tokens también puede ocurrir a través de la ingeniería social, en cuyo caso puede ser necesaria la acción del usuario para conceder el acceso. Una aplicación que desea acceder a servicios basados en la nube o API protegidas puede obtener acceso utilizando OAuth 2.0 a través de una variedad de protocolos de autorización. Un ejemplo de secuencia comúnmente utilizada es el flujo de concesión de código de autorización de Microsoft. Un token de acceso de OAuth permite que una aplicación de terceros interactúe con recursos que contienen datos de usuario de las formas solicitadas por la aplicación sin obtener credenciales de usuario.

Los adversarios pueden aprovechar la autorización de OAuth mediante la construcción de una aplicación maliciosa diseñada para que se le conceda acceso a los recursos con el token de OAuth del usuario objetivo. El adversario deberá completar el registro de su aplicación con el servidor de autorización, por ejemplo, Microsoft Identity Platform utilizando Azure Portal, el IDE de Visual Studio, la interfaz de línea de comandos, PowerShell o llamadas de API REST. Luego, pueden enviar un enlace de spearphishing al usuario objetivo para incitarlo a conceder acceso a la aplicación. Una vez que se concede el token de acceso de OAuth, la aplicación puede obtener acceso potencialmente a largo plazo a las características de la cuenta del usuario a través del token de acceso de la aplicación.

Los tokens de acceso de aplicaciones pueden funcionar dentro de un tiempo de vida limitado, lo que limita el tiempo que un adversario puede utilizar el token robado. Sin embargo, en algunos casos, los adversarios también pueden robar tokens de actualización de aplicaciones, lo que les permite obtener nuevos tokens de acceso sin solicitar la acción del usuario.

## T1649 Steal or Forge Authentication Certificates

Los adversarios pueden robar o falsificar certificados utilizados para la autenticación y acceder a sistemas o recursos remotos. Los certificados digitales a menudo se utilizan para firmar y cifrar mensajes y/o archivos. También se utilizan como material de autenticación. Por ejemplo, los certificados de dispositivo de Azure AD y los certificados de servicios de certificados de Active Directory (AD CS) se vinculan a una identidad y se pueden utilizar como credenciales para cuentas de dominio.

Los certificados de autenticación pueden ser robados y falsificados. Por ejemplo, los certificados AD CS se pueden robar del almacenamiento cifrado (en el Registro o archivos), archivos de certificados extraviados (es decir, credenciales no seguras) o directamente desde el almacén de certificados de Windows a través de varias API criptográficas. Con los derechos de inscripción apropiados, los usuarios y/o máquinas dentro de un dominio también pueden solicitar y/o renovar manualmente certificados de autoridades de certificación (CA) empresariales. Este proceso de inscripción define varios ajustes y permisos asociados con el certificado. Cabe destacar que los valores de uso de clave extendida (EKU) del certificado definen los casos de uso de firma, cifrado y autenticación, mientras que los valores de nombre alternativo de sujeto (SAN) del certificado definen los nombres alternativos del propietario del certificado.

El abuso de los certificados para obtener credenciales de autenticación puede permitir otros comportamientos, como el movimiento lateral. Las configuraciones incorrectas relacionadas con los certificados también pueden permitir oportunidades de escalada de privilegios, permitiendo a los usuarios suplantar o asumir cuentas o permisos privilegiados a través de las identidades (SAN) asociadas con un certificado. Estos abusos también pueden permitir la persistencia mediante el robo o falsificación de certificados que se pueden utilizar como cuentas válidas durante la validez del certificado, a pesar de los reinicios de contraseña del usuario. Los certificados de autenticación también pueden ser robados y falsificados para cuentas de máquina.

Los adversarios que tienen acceso a las claves privadas de los certificados de CA raíz (o subordinados) (o a los mecanismos que protegen/administran estas claves) también pueden establecer persistencia mediante la falsificación de certificados de autenticación arbitrarios para el dominio víctima (conocidos como certificados "dorados"). Los adversarios también pueden dirigirse a los certificados y servicios relacionados para acceder a otras formas de credenciales, como los tickets de concesión de tickets (TGT) de Golden Ticket o el texto sin formato de NTLM.

## T1539 Steal Web Session Cookie

Un adversario puede robar cookies de sesión de aplicaciones web o servicios y usarlas para acceder a aplicaciones web o servicios de Internet como un usuario autenticado sin necesidad de credenciales. Las aplicaciones web y los servicios a menudo utilizan cookies de sesión como un token de autenticación después de que un usuario se ha autenticado en un sitio web.

Las cookies suelen ser válidas por un período de tiempo prolongado, incluso si la aplicación web no se utiliza activamente. Las cookies se pueden encontrar en el disco, en la memoria del proceso del navegador y en el tráfico de red hacia sistemas remotos. Además, otras aplicaciones en la máquina del objetivo pueden almacenar cookies de autenticación sensibles en la memoria (por ejemplo, aplicaciones que se autentican en servicios en la nube). Las cookies de sesión se pueden utilizar para evitar algunos protocolos de autenticación multifactor.

Existen varios ejemplos de malware que apuntan a las cookies de los navegadores web en el sistema local. También existen frameworks de código abierto como Evilginx 2 y Muraena que pueden recopilar cookies de sesión a través de un proxy malicioso (por ejemplo, un adversario en el medio) que puede ser configurado por un adversario y utilizado en campañas de phishing.

Después de que un adversario adquiere una cookie válida, puede realizar una técnica de Cookie de Sesión Web para iniciar sesión en la aplicación web correspondiente.

## T1552 Unsecured Credentials

Los adversarios pueden buscar en sistemas comprometidos para encontrar y obtener credenciales almacenadas de manera insegura. Estas credenciales pueden ser almacenadas o extraviadas en muchos lugares en un sistema, incluyendo archivos de texto sin formato (por ejemplo, Historial de Bash), repositorios específicos del sistema operativo o aplicación (por ejemplo, Credenciales en el Registro) u otros archivos/artefactos especializados (por ejemplo, Claves privadas).

# Detección

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

## Detección de actividades de phishing o spear phishing

Mediante el análisis de correos electrónicos entrantes y salientes, registros DNS, registros de cortafuegos y registros de proxy web.

## Detección de actividad inusual en cuentas de usuario

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.

## Detección de actividad de fuerza bruta

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

## Detección de credenciales en texto claro

Como la lectura de archivos de configuración, la monitorización de bases de datos y la exploración de sistemas.

## Monitoreo de registros

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.

## Análisis de tráfico de red

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. La monitorización de los patrones de tráfico inusual o no autorizado puede ayudar a detectar el robo de credenciales.

## Monitorización de endpoints

Las herramientas de seguridad en endpoints pueden detectar actividades sospechosas relacionadas con el robo de credenciales, como el uso de herramientas de hacking o el acceso a archivos y carpetas de sistema no autorizados. La monitorización de los endpoints también puede ayudar a detectar el uso de credenciales robadas para acceder a recursos de red.

## Monitoreo de cuentas de usuario

El monitoreo regular de las cuentas de usuario puede detectar actividad sospechosa, como el inicio de sesión en una nueva ubicación o la actividad de la cuenta fuera de las horas normales de trabajo. El monitoreo también puede detectar el uso de credenciales robadas para acceder a recursos de red y puede ayudar a tomar medidas inmediatas para bloquear las cuentas comprometidas.

# Fuentes de datos

## 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.

## Monitorización 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.

## Detección de malware

La detección de malware puede ser una señal de que se ha producido un robo de credenciales. Muchos tipos de malware están diseñados para robar credenciales, por lo que la detección de un malware sospechoso podría ser una indicación de que se ha producido un robo de credenciales.

## 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.

## 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.

## Análisis de actividad del sistema

Algunos ataques de robo de credenciales pueden dejar rastros en la actividad del sistema. Por ejemplo, si un adversario está utilizando una herramienta de keylogging para robar credenciales, es posible que se detecten patrones inusuales de actividad del sistema que indiquen la presencia de la herramienta.

# Diagrama

