

## Riesgo de Venta de Credenciales en la Dark Web

Reenviamos comunicación informática del colaborador en ciberseguridad de FETEIA-OLTRA, **Apolo Cybersecurity**

Apreciado asociado de FETEIA:

Somos Apolo Cybersecurity, una empresa especializada en soluciones de ciberseguridad. Nos dirigimos a ustedes para informarles sobre una potencial amenaza que podría afectar a empresas del sector logístico en España.

El día 17/09/2024 detectamos en la dark web la venta de un acceso no autorizado que supuestamente pertenece a una empresa logística española. Un grupo de atacantes conocido como Mykarma está ofreciendo acceso RDP (Remote Desktop Protocol) a los sistemas internos de una compañía de transporte y almacenamiento en España.

### Detalles del anuncio:

- **Grupo atacante:** Mykarma
- **Industria objetivo:** Servicios de transporte y logística
- **Detalles técnicos:**
  - Usuario en dominio
  - Servidor Windows 2016
  - Antivirus: Windows Defender
  - 86 hosts
- **Condiciones de venta:**
  - Precio inicial: \$500
  - Incrementos: \$100
  - Compra inmediata: \$1,000
  - Subasta: Última oferta en 24 horas

Aunque no se ha confirmado la identidad exacta de la empresa afectada, consideramos crucial que todas las empresas asociadas a FETEIA tomen medidas preventivas para proteger sus sistemas y datos.

### **Recomendaciones:**

- **Actualizar contraseñas y políticas de acceso:** Asegúrense de que todas las contraseñas sean robustas y se cambien regularmente.
- **Actualizar sistemas y software:** Verifiquen que todos los sistemas operativos y aplicaciones estén al día con los últimos parches de seguridad.
- **Implementar autenticación multifactor (MFA):** Añadan capas adicionales de seguridad en los accesos remotos y críticos.
- **Monitorizar actividades sospechosas:** Revisen los registros de acceso y logs de seguridad para detectar cualquier actividad inusual.
- **Formación en ciberseguridad:** Eduquen a su personal sobre las mejores prácticas en seguridad informática y cómo identificar posibles amenazas.

En Apolo Cybersecurity, estamos comprometidos con la protección de las empresas del sector logístico. Por ello, ofrecemos una consultoría gratuita, por ser miembros de FETEIA, para analizar la gestión de su seguridad informática y recomendar acciones específicas para su empresa.

Si desean programar una consultoría o tienen alguna duda, pueden **hacer click aquí** y nos pondremos en contacto lo antes posible. Estamos aquí para ayudarles a fortalecer su seguridad y proteger sus activos digitales.

Apolo Cybersecurity

T: +34 937 94 83 78



Secretaría.

Irun, 23 de septiembre de 2022