Quantalytics

Q-Hpot®

The **Q-Hpot**® is a honeypot running on an extremely small form factor, ultra-low-power-consumption server, and built upon three open source packages: **Honeyd** and **NOVA** ("Network Obfuscation and Virtualized Anti-Reconnaissance"), plus **HoneyBadger**, a comprehensive TCP attack inquisitor capable of detecting and recording a variety of TCP stream injection attacks, including 0-Day ("Zero Day") attacks. **HoneyBadger** has been combined with geolocation to identify the location of the attacker.

A honeypot is a decoy server which is used for network obfuscation, denying the attacker access to actual network data while giving the attacker false information on the number and types of systems on the network. The combination of these two honeypot packages, which includes an update to **Honeyd**, **enables the creation of multiple virtual, realistic, decoy servers**.

These virtual servers offer attack surfaces for hackers, and emulate almost any operating system and network service, with any desired open ports, and for any network topology. The **Q-Hpot** can give a network the appearance of having literally 100 or more additional servers, in addition to the actual servers on the network it is protecting, thereby providing network obfuscation and concealment of the actual network servers. The only limitation on the number of decoy servers is the number of available LAN IP addresses.

The addition of **HoneyBadger** gives administrators using the **Q-Hpot**, unlike other honeypot systems, the ability to fight back by identifying the attacker's location via geolocating the attacker's IP address(es), as well as prevent TCP injection attacks, including 0-day (Zero Day) attacks.

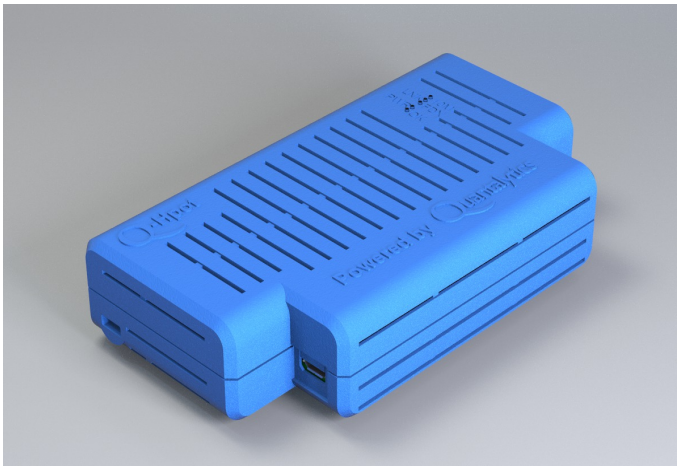
As a result, the **Q-Hpot** greatly increases the likelihood of an attack being caught before servers or workstations are compromised, and data, exfiltrated.

Contact: Richard Avery
646-449-7810
Q-Hpot@quantalytics.com

Quantalytics. In-depth network defenses.

Q-Hpot®

NOVA includes machine learning algorithms in order to determine which network nodes are hostile or benign. **NOVA** also allows the white listing of network objects to prevent false positives. The machine learning algorithms process aggregate flow data, which includes packet sizes, destination addresses, and the contacted TCP and UPD ports. This enables **NOVA**'s machine learning algorithms to work effectively even if encryption is used by an attacker to evade Deep Packet Inspection (DPI). If an attack on any of the **NOVA** virtual servers is detected, network admins are notified via e-mail, libnotify messages, and syslog entries. **NOVA**'s warnings are also integrated with **Nagios**® on the **Q-Box**® as an additional monitoring and notification mechanism. **NOVA** provides a Web interface for monitoring the **Q-Hpot**'s security status, and integrates with the **Q-Box** for centralized monitoring.



Q-Hpot Hardware Specifications:

- 126 mm x 70 mm x 28 mm – 170 grams (5.0" x 2.8" x 1.1" – 6 oz)
- Power consumption under full load: 8 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)

The **Q-Hpot** includes:

- **Honeyd – Honeyd** is the leading open source, enterprise-class, honeypot server software solution.
- **NOVA – NOVA** is the leading open source Web management and configuration tool for **Honeyd**, combined with an update to **Honeyd**. **NOVA** also incorporates Machine Learning to study traffic in order to help identify attacks and alert administrators. **The number of deployed decoy attack surfaces is limited only by the number of available LAN IP addresses.**

Contact: Richard Avery
646-449-7810
Q-Hpot@quantalytics.com

Quantalytics. In-depth network defenses.

Quantalytics

Q-Hpot®

- **HoneyBadger – HoneyBadger** is an open source, comprehensive TCP stream analysis tool for detecting and recording TCP attacks. **HoneyBadger** combines a variety of TCP stream injection attacks to help insure that the TCP attack identification is reliable, and not a false positive. **HoneyBadger** includes geolocation to pinpoint the attacker(s) physical location.

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

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

- **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. **THP** is intended to protect the underlying server infrastructure in case the user-defined honeypots are ignored.

- **ClamAV® – ClamAV** is the leading open source anti-viru s package.

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

The addition of WiFi makes it possible for administrators to create a honeypot system for WiFi networks in addition to wired LANs. **Both can be active at the same time.**

The **Q-Hpot** network appliance is also available as a Virtual Machine (VM).

The **Q-Hpot** is completely administered through a Web GUI. All package usage is via Web interfaces. No Command Line Interface (CLI) or Linux skill is required.

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. The **Q-Hpot** network appliance can be integrated with **Nagios®** on the **Q-Box®** as another notification route. SMS notification is available as an option. The **Q-Hpot** network appliance can also be integrated with the **Q-Log®** network appliance or any other Syslog or SIEM (Security Information and Event Management) solution.

Contact: Richard Avery
646-449-7810
Q-Hpot@quantalytics.com

Quantalytics. In-depth network defenses.