

Huntsman la prévention intelligente contre les menaces

WebDefense et MailControl

Huntsman offre une protection indispensable contre les menaces immédiates qui exploitent la fenêtre d'exposition inhérente à tout anti-virus basé sur la reconnaissance de signatures. Huntsman, l'un des composants des solutions de sécurité à la demande pour le Web et la messagerie de SurfControl, n'a jamais laissé une menace immédiate atteindre le moindre de ses utilisateurs.

La menace de nouveaux virus, cheval de troie, spyware et autre malware s'intensifie et les entreprises sont plus que jamais exposées à ces risques, et le Gartner estime le coût moyen de désinfection à 100 000 \$ (54 000 £) pour une société de 500 employés.

Les menaces liées aux malware persistent car leurs auteurs sont très attachés à la création de nouvelles menaces immédiates, exploitant les fenêtres d'exposition, c'est-à-dire le délai qui s'écoule entre l'apparition d'une nouvelle menace et la mise à disposition d'une protection efficace par un éditeur d'anti-virus traditionnel. La fenêtre d'exposition peut varier de seulement quelques heures à plusieurs semaines en fonction de l'importance que l'éditeur d'anti-virus donne à la menace.

Comment les créateurs de malware exploitent la fenêtre d'exposition

Les créateurs de malware ont accès à des botnets, d'importants réseaux de systèmes corrompus, qui peuvent propager des attaques via e-mails à très grande échelle et à une vitesse considérable, ce qui permet de répandre les malware à un large public pendant la fenêtre d'exposition.

D'autres vecteurs d'attaques sont utilisés pour contourner les défenses traditionnelles. Les attaques combinées, telles que l'utilisation d'un e-mail contenant une adresse URL qui mène les utilisateurs à un site Internet d'où le malware est automatiquement téléchargé, sont des méthodes extrêmement répandues.

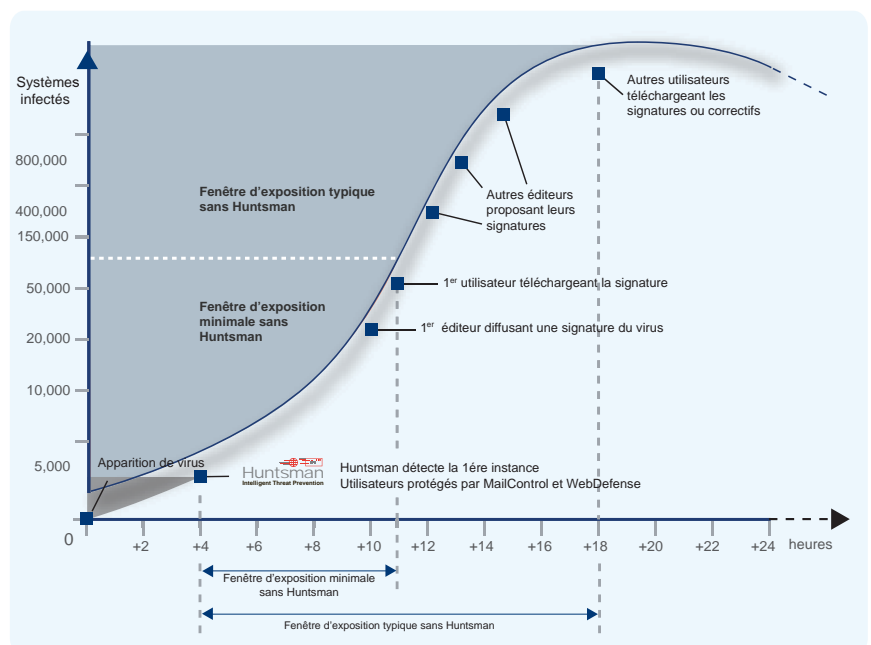
En créant de multiples variantes d'un nouveau malware et en les lançant simultanément ou à intervalle restreint, les créateurs de malware forcent les éditeurs d'anti-virus à faire paraître de nombreuses mises à jour, ce qui consomment des ressources, ralentit les mises à jour et allonge la fenêtre d'exposition.

Pire encore, les créateurs de malware testent leurs nouvelles créations contre tous les anti-virus principaux basés sur la reconnaissance de signatures, afin de s'assurer, qu'une fois le malware lancé, il infectera un grand nombre de machines.

Comment une entreprise peut se protéger

Huntsman est un système intelligent de prévention des menaces basées sur la technologie heuristique. Ce filtre contre les menaces est incorporé dans les services de sécurité à la demande pour le Web et la messagerie de SurfControl, parallèlement aux moteurs anti-virus traditionnels et aux analyses des menaces faites par des experts.

Huntsman bloque les menaces immédiates et ferme la fenêtre d'exposition. Depuis son lancement en 2003, Huntsman a bloqué des millions d'e-mails contenant une menace non-interceptée par l'un des trois moteurs anti-virus aussi utilisés par nos services. Jusqu'ici, Huntsman n'a jamais laissé une menace immédiate atteindre un client.



Les trois raisons principales du succès de Huntsman dans ce domaine sont les suivantes :

- Il détecte très bien les menaces immédiates
- Les défenses sont mises à jour immédiatement après détection de la première apparition d'une menace
- Les créateurs de malware ne peuvent pas tester leurs nouvelles créations contre Huntsman avant de les lancer

Comment Huntsman identifie les menaces immédiates

Huntsman est un élément à part entière des solutions de sécurité à la demande de SurfControl. En tant que tel, il a accès à des données additionnelles contenues dans l'e-mail lui-même et Huntsman analyse chaque email avec une série de tests, comprenant:

■ Analyse de la charge virale

La taille et le type de pièce-jointe sont actuellement de bons indicateurs d'une menace. Par exemple, les petits fichiers .exe ou encore les petits .zip contenant un seul .exe sont souvent des virus.

■ Analyse contextuelle

La structure de l'e-mail est examinée : les anomalies telles que des en-têtes falsifiées ou des noms de pièces-jointes obscures sont parmi les caractéristiques d'e-mails porteurs d'un virus. La délivrance d'e-mails comporte aussi des données importantes : s'ils proviennent d'un expéditeur ayant une mauvaise réputation ou du DUL d'un client (Dial Up Link), il y a alors de fortes chances qu'un système infecté en soit la source. Huntsman offre une vérification pro-active, par exemple en tentant de se connecter en retour à l'expéditeur d'un e-mail suspect.

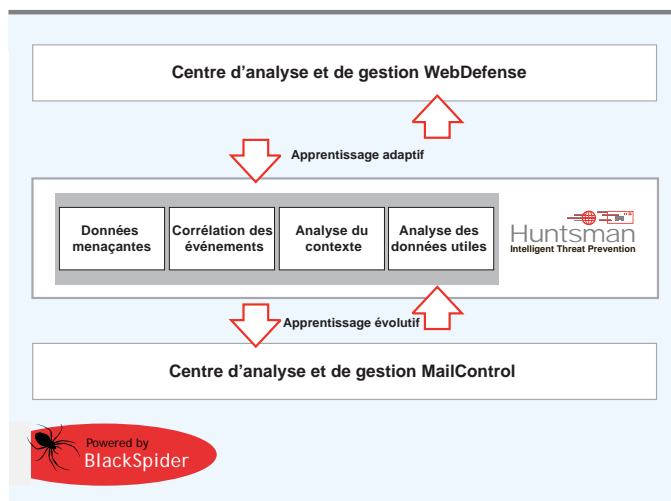
■ Corrélation des événements

Les attaques combinées peuvent facilement être identifiées en examinant l'historique des événements. Par exemple, on peut citer les virus polymorphes qui se manifestent avec différentes charges virales ou dans des e-mails différents. L'analyse des activités telles que la fréquence d'arrivée des e-mails ou une attaque via différents vecteurs (combinaison Web et e-mail par exemple) donne une vision globale d'une attaque ainsi que les données nécessaires pour la bloquer.

■ Volume de données relatives à la menace

Le succès des analyses liées au contexte et à la corrélation dépend beaucoup des données disponibles pour l'analyse. Huntsman traite quotidiennement, lors de sa recherche de menaces immédiates, pas moins de 20 millions d'e-mails et un million de connexions serveur grâce à tous ses utilisateurs.

La prévention Intelligente contre les menaces de Huntsman



Les créateurs de malware ne peuvent pas contourner Huntsman

Huntsman possède des heuristiques "privés" qui ne peuvent pas être acquis ou testés séparément. Les créateurs de malware ne peuvent donc pas créer une menace et la tester contre Huntsman avant son lancement. Les créateurs de malware font l'acquisition des anti-virus principaux du marché et testent leur nouveau malware contre ces derniers anti-virus afin de s'assurer qu'ils ne seront pas bloqués avant qu'une mise à jour n'apparaisse.

Huntsman offre une protection multi-services immédiate

Huntsman fonctionne en temps réel. Dès l'instant où une nouvelle menace est identifiée, les défenses sont mises à jour et la totalité du réseau d'utilisateurs est protégée, aussi bien sur le Web qu'à travers les services e-mails.

Pourquoi Huntsman ne peut pas comparé aux autres produits heuristiques

Certains anti-virus basés sur une reconnaissance des signatures prétendent avoir des capacités heuristiques. Cependant, ces programmes sont limités à la fois dans leur aptitude à détecter de nouvelles menaces et dans leur capacité à mettre à jour rapidement et efficacement leurs défenses. Ils ne sont pas à la hauteur de Huntsman pour les raisons suivantes :

■ Les heuristiques publics

Les heuristiques sont « publics », ce qui signifie qu'ils peuvent être achetés afin de tester les nouveaux malware et ainsi éviter qu'ils ne soient ensuite bloqués.

■ La vitesse de la protection

Les heuristiques se fient aux données récoltées par des programmes installés au sein des réseaux des utilisateurs, qui sont ensuite téléchargées par l'éditeur. Une fois l'analyse effectuée, les données de prévention des menaces mises à jour doivent être téléchargées sur le réseau du client. Ce système provoque des retards et dépend du bon déroulement de chaque étape.

■ Une protection multi-services

Aucun autre programme (ou service) n'offre la protection multi-services et en temps réel qu'offre Huntsman

■ La corrélation entre le contexte et les événements

Les heuristiques n'analysent que la charge virale suspecte, sans pour autant avoir la capacité d'analyser les mécanismes de délivrance qui sont pourtant symptomatiques des e-mails malveillants, tels que la structure du message ou les caractéristiques de la délivrance.

■ Volume des données menaçantes

Les solutions basées sur un programme (ainsi que certains services à la demande) éliminent de nombreux e-mails au niveau de la connexion pour économiser de la bande passante et maintenir une bonne performance. Ces solutions ne tirent aucun enseignement de l'analyse des données menaçantes.

Gestion des e-mails bloqués par Huntsman

Les e-mails bloqués par Huntsman sont mis en quarantaine avec les emails bloqués par les moteurs anti-virus. Les mêmes fonctionnalités de gestion sont disponibles : des notifications peuvent être envoyées, un administrateur peut contrôler et, si nécessaire, permettre la délivrance d'un e-mail.

Avantages de Huntsman

- Bloque 100% des nouvelles attaques dès le premier jour
- Protège les services MailControl et WebDefense
- Protège contre une nouvelle menace dès sa première apparition

Exemple du blocage d'une menace par Huntsman dès son premier jour - mars 2006

Ce tableau montre que Huntsman a bloqué plus de 42 000 e-mails qui étaient passés à travers les trois moteurs de détection anti-virus du service MailControl. Lorsque les e-mails bloqués passent de nouveau par les moteurs anti-virus, ils sont identifiés en tant que virus, cheval de troie, spyware ou autre malware. La fenêtre d'exposition représente le temps écoulé entre le blocage de la première menace par Huntsman et l'identification de la menace par le premier moteur anti-virus mis à jour.

Nom du virus	Occurrences interceptées par Huntsman	Fenêtre d'exposition - en heures
Trojan-Downloader.Win32.Small.cnk	15,624	8.5 heures
Trojan-Downloader.Win32.Agent.abb	11,657	5 heures
Trojan-Downloader.Win32.Agent.adu	5,168	2.8 heures
Trojan-Downloader.Win32.Small.coc	3,646	3 heures
PWSteal.Tarno.T	3,484	3.1 heures
Trojan-Dropper.Win32.Small.anc	3,005	2.4 heures
les autres	271	en moyenne 32 heures
Total	42,855	

Avantages clés des solutions de sécurité à la demande pour le Web et la messagerie de SurfControl : WebDefense and MailControl

La technologie de prévention intelligente contre les menaces, Huntsman fait partie intégrante des solutions de protection à la demande du Web et de la messagerie de SurfControl qui délivre une réelle protection pour un coût de possession total bas.

✓ WebDefense




- Protège contre les menaces web y compris les virus, chevaux de Troie, vers et attaques de phishing
- Evite la perte de productivité et l'usage excessif et non autorisé du web par les employés
- Protège les employés de contenus web illégaux ou indésirables
- Protège les communications webmail de tout malware potentiel
- Réduit la responsabilité pénale d'avoir des contenus illégaux sur le réseau
- Rentabilise les coûts informatiques en optimisant la bande passante
- Mise en oeuvre simple, souple et économique sans matériel ni logiciel à installer, et intégration minimale
- Une seule solution pour les sites multiples et les utilisateurs itinérants sans point faible
- Minimise le coût total de possession

✓ MailControl

- Les menaces sur le courrier électronique sont bloquées au niveau de l'Internet, bien avant votre réseau
- La technologie de prévention intelligente Huntsman analyse tous les courriers électroniques pour identifier les nouvelles menaces et mettre à jour les défenses en temps réel afin de réduire la fenêtre d'exposition
- Une mise en œuvre simple, souple et économique, une intégration minimale
- Des moteurs anti-virus multiples, issus des meilleures pratiques du secteur de la sécurité informatique
- La mise à jour globale et en temps réel des règles de sécurité du courrier électronique
- Une seule solution pour des sites multiples, sans point de défaillance unique
- Une architecture à haute disponibilité qui assure la continuité des services du courrier électronique
- Des fonctionnalités de reprise sur sinistre : les e-mails sont mis en attente si le serveur de courrier d'un client n'est pas disponible

SurfControl - Une protection encore plus élevée

La pénétration mondiale, la puissance financière et la spécialisation de SurfControl sur les solutions de sécurité Internet et du courrier électronique nous positionnent comme LE partenaire de sécurité incontournable auprès de la plupart de nos clients. Nous proposons des solutions de sécurité du contenu depuis 1997 et nous avons des milliers de clients satisfaits dans le monde entier, ce qui nous permet de développer nos futures solutions sur la base des besoins réels de nos références.

	Protection Web	Protection E-mail	Protection poste client
 <p>On-Demand</p>	✓	✓	
 <p>Network Appliances & Software</p>	✓	✓	
 <p>Desktop/Laptop</p>	✓		✓



Evaluation gratuite

Découvrez la protection immédiate contre les menaces de l'E-mail et du Web sans risque...

www.surfcontrol.com