PSC FRANCE

GORILLE

CYBER-SECURITY SOFTWARE BY CYBER DETECT©

GORILLE ANTIVIRUS DES MENACES INCONNUES

Disponible dans le catalogue UGAP

SCC France.scc.com

contact@psc-france.com

+33 9 72 35 13 56

2 Rue Diderot Villeneuve st Georges 94190

https://www.psc-france.com

Contrecarrer les attaques sophistiquées

La suite logicielle **GORILLE CLOUD** caractérise les logiciels malveillants qui passent à travers les antivirus et les systèmes de défense classiques.

Quelles que soient les mutations, transformations et protections des malware, **GORILLE CLOUD** détectent les souches qui passent sous les radars des protections antivirus classiques en se basant sur la lecture des comportements embarqués et non sur leur signature

CONTEXTE

On estime qu'environ **5%** des attaques sophistiquées (inconnues ; ciblées, persistantes packées …), entrainent potentiellement **95%** des coûts liés à la cybersécurité.

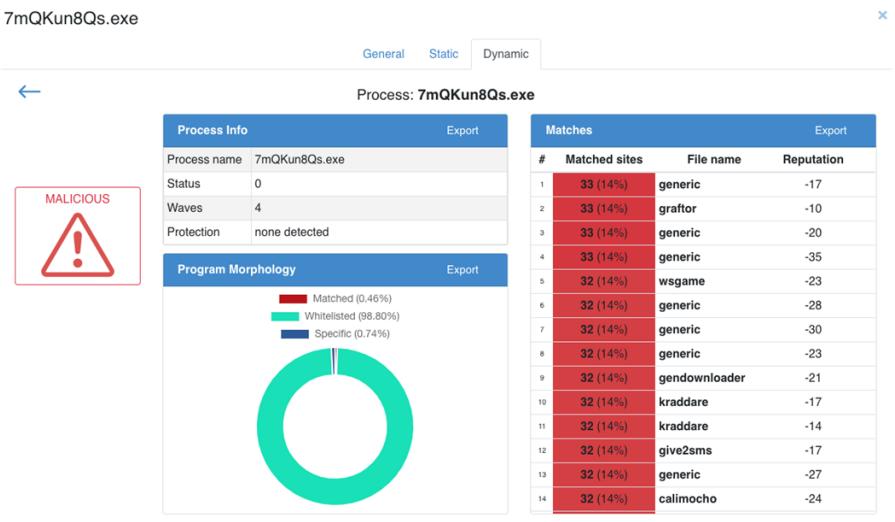
Les antivirus classiques basés sur les signatures mettent près d'un mois à contrer efficacement ces menaces. La solution **GORILLE CLOUD** caractérise les menaces « Zero day » en analysant la morphologie et le comportement et non les signatures des malware.

LA SOLUTION LOGICIELLE

GORILLE CLOUD analyse et qualifie des fichiers exécutables, aussi simplement qu'un glisser/déposer. L'exploitation de l'API GORILLE permet une levée de doute rapide et accélère la prise de mesures efficaces dans la gestion des incidents manuelles ou automatisées (ACL, alerte, diffusion, quarantaine, etc.). Le serveur **GORILLE CLOUD** effectue à distance des analyses faciles et rapides. Avec son API, il n'a jamais été aussi facile d'automatiser et de personnaliser les analyses pour chaque organisation.

FONCTIONNALITES

- Analyse statique simple et rapide - 1 seconde seulement pour analyser une menace.
- Analyse dynamique pour caractériser les menaces sophistiquées dans un environnement sécurisé (30 à 40 secondes) sans analyse ni reverse engineering manuel.
- Analyse comparative (version expert) entre plusieurs souches. Instantanée et sans reverse
- Classification, Clusterisation et Caractérisation des malware. Ni faux positifs ni faux négatifs
- Serveur Cloud à haute disponibilité. Version Appliance pour installation On-Premises, en mode connecté ou non.
- Une API JSON pour une intégration simplifiée de la protection et la détection ainsi qu'une automatisation/orchestration unique de la réponse offerte aux solutions EDR, NDR & ADR
- Utilisable Mode station blanche, expert ou interfacé avec des capacités SOAR



L'ANALYSE MORPHOLOGIQUE

Gorille se base sur la technologie unique et innovante d'Analyse Morphologique. Cette technologie mise au point au sein du Laboratoire de Haute Sécurité du LORIA (CNRS, Inria, Université de Lorraine.
Elle analyse dynamiquement (par exécution) et instantanément les fonctionnalités embarquées dans une application.
En qualifiant les codes (sites) malveillants ainsi détectés, l'Analyse Morphologique permet de repérer des attaques inconnues, sophistiquées ou encore obfusquées.
Combinant Intelligence artificielle (apprentissage de nouvelle menace, identification de fonctions), les outils de méthodes formelles, et les techniques de reverse-engineering (désassemblage, désobfuscation) notre technologie offre une précision unique et inégalée sur les exécutables sans nécessiter de phase d'apprentissage ni tuning local.

DES DELAIS DE REACTION CRITIQUES

On le constate quotidiennement à travers les expériences de nos partenaires. **GORILLE** fournit une qualification complète de l'infection d'une application dans un délai très court. Le délai d'analyse d'investigation numérique est reconnu comme un facteur clé de préservation des actifs des clients finaux, ce qui fait de **GORILLE CLOUD** un outil unique et idéal pour :

- Sécuriser les postes nomades,
- Limiter les pertes d'exploitation, fuites de données,
- Détecter les infections au sein d'un système d'information
- Caractériser une attaque pour réduire au maximum les délais de remédiation