Q-ConPot®

L'appliance réseau **Q-ConPot**® (Control System Honeypot) est un honeypot ICS et SCADA. Les honeypots réseau fournissent l'obscurité du réseau (se cachant à la vue) et nie la reconnaissance facile du réseau de pirates informatiques, tout en augmentant considérablement la chance de détecter une violation du réseau. Le **Q-ConPot** utilise **Conpot**, un progiciel open source qui possède une large gamme de protocoles industriels intégrés afin que les administrateurs puissent créer des surfaces d'attaque qui imitent leur environnement actuel ou représentent une infrastructure très complexe et fictive. Cela permet aux administrateurs de créer une obstruction et une déception du réseau, ce qui interdit aux pirates informatiques une carte précise du réseau et de ses machines, ainsi que l'augmentation de la probabilité que le réseau soit rattrapé par un système de détection d'intrusion (IDS) tel que le **Q-Box**® ou par le **Q-ConPot** lui-même. **Le nombre de surfaces d'attaque de leurres déployées est limité uniquement par le nombre d'adresses IP LAN disponibles.**

Afin d'augmenter les capacités de déception de **Conpot**, l'administrateur peut créer dans les interfaces homme-machine personnalisées («HMI») du **Q-Conpot**, ce qui augmente le nombre et le type de surfaces d'attaque. Le temps de réponse des surfaces d'attaque peut également être ajusté pour différents temps de retard afin d'imiter le comportement d'un système industriel sous charge constante. **Conpot** peut être consulté à l'aide de la production d'Interfaces Homme-Machine (IHM) ou via une interface Web.

ntopng et **xplico**, deux logiciels open source, de capture de paquets complets de classe entreprise, d'indexation et de forensics sont également inclus, de sorte qu'en cas d'alerte, les administrateurs peuvent immédiatement capturer des paquets pour une analyse légale; HoneyBadger, qui permet aux administrateurs d'utiliser le Q-ConPot, contrairement aux autres systèmes de pots de miel, pour repérer l'emplacement de l'attaquant via la géolocalisation des adresses IP de l'attaquant et empêcher les attaques par injection de TCP, y compris les attaques de 0-Jour («Zero Day»).

Un bref résumé de chaque colis est ci-dessous. Nous vous encourageons à consulter notre site Web, www.quantalytics.com, pour une explication plus complète des caractéristiques de chaque paquet.

Spécifications matérielles du ***Q-ConPot***:

- 108 mm x 64 mm x 26 mm – 170 grammes (4.25” x 2.50” x 1.125” – 6 oz)
- Consommation électrique à pleine charge: 12 watts, 120v-240v
- Pas de ventilateur ou de pièces mobiles. Doit être installé dans un espace bien ventilé.
- Fonctionne de 0°C à 70°C (32°F–158°F)

Indicateurs LED:

- Pouvoir électrique
- Lien (connexion physique au réseau)
- Activité (trafic réseau)
- 1000 mbps (gigabit) NIC connexion
- WiFi Bi-Bande. (2.4 GHz & 5 GHz)

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

Quantalytics. Défenses de réseau en profondeur.

Q-ConPot®

L'appliance réseau **Q-ConPot** comprend:

- **Conpot - Conpot** est un système open source, hôte et honeypot conçu pour fournir une obscurcissement et une déception du réseau sur les réseaux de machine ICS et SCADA. **Conpot** permet à l'administrateur de créer des surfaces d'attaque qui reflètent l'environnement de production réel, ainsi que des surfaces d'attaque supplémentaires pour créer un labyrinthe d'équipements faux ("surfaces d'attaque") que le pirate informatique doit naviguer. Cela prend du temps et augmente considérablement le risque que le pirate informatique soit découvert avant que le matériel industriel ne soit compromis.
- **Xplico – Xplico** est un package open source de premier plan pour la capture de paquets sur le réseau et l'analyse judiciaire. En cas d'activité suspecte, les administrateurs réseau peuvent capturer et examiner en profondeur le trafic en temps réel pour une analyse plus approfondie du trafic réseau suspect. En plus de l'inspection des paquets, **Xplico** permet de reconstituer le trafic réel. PAR EXEMPLE. Courriels, textes, messages instantanés, photos, etc.
- **ntopng - ntopng** ("ntop next generation") est la dernière itération de ntop, utilisée pour sonder tout le trafic réseau. Certaines de ses caractéristiques comprennent le trafic réseau en temps réel et les hôtes; créer des rapports à long terme pour le débit du réseau, les protocoles d'application et d'application; surveiller et signaler le débit en direct, les latences de réseau et d'application, le RTT et les statistiques TCP complètes; découvrir les protocoles d'application (par exemple Facebook, BitTorrent, etc.) en exploitant nDPI (ntop Deep Packet *I*nspection); caractériser le trafic HTTP en utilisant les services de caractérisation fournis par Google et HPPT Blacklist; fournir une cartographie de géolocalisation des hôtes; trier tout le trafic réseau via des critères incluant l'adresse IP, le port, le protocole L7, le débit, les systèmes autonomes (AS); analyser le trafic IP et trier par source et destination; Support IPv6; prise en charge complète de la couche 2, y compris les statistiques ARP; et un moteur d'alertes pour capturer les hôtes anormaux et suspects.
- **HoneyBadger – HoneyBadger** est un outil d'analyse de flux TCP complet, ouvert, permettant de détecter et d'enregistrer des attaques TCP. **HoneyBadger** combine une variété d'attaques d'injection de flux TCP pour aider à s'assurer que l'identification de l'attaque TCP est fiable et non un faux positif. **HoneyBadger** inclut la géolocalisation pour identifier l'emplacement physique des attaquants.
- **Webmin - Webmin** est utilisé pour l'entretien ménager des réseaux et la configuration du réseau. **Webmin** permet également le couplage de plusieurs appliances **Q-Conpot** pour une administration simplifiée.
- **HA Proxy – HA Proxy** est le premier fournisseur open source pour le basculement automatique et l'équilibrage de charge. Jusqu'à 32 appareils réseau **Q-Conpot** peuvent être liés pour le basculement automatique ou l'équilibrage de charge pour la couverture de réseaux extrêmement importants. L'administration se fait via un web gui. **Le nombre de surfaces d'attaque déployées est limité uniquement au nombre d'adresses IP LAN disponibles.**

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

Quantalytics. Défenses de réseau en profondeur.

- **ModSecurity® – ModSecurity®** («**ModSec**») est le principal pare-feu d'applications Web (WAF) open source pour la protection contre les attaques par script croisé. Nous avons durci le serveur Web Apache intégré du **Q-ConPot** pour éviter les attaques concevables.
- **Tiny Honeypot (THP) - THP** trompe les attaquants en faisant apparaître que l'attaque fonctionne, tout en enregistrant les informations d'attaque. **THP** gaspille le temps d'un attaquant et crée l'opportunité de détecter l'intrusion du réseau en offrant à l'attaquant ce qui semble être des milliers de services.
- **ClamAV®** – **ClamAv®** est le premier package antivirus open source.

Le **Q-ConPot** possède à la fois un NIC Gigabit (1000 mbps) et un WiFi Dual Band 802.11. (2,4 GHz et 5 GHz.)

Le **Q-ConPot** est également disponible en tant que Machine Virtuelle («VM»).

L'appliance réseau **Q-ConPot** est complètement administrée via une interface graphique Web. L'utilisation de tous les packages se fait via des interfaces Web, ouvrant ainsi une détection d'intrusion sophistiquée, une analyse légal en réseau et une surveillance de réseau même aux administrateurs réseau novateurs. Aucune interface de ligne de commande (CLI) ou Linux n'est requise.

En utilisant le module **Webmin** fourni, l'authentification à deux facteurs peut être ajoutée à l'aide de **Google Authenticator** ou **Authy**, un service commercial avec sa propre application. **Google Authenticator** s'exécute sur les appareils Android, IOS et Blackberry, et utilise le protocole standard de TOTP.

Les notifications sont fournies par e-mail à l'aide de **SendMail**, qui est configuré avec un module dans **Webmin** et les entrées syslog. L'appliance de réseau **Q-ConPot** peut être intégré à **Nagios®** sur le **Q-Box®** comme autre voie de notification. La notification par SMS est disponible en option. L'appliance de réseau **Q-ConPot** peut également être intégré au **Q-Log®** ou à toute autre solution Syslog ou SIEM (Security Information and Event Management).

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