Q-Hpot®

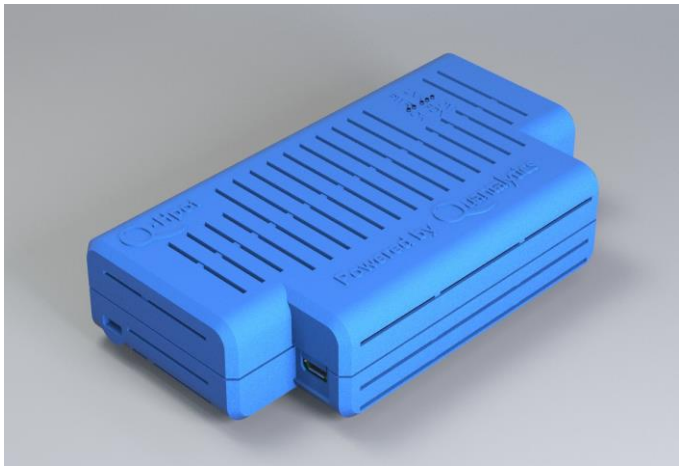
El **Q-Hpot**® es un honeypot que funciona con un factor de forma extremadamente pequeño, un servidor de consumo de muy bajo consumo y se basa en tres paquetes de código abierto: **Honeyd** y **NOVA** ("Obfuscation de la red y Anti-Reconocimiento Virtualizado"), además de **HoneyBadger** , Un intruso comprensivo del ataque del TCP capaz de detectar y de registrar una variedad de ataques de la inyección del flujo del TCP, incluyendo ataques del día 0 (día cero). **HoneyBadger** se ha combinado con la geolocalización para identificar la ubicación del atacante.

Un honeypot es un servidor señuelo que se utiliza para la ofuscación de la red, negando el acceso del atacante a los datos reales de la red mientras que da al atacante la información falsa en el número y tipos de sistemas en la red. La combinación de estos dos paquetes de honeypot, que incluye una actualización de **Honeyd**, **permite la creación de múltiples servidores virtuales, realistas y señuelos.** Estos servidores virtuales ofrecen superficies de ataque para hackers y emulan casi cualquier sistema operativo y servicio de red, con cualquier puerto abierto deseado y para cualquier topología de red. El **Q-Hpot** puede dar a una red la apariencia de tener literalmente 100 o más servidores adicionales, además de los servidores reales en la red que está protegiendo, proporcionando así ofuscación de red y ocultación de los servidores de red reales. La única limitación en el número de servidores de señuelo es el número de direcciones IP de LAN disponibles.

La adición de **HoneyBadger** ofrece a los administradores que usan el **Q-Hpot**, a diferencia de otros sistemas de honeypot, la capacidad de combatir identificando la ubicación del atacante a través de la geolocalización de las direcciones IP del atacante, así como prevenir ataques de inyección TCP, incluyendo 0 días Zero Day).

Como resultado, el **Q-Hpot** aumenta en gran medida la probabilidad de un ataque que se captura antes de servidores o estaciones de trabajo se ven comprometidos, y los datos, exfiltración.

NOVA incluye algoritmos de aprendizaje de máquina para determinar qué nodos de red son hostiles o benignos. **NOVA** también permite la lista blanca de objetos de red para evitar falsos positivos. Los algoritmos de aprendizaje de máquina procesan datos de flujo agregado, que incluyen tamaños de paquetes, direcciones de destino y los puertos TCP y UPD contactados. Esto permite que los algoritmos de aprendizaje de máquina de **NOVA** funcionen eficazmente aunque un atacante use el cifrado para evadir la inspección profunda de paquetes (DPI). Si se detecta un ataque a cualquiera de los servidores virtuales de **NOVA**, los administradores de red son notificados por correo electrónico, mensajes de libnotify y entradas de syslog. Las advertencias de **NOVA** también están integradas con **Nagios**® en el **Q-Box**® como un mecanismo adicional de monitoreo y notificación. **NOVA** proporciona una interfaz Web para supervisar el estado de seguridad del **Q-Hpot** y se integra con el **Q-Box** para el monitoreo centralizado.



Especificaciones de Hardware **Q-Hpot**:

- 126 mm x 70 mm x 28 mm – 170 gramos
  (5.0” x 2.8” x 1.1” – 6 oz)
- Consumo de energía a plena carga: 8 watts, 120v-240v
- No hay ventilador ni ninguna pieza móvil. Debe instalarse en un espacio bien ventilado.
- Funciona de 0°C a 70°C (32°F–158°F)

Indicadores LED:

- Energia electrica
- Link (physical connection to network)
- Enlace (conexión física a la red)
- FDX (duplex completo)
- 100 (10/100 mbps)

Quantalytics, Inc.
220 Henley Rd.
Woodmere, NY 11598

Contacto: Richard Avery
+1 646-449-7810
q-hpot@quantalytics.com

Derechos de autor © 2017 Quantalytics, Inc. Todos los derechos reservados.

Q-Hpot®

El **Q-Hpot** incluye:

- **Honeyd** –**Honeyd** es la solución de software líder de código abierto, de clase empresarial, servidor de honeypot.
- **NOVA** – **NOVA** es la principal herramienta de gestión y configuración de Web de código abierto para Honeyd, combinada con una actualización de **Honeyd**. **NOVA** también incorpora el aprendizaje de la máquina para estudiar el tráfico con el fin de ayudar a identificar ataques y administradores de alerta. **El número de superficies de ataque de señuelo desplegadas está limitado sólo por el número de direcciones IP de LAN disponibles.**
- **HoneyBadger** – **HoneyBadger** es una herramienta de análisis de flujo TCP de código abierto para detectar y registrar ataques TCP. **HoneyBadger** combina una variedad de ataques de inyección de flujo TCP para ayudar a asegurar que la identificación del ataque TCP es fiable y no un falso positivo. **HoneyBadger** incluye geolocalización para identificar la ubicación física del atacante.
- **Webmin - Webmin** es el principal paquete de GUI Web de código abierto para la configuración y el mantenimiento del servidor. **Webmin** también permite la vinculación de múltiples dispositivos **Q-Box** para la administración simplificada.
- **ModSecurity® – ModSecurity**® ("**ModSec**") es el principal paquete de protección contra ataques de scripts cruzados de código abierto para endurecer el servidor web Apache de Q-Box y prevenir ataques concebibles.
- **Tiny Honeypot (THP) - THP** engaña a los atacantes haciendo que parezca que el ataque está funcionando, mientras que mientras registra la información de ataque. **THP** desperdicia el tiempo de un atacante y crea una oportunidad para detectar la intrusión de red ofreciendo al atacante lo que parece ser miles de servicios.
- **ClamAV® – ClamAv®** es el paquete de software antivirus de código abierto líder.

El **Q-Hpot** tiene un NIC 10/100 y un 802.11 b / g / n WiFi.

La adición de WiFi permite a los administradores crear un sistema de honeypot para redes WiFi, además de LAN cableadas. Ambos pueden estar activos al mismo tiempo.

El dispositivo de red **Q-Hpot** también está disponible como una máquina virtual (VM).

El **Q-Hpot** se administra completamente a través de una GUI Web. No se requiere ninguna habilidad de interfaz de línea de comandos (CLI) o Linux.

Usando el módulo **Webmin** proporcionado, la autenticación de dos factores se puede agregar usando **Google Authenticator** o **Authy**, un servicio comercial con su propia aplicación. **Google Authenticator** se ejecuta en dispositivos Android, IOS y Blackberry y utiliza el protocolo TOTP estándar.

Las notificaciones se proporcionan por correo electrónico utilizando **SendMail**, que está configurado con un módulo en **Webmin**, y las entradas de syslog. El dispositivo de red **Q-Hpot** se puede integrar con **Nagios**® en el **Q-Box**® como otra ruta de notificación. La notificación por SMS está disponible como opción. El dispositivo de red **Q-Hpot** también se puede integrar con el dispositivo de red **Q-Log**® o cualquier otra solución Syslog o SEIM.

Q-Hpot® *and y todas las marcas registradas anteriores son propiedad de sus respectivos propietarios.*

Quantalytics, Inc.
220 Henley Rd.
Woodmere, NY 11598

Contacto: Richard Avery
+1 646-449-7810
q-hpot@quantalytics.com

Derechos de autor © 2017 Quantalytics, Inc. Todos los derechos reservados.