Q-Gaspot

The **Q-Gaspot**® is a network honeypot solution built specifically to simulate Veeder-Root Guardian AST Tank Gauges, and runs on an extremely small form factor, low-power-consumption network appliance. Veeder Root Guardian Tank Gauges are widespread in the oil and gas industry, and used for, among other things, inventorying fuels. The **Q-Gaspot** was designed to randomize the gauges as much as possible so no two instances look exactly alike. This makes it possible for the **Q-Gaspot** to display literally hundreds of realistic attack surfaces ("decoys") on a network, which, in turn, can help catch, and stymie, a hacking attempt. To the hacker, it appears to be a very large fuel depot. If the hacker probes an attack surface, the hacking incident is caught, and an alert is issued. Having hundreds of attack surfaces radically shifts the odds in favor of the defender, and against a successful hack.

The **Q-Gaspot** is the only honeypot appliance specifically built to provide network obfuscation (camouflaging of network assets) for Operations Technology (OT) networks with Veeder-Root Guardian Gas Gauges.

Q-Gaspot Hardware Specifications:

- 108 mm x 64 mm x 26 mm – 170 grams
  (4.25" x 2.50" x 1.125" – 6 oz)
- Power consumption under full load:
  12 watts, 120v-240v
- No fan or any moving parts. Must be installed in a well-ventilated space.
- Operates 0°C–70°C (32°F–158°F)

LED indicators:

- Power
- Link (physical connection to network)
- Activity (network traffic)
- 1000 mbps (gigabit) NIC connection
- Dual Band WiFi. (2.4 GHz & 5 GHz)

Contact: Richard Avery
+1 646-449-7810
Q-Gaspot@quantalytics.com

Quantalytics. In-depth network defenses.

Quantalytics

Q-Gaspot

The **Q-Gaspot** includes:

- **Gaspot – Gaspot** is the only open source, enterprise-class, honeypot solution specifically designed to emulate Veeder-Root Guardian Gas Gauges. Gaspot randomizes its gauge emulations, so that to an attacker, there appear to be literally hundreds of targets.

- **ntop-ng – ntop-ng** ("**ntop next generation**") is the latest iteration of ntop, which is used to probe all network traffic. Some of its features include showing realtime network traffic and hosts; create long term reports for network throughput, application and application protocols; monitor and report live throughput, network and application latencies, RTT, and full TCP stats; discover application protocols (e.g. Facebook, BitTorrent, etc.) by leveraging nDPI (ntop Deep Packet Inspection); characterize HTTP traffic using characterization services provided by Google and HPPT Blacklist; provide geolocation mapping of hosts; sort all network traffic via criteria including IP address, port, L7 protocol, throughput, Autonomous Systems (ASs); analyze IP traffic and sort by source and destination; IPv6 support; full Layer 2 support, including ARP stats; and an alerts engine to capture anomalous and suspicious hosts.

- **ModSecurity® – ModSecurity®** ("**ModSec**") is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. We have hardened the **Q-Gaspot**'s built-in Apache web server to prevent conceivable attacks.

- **ClamAV® – ClamAV®** is the leading open source anti-virus software package.

- **Tiny Honeypot (THP) - THP** fools attackers by making it appear that the attack is working, while meanwhile logging the attack info. **THP** wastes an attacker's time, and creates an opportunity to detect the network intrusion by offering to the attacker what appears to be thousands of services.

- **Webmin – Webmin** is the leading open source Web GUI package for server configuration and maintenance. **Webmin** also allows for the linkage of multiple **Q-Gaspot** appliances for simplified administration.

Contact: Richard Avery
+1 646-449-7810
Q-Gaspot@quantalytics.com

Quantalytics. In-depth network defenses.

The **Q-Gaspot** is completely administered through a Web GUI. All package usage is via Web interfaces, thereby opening up sophisticated intrusion detection, network forensic analysis, and network monitoring to even novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

The **Q-Gaspot** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.)

The **Q-Gaspot** is also available as a Virtual Machine (VM).

Using the provided **Webmin** module, two-factor authentication can be added using **Google Authenticator** or **Authy**, a commercial service with its own app. **Google Authenticator** runs on Android, IOS, and Blackberry devices, and uses the standard TOTP protocol.

Notifications are provided by e-mail using **SendMail**, which is configured with a module in **Webmin**, and syslog entries. SMS notification is available as an option. The **Q-Gaspot** can also be integrated with the **Q-Log**® network appliance or any other Syslog or SIEM (Security Information and Event Management) solution, and monitored via the **Q-BOX**.

Contact: Richard Avery
+1 646-449-7810
Q-Gaspot@quantalytics.com