

Protection « Zero-Hour » contre les attaques massives de virus

Totalement indispensable à la sécurité de la messagerie Internet de votre entreprise

Vue d'ensemble

Chaque entreprise possède déjà une solution antivirusale mise en place en raison de la prolifération croissante de malwares. Les auteurs de virus ont identifié le point faible des moteurs antivirus traditionnels comme étant le temps nécessaire pour développer une signature contre un nouveau virus. Ils ont exploité à leur avantage cette vulnérabilité en inondant simultanément Internet avec des milliers de variantes distinctes de nouveaux virus. Ces derniers, nommés « Server-Side Polymorphic Viruses¹ ou virus polymorphe », ont surpris les sociétés non protégées contre ce nouveau type d'attaque et ont causé des millions d'euros en dommages et en perte de productivité.

Ce livre blanc présente la technologie Commtouch Zero-Hour Virus Outbreak Protection (ou Zero-Hour AV), un complément essentiel aux protections antivirus traditionnelles. Basé sur la technologie de Recurrent Pattern Detection ou Détection des Signatures Recurrentes (RPD™), Zero-Hour AV permet de bloquer les attaques massives de virus polymorphiques plusieurs heures et même plusieurs jours avant les AV traditionnels, comblant ainsi le manque de protection contre ce nouveau fléau.

Une agression permanente envers les messageries Internet

Les courriels, un des outils de communication les plus importants, sont les principaux vecteurs de propagation de virus. Ils représentent 23% de toutes les infections de malwares des entreprises². Selon Osterman Research³, 84% des réseaux d'entreprise ont été pénétrés par des virus, des vers ou des chevaux de Troie attachés à des courriels.

Sécuriser les courriels est un challenge particulièrement difficile car le flot des messages est vital pour le fonctionnement de l'entreprise. Les administrateurs de réseaux doivent faire la balance entre une sécurité renforcée et un flot d'information ouvert ; les compromis coûteux sont malheureusement très courants. La plupart des entreprises ne peuvent pas prendre le risque qu'un message légitime soit pris pour un virus et donc bloqué. De plus, elles se retrouvent contraintes de prendre des mesures plus importantes comme celle de bloquer tous les fichiers exécutables du fait que leur solution AV n'est pas capable de reconnaître les programmes malveillants qui sont attachés et de les bloquer. Ce type de politique restrictive conduit à bloquer des messages légitimes (ou des faux positifs) et crée de la frustration chez les utilisateurs.

L'infection peut tout d'abord passer inaperçue

Dans le passé, lorsque les auteurs de virus et les distributeurs de virus étaient de simples "pirates adolescents" ou des utilisateurs avertis recherchant une certaine notoriété, les antivirus traditionnels

pouvaient être suffisants. Lorsqu'un utilisateur était infecté, il s'en apercevait clairement car le disque devait être formaté ou le virus s'envoyait lui-même vers la liste des contacts de l'utilisateur. La réalité d'aujourd'hui est que la majorité des virus sont maintenant invisibles aux utilisateurs. Ces malwares sont conçus pour générer des revenus illicites, tranquillement, sans être détectés. Le potentiel pour d'énormes profits a encouragé le développement d'une espèce nouvelle de malwares malveillants, capable d'échapper à la détection des solutions antivirus traditionnelles.

La plupart des malwares modernes sont conçus pour pouvoir effectuer en toute quiétude leurs activités malveillantes sans créer de symptômes évidents. Les enregistreurs de frappe permettent de récupérer des informations financières et les mots de passe, les composeurs peuvent transmettre ces informations sensibles en dehors de la société, les « backdoors ou portes dérobées » ouvrent des connexions réseaux aux hackers pour entrer et envoyer des malwares et des spams directement à partir du réseau d'entreprise. Toutes ces activités se déroulent sereinement, sans créer la moindre interruption et sans être inquiétées.

Le pire de cette situation est que les sociétés elles-mêmes pensent être protégées contre ces dangereux malwares. Si les responsables informatiques recherchent un virus en particulier sur le site de leur fournisseur d'AV, ils trouveront des dizaines de virus similaires pris en compte par la protection de l'AV. Cependant, ils ne réaliseront peut-être pas que des milliers de différentes variantes avec un nom similaire (chacune d'elle nécessitant un différent type de protection) peuvent attaquer leur organisation.

Antivirus traditionnel : L'ABC

Pour mieux comprendre pourquoi les antivirus traditionnels ne peuvent pas offrir de protection contre les malwares d'aujourd'hui, il est tout d'abord nécessaire de mieux connaître le fonctionnement des outils conventionnels. Il existe deux technologies de base utilisées dans les solutions AV : les signatures et les heuristiques.

Les antivirus basés sur la Signature sont ceux avec lesquels nous sommes le plus familiarisés. Lorsque chaque nouvelle variante d'un virus est identifiée, les spécialistes de la société d'AV prennent un échantillon du virus dans leur laboratoire, décomposent le code, développent une signature ou un "scan-string" permettant de l'identifier, puis le distribuent à ses utilisateurs. Cette méthode possède plusieurs inconvénients, dont :

- La méthode des Signatures ne convient qu'aux virus connus et identifiés.
- Elle ne convient en général qu'à une seule variante ou à un petit groupe de variantes possédant une grande partie du code en commun.
- Elle prend du temps (un minimum de trois heures, mais elle peut prendre aussi des jours) pour créer et distribuer des signatures.

Les efforts énormes et le temps nécessaire pour créer des signatures sont tels, que quelques sociétés AV leaders ont pris la décision d'ignorer plusieurs menaces et de ne pas produire de nouvelles signatures, même si les virus étaient déjà dans la boîte aux lettres des utilisateurs.

Eugène Kaspersky, fondateur de Kaspersky Lab Inc a déclaré :

"L'industrie des antivirus abandonne petit à petit parce qu'il est de plus en plus difficile de résister au nombre sans cesse croissant des menaces⁴"

Les moteurs antivirus de type Heuristique (basés sur des règles) ont été développés pour automatiser de manière partielle la défense AV et adopter une approche plus proactive pour identifier les virus inconnus. Pour créer des nouvelles règles heuristiques, les laboratoires AV ont encore besoin de scruter

le code viral afin de trouver si ce dernier contient des commandes malicieuses. Ensuite, nos spécialistes créent une série de règles basées sur chaque composant suspect identifié. Ces nouvelles règles sont diffusées et utilisées par les entreprises équipées de ces dites solutions. Le principal avantage de cette méthode par rapport à celle des signatures est qu'elle peut offrir une protection contre des virus qui étaient jusque-là inconnus. Cependant, il reste encore un certain nombre d'inconvénients majeurs :

- Elle demande du temps pour développer et distribuer aux utilisateurs de nouvelles règles heuristiques
- Elle ne permet pas d'identifier toutes les variantes des virus

Donc, comme dans le fameux conte "Les habits neufs de l'empereur", les auteurs de virus, les fournisseurs AV et les responsables sécurité des entreprises peuvent trouver une certaine satisfaction dans cette situation, mais en réalité les technologies AV traditionnelles ne sont pas capables de protéger correctement les entreprises. Tous les trimestres, les fournisseurs d'AV reçoivent des laboratoires de tests, des «certifications» basées uniquement sur des virus "connus" et non sur les virus inconnus qui représentent la vraie menace aujourd'hui. Les utilisateurs ne se rendent pas forcément compte qu'ils sont infectés. Ils pensent être protégés par les toutes dernières signatures de virus, sans réaliser qu'un simple nom de virus peut comprendre des dizaines de milliers de variantes, contre lesquelles la signature ne protège pas. En fin de compte, les auteurs de virus continuent de perpétrer leurs attaques lucratives sans le moindre souci.

Les Malwares d'aujourd'hui échappent aux AV traditionnels

Autrefois, les moteurs AV traditionnels étaient efficaces. Comment en sommes-nous donc arrivés à la situation actuelle ? Les tout premiers virus étaient le plus souvent envoyés sous la forme d'une seule variante en quantité énorme. Lorsque le nouveau virus était identifié, les responsables informatiques pouvaient informer leurs utilisateurs de ne pas ouvrir de courriels possédant un sujet ou un attachement particulier. C'était généralement suffisant pour protéger les utilisateurs jusqu'à ce que la signature soit disponible, quelques heures ou quelques jours après.

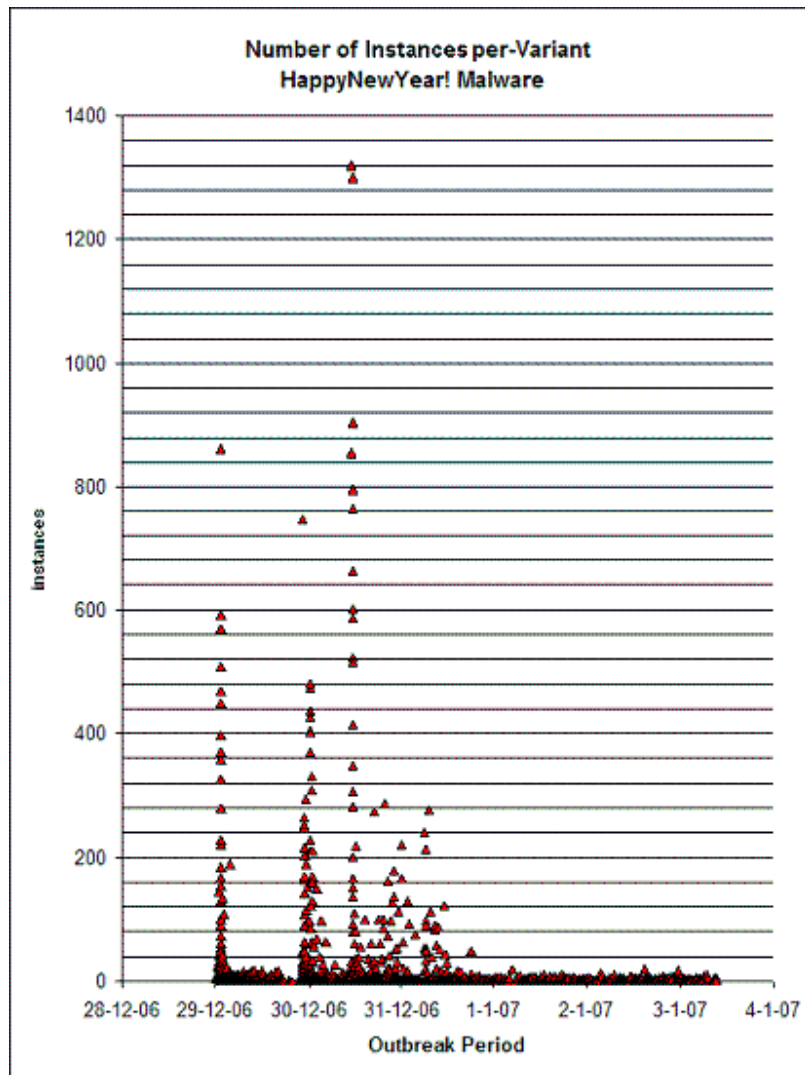
Plusieurs expériences faites par des auteurs de virus ont montré que les variantes des virus pouvaient être utilisées pour échapper aux moteurs AV basés sur des signatures. Une variante est une version légèrement modifiée du code d'un malware. Bien que les virus de type variante effectuent les mêmes actions malveillantes, les différences dans le code trompent le moteur AV qui recherche une correspondance exacte.

Fort de ce succès, les auteurs de virus ont poussé leurs raisonnements à l'extrême. Ils ont développé les « malwares polymorphes ou server-side polymorphic malware ». Ces derniers font appel à la technique consistant à créer une énorme quantité de malwares avec des petites différences dans le code et de les envoyer par rafales rapides. L'envoi d'une énorme quantité de variantes de virus (quelques heures seulement) permet d'intensifier la pénétration en concentrant l'attaque sur l'intervalle de temps très court précédant ainsi la disponibilité d'une signature.

L'un des premiers malwares de ce type, fin de l'année 2006/ début 2007, était le virus Tibs/Zhelatin que nous avons retrouvé dans nos boîtes aux lettres sous l'intitulé « Happy New Year » suivi de peu par ses variantes qui sont apparues sous les intitulés de « Storm Worm » et « Valentine's Days Greetings ». Même un virus ancien comme Bagle, datant de plus de trois ans et qui a débuté comme un virus courant, avec une seule variante, est maintenant qualifié de virus polymorphe, avec une moyenne de 600 nouvelles variantes par jour.

Même si les fournisseurs d'AV ont amélioré leur délai de livraison des signatures/règles heuristiques en le passant à quelques heures dans certains cas, les dernières générations de virus savent profiter de ces d'opportunités et utilisent toutes leurs munitions pour tirer parti de cette vulnérabilité.

Malwares polymorphes :
Des centaines de variantes



Source: Commtouch Labs

La stratégie des Malwares polymorphes

La grande vitesse de propagation des virus polymorphes s'appuie sur les stratégies suivantes qui permettent d'éviter les défenses des AV traditionnels :

Importante quantité de variantes : Ces malwares sont distribués avec un très grand nombre de variantes. Ainsi, Commtouch a mesuré et bloqué plus de 800 variantes distinctes du virus "Happy New Year" sur une période de cinq minutes seulement.

« Storm Worm » a été envoyé avec plus de 7000 variantes distinctes sur une période de plusieurs jours et plus de 40,000 sur une période de 12 jours. Comme chacune des variantes ou groupe de variantes nécessite une signature différente, il est impossible pour un moteur antivirus de suivre le rythme de cet embrasement.

Courte durée de vie des variantes : La durée de vie de chaque variante est très courte, en moyenne de deux ou trois heures seulement. Chaque variante apparaît rarement plus d'une seule fois. Comme le développement d'une nouvelle signature ou règle heuristique nécessite plusieurs heures et sa distribution aux utilisateurs plusieurs jours, ces variantes d'une durée de vie si courte, ne sont déjà plus en circulation lorsque les signatures des AV traditionnels sont afin disponibles.

Piratage psychologique : Plusieurs sujets ou noms de pièces jointes sont utilisés pour embrouiller les utilisateurs. Ces derniers ne peuvent plus être protégés en évitant simplement les messages avec un sujet ou une pièce attachée connus. Les sujets axés sur l'actualité sont utilisés pour attirer les personnes à ouvrir les messages. Par exemple, le « Storm Worm » reprend le thème des tempêtes qui se sont abattues en Europe.

Les moteurs AV traditionnels restent loin d'une protection instantanée ou « Zero Hour »

L'envoi rapide de variantes de virus, pouvant atteindre plusieurs centaines par minutes, tire profit du délai de disponibilité des nouvelles souches virales observé par les moteurs AV traditionnels basés sur les signatures. Le comparatif, basé sur les sources AV-Test.org, institution indépendante basée en Allemagne, permet de montrer que les leaders du marché de la sécurité informatique distribuent des signatures après plusieurs heures voire plusieurs jours après l'apparition d'un nouveau virus sur Internet.

Variant MD5 checksum	Date & AV-Test.org ID	Commtouch®	CA e Trust	Kaspersky	McAfee	Microsoft	Panda	Sophos	Symantec	Trend Micro
7e9a27662fa6422a1ad83bf6429cf01	2007-06-25_21-04_0002			283:56						
dad2eeba40f0abd060d268f8c01f7	2007-06-25_21-04_0002			8:55	115:48	118:56			32:31	
29b9f1a1c3842e78166767ef6e55cb1	2007-06-24_21-02_0004			39:17						
d571ad9595bfb9e432d226c8b34b37	2007-06-24_21-02_0004			38:00						
7b7b3354048d7bce3cc84fee869df442	2007-06-23_21-04_0002			12:15	65:04			6:451	53:37	
a349681365d14314ac8b76525af342c	2007-06-22_12-46_0040			30:31		42:09				
266a6bf521d2addc20af3a574620bd5	2007-06-20_21-04_0004			22:17	74:51					
fb5a9f21c00b470a61455e9a432c16a	2007-06-20_21-04_0004			50:31	15:03				71:29	
96cd7cb47859e9c9b35ca21c7831a96	2007-06-18_21-06_0001			99:34	45:50				89:48	
62929400c709bffe03c72e2b478db66	2007-06-16_21-03_0001			3:27		138:30	42:22		26:22	
168302a758121dcbce8395f5b9e108	2007-06-15_21-03_0002			21:18						
74c48d3a1e68226de731d370d9978d5	2007-06-10_09-08_0005			40:13				48:55	34:47	
27e1e3e4eb00b3628c445a4b71990	2007-06-10_09-08_0001			33:06	9:21				74:29	
14f34714c62e240dd74bf82c784f8885	2007-06-10_09-07_0002			13:02	8:57					
055a0a89500508700a94fce88295b23	2007-06-04_21-04_0002			8:57						

- Détection Zero-hour
- Une partie de l'attaque bloquée
- Pas de détection pendant la période d'analyse

Note : Le temps mentionné, pour chaque fournisseur d'AV, correspond au délai entre le moment où la signature est disponible (sources AV-Test.org) et l'heure de détection de Commtouch (source Commtouch RPD™). L'heure de détection de Commtouch n'est pas incluse dans les rapports de AV-Test.org.

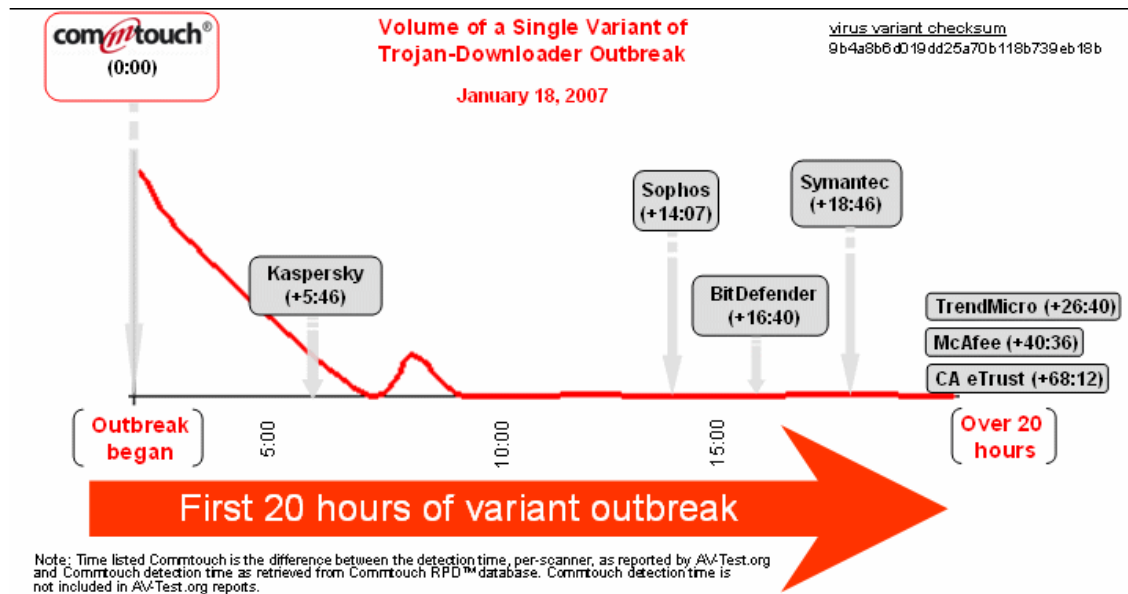
Les fournisseurs d'AV sont conscients de leur vulnérabilité et investissent des efforts considérables pour sortir des signatures et des règles heuristiques aussi rapidement qu'ils le peuvent. Cependant, cette approche dépend d'une analyse humaine et de ce fait, elle sera toujours soumise à des délais. Même le moteur AV le plus rapide laisse ces clients exposés pendant plusieurs heures, délai correspondant au processus de mise à jour des signatures.

Commtouch Zero-Hour Outbreak Protection

Commtouch, grâce à sa technologie Zero-Hour Outbreak Protection adopte une autre approche dans la défense contre les malwares. Basée sur les technologies propriétaires de Détection des Signatures Récurrentes RPD™ (Recurrent Pattern Detection), Commtouch Zero-Hour AV met l'accent sur l'identification et la classification en temps réel de l'empreinte unique présente dans chaque attaque massive plutôt que sur l'analyse du contenu de chaque message. Au lieu de se concentrer sur la recherche de nouveaux virus et de les arrêter grâce à une signature ou une nouvelle règle heuristique, Commtouch est à l'écoute chaque jour de plusieurs milliards de messages en provenance du monde entier, identifie, classifie et bloque toutes nouvelles attaques de malwares à l'instant où elles apparaissent.

Ainsi, Zero-Hour AV stoppe les malwares des courriels en temps réel et fournit une protection immédiate contre les nouvelles variantes durant les premières heures d'une attaque.

Comparaison Zero-Hour



Patent #6-330-590

Les techniques qui permettent de générer rapidement des nouvelles variantes de malwares continuent de se développer. La technologie temps réel Commtouch Zero-Hour Outbreak Protection a prouvé son efficacité contre toutes ces nouvelles attaques. Zero-Hour AV est le complément indispensable de toutes solutions AV traditionnelles, ajoutant ainsi une nouvelle protection temps réel contre les nouvelles attaques de virus.

La Détection des Signatures Récurrentes (Recurrent Pattern Detection) et RPD sont des marques et Commtouch est une marque déposée de Commtouch Software Ltd. Brevet U.S. No. 6,330,590 est la propriété de Commtouch.

Copyright © 2007

¹ Un malware polymorphe est un virus qui se modifie à chaque reproduction, ce qui le rend très difficile à cerner par un moteur antivirus. Les malwares polymorphes Server-side font référence au fait que de multiples variantes sont développées du côté du serveur, avant d'être distribuées vers les cibles

² *The 2007 Malware Report*, Computer Economics, p. 14

³ *Messaging Security Market Trends, 2006-2009*, Osterman Research, p. 11

⁴ SearchSecurity "SecurityWire Weekly, Episode 7, Eugene Kaspersky"

http://media.techtarget.com/searchSecurity/downloads/Security_Wire_Weekly_RSA_Kaspersky_02_08_2007.mp3