FIREEYE™

## FICHA TÉCNICA

# Cyber Physical Threat Intelligence

**Céntrese en los ataques contra sistemas físicos complejos, interconectados y administrados por software.**

### ASPECTOS DESTACADOS

- Análisis e informes sobre vulnerabilidades físicas cibernéticas
- Análisis técnico de las TTP de los autores de amenazas cibernéticas enfocadas al daño físico
- Análisis de información de todas las fuentes de amenazas físicas cibernéticas
- Análisis de noticias e investigación operacional centradas en la tecnología
- Acceso a contenido educacional para aumentar la concientización de la seguridad en todo su equipo

La creciente importancia de las tecnologías de comunicación en diferentes industrias ha impulsado una creciente integración de características digitales que apoyan el control y mantenimiento de los procesos físicos. Esta intersección entre lo virtual y lo físico ha llevado no solo a una conectividad e instrumentación revolucionaria, sino también a riesgos significativos de seguridad.

Es cada vez más importante aprender y compartir de manera proactiva las vulnerabilidades técnicas y las tácticas, técnicas y procedimientos (TTP) viables de los autores de amenazas, a fin de poder anticipar y evitar ataques cibernéticos.

FireEye Cyber Physical Threat Intelligence es un servicio de suscripción que brinda contexto, datos y análisis práctico sobre las amenazas en sistemas físicos cibernéticos, incluyendo tecnología operativa, sistemas industriales de control, Internet de las cosas y otros equipos utilizados para apoyar los procesos físicos en los sectores médicos y de telecomunicaciones, por ejemplo.

**Lo que la subscripción le ofrece**

Para las organizaciones encargadas de mantener la seguridad y la continuidad de estos sistemas, Cyber Physical Intelligence proporciona alertas tempranas sobre vulnerabilidades críticas, así como las campañas de amenazas y los adversarios que las atacan. Con Cyber Physical Intelligence, los equipos de seguridad pueden estar un paso por delante de los atacantes y tomar decisiones mejor informadas sobre el nivel de seguridad de sus sistemas físicos cibernéticos.

La suscripción de Cyber Physical Intelligence incluye informes detallados sobre malware cibernético enfocado al daño físico y tácticas, técnicas y procedimientos maliciosos, autores de amenazas, actividad de amenazas, vulnerabilidades e información estratégica. La tabla 1 detalla las áreas de cobertura cruciales en las que FireEye brinda información en profundidad para los equipos encargados de defender estos sistemas.

**Tabla 1.** Áreas de cobertura de FireEye Cyber Physical Threat Intelligence

| Área de cobertura | Descripción |
|---|---|
| **Inteligencia actual** | El análisis táctico y estratégico de la actividad de amenaza, derivado de los compromisos de FireEye Mandiant, implementó la tecnología FireEye y una extensa red de sensores FireEye implementados en todo el mundo. |
| **Referencia física cibernética** | Revisión de la terminología, arquitectura de la red, seguridad del protocolo y de puertos ICS [Industrial Control System (sistemas de control industrial)] y autores de amenazas cibernéticas enfocadas al daño físico. |
| **Vulnerabilidades físicas cibernéticas** | Informes tácticos sobre las vulnerabilidades de ICS |
| **Actividad en la red de ICS** | Análisis del tráfico en la red de los puertos ICS basados en datos de acceso del firewall. |
| **Resumen de seguridad de ICS** | Recopilación, análisis e implicaciones de las publicaciones de ICS en los medios. |
| **Obtención de información desde FireEye Mandiant** | Revisión continua de los compromisos de Mandiant que examina los datos de tendencias y las mejores prácticas de seguridad. |
| **Herramientas de investigación** | Investigación y análisis de herramientas de reconocimiento y ataque centradas en ICS. |

## Esté un paso por delante de la siguiente generación de amenazas

Los sistemas físicos cibernéticos vienen con un conjunto complejo de beneficios y riesgos. Para anticipar y bloquear las amenazas que tienen como objetivo los sistemas físicos cibernéticos, debe mantener información actualizada sobre los requisitos de seguridad únicos de estas tecnologías:

- Aumente la concientización sobre las vulnerabilidades de seguridad física cibernética relevantes y apoye los esfuerzos de gestión de vulnerabilidades a través de la calificación de vulnerabilidad FireEye y el análisis de las opciones de corrección.
- Obtenga concientización situacional de las amenazas, campañas y autores que tienen como objetivo sus sistemas físicos cibernéticos.
- Capacite a sus equipos internos y partes interesadas externas con materiales de referencia en profundidad y cobertura de eventos temáticos adaptados al mundo físico cibernético.
- Tome decisiones mejor informadas acerca del programa y los controles cambiantes de seguridad física cibernética.
- Obtenga información procesable para ayudar a evolucionar su postura de gestión de riesgos físicos cibernéticos de reactiva a proactiva.

Para obtener más información sobre cómo FireEye Cyber Physical Intelligence puede ayudar a que su equipo de seguridad tome decisiones de seguridad mejor informadas, visite **www.FireEye.com**

**FireEye, Inc.**
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com



**Acerca de FireEye, Inc.**

FireEye es una empresa de seguridad basada en inteligencia. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a la de una nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.