

FONCTIONNALITES D'HORNET SECURITY ET CONSEILS D'UTILISATION

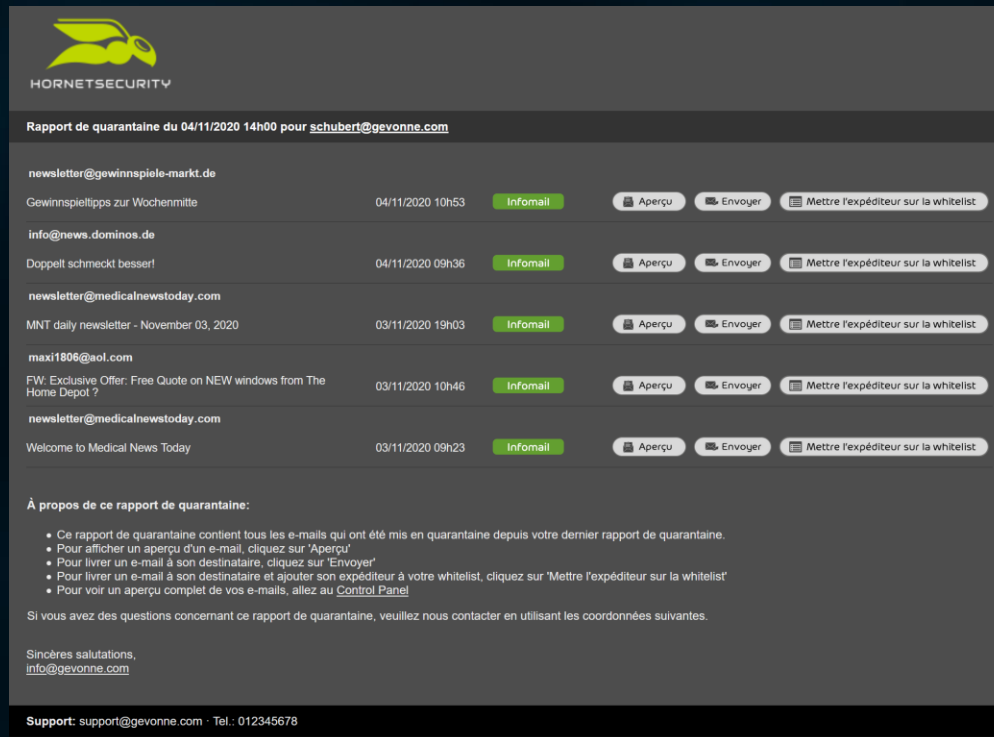
USER PANEL



HORNETSECURITY

ZONE DE QUARANTAINE

Suite à la mise en place de la solution Hornetsecurity, vous recevrez régulièrement un rapport de quarantaine par email comme celui-ci (le format peut varier selon ce qui a été paramétré) :



Ces rapports de quarantaine permettent à la fois de consulter les emails qui ont été bloqués par la solution, et de les libérer.

*Pour comprendre les catégorisations voir page 3



HORNETSECURITY

COMPRENDRE LES CATEGORISATIONS

Je peux
libérer ce mail

Infomail

Ces courriels sont à caractère publicitaire. Les infomails incluent également les newsletters envoyées par courriel.

Spam

Ces courriels ne sont pas souhaités et présentent souvent un caractère publicitaire ou malveillant.

Contenu

Ces courriels ont une pièce jointe non-conforme.

Menace

Ces courriels présentent des contenus dangereux, comme des pièces jointes ou des liens malveillants, ou sont envoyés pour commettre des infractions, telles que le Phishing.

AdvThreat

Advanced Threat Protection a identifié ces courriels comme une menace. Les courriels sont utilisés à des fins illégales et font appel à des moyens techniques sophistiqués qui ne peuvent être contrés qu'à l'aide de procédures dynamiques avancées.



HORNETSECURITY

Je dois
demander à
un admin de
libérer ce mail

PROTECTION DES URLs

Chaque URL présente dans un mail est réécrite* par la solution.

C'est une protection supplémentaire au moment du clic.

Une page Hornet Security sera affichée pendant l'analyse et en cas de blocage.



HORNETSECURITY



ANALYSE EN COURS

Merci de patienter pendant que nous analysons la page web pour détecter tout code malveillant éventuel.

Vous serez redirigé vers la page web dans un instant.

Soyez à l'affût des fautes de grammaire et de frappe car elles peuvent être des signes d'un email malveillant.



*La réécriture d'URL consiste à modifier les liens présents dans les emails pour rediriger les clics via un serveur de sécurité. Cela permet d'analyser les liens en temps réel pour détecter les menaces potentielles, comme le phishing ou les malwares.

Exemple d'affichage (analyse en cours)



HORNETSECURITY