Investigación Forense
Ciencia, Tecnología y Comportamiento

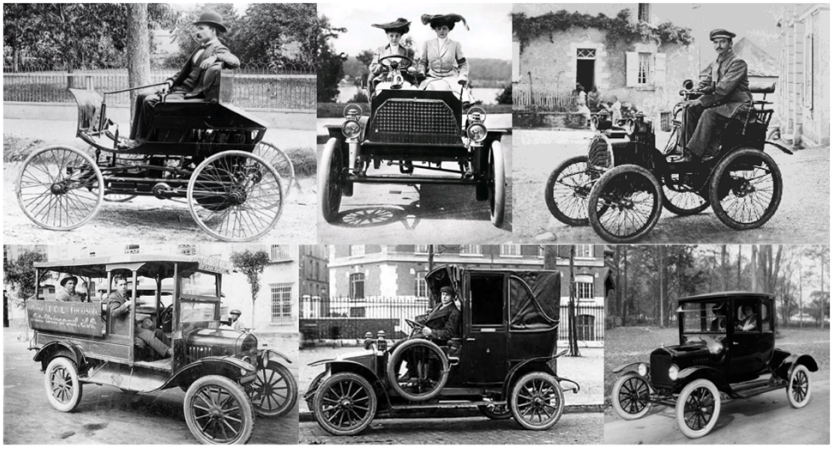
Artículo de Investigación

La Ciberseguridad en Gasolineras

José R. Leonett

Gerente de CiberSeguridad en INFO Y MAS Guatemala.
Founder & Exceo del Observatorio Guatemalteco de Delitos Informáticos -OGDI- .
Miembro e instructor en el International Association Of Crime Analysts – IACA.
Fundador del Grupo de Analistas Criminales de IACA en Guatemala
Delegado de IACA para Guatemala.
Corresponsal de la Red Iberoamericana El Derecho Informático EDI
Corresponsal de la Red Latinoamérica de Informática Forense REDLIF - Capitulo Guatemala.

¿Alguna vez te has preguntado cómo funciona una gasolinera o qué sucede cuando pagas con tu tarjeta de crédito o débito? ¿Cómo se interconectan sus sistemas informáticos con el dispensador de gasolina? ¿O si alguien está manipulando la estación cuando tú te encuentras parado sobre los tanques subterráneos? Desde la aparición de los primeros vehículos hasta hoy en día, todos necesitan una fuente de energía, y la más difundida ha sido la de vehículos que utilizan energía fósil.



La demanda energética proveniente de los vehículos ha generado una maquinaria mundial de millones y millones de dólares en la exploración, producción, generación, traslado, almacenamiento y procesamiento del petróleo en muchas latitudes, con el fin de poder atender la alta demanda de combustibles en el mundo.

Este combustible muchas veces debe viajar largas distancias desde su fuente hasta las estaciones de gasolina que se expanden por toda Hispanoamérica en contenedores como pipas, gandolas, trailers y camiones, los cuales se desplazan por el entramado de carreteras para cumplir con los pedidos de cada estación de servicio que despacha dicho producto. Es aquí donde iniciaremos nuestra investigación:

Una estación de gasolina es un ecosistema muy bien diseñado y configurado para que cada gestión que sucede dentro de ella pueda brindar un servicio de calidad a cada usuario que va a llenar su tanque con el preciado líquido. Detrás de los sistemas de despacho, se encuentra un entramado tecnológico que controla el sistema de administración de la gasolinera, el sistema de pago por consumo de combustible, el control de cada estación de despacho, el contenido de los tanques subterráneos, el control de pago de autoservicios, los POS automatizados de pagos y el control de inventarios de la tienda, entre tantos otros temas que deben ser controlados de manera automatizada dentro de la estación de gasolina.

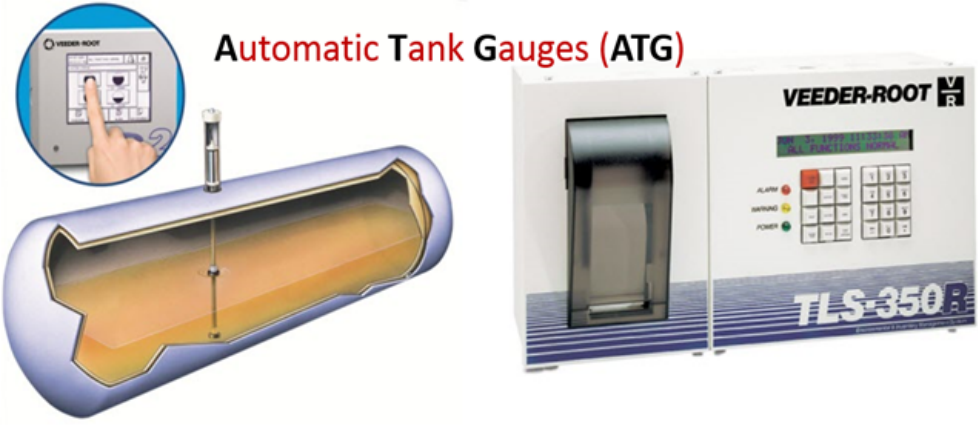
Con todos estos detalles, podemos ver que una gasolinera es una infraestructura crítica que debe ser administrada de manera correcta para no comprometer su ciberseguridad, la cual se centra en tres accesos no autorizados:

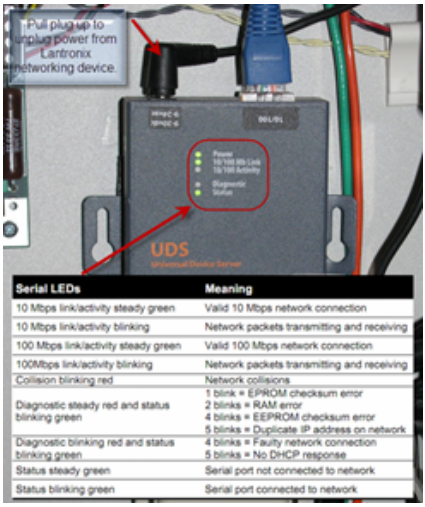
- Disco duro del server
- ·Sistema de administración de gasolina
- Medidores Automáticos de Tanques (ATG)

Los Medidores Automáticos de Tanques (ATG: Automatic Tank Gauges) son nuestro punto neural ya que ellos proveen información crítica de todo lo que se encuentra dentro de los tanques subterráneos de combustibles. Estos ATG se usan para monitorear los niveles de:

- El inventario de los tanques de combustibles.
- El rastreo de entregas
- Las alarmas que indican problemas en los tanques (como un derrame de combustible) y,
- para realizar pruebas de fugas de acuerdo a las normas ambientales.

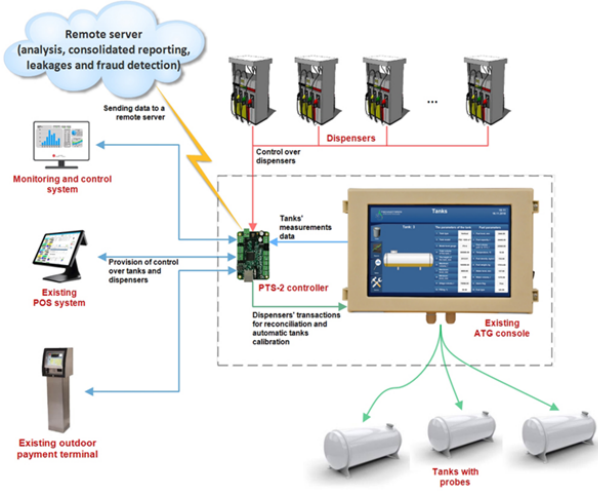
Los ATG son utilizados por las estaciones de servicios en toda Latinoamérica y a nivel internacional.





Serial LEDs	Meaning
10 Mbps link/activity steady green	Valid 10 Mbps network connection
10 Mbps link/activity blinking	Network packets transmitting and receiving
100 Mbps link/activity steady green	Valid 100 Mbps network connection
100Mbps link/activity blinking	Network packets transmitting and receiving
Collision blinking red	Network collisions
Diagnostic steady red and status blinking green	1 blink = EPROM checksum error 2 blinks = RAM error 4 blinks = EEPROM checksum error 5 blinks = Duplicate IP address on network
Diagnostic blinking red and status blinking green	4 blinks = Faulty network connection 5 blinks = No DHCP response
Status steady green	Serial port not connected to network
Status blinking green	Serial port connected to network

Un ATG “Es un medidor de tanque cuya dirección de Protocolo de Internet (IP) se encuentra fácilmente, y al que se puede acceder a través de Internet para leer información y realizar todos los cambios de configuración, utilizando herramientas fácilmente disponibles como Telnet". A diferencia de un ataque físico, un ataque cibernético no puede dejar rastros. Los cambios de configuración se pueden hacer y luego revertir sin saber cómo ocurrieron. **Fuente:** kachoolie



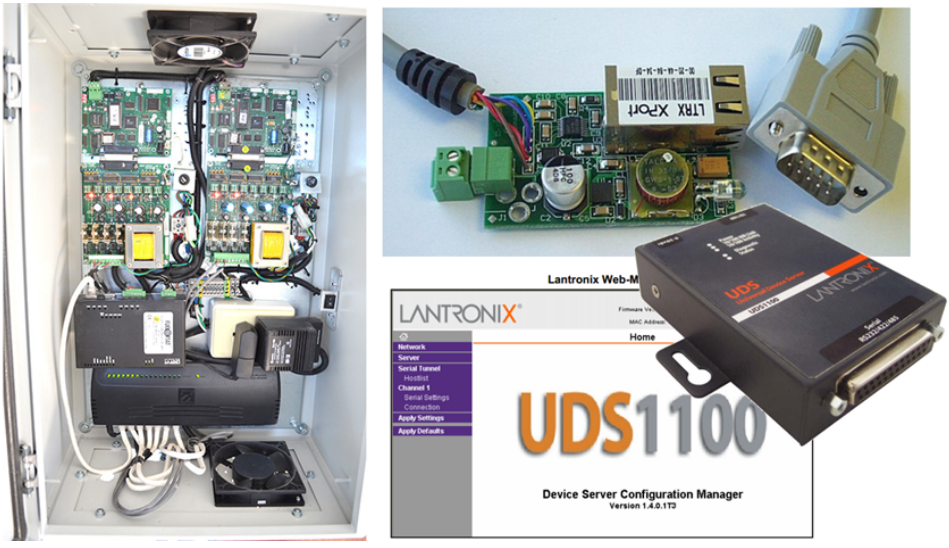
La marca más difundida entre los ATG son los UDS1100 Serial to Ethernet Adapter de la empresa Lantronix. Estos pueden programarse y monitorearse a través de una serie de puertos incorporados, como el puerto serie, fax/módem o TCP/IP. Para monitorear estos sistemas de forma remota, muchos operadores utilizan la conexión TCP/IP para acceder a la interfaz serie del ATG. Aunque algunos sistemas tienen la capacidad de proteger las interfaces seriales con contraseña, esto no es comúnmente implementado.

Un ciberdelincuente con acceso al ATG puede apagar la estación de gasolina, falsificar los niveles de combustibles, generar falsas alarmas y bloquear el servicio de monitoreo fuera del sistema. Los fallos de funcionamiento del ATG del tanque se consideran un problema grave debido a los riesgos de seguridad, ya que podrían comprometer desde el sistema de acumulación de gases hasta el control de derrames, convirtiendo la estación en un blanco de terrorismo. Esto va más allá de la manipulación de una gran cantidad de sensores, tales como:

- ·Prueba de detección de fugas en el tanque
- Informe de estado del sistema y de los tanques
- Informe de historial de alarmas de prioridad
- Informe de alarma activa
- Informe de inventario/entrega en el tanque
- Informe de detección de fugas en el tanque
- Informe de inventario de cambios en el tanque
- Informe de historial de alarmas en el tanque
- Perfil del o los tanques
- Informe de inventario en el tanque con un 90/95% de temperatura
- Informe de estado del sensor de líquido
- Informe de historial de alarmas de sensor de líquido
- Registro de instalación del sensor inteligente
- Historial de pruebas de fugas en la línea de presión (con datos de prueba de 0.20)
- Estado de fuga de la línea de presión
- Historial de pruebas de fugas en la línea de presión (solo datos de prueba 0.10)
- Informe de estado de entrada
- Establecer tipo de sistema y banderas de idioma
- Cambiarle el nombre a los tanques
- Ajuste de 04 tanques punto de altura completa Volumen
- Establecer el diámetro del tanque
- Establecer los parámetros de flotación programables del tanque

- Establecer el factor de pérdida de vapor del tanque
- Establecer nivel de filtro de alarma de agua del tanque
- Establecer categoría de sensor de líquido
- Impresión de diagnóstico en el tanque
- Indicadores de prueba de fuga de la sonda - Prueba almacenada
- Diagnóstico de CSLD: tabla de promedios móviles
- Informe de diagnóstico de corte de energía
- Informe de diagnóstico del sensor de líquido

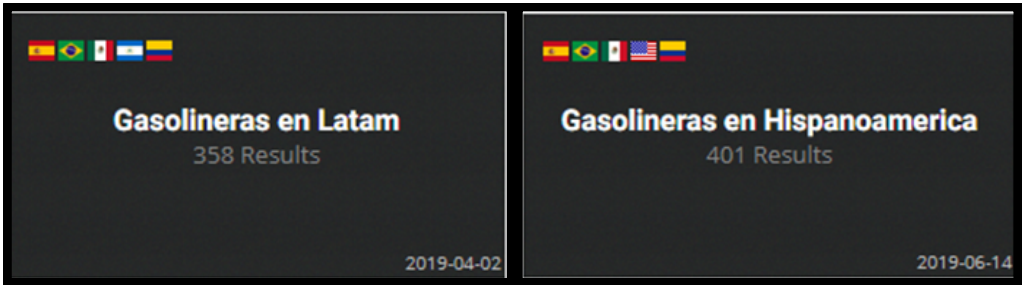
Entre más de 600 tipos de alarmas y configuraciones críticas, esa pequeña lista puede ser manipulada de manera remota si un ciberdelincuente logra acceder al ATG.

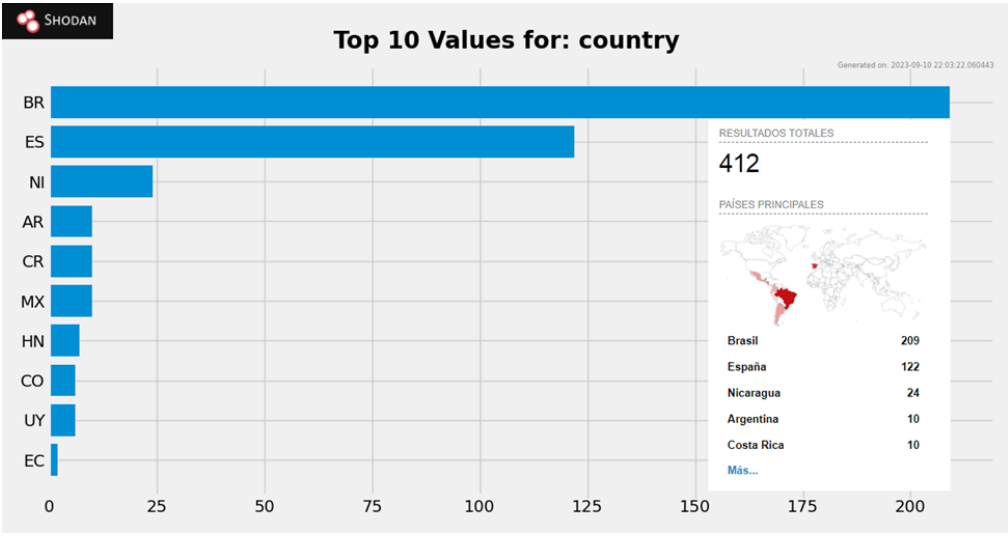


Los ATG están diseñados para detectar fugas y otros problemas en los tanques de combustible subterráneos. El acceso remoto por parte de un ciberdelincuente podría brindarle la capacidad de reconfigurar los umbrales de alarmas, reiniciar los sistemas e incluso interrumpir el funcionamiento de los tanques de combustible.

Además, podría acceder a información como la cantidad de combustible expedido por cada turno. Teóricamente, un ciberdelincuente podría cerrar más de 9000 estaciones de combustible en todo el mundo automatizándolo a través de una API, ya que los manuales de los ATG están disponibles en la red.

Podemos ver el incremento de fallos debido a la mala configuración de los ATG, en un estudio que realice utilizando Shodan en Latinoamérica del 02/04/2019 que se detectaban 358 gasolineras expuestas, para el 14/06/2019 existían 401, en el 13/12/2019 un total de 303 y hoy 10/09/2023 un total de 412.





Pero, ¿Qué pasaría si alguien pudiese acceder y cambiar los datos del sistema a su antojo? ¿Y si cambiase la temperatura del tanque o lo hiciese parecer que está lleno cuando en realidad está vacío? ¿Qué sucedería si se desactivan las alarmas de acumulación de Gases? ¿Y si se desactiva la verificación de temperatura de los tanques?

Los números son alarmantes, pues existen diversas formas de entrar a las gasolineras conectadas al internet, de las cuales una se encuentra muy documentada por grupos de cibercriminales dentro de muchos foros del undergroud.

Las estadísticas para Latinoamérica solo del acceso por fallos del dispositivo ATG el 14 de diciembre 2019 era de 321 ATG expuestos y hoy 10/09/2023 un total de 412, en otro análisis se puede realizar el mismo acceso sin ningún tipo de contraseña a más de 412 estaciones de gasolinas, sin contar los accesos directamente al disco duro que suman más de 48 estaciones.

Estas amenazan son latentes y se encuentran activas desde hace más de 5 años, sin contar con los nuevos vectores que utilizan malware para tomar el control de los ATG.

La pregunta ante esta gravedad es sencilla: **¿Podrían usar una gasolinera como herramienta Terrorista?**