Table of Contents

Trend Micro

¿Que es Trend Micro?

Trend Micro es una empresa global de **ciberseguridad** que ofrece una amplia gama de soluciones para **proteger dispositivos, redes y datos** en entornos empresariales, en la nube, y para usuarios finales. Fundada en 1988, Trend Micro se ha destacado en la industria por sus productos de software antivirus, seguridad en la nube, seguridad en servidores, y soluciones de detección y respuesta a amenazas (EDR), además de su capacidad de **identificar y bloquear amenazas emergentes** mediante el uso de inteligencia artificial, machine learning y una extensa red global de detección de amenazas.

Alianza con Trend Micro Cybersecurity

VIVOTEK es el primer fabricante de soluciones de vigilancia en red del mundo que coopera con la empresa de ciberseguridad de renombre mundial, Trend Micro. A través de cámaras de red equipadas con el software antiintrusión de Trend Micro, VIVOTEK ofrece alta seguridad y una vigilancia de red sólida para proteger vidas y datos.

En colaboración con socios de software de ciberseguridad, VIVOTEK se centra en la creación de productos y software de seguridad de red que cumplan con los protocolos de la industria, así como en el desarrollo constante de escudos para aumentar su protección contra diversos ciberataques. Al elegir las soluciones de VIVOTEK, los usuarios pueden experimentar no solo productos de alta calidad, sino también entornos de red más seguros.

Trend Micro

Protección multicapa con Trend Micro IoT Security

La protección multicapa que incluye detección de ataques de fuerza bruta, detección y prevención de intrusiones y control de daños instantáneo protegerá automáticamente su sistema de red con las últimas actualizaciones de firmas.

Gestión de alarmas de ciberseguridad con alertas instantáneas

Una vez configuradas las notificaciones de eventos en las cámaras de red y VAST 2 VMS, la solución de vigilancia de VIVOTEK recibirá alertas inmediatas cuando se produzcan ciberataques.

Informe de eventos de ciberseguridad con panel interactivo

Conozca rápidamente la tendencia y el estado de los ataques y adquiera información sobre ellos para diagnosticar rápidamente su red en los VMS y NVR VAST 2 de VIVOTEK.

Notificaciones de eventos instantáneos

Eventos de ataque de fuerza bruta

Cuando el sistema detecta ataques de fuerza bruta, activará automáticamente un mecanismo de defensa para bloquear esa dirección IP y evitar futuros ataques.

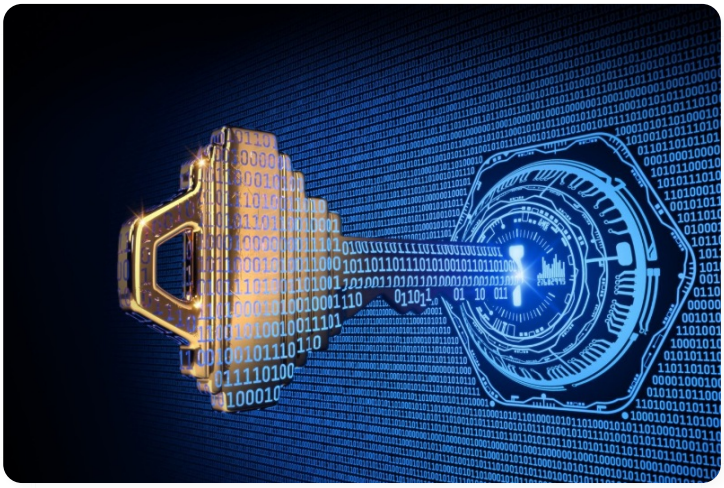
Eventos de ciberataques

Cuando el sistema detecta cualquier tipo de ataque de seguridad cibernética además de ataques de fuerza bruta, activará automáticamente un mecanismo de defensa para bloquear esa dirección IP y evitar futuros ataques.

Eventos de cuarentena

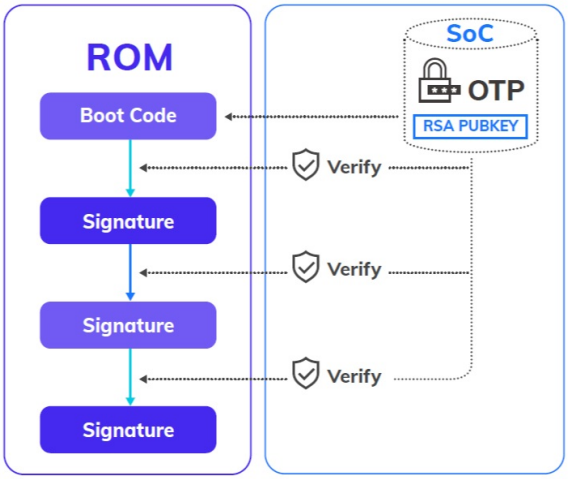
Si un dispositivo sospechoso intenta acceder a la red, o si un dispositivo sospechoso intenta acceder a cámaras IP y accede a un comportamiento de red que cumple con la regla de firma de Trend Micro, el sistema pondrá en cuarentena el comportamiento del ataque para evitar daños mayores.

Producto con seguridad reforzada



Firmware firmado - Firmware autorizado de VIVOTEK

El firmware firmado de VIVOTEK requiere una firma digital en el firmware y la verificación de la firma por parte de VIVOTEK, lo que garantiza que los usuarios puedan confiar en que el firmware no ha sido alterado. Un dispositivo con firmware firmado puede validar el firmware antes de permitir la instalación. Al aplicar los certificados y las claves firmadas al firmware, se garantiza que todos los datos estén protegidos y cifrados sin exposición ni riesgo de alteración por parte de piratas informáticos.



Arranque seguro: seguro desde el principio

Al aplicar el firmware firmado de VIVOTEK, la cámara puede iniciarse de forma segura paso a paso. El arranque seguro es un mecanismo que protege el firmware del producto instalado. Durante el proceso de arranque, el arranque seguro bloquea el código no autenticado o alterado. Además, el firmware firmado garantiza que la cámara se restablezca de forma segura a los valores predeterminados de fábrica y el arranque seguro garantiza que se rechace el código no autenticado, lo que protege al sistema de la cámara de ataques o infecciones por código externo malicioso.

Consola segura: conexión protegida constante

Sobre la base del arranque seguro, actualizamos el mecanismo de seguridad de acceso remoto y desactivamos la consola de la cámara desde el protocolo SSH y SFTP, lo que defiende la vulnerabilidad del sistema. El permiso de VIVOTEK con autenticación basada en clave es la única forma de acceder, lo que proporciona una conexión más segura para el sistema de vigilancia.

VADP seguro: seguridad mejorada para la integración con terceros

La plataforma de desarrollo de aplicaciones de VIVOTEK (VADP) ofrece una plataforma abierta que permite a los desarrolladores agregar funciones para escenarios o aplicaciones específicos con las cámaras de VIVOTEK. Proteger la VADP con seguridad mejorada es fundamental. La aplicación de la VADP segura con capacidades de firma digital y cifrado la hace más segura y confiable para la integración de terceros.

Abstracto

Incentivos para hackear cámaras de vigilancia IP

Hoy en día, la principal motivación de los hackers es la monetización. En lo que respecta a la monetización, las cámaras de vigilancia IP son grandes objetivos por las siguientes razones:

1. Constantemente conectado: la alta exposición a Internet hace que sea fácil para los piratas informáticos encontrar el dispositivo. Una vez pirateado, el dispositivo estará constantemente disponible para satisfacer las necesidades de los piratas informáticos.

2. Bajas inversiones en piratería: a diferencia de piratear una PC, una vez que los piratas informáticos ven una forma de piratear un dispositivo, el mismo enfoque generalmente se puede aplicar a otros dispositivos de modelos similares, lo que genera un costo de piratería por dispositivo muy bajo.

3. Falta de supervisión: a diferencia de las computadoras de oficina, las cámaras de vigilancia IP no están bien administradas por personal con conocimientos en ciberseguridad. Tampoco es posible instalar una aplicación antimalware en el mercado secundario.

4. Alto rendimiento: la potencia informática inactiva dentro de una cámara de vigilancia IP suele ser lo suficientemente buena para realizar tareas específicas de los piratas informáticos, como la minería de criptomonedas, incluso sin que los usuarios finales lo noten.

5. Gran ancho de banda frente a Internet: el ancho de banda enorme y rápido de conexión permanente diseñado para la comunicación por vídeo es el objetivo perfecto para que los piratas informáticos inicien ataques DDoS.

Cadena de piratería/infección

La cadena de infección típica de las cámaras de vigilancia IP consta de los siguientes pasos:

1. Descubrir dirección: Localizar la dirección IP de un dispositivo víctima potencial, tarea que suelen realizar los rastreadores de Internet. Los servicios web como “Shodan” también pueden ofrecer una lista de dispositivos descubiertos.

2. Obtener acceso: utilice la contraseña predeterminada o el diccionario de contraseñas para iniciar sesión en el dispositivo. Una vez que obtengan el privilegio de administrador, los piratas informáticos podrán seguir utilizando el sistema para sus acciones maliciosas.

3. Explotar vulnerabilidades: analizar las vulnerabilidades del sistema y aprovecharlas. Las vulnerabilidades del sistema son inevitables, especialmente en un mundo de TI en constante cambio, donde se utilizan ampliamente los códigos de fuente abierta.

4. Inyección de malware: instala malware en la cámara de vigilancia IP. El malware generalmente consta de un agente que maneja la comunicación y un cuerpo principal que cumple las funciones principales diseñadas por los piratas informáticos.

5. Comando y control: controle a las víctimas de forma remota para habilitar una función de servicio específica. Por ejemplo, los piratas informáticos pueden iniciar un ataque DDoS y ordenar a todos los dispositivos infectados que apunten a un destino específico.