Fecha: 2025.11.25
Clasificación: Confidencial/ Uso interno RTE
Destinatario: CISO de la RTE (Réseau de Transport d'Électricité)

Evaluación de riesgo y mitigación RTE (2026): Análisis de amenaza híbrida IAB[1], la infraestructura energética y su riesgo de colapso.

El presente análisis identifica que las TTPs[2] asociadas con IABs con mayor probabilidad de afectar los Sistemas de Transmisión RTE especialmente en conjunto con vectores de Ingeniería Social que explotan el error humano y las medidas estratégicas a priorizar en 2026 para mitigar sus daños. Se identificó que este tipo de accesos iniciales pueden llevar a posicionar la Escalada Hibrida IT/OT[3] como riesgo más probable con la falla crítica causada por la falta de segmentación de la red, lo cual justifica una estrategia de Inversión enfocada en corregir y afrontar el pivote como prioridad máxima.

Puntos Claves

- Se determina que las TTP' de los IABs con mayor probabilidad de impacto sobre las redes de Operadores de Sistemas de Transmisión europeos es la T1078[4] obtenida mediante Ingeniería Social/Phishing.
- Las medidas del punto de vista estratégico que podrían priorizarse por parte de la RTE para mitigar este riesgo en 2026 son el fortalecimiento de los controles de Autenticación (MFA[5], Zero-Trust[6] y el PoLP[7]) para neutralizar el vector T1078, la Micro-Segmentación de la red para asegurar el Pivote IT/OT, y el desarrollo de capacidades de Inteligencia Proactiva para cubrir la brecha de visibilidad ante actores avanzados.
- Se identifica que el riesgo de una escalada híbrida IT/OT es crítico, debido a que las capacidades de reconocimiento explotan la falta de segmentación de la red para pivotar hacia el control de la infraestructura física.
- El riesgo no puede ser mitigado sin haber enfrentado ambos elementos en conjunto si un ataque puede ocurrir, va a ocurrir.

---

[1] Initial Access Broker (Actor que vende acceso inicial a redes comprometidas).
[2] Tácticas, Técnicas y Procedimientos.
[3] Information Technology / Operational Technology (Redes Corporativas / Redes de Control).
[4] Valid Accounts (Cuentas Válidas), TTP del framework MITRE ATT&CK.
[5] Multi-Factor Authentication (Autenticación Multifactor).
[6] Nunca confiar, siempre verificar.
[7] Principle of Less Privilege (Principio del Mínimo Privilegio), accesos mínimos necesarios para desempeñar funciones laborales.

Análisis

La RTE, debido a su función como Operador del sistema de Transmisión de Francia, representa una Infraestructura crítica clave cuya interrupción representa un impacto sistémico para la seguridad energética de la unión europea, esto lo convierte en el blanco de actores maliciosos por las altas consecuencias que tendría el cese de sus operaciones.

El análisis se llevó a cabo en tres fases de producción concatenadas las cuales determinaron que la Escalada Híbrida IT/OT representa el riesgo más probable y crítico para la RTE.

El análisis ACH[8] reveló que el Vector de Ataque más probable es el TTP T1078, obtenidas por los IABs de forma oportunista vía Phishing y dirigida a la red corporativa (IT) el alto valor de la RTE como infraestructura crítica atrae actores maliciosos, que aprovechan la ingenuidad de las personas y el error humano con tal de acceder a la red corporativa por medio del engaño. La venta posterior de las credenciales permite a grupos de mayores recursos (como los RaaS[9]) pasar directamente a la fase de reconocimiento de la red y explotación. El punto más crítico de esta escalada reside justamente en el Pivote IT/OT, en donde, la falta de segmentación entre las redes convierte este acceso inicial en una vulnerabilidad idónea a explotar los Sistemas de Control SCADA[10] al no haber nada que obstaculice el movimiento lateral y persistencia en la red.

Esta secuencia vuelve el sistema vulnerable a la posibilidad de que el adversario efectúe la Manipulación de Control Físico, comprometiendo la continuidad operacional de la RTE. Esto hace que se vuelva prioritario establecer una estrategia que se enfoque en una respuesta de Supervivencia y Defensa, esto se consigue implementando controles como lo son MFA, Zero-Trust y el PoLP que proporcionan a los empleados frameworks[11] libres de bias cognitivos para efectuar acciones siendo siempre respaldadas por la necesidad real y sus superiores. Esto dificulta enormemente la capacidad de los IABs para engañar y romper la primera línea de defensa de la RTE: las personas. Por otra parte, la falta de resultados por parte de la herramienta TECHINT[12] refuerza la necesidad de una prospectiva ofensiva, reforzar las capacidades de inteligencia de la organización, con el fin de detectar actores avanzados que utilizan infraestructuras privadas.

En suma, el riesgo de una Escalada Híbrida es una realidad inminente que requiere una respuesta estratégica holística: reforzar el acceso inicial para mitigar la explotación oportunista y aislar el entorno OT para garantizar la ciberresiliencia frente a una intrusión exitosa. Estas conclusiones sientan las bases para la planificación estratégica de seguridad de la RTE para el año 2026.

---

[8] Análisis de Hipótesis Competitivas.

[9] Ransomware as a Service/ como servicio, Modelo de negocio de ciberdelincuencia donde el desarrollador del malware licencia su uso a afiliados para que realicen los ataques.

[10] Supervisory Control and Data Acquisition (Sistemas de Control Industrial).

[11] Marcos de trabajo predefinidos que ofrecen una estructura, metodologías y herramientas para estandarizar y optimizar procesos en diversas áreas de una empresa

[12] Technical Intelligence (Inteligencia Técnica).