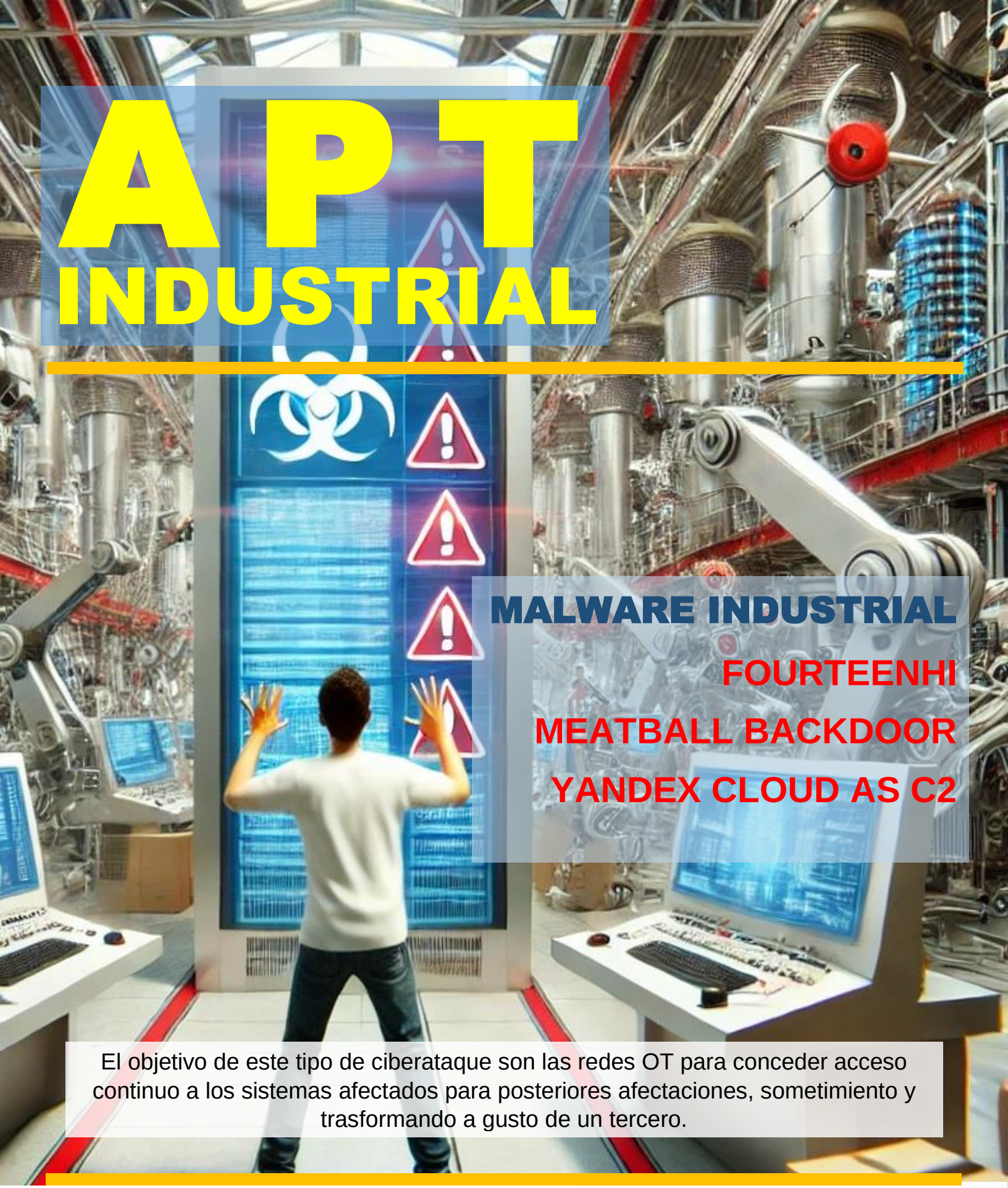
APT INDUSTRIAL



MALWARE INDUSTRIAL

FOURTEENHI

MEATBALL BACKDOOR

YANDEX CLOUD AS C2

El objetivo de este tipo de ciberataque son las redes OT para conceder acceso continuo a los sistemas afectados para posteriores afectaciones, sometimiento y trasformando a gusto de un tercero.

Gobierno DIGITAL

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones

La práctica APT involucra el reconocimiento del objetivo, aprovechando cualquier vulnerabilidad para establecer puertas traseras para indagar prolongada y desapercibidamente las actividades, procesos y rutinas de su víctima creando nuevos y mayores privilegios a la vez que realiza replicación y masificación aprovechando de que se encuentra dentro de la organización u empresa. Luego de establecerse y conocer la operatividad toma el control para sus propósitos o para venderlo a otro.

Las grandes industrias son el objetivo de estas prácticas maliciosas, pero no descarta la posibilidad de las medianas y de los pequeños emprendimientos donde afectan las tecnologías de las operaciones (OT), cambiando procesos físicos, alterando el monitoreo, trasformando hasta la administración y funcionamiento de los dispositivos.

FourteenHi

Malware con arquitectura (x86 y x64) con protocolos de comunicación C2 capacidad de persistencia, protocolo RC4 (para cifrado) de forma segura para el atacante reemplazando una aplicación legítima pero vulnerable con la suplantación de DLL por medio de un archivo binario.

MeatBall Backdoor

Arquitectura (x86 y x64). Capacidad de acceso remoto, crea listas de procesos en ejecución, dispositivos, discos conectados, etc. Al Igual que FourteenHi, se basa en la técnica del secuestro de DLL, implanta parámetros crea accesos descifra claves y mantiene comunicación cifrada a un remoto.

Yandex Cloud as C2

Malware especializado en obtener información sensible de su víctima implantándose al igual que los anteriores crea directorios extrae nuevas cargas útiles para su ejecución.

Recomendación:

Separar las conexiones IT de las OT es importante usar segmentación y segregación de red; es imperativo proteger los activos OT que suelen por lo general tener un largo ciclo vida útil donde pierden soporte o se dificulta la actualización. Es necesario implementar y ejecutar planes de protección de endpoints OT que, aunque parezcan aislados pueden proporcionar puertas de enlace para algún ciberataque a la vez de ser vulnerables.