Note de Version GBox 2.5.3.100

Gatewatcher

Created on : Janvier, 2021

Last updated : janvier, 2021

Table des matières

Chapitre 1

Note de Version GBox 2.5.3.100

Vous trouverez :
- Fonctionnalités.
- Problèmes connus.

Chapitre 2

Fonctionnalités

2.1 Gatewatcher Licensing Center

Le serveur d'analyses (GBox) utilise le nouveau système de licence GATEWATCHER LICENSING CENTER (GLC).

La licence se compose au minimum d'une licence GWAPI perpétuelle associée à une GBox.

L'administrateur doit ajouter une licence afin de configurer l'équipement.

L'opérateur, peut quant à lui, accéder aux données de la GBox.

Pour obtenir une licence version 2.5.3.100, merci de vous rapprocher de votre ingénieur d'affaire GATEWATCHER ou contacter commerciaux@gatewatcher.com.

2.2 Gatewatcher Update Manager

Les GBox se basent sur un nouvel outil de mise à jour unifié Gatewatcher Update Manager (GUM).

Il permet la gestion des différents types de mises à jour : update, upgrade, hotfix.

Un statut en temps réel est visible depuis l'interface WEB de la GBox.

Les updates sont désormais unifiées en un seul package avec les moteurs souhaités (SandBox et Malcore) et peuvent se faire :

- En ligne via https://update.gatewatcher.com/update/ et https://gupdate.gatewatcher pour Malcore. Ceci requiert un compte intelligence.
- Localement, en définissant un répertoire par défaut.

La mise à jour de Malcore en ligne est différentielle et chiffrée.

La personnalisation de l'horaire souhaité est possible via l'interface WEB de la GBox.

Les hotfix permettent d'injecter un correctif sans qu'un redémarrage de la GBox soit nécessaire.

Il est possible de conserver jusqu'à trois paquets d'upgrade GBox.

La configuration de GUM est possible via un serveur mandataire (PROXY).

2.3 Analyses

La GBox permet différentes approches d'analyse pour un ou plusieurs fichiers soumis.

L'analyse heuristique, qui est soumise à différents moteurs anti-virus (16 possibles). Un score de menace est calculé en fonction des différentes analyses effectuées par les moteurs.

L'analyse statique, permet de retourner les informations des méta données du fichier soumis sans exécution de celui-ci.

L'analyse dynamique, permet l'exécution du fichier dans une sandbox et d'exfiltrer toutes les actions de celui-ci sur le système sous forme de rapport. Un graphique est présenté pour catégoriser le fichier soumis tout en lui attribuant un score de menace.

L'analyse de shellcode, permet de savoir si celui-ci est malveillant.

Ces différentes approches sont catégorisées par quatre moteurs d'analyse appelés 'Analyzer' :

— GOASM
— GNEST
— GMACLORE
— GRIP

2.4 Template

La création d'un template permet de personnaliser vos analyses en y incluant les Analyzers souhaités.
Un template par défaut est nécessaire pour lancer une analyse et/ou analyser les fichiers depuis un serveur de management (GCenter).

2.5 Rapport

Les rapports sont consultables directement depuis la WebUI de la GBox et/ou bien en téléchargement au format '.html' ou '.pdf'.
La composition de celui-ci diffère en fonction des Analyzers choisis pour analyse.

2.6 Analyse d'url

Les urls peuvent être soumises à nos moteurs d'analyses et de détection afin de définir le potentiel malveillant de celles-ci.

2.7 Champ de recherche

Il est possible d'effectuer une recherche sur une analyse déjà soumise via la WebUI de la GBox.

2.8 Export journaux

Les journaux peuvent être exportés via la WebUI de la GBox.

2.9 Management des utilisateurs

Il est possible d'éditer un compte utilisateur (création/modification/suppression) via la WebUI de la GBox.
Une vue de l'historique des authentifications et permissions accordées à un compte utilisateur est accessible via la WebUI de la GBox.
Le management des utilisateurs se fait via un compte Administrator.

2.10 Emergency mode

Une suppression automatique des analyses est effectuée si celles-ci dépassent un certain seuil de remplissage.

2.11 API externe

La GBox intègre une API REST qui permet :
— D'envoyer un fichier pour analyse.
— Le téléchargement d'un rapport.
— D'obtenir la version de celle-ci.

Chapitre 3

Problèmes connus

3.1 Interruption des analyses effectuées par GNEST

Lors de la configuration de l'analyzer GNEST, la création d'une ou plusieurs machines virtuelles entraîne un redémarrage de celui-ci. Cela impacte les analyses de GNEST en cours les mettant en « erreurs ».
Solution de contournement : Pas de solution.

3.2 Accès au panneau Tools

Le délai d'accès au panneau Tools via la WebUI de la GBox est allongé lorsqu'une machine virtuelle est en cours de création via la configuration de l'analyzer GNEST. Ce délai peut être amené à évoluer en fonction du nombre de machines virtuelles.
Solution de contournement : Pas de solution.

3.3 GBox - LOGS

Export : L'export des journaux de la GBox supérieur à 10GO rencontre un problème.
Accumulation : Les logs ne sont pas supprimés sur la GBox.
Solution de contournement : Pas de solution.

3.4 Configuration Proxy

GUM - Mode local : Si la GBox est configurée pour utiliser un serveur mandataire, GUM utilisera ce proxy pour récupérer les mises à jours en mode local.
Analyses URLs : Si la GBox est configurée pour utiliser un serveur mandataire, l'analyse d'URL locale utilisera ce proxy pour effectuer ses recherches.
Message d'erreur : Un message d'erreur peut survenir lors de la configuration du proxy. Il indique que le nom de celui-ci est incorrect. Le nom peut être correct mais celui-ci est injoignable.
Solution de contournement : Pas de solution. Vérifiez les règles de votre proxy.