



## ÉTUDE DE CAS

### SCÉNARIO CLASSIQUE DE RISQUE D'ÉVOLUTION

La menace ZoTob.A a évolué comme VeriSign l'avait prévu dans son analyse de Copa.A. Précisément, l'analyse prévoyait qu'au moment où les menaces passeraient d'un code d'exploit public à un outil tel que Copa.A, des chevaux de Troie, voire un ver, ne tarderaient probablement pas à suivre. La dernière fois que des événements comparables se sont produits remonte à la vulnérabilité MS03-026 qui a mené à un outil de type autoroot, à plusieurs chevaux de Troie, puis aux vers Blaster et Welchia.

### AVANTAGES CLÉS

#### *Intelligence inégalée en matière de sécurité*

Les services iDefense Security Intelligence Services de VeriSign tirent parti des éléments soumis par un réseau mondial et privé de chercheurs en sécurité indépendants. Ces chercheurs consignent leurs soumissions par le biais de notre Vulnerability Contributor Program (VCP) qui regroupe des centaines de chercheurs issus de plus de 30 pays qui fournissent des solutions intelligentes en 12 langues. VeriSign a reçu des milliers de soumissions par le biais du VCP au cours des trois dernières années. Dès que VeriSign reçoit ces soumissions, un processus de recherche interne complet est

## La réponse de VeriSign à ZoTob.A

Les services iDefense® Security Intelligence Services de VeriSign® constituent un composant important de la célèbre suite de services Managed Security Services de VeriSign (MSS). Ces services fournissent une gamme complète de solutions intelligentes pertinentes concernant les menaces et vulnérabilités qui mettent en péril la sécurité des réseaux. Grâce à ces services, les organisations sont en mesure de protéger de manière proactive leurs données critiques et leur infrastructure contre les attaques.

S'appuyant sur une équipe formée d'experts expérimentés dans le domaine de la sécurité, VeriSign débarrasse l'Internet des menaces potentielles, comme les nouveaux codes malveillants, les nouveaux exploits ou les bandes organisées de pirates qui se livrent à des cybercrimes et autres actions étendues de cyberterrorisme. VeriSign combine cela avec des solutions intelligentes techniques et standard afin de fournir des fonctions avancées d'alerte et d'analyse concernant ces menaces. Ces fonctions aident les sociétés à protéger leur infrastructure critique.

Parallèlement au composant essentiel que représentent les services iDefense Security Intelligence Services de VeriSign pour tout programme performant de sécurité des informations, l'expertise et l'intelligence proposées par notre produit iDefense offrent également des avantages non négligeables aux autres clients des services Managed Security Services de VeriSign.

L'étude de cas ci-après fournit un exemple illustrant la manière dont VeriSign réussit à combiner les points forts de personnes compétentes, processus, technologies et intelligence efficaces pour identifier plus rapidement les menaces qui surviennent et pour pouvoir y répondre dans les plus brefs délais afin de garantir une plus grande sécurité à nos clients.

### + Chronologie des événements

Jour 1 - Mardi 9 août 2005

Microsoft® publie le bulletin d'alerte MS05-039 concernant une vulnérabilité de type Buffer Overflow Plug-and-Play. VeriSign envoie rapidement le rapport de renseignements Flash de VeriSign iDefense « ID# 418964:HIGH:Microsoft Plug-and-Play Buffer Overflow Vulnerability » à l'ensemble des clients des services iDefense Security Intelligence Services de VeriSign et commence ses recherches concernant la menace.

Jour 2 - Mercredi 10 août 2005

VeriSign envoie de nombreuses mises à jour du rapport initial aux clients des services iDefense Security Intelligence Services de VeriSign.

Jour 3 - Jeudi 11 août 2005

VeriSign découvre un code d'exploit public, augmentant considérablement le risque si peu de temps après le bulletin de sécurité émis par Microsoft. Par conséquent, VeriSign envoie un rapport de renseignements Flash de VeriSign iDefense à tous les clients des services iDefense Security Intelligence Service.



Where it all comes together.™

lancé afin de valider la soumission. Après validation, une notification fait état du fournisseur concerné et des clients des services iDefense Security Intelligence Services de VeriSign. VeriSign travaille en étroite collaboration avec des fournisseurs tels que Microsoft afin de garantir l'identification des vulnérabilités potentielles et de permettre aux fournisseurs de créer des correctifs aussi vite que possible. Les clients sont également informés de ces vulnérabilités pendant que VeriSign travaille avec le fournisseur. VeriSign a ainsi pu communiquer à ses clients des centaines de rapports iDefense initiaux et uniques à propos des vulnérabilités. Mais surtout, en moyenne, les clients des services iDefense Security Intelligence Services de VeriSign reçoivent des notifications concernant ces vulnérabilités 45 jours avant leur communication au public par les fournisseurs.

### *Intelligence personnalisée*

Les services iDefense Security Intelligence Services de VeriSign proposent un ensemble de services intelligents hautement personnalisables qui fourniront à votre entreprise l'intelligence dont elle a besoin, au moment où elle en a besoin.

### *La valeur de l'intelligence*

Ces dernières années, les coûts qui découlent d'une faille de sécurité ont considérablement augmenté (perte de temps, de données, d'image de marque). Parallèlement, le nombre de vulnérabilités a connu une croissance exponentielle, en même temps que le rythme des vulnérabilités et exploits s'accélère. Par conséquent, il est de plus en plus essentiel pour les entreprises d'être en mesure de se protéger de manière proactive. VeriSign, qui opère un suivi des événements de sécurité sur une base globale, fait état des vulnérabilités et exploits lorsqu'ils sont identifiés. Il fournit

En outre, le rapport bimensuel de VeriSign MSS sur les vulnérabilités est envoyé aux grandes entreprises de notre clientèle. Il les informe des nouvelles vulnérabilités et présente certains codes d'exploit.

#### Jour 4 - Vendredi 12 août 2005

VeriSign identifie d'autres codes d'exploit en indiquant le code d'exploit HOD, qui a publié le code d'exploit du LSASS en 2004 qui a conduit à Sasser et à d'autres vers.

VeriSign met à niveau le degré d'alerte sur EXTRÊME lorsqu'il détecte trois codes d'exploit et une activité intense des pirates. Il envoie également une notification aux clients des services iDefense Security Intelligence Services de VeriSign. Ces avertissements sont complétés par l'ajout d'informations de signature Snort et d'autres données qui contribuent à limiter le champ d'action du ver.

Parallèlement, VeriSign MSS met en œuvre un ensemble de signatures personnalisées et publiques sur diverses plates-formes afin de contribuer à protéger les clients des services Managed IDS / IPS Service contre l'exploit MS05 039.

#### Jour 5 - Samedi 13 août 2005

L'équipe qui s'occupe des codes malveillants surveille les activités des pirates liées à l'exploit MS05 039. Ses membres découvrent que trois programmes binaires compilés sont issus des exploits publics et sont en train de générer un outil, un cheval de Troie et un exploit de code malveillant automatisé.

#### Jour 6 - Dimanche 14 août 2005

VeriSign identifie le premier outil qui survient et contribue à automatiser l'exploitation des ordinateurs vulnérables (exclusif à iDefense). Cela représente une avancée significative dans la gestion du risque d'évolution, et pourtant il s'agit d'un code relativement simple.

VeriSign envoie un rapport de renseignements Flash de VeriSign iDefense prédictif à l'ensemble des clients des services iDefense Security Intelligence Services de VeriSign sur la base de l'ensemble des facteurs liés au risque global et à l'évolution de cette menace.

VeriSign MSS déploie des signatures supplémentaires sur diverses plates-formes afin de contribuer à protéger les clients Managed IDS / IPS contre les « programmes bot » MS05 039.

#### Jour 7 - Lundi 15 août 2005

Sept nouveaux programmes bot sont signalés le 15 août 2005. Trois d'entre eux sont signalés en premier par l'équipe VeriSign® Rapid Response (alors qu'aucun autre rapport public ne fait état du code) :

419659:RBot.BJK

419662:RBot.BJL

419691:SdBot.TPR

VeriSign valide plusieurs codes pour la fonction de messagerie et des vecteurs d'exploit afin de qualifier complètement l'évolution des menaces de type programme bot qui exploitent MS05-039.

#### Jour 8 - Mardi 16 août 2005

Plus d'une demi-douzaine de programmes bots voient le jour, entraînant au sein des grandes compagnies les incidents associés à la variante RBot.BJT, etc. Les clients de VeriSign Managed IDS et IPS ont été informés de la menace et disposent des signatures nécessaires pour les identifier. Étant donné l'agressivité des attaques de type programme bot et des variantes liées à MS05-039, et le succès de la variante RBot.BJT en particulier, VeriSign publie un rapport de renseignements Flash de VeriSign iDefense à l'attention de tous les clients des services iDefense Security Intelligence Services de VeriSign (419872:EXTREME:FLASH(v1): RBot.BJT Worm Exploits Microsoft Plug-and-Play Buffer Overflow Vulnerability, Aggressively Spreading in the Wild).

rapidement des informations et des conseils pertinents afin d'aider à limiter les risques avant que les assaillants en tirent profit. Les services iDefense Security Intelligence Services de VeriSign adoptent une approche proactive afin de maintenir un environnement sécurisé. Ils permettent aux utilisateurs d'économiser du temps et de l'argent en leur épargnant d'avoir à passer des heures à explorer les sites Web et e-mails, en regroupant et distribuant les informations et en procédant à un suivi des résultats.

#### *Surveillance de la sécurité et gestion des risques*

Surveillance des événements de sécurité 24 heures/24, 7 jours/7 : détection, analyse et corrélation en temps réel par votre équipe Vulnerability Aggregation dont les membres sont chargés de fournir des analyses principales et secondaires des nouvelles vulnérabilités. Les événements suspects et malveillants sont donc identifiés de façon proactive, ce qui limite les risques potentiels encourus par l'entreprise.

#### *Réseau global d'analystes spécialistes en intelligence*

Constitué de centaines d'analystes dans plus de 30 pays, le réseau multilingue de VeriSign offre une vision précoce et unique de l'univers cybernétique caché et des vulnérabilités logicielles autrefois inconnues.

### **+ Conclusion**

Les services Managed Security Services de VeriSign proposent une combinaison unique de solutions qui permettent une meilleure détection des menaces, une analyse plus fiable et une réponse sans précédent à ces menaces. Les clients des services iDefense Security Intelligence Services de VeriSign ont bénéficié de l'intelligence la plus récente contre les menaces à tous les stades d'évolution. Parallèlement, VeriSign a pu déployer des signatures afin de détecter les exploits sur de nombreuses plates-formes IDS/IPS commerciales et open source, ce qui offre une meilleure protection à nos clients Managed IDS/IPS.

### **+ Faites la différence avec VeriSign**

**Surveillance, intelligence et contrôle à l'échelle mondiale** – En tant que fournisseur principal de services d'infrastructure Internet essentiels, VeriSign dispose d'une visibilité unique en ce qui concerne les modèles de sécurité, les tendances et les menaces. Il extrait et assimile les informations de sa base de clients à l'échelle mondiale et du réseau de périphériques de sécurité qu'il gère. Tirant parti de ces informations et de cette intelligence, VeriSign est le partenaire idéal des sociétés auxquelles il fournit une visibilité, une consolidation et une corrélation des événements Internet mondiaux. Il identifie de façon proactive les tendances d'attaques et alerte ses clients.

**Partenaires de confiance** – VeriSign possède une solide expérience dans la gestion de services de sécurité. Pour cette raison, des milliers d'organisations profitent au quotidien d'un tel savoir-faire. Avec l'authentification renforcée, la sécurité des applications et du e-commerce, les services Managed Security Services de VeriSign® marquent l'engagement sans précédent de VeriSign à proposer des services permettant aux entreprises de se lancer sereinement dans le commerce électronique, les communications et le travail collaboratif.

**Consultants performants** – L'équipe de consultants en sécurité de VeriSign regroupe la plus forte concentration d'experts reconnus de l'industrie. Possédant en moyenne 10 ans d'expérience dans la sécurité des informations des entreprises et souvent au moins trois certifications dans le secteur, les consultants de VeriSign sont de véritables experts dans le domaine entier de la sécurité et de la confidentialité des informations. L'équipe VeriSign a collaboré avec des organismes de toutes tailles à travers le monde, des agences gouvernementales aux petites start-ups en passant par les sociétés qui figurent dans le classement Fortune 1000. Parmi les clients de VeriSign figurent des agences municipales et fédérales, des institutions financières, des organismes de santé, des entreprises de télécommunications et des cybermarchands.

**Solutions haut de gamme** – En tant que fournisseur indépendant de services de sécurité, VeriSign évalue, certifie et prend en charge des produits de sécurité haut de gamme. Il figure parmi les tous premiers fournisseurs de technologie de norme ouverte dans le domaine de l'authentification d'identité et des autres solutions de sécurité. La société conçoit et déploie des solutions de sécurité fondées sur les besoins et exigences de ses clients, et réévalue et améliore régulièrement ses propres offres de service, ainsi que les produits de sécurité tiers pris en charge.

### **+ Ne tardez pas**

Pour plus d'informations sur les services iDefense® Security Intelligence Services de VeriSign®, veuillez composer le 0800 90 43 51 ou envoyer un courrier électronique à l'adresse suivante : [ventes-entreprises@verisign.fr](mailto:ventes-entreprises@verisign.fr).

**Pour plus d'informations, visitez notre site sur [www.verisign.fr](http://www.verisign.fr).**

© 2006 VeriSign France S.A. Tous droits réservés. VeriSign, le logo VeriSign, « Where it all comes together », TeraGuard et les autres marques commerciales, marques de services et logos sont des marques commerciales déposées ou non de VeriSign et de ses filiales aux États-Unis et dans d'autres pays. Toutes les autres marques, déposées ou non, et marques commerciales appartiennent à leur propriétaire respectif.