INFOS TECHNOLOGIQUES :

LUTTE CONTRE BLASTER ET AUTRES VERS INTERNET

100 QUESTIONS ET REPONSES

1. EST-IL POSSIBLE DE LIMITER LE NOMBRE DE TRADUCTIONS D'ADRESSES RESEAU (NAT) DANS LES ADRESSES IP GLOBALES AVEC LE LOGICIEL CISCO IOS® ? LE VER NACHI, QUI SE PROPAGE SELON LE MEME MECANISME QUE BLASTER, A PROVOQUE UNE SATURATION DES RESSOURCES NAT PAR LE PROTOCOLE ICMP (INTERNET CONTROL MESSAGE PROTOCOL) SORTANT.

Oui. La commande « ip nat translation max-entries » permet de définir une limite. Consultez :

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a0080091cb9.shtml

Le pare-feu Cisco PIX® peut également limiter le nombre de connexions NAT. Consultez :

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727ab.html#1032127

2. COMMENT LE VER A-T-IL PU TRAVERSER LE PARE-FEU ?

Les vers se propagent en prenant l'aspect d'un trafic de réseau normal. Par exemple, lorsqu'un pare-feu contrôle l'accès à un serveur Web via le protocole HTTP (port TCP [Transmission Control Protocol] 80), il suffit que le ver se présente comme une requête HTTP GET valide pour que le trafic infecté soit admis sur le serveur. Pour lutter efficacement, installez des solutions de détection des intrusions ou d'autres moteurs d'inspection de contenu (par exemple, NBAR [Network-Based Application Recognition]).

3. LE BLOCAGE DE L'ACCES AUX PORTS 135-139 EST-IL EFFICACE ?

Pour s'infiltrer sur le réseau, le ver doit pouvoir se connecter aux ports NetBIOS du système cible. Il s'agit des ports 135 et 139, tous deux TCP et UDP. Bloquer l'accès à ces ports empêche le ver d'exploiter la vulnérabilité du système cible. Cette méthode s'est avérée très efficace pour enrayer la diffusion du ver.

4. LORS DE L'INSTALLATION D'UN PARE-FEU, CERTAINS PORTS DOIVENT ETRE OUVERTS, D'AUTRES FERMES. LES ATTAQUES DE VER VIA UN PARE-FEU CIBLENT-ELLES CERTAINS PORTS EN PARTICULIER ? EST-IL POSSIBLE DE FERMER CES PORTS ?

Par défaut, les pare-feu sont généralement configurés pour refuser tous les accès et en admettre certains par exception. Toutefois, il est préférable de vérifier que les seuls ports ouverts sont ceux dont l'ouverture aux réseaux externes est indispensable. Les ports ouverts les plus courants sont DNS (Domain Name System) (UDP/TCP 53), SMTP (Simple Mail Transfer Protocol) (TCP 25) et HTTP (TCP 80). Le ver Blaster utilise les ports 135 TCP, 4444 TCP et 69 UDP. Dans la plupart des infrastructures d'entreprise, il n'est pas nécessaire d'ouvrir ces ports aux accès externes.

5. NBAR A REUSSI A BLOQUER CODE RED. EST-IL AUSSI EFFICACE CONTRE LES VERS ACTUELS ?

NBAR est un bon outil tactique qui bloque les paquets malveillants tandis que vous appliquez des correctifs ou mettez en œuvre d'autres défenses contre un ver. Cependant, il doit reconnaître la signature unique de ce ver. Contre les vers Code Red, Cisco utilise une reconnaissance HTTP sur les signatures de trafic par défaut. Pour Blaster, nous recherchons des paquets SQL d'une longueur spécifique.

6. COMMENT SAVOIR SI VOUS AVEZ ETE INFECTE PAR LE VER BLASTER ?

Pour savoir si votre ordinateur est infecté, il suffit d'analyser votre système XP ou 2000. Recherchez les processus actifs dans le Gestionnaire des tâches. Si MSBlaster figure dans la liste, votre ordinateur est infecté. Téléchargez le correctif sur le site de Microsoft et effectuez les modifications Cisco décrites dans :

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

7. LE PARE-FEU CISCO PIX CONTIENT-IL UNE COMMANDE PERMETTANT D'IDENTIFIER LES MACHINES CONTAMINEES PAR LE VER NACHI ? UNE RAREFACTION DES ADRESSES IP GLOBALES SUR MON PARE-FEU CISCO PIX M'OBLIGE À EFFACER TOUTES LES HEURES.

Au-delà d'un nombre raisonnable, vous pouvez enregistrer dans un journal les tentatives de connexion ICMP (à partir de 50 par minute, par exemple). Le rapport généré fournit alors la liste des hôtes infectés. La console Cisco VMS contient des outils, notamment SIMS, qui simplifient cette tâche.

8. UNE POLITIQUE DE QUALITE DE SERVICE (QOS) PEUT-ELLE PROTEGER VOTRE RESEAU D'UN VER DU TYPE BLASTER ?

Dans certains cas, oui. Pour en savoir plus sur l'atténuation des effets de Nachi, visitez :

http://www.cisco.com/warp/public/707/cisco-sn-20030820-nachi.shtml

9. LE LOGICIEL CISCO IOS PERMET-T-IL DE FILTRER LES PAQUETS ICMP CONTENANT DES DONNEES SPECIFIQUES ?

Avec une liste de contrôle d'accès (ACL) étendue, vous pouvez créer des entrées ACL correspondant à des types de message ICMP.

10. LA TRADUCTION D'ADRESSES NAT SIGNALE LE PROTOCOLE ICMP SUR LE PORT 1024 (ENTRE AUTRES PORTS). COMMENT SAVOIR DE QUEL TYPE ICMP IL S'AGIT ?

Il est impossible de déduire le type ICMP du résultat d'une requête « show ip nat translation ». Cette commande répertorie uniquement les protocoles. Le port figurant dans la liste constitue un identificateur au sein du paquet ICMP et ne correspond pas directement au type ICMP, « echo » ou « echo reply ».

11. LE SYSTEME DE DETECTION DES INTRUSIONS D'HOTE (HIDS) PERMET-IL DE DETECTER, DE SIGNALER ET D'ELIMINER LE VER BLASTER ET TOUTES SES VARIANTES ?

Le système Cisco HIDS (Cisco Security Agent) détecte et signale le ver et, plus important, empêche la contamination des hôtes. Les politiques par défaut de Cisco Security Agent ont arrêté Blaster et toutes ses variantes sans nécessiter de mises à jour ou de signatures.

12. COMMENT PROTEGER VOTRE RESEAU DES MACHINES INFECTEES CONNECTEES VIA UN VPN ?

Le meilleur moyen de protéger votre VPN consiste à interrompre le tunnel qui fait face au pare-feu, puis à bloquer les ports 135, 444 et UDP 69, conformément aux instructions du Cisco PSIRT (Product Security Incident Response Team). Ces précautions devraient suffire à arrêter la propagation du ver. Veillez à appliquer les correctifs Microsoft.

13. EXISTE-T-IL UN PRODUIT DE SURVEILLANCE CISCO CAPABLE DE DETECTER LES TRAFICS INHABITUELS EVOQUANT DES VERS ?

Oui, des produits Cisco IDS peuvent surveiller le trafic et protéger votre réseau contre les vers et les virus. En outre, le partenaire Cisco Arbor Networks a mis au point un système de détection des anomalies qui s'appuie sur Cisco NetFlow et sur la recopie de port distant RSPAN (Remote Switched Port Analyzer) pour renforcer la sécurité. Pour en savoir plus, visitez :

http://www.cisco.com/en/US/tech/tk648/tk362/tk812/tech_protocol_home.html

http://www.cisco.com/en/US/products/hw/vpndevc/index.html

http://www.arbornetworks.com for more information

14. EN QUOI CONSISTE EXACTEMENT LA COMMANDE « NO IP UNREACHABLES » DANS LA PROCEDURE DE « MITIGATION » DU VER NACHI ?

Désactiver les adresses IP inaccessibles est indispensable car le refus de paquets par les ACL entraîne l'envoi d'un message d'erreur ICMP à l'adresse IP source. Il en résulte une surcharge du périphérique qui génère la réponse. Le trafic réseau double (une réponse par demande reçue) et, dans le cas d'un trafic imité, le message peut être dirigé vers un autre réseau que celui qui a véritablement émis le paquet.

15. QUELLES SONT LES ACTIONS SPECIFIQUES DES PRODUITS CISCO IDS FACE A UNE ATTAQUE DU VER BLASTER ?

Les produits Cisco Network IDS peuvent émettre une alarme visible sur la console SecMon du système Cisco VMS (Vector Managing System). Selon que la signature par défaut de l'attaque utilisée par le ver a été adaptée ou non, le sonde IDS peut transmettre des réinitialisations TCP ou fermer ou bloquer l'accès des pare-feu et des routeurs pour arrêter le trafic infecté entrant. En ce qui concerne la prévention des intrusions sur l'hôte, Cisco Security Agent empêche l'exécution du code malveillant et enraye ainsi la contamination. Cisco Security Agent peut détecter les actions d'un ver ; les sondes de Cisco IDS, en revanche, détectent le ver à condition que la signature du ver ait été enregistrée. D'où l'importance de maintenir à jour la liste des signatures.

16. CISCO PROPOSE-T-IL UN MOYEN D'ENREGISTRER DES ADRESSES D'ORDINATEURS SUR LE RESEAU EN VUE D'INTERDIRE LA CONNEXION DE NOUVELLES MACHINES ?

Il y a plusieurs réponses à cette question. Vous pouvez activer la sécurité des ports sur les commutateurs pour bloquer des adresses MAC (media access control) spécifiques au niveau de certains ports. Un certain nombre de fonctionnalités

récentes des commutateurs Cisco Catalyst® évitent d'autres attaques de niveau 2 telles que les attaques DHCP (Dynamic Host Control Protocol), GARP (General Attribute Registration Protocol) et Spanning Tree Protocol. Cependant il peut être judicieux d'utiliser la méthode d'authentification 802.1X, qui impose l'authentification des hôtes et des utilisateurs au niveau des ports du réseau (ou des points d'accès dans une infrastructure sans fil) avant l'attribution de VLAN. Le port peut ainsi faire suivre le trafic sur l'ensemble du réseau.

17. OÙ TROUVER LES INFORMATIONS DE SECURITE LES PLUS RECENTES PUBLIEES PAR CISCO DURANT UNE ATTAQUE DE VIRUS ?

Le Cisco PSIRT (Cisco Product Security Incident Response Team) fournit des informations parfaitement à jour sur les questions de sécurité de réseau, les correctifs, etc., applicables aux produits Cisco. Pour en savoir plus, visitez le site :

http://www.cisco.com/warp/public/707/advisory.html

18. QUEL EST LE MEILLEUR MOYEN DE PROTEGER L'ORDINATEUR HOTE DURANT L'UTILISATION D'UN CLIENT VPN AVEC UNE CONNEXION COMMUTEE ?

Cisco Security Agent travaille avec le client Cisco VPN au travers de la fonction AYT (Are You There). Le VPN peut s'assurer que Cisco Security Agent est installé avant d'activer le tunnel. Cisco Security Agent protège le réseau contre Blaster et les autres vers.

19. COMMENT SAVOIR SI DES PORTES DEROBEES ONT ETE INSTALLEES SUR NOS SYSTEMES ?

Plusieurs offres logicielles permettent de déterminer si une porte dérobée a été installée sur vos systèmes. Une méthode simple consiste à utiliser un scanner de port pour analyser les systèmes et rechercher des ports ouverts alors qu'ils devraient être fermés. Dans ce cas, il est nécessaire de connaître les ports qui doivent être ouverts sur votre système. D'autres logiciels, par exemple Nessus, identifient les portes dérobées éventuelles. Vous pouvez également essayer le logiciel libre CHK rootkit, disponible à l'adresse :

http://www.chkrootkit.org

20. QUELLE EST L'INFLUENCE DU DEBIT CAR (COMMITTED ACCESS RATE) SUR LA SECURITE DU RESEAU ?

Le débit CAR, l'élaboration de politiques de trafic et autres mécanismes de qualité de service sont des outils efficaces. Pour en savoir plus, visitez :

http://www.cisco.com/en/US/products/sw/iosswrel/ps1820/products_feature_guide09186a00800f4890.html

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008008044c.html

21. MON FOURNISSEUR D'ACCES ME DEMANDE DE LAISSER LE PORT ICMP OUVERT POUR RECEVOIR UN JEU D'ADRESSES IP QU'IL M'ENVOIE AFIN DE CONNAITRE MON STATUT DE CONNEXION A INTERNET A TOUT MOMENT. SI J'OUVRE LE PORT UNIQUEMENT POUR CES ADRESSES, SUIS-JE PROTEGE ? LES ADRESSES IP FOURNIES SE TERMINENT PAR /24 ET /23.

Il est préférable de déterminer les adresses IP qui doivent rester ouvertes. La nécessité d'être visible ne signifie pas que vous devez accepter tous les messages ICMP. Les seuls messages à admettre sont « echo », « echo reply », « time exceeded », « packet-too-big », « traceroute » et « unreachable ».

22. COMMENT SE REPECUTE LA PRESENCE D'ACL SUR VOS ROUTEURS PERIPHERIQUES SUR VOTRE RESEAU LORSQUE LE TRAFIC QUI LES TRAVERSE EST TROP ELEVE ?

Si le débit est trop important, l'augmentation de l'utilisation de l'UC sur le routeur ralentit ce dernier. Ce problème reste rare car le code ACL s'exécute au sein de circuits ASIC (application-specific integrated circuits) dans la file d'attente d'entrée. Si vous constatez un ralentissement, appliquez NBAR à partir de l'ISP pour limiter le débit du trafic. Reportez-vous aux annonces du Cisco PSIRT et au schéma directeur SAFE :

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801aedd6.shtml

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

23. LA TECHNOLOGIE de « CAPTURE DE TRAFIC » (SNIFFING) CONSTITUE-T-ELLE LE SEUL MOYEN D'IDENTIFIER LES ORDINATEURS CONTAMINES PAR BLASTER SUR LE RESEAU ?

Pour savoir si votre ordinateur est infecté, il suffit d'analyser votre système XP ou 2000. Recherchez les processus actifs dans le Gestionnaire des tâches. Si MSBlaster figure dans la liste, votre ordinateur est infecté. Téléchargez le correctif sur le site de Microsoft et effectuez les modifications Cisco décrites dans :

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

24. EN TERMES DE METHODOLOGIE DE « MITIGATION », L'IDENTIFICATION DU VER EST-ELLE PLUS URGENTE QUE L'ARRET DE SA PROPAGATION ?

Non. Il est impératif de contenir l'infection le plus rapidement possible. L'identification du ver est l'étape suivante. Vous devez commencer par bloquer la propagation du ver sur votre réseau ou au-delà.

25. QUE SE PASSE-T-IL SI ON APPLIQUE L'ACL A L'INTERFACE EXTERIEURE D'UN ROUTEUR CISCO 1721 ALORS QU'UNE FONCTION DE PARE-FEU EST ACTIVEE ET QUE DES TUNNELS VPN ABOUTISSENT A L'INTERFACE EXTERIEURE ?

Les ACL étendues de Cisco sont à commutation rapide, aussi l'impact sur les performances est-il négligeable.

26. MA SOCIETE UTILISE LE PORT 135 POUR EXECUTER UNE APPLICATION PRIVEE. QUE PUIS-JE FAIRE SANS BLOQUER CE PROCESSUS ?

Dans le cas où des ports connus tels que TCP/UDP 135 sont utilisés pour accéder à des sites distants via Internet, la technologie VPN constitue une solution plus sûre. Pour en savoir plus, visitez le site :

http://www.cisco.com/en/US/netsol/ns110/ns170/net_solution_home.html

27. BLOQUER LE PORT 135 PERMET DE CONTENIR L'EXPANSION DU VER MAIS ARRETE CERTAINES FONCTIONS DE WINDOWS 2000 SERVER. SUR LES RESEAUX DE PLUSIEURS CENTAINES DE SERVEURS, LES ACL SONT DIFFICILES A GERER. EXISTE-T-IL UNE METHODE PLUS EFFICACE POUR LUTTER CONTRE LES VERS QUI EXPLOITENT DES PORTS ET DES SERVICES NECESSAIRES ?

Cisco Security Agent permet de bloquer n'importe quel port sur vos hôtes. Toutefois, le blocage des attaques au niveau des ports n'est pas la seule méthode de protection contre les dégradations. Cisco Security Agent assure une « défense approfondie » et offre plusieurs couches de protection. Par exemple, Cisco Security Agent empêche Blaster de lancer la commande shell et de s'exécuter.

28. COMMENT INTERVIENT LE PAQUET ICMP DE 92 OCTETS DANS LA PROPAGATION DE LA VARIANTE DU VER BLASTER ?

Le paquet ICMP de 92 octets n'a rien à voir avec le ver Blaster, il s'agit de la signature du ver Nachi. Toutefois, au cours de nos tests, aucun utilitaire de ping standard (générateur de requête ICMP echo) n'a généré de paquet de 92 octets par défaut. Connaissant ce comportement unique du ver, il est possible d'affirmer que les paquets ICMP de 92 octets proviennent d'un hôte contaminé par Nachi.

29. QU'EST-CE QUE NBAR ?

NBAR signifie Network-Based Application Recognition (reconnaissance d'application sur le réseau). Cette fonctionnalité intégrée des routeurs Cisco permet de marquer le trafic spécifique aux applications ou aux services en vue de l'ignorer, de le formater ou de le réglementer à l'aide de divers mécanismes de qualité de service ou ACL. Pour en savoir plus, visitez le site :

http://www.cisco.com/warp/public/732/Tech/qos/nbar/

30. CISCO SECURITY AGENT PEUT-IL VOUS EMPECHER D'EXECUTER LA COMMANDE CMD ?

Par défaut, Cisco Security Agent empêche l'exécution de la commande CMD par certaines applications. Cette précaution évite l'exécution d'un code malveillant sur votre système. Cisco Security Agent permet en outre d'adapter les politiques de sécurité aux besoins de votre environnement. Vous pouvez par exemple instaurer une règle interdisant l'exécution de la commande CMD sur l'ensemble de vos hôtes.

31. LES PORTS 135 ET 139 SONT UTILISES PAR NETBIOS ET FTP. BLOQUER CES TRAFICS EQUIVAUT A ARRETER LES CLIENTS ET SERVEURS MICROSOFT, ET DONC A EMPECHER LES UTILISATEURS DE TRAVAILLER. EXISTE-T-IL UNE ALTERNATIVE AU BLOCAGE DU TRAFIC ?

NetBIOS utilise les ports 135 et 139 ; FTP utilise les ports 20 et 21. Bloquer les ports NetBIOS pose des problèmes, en particulier si vous utilisez les fonctions réseau de Microsoft Windows (partage de disques, WINS, etc.). La seule alternative au blocage des ports 135 et 139 (s'ils sont indispensables à l'activité de votre réseau) consiste à maintenir tous vos systèmes à jour en matière de correctifs.

32. COMMENT DEPLOYER CISCO SECURITY AGENT SUR MON RESEAU ?

Il existe plusieurs moyens de déployer Cisco Security Agent sur un réseau. Vous pouvez l'intégrer à un script d'ouverture de session, le distribuer par des méthodes classiques (SMS, envoi d'un fichier exécutable par courrier électronique) ou inviter l'utilisateur final à télécharger le programme à partir d'un site Web. Vous pouvez enfin l'installer manuellement à l'aide d'un CD-ROM.

33. DES PROCEDURES DE CORRECTION PLUS RAPIDES AURAIENT-ELLES PU LIMITER LA DIFFUSION DU VER BLASTER ET DE SES VARIANTES ? OUTRE LES MISES A JOUR AUTOMATIQUES DE WINDOWS, QUELS SONT LES PRODUITS QUI PEUVENT SIMPLIFIER LA CORRECTION ?

L'application rapide des correctifs, toujours recommandée, est souvent complexe d'un point de vue administratif. Si un seul correctif est publié chaque semaine, la productivité de votre réseau supportera-t-elle l'inactivité requise par l'application et le redémarrage du correctif ? Un solide argument en faveur de la mise en œuvre de Cisco Security Agent

est son aptitude à gérer et modifier les profils immédiatement pour éviter l'inactivité des serveurs, tout en vous permettant d'adopter un programme de correction régulier plutôt que réactif.

34. LE NOUVEAU MODULE SUPERVISOR ENGINE 720 POUR LA GAMME CISCO CATALYST 6500 EST-IL CAPABLE DE FILTRER LES PAQUETS EN FONCTION DE LEUR TAILLE SANS LES TRANSMETTRE A L'UC ?

Non. Lorsque vous consultez les données d'un paquet, vous utilisez l'UC.

35. COMMENT L'EXECUTION DE NBAR SUR UN GRAND NOMBRE DE SYSTEMES INFECTES SE REPERCUTE-T-ELLE SUR LES PERFORMANCES ?

Les répercussions varient selon la plate-forme (certaines, dont Cisco Catalyst 6500, bénéficient d'un support matériel) et les actions prévues. Pour une efficacité optimale de NBAR, définissez la qualité de service de façon à ignorer les actions « conform » et « exceed ». Cela se traduira par une utilisation de l'UC inférieure à 10 % sur Cisco 7206.

36. NOUS UTILISONS LES FLUX MLS (MULTILAYER SWITCHING) POUR SURVEILLER LE TRAFIC ICMP ET DETECTER LE VER NACHI, MAIS IL S'AGIT LA D'UN PROCESSUS MANUEL. EST-IL POSSIBLE DE L'AUTOMATISER ?

Cisco NetFlow, associé à des outils ou produits tels que le système de détection des anomalies d'Arbor Networks (partenaire développeur de Cisco), est utile dans ce cas. Pour en savoir plus, visitez le site :

http://www.cisco.com/en/US/tech/tk648/tk362/tk812/tech_protocol_home.html

37. CISCO IDS UTILISE-T-IL UN PROCESSUS AUTOMATIQUE DE RECUPERATION DE SIGNATURES ?

Oui. Les sondes IDS peuvent être configurés pour télécharger leurs Service Packs via la console d'administration Cisco IDS sous Cisco VMS.

38. LE BLOCAGE DES PORTS 135 ET 139 SUR UDP ET TCP PEUT-IL PERTURBER UN UTILISATEUR DISTANT CONNECTE AU RESEAU VIA UN VPN ?

Oui. Il affecte la capacité de l'utilisateur à accéder aux services de réseau Windows.. Vous pouvez envisager de coder ces informations dans le fichier LMHOSTS.

39. SI VOUS FILTREZ LE TRAFIC EN FONCTION DE LA LONGUEUR DES PAQUETS, VOTRE RESEAU EST-IL EXPOSE À UN NOUVEAU VER GENERANT DES PAQUETS D'UNE LONGUEUR DIFFERENTE ? POURREZ-VOUS REAGIR SUFFISAMMENT RAPIDEMENT POUR EVITER UNE ATTAQUE ?

La mesure liée à la longueur des paquets est spécifique au ver Nachi. Pour en savoir plus, visitez le site :

http://www.cisco.com/warp/public/707/cisco-sn-20030820-nachi.shtml

En outre, nous invitons nos clients à consulter les conseils les plus récents du Cisco PSIRT à l'adresse :

http://www.cisco.com/warp/public/707/advisory.html

Nous recommandons également de travailler avec le centre d'assistance technique (TAC) Cisco et l'équipe chargée de votre compte pour résoudre vos problèmes de sécurité de réseau.

40. J'AI INSTALLE CISCO SECURITY AGENT SUR MON RESEAU, MAIS IL SEMBLE EMPECHER LES PROGRAMMES ANTIVIRUS DE METTRE A JOUR LEURS FICHIERS. COMMENT CELA SE FAIT-IL ?

Probablement parce que Cisco Security Agent détecte un code exécutable téléchargé à partir du réseau et tentant de s'exécuter. Vous pouvez ajuster la politique pour autoriser les programmes de mise à jour des signatures antivirus (par exemple, Symantec LiveUpdate.exe) afin d'éviter ce problème.

41. COMMENT LE BLOCAGE DES PORTS 135, 139 ET 445 SE REPERCUTE-T-IL SUR LES APPLICATIONS UTILISEES ? NOUS AVONS BLOQUE CES PORTS ET PLUSIEURS APPLICATIONS NE FONCTIONNEMENT PLUS NORMALEMENT.

Le blocage des ports 135, 139 et 445 perturbe le fonctionnement des applications qui accèdent normalement à ces ports. Il est préférable de bloquer l'accès aux ports durant les procédures de contention et d'éradication du ver. Une fois le ver éliminé et les correctifs appropriés appliqués sur les systèmes, l'accès aux ports 135, 139 et 445 peut être autorisé. Avertissement : Cisco recommande de ne pas autoriser l'accès à ces ports depuis Internet. Pour plus de sécurité, autorisez l'accès à ces ports uniquement depuis votre LAN d'entreprise.

42. COMMENT CONFIGURER CISCO NETFLOW POUR SURVEILLER LE TRAFIC ICMP SUR LES COMMUTATEURS DE NIVEAU 2 ET 3 ?

L'utilisation de Cisco NetFlow est fonction de la situation. Pour en savoir plus sur NetFlow, visitez le site :

http://www.cisco.com/en/US/tech/tk648/tk362/tk812/tech_protocol_home.html

Arbor Networks, partenaire de Cisco, offre un système de détection des anomalies qui s'appuie sur Cisco NetFlow pour détecter divers types de trafic anormal. Pour en savoir plus, visitez le site : http://www.arbornetworks.com

43. J'UTILISE DES SYSTEMES DES GAMMES CISCO 4000, 2500 ET 1600 ET CISCO IOS 11.3 ET 12.1. PUIS-JE UTILISER TOUTES LES FONCTIONNALITES INTEGREES DE CES ROUTEURS POUR ME PROTEGER CONTRE LES VERS ?

Oui. Les listes d'accès de base et la limitation du débit sont les solutions les plus sûres. Si la version du logiciel Cisco IOS® que vous utilisez ne supporte pas la limitation de débit ou NBAR, essayez de négocier avec votre fournisseur de services pour qu'il limite le trafic à votre place. Consultez les articles suivants pour appliquer des correctifs aux routeurs :

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801aedd6.shtml

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

44. SI LE CONTROLE DES TEMPETES DE BROADCAST EST DESACTIVE AU NIVEAU D'UN PORT, LE PORT EST-IL REACTIVE UNE FOIS DEBRANCHE ?

Le port est inactivé lorsqu'il est débranché.

45. LA MISE EN ŒUVRE DE LA COMMUTATION CISCO NETFLOW SUR UN ROUTEUR DESACTIVE-T-ELLE OU REMPLACE-T-ELLE CISCO EXPRESS FORWARDING ?

Cisco NetFlow n'est pas un chemin de commutation et fonctionne en harmonie avec Cisco Express Forwarding et distributed Cisco Express Forwarding sur les plates-formes concernées. Pour en savoir plus, visitez le site :

http://www.cisco.com/en/US/tech/tk648/tk362/tk812/tech_protocol_home.html

46. UN VLAN PRIVE COUVRE-T-IL PLUSIEURS COMMUTATEURS ?

Les ports de VLAN privé peuvent être situés sur différents périphériques de réseau à condition que ces équipements soient connectés au réseau principal et que les VLAN principaux et secondaires n'aient pas été éliminés du réseau principal.

47. EN QUOI LA SIGNALISATION CAS (CHANNEL ASSOCIATED SIGNALING) DIFFERE-T-ELLE DE LA SURVEILLANCE HEURISTIQUE PROPOSEE PAR CERTAINS PRODUITS ANTIVIRUS ?

Cisco Security Agent ne surveille pas uniquement le comportement mais déduit d'événements comportementaux leur caractère malveillant ou normal.

48. LORSQUE LES PORTS NE SONT PAS OUVERTS, DEVONS-NOUS NOUS CRAINDRE UNE INTRUSION AU TRAVERS DU PARE-FEU ?

Certaines attaques et codes connus peuvent acheminer le trafic par des moyens peu courants, tels qu'un TUNNEL LOKI. Vous avez de grandes chances d'être protégé, mais le risque ne peut être complètement écarté.

49. CISCO 4507 SUPPORTE-T-IL LES VLAN PRIVES ?

Oui. Consultez :

http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a008019d0e2.html

50. EST-IL NECESSAIRE DE METTRE A JOUR LA POLITIQUE DE COMPORTEMENT DE CISCO SECURITY AGENT ?

Des outils de réglage intégrés permettent d'adapter les politiques par défaut à votre environnement. Ce processus est comparable à l'adaptation des signatures IDS lorsque vous utilisez un produit HIDS. Toutefois, Cisco Security Agent ne reposant pas sur les signatures (il s'agit d'une architecture « sans mise à jour »), vous n'aurez pas à « réadapter » la politique.

51. LE VER BLASTER GENERE UN GRAND NOMBRE DE REQUETES TCP 135 PAR SECONDE. EXISTE-T-IL UN MOYEN DE DETECTER AUTOMATIQUEMENT CETTE ANOMALIE ET DE FERMER AUTOMATIQUEMENT LE PORT DE COMMUTATION ?

Nous pouvons détecter le trafic anormal, mais la fermeture du port de commutation doit être effectuée manuellement.

52. EST-IL UTILE DE PLACER UNE ACL SUR VOTRE ROUTEUR DE PERIPHERIE AINSI QUE SUR LES ROUTEURS CENTRAUX ?

Il est conseillé de placer une ACL sur les routeurs périphériques. En général, il est judicieux de placer les ACL à proximité de la source du trafic. Les routeurs centraux étant configurés pour acheminer le trafic le plus rapidement possible, des ACL ralentiraient le processus.

53. DES PARAMETRES DE QUALITE DE SERVICE PEUVENT-ILS EMPECHER UN VER DE TYPE BLASTER D'AFFAIBLIR LE RESEAU ?

Il est possible de faire appel à la qualité de service, toutefois NBAR et l'option de limitation de débit reconnaissent plus rapidement le trafic suspect, avec des répercussions moindres sur les performances. Pour en savoir plus, visitez :

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801aedd6.shtml

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

54. EST-IL INDISPENSABLE D'ACHETER CISCO VMS POUR POUVOIR UTILISER TOUTES LES FONCTIONS DE CISCO SECURITY AGENT ?

Cisco Security Agent est un produit non autonome administré centralement. Pour le contrôler, vous aurez besoin de la console d'administration Cisco VMS.

55. UN SERVEUR CISCO SECURITY AGENT PEUT-IL COLLECTER LES EVENEMENTS DES CLIENTS EN VUE DE GENERER UN RAPPORT CENTRALISE ?

Oui. Cisco Security Agent collecte les événements enregistrés dans les journaux d'événements et de sécurité NT ou à partir de UNIX syslog. En outre, la console Cisco Security Agent Management Center met en relation les événements reçus de différents agents. Par exemple, une attaque distribuée de découverte de mot de passe par brute de force peut être détectée en reliant des événements d'échec de connexion enregistrés par plusieurs agents.

56. LA SONDE CISCO IDS CONNAISSAIT-IL LA SIGNATURE DE BLASTER LORSQUE LE VER A ENVAHI INTERNET ?

Oui. Cette signature figurait dans la mise à jour Signature Update 50.

57. QUELS SONT LES EFFETS DU VER BLASTER SUR LES SYSTEMES UNIX ?

Pour en savoir plus sur l'utilisation de NBAR contre Blaster, reportez-vous au schéma directeur SAFE du livre blanc Cisco relatif à Blaster, à l'adresse :

http://www.cisco.com/go/SAFE

58. EXISTE-T-IL UN DOCUMENT DECRIVANT LE BLOCAGE DES PAQUETS EN FONCTION DE LEUR TAILLE ?

Vous trouverez une démonstration de blocage du trafic ICMP Nachi à l'adresse :

http://www.cisco.com/warp/public/707/cisco-sn-20030820-nachi.shtml

59. CE VER ATTAQUE-T-IL UNIQUEMENT LE PROTOCOLE ICMP ?

Le ver attaque le protocole DCOM via les ports ICMP, TCP 135, 4444 et UDP 69. Pour en savoir plus, visitez :

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801aedd6.shtml

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

60. EXISTE-T-IL UNE VERSION DE CISCO SECURITY AGENT/HIDS POUR UNIX ?

Cisco Security Agent est pris en charge sur Solaris 2.8.

61. OÙ TROUVER DES INFORMATIONS SUR LES NUMEROS DE PORT ET LEUR ACTION ?

Vous pouvez commencer avec le registre, sur le site Web d'IANA :

http://www.iana.org/assignments/port-numbers

62. JE RELEVE DE NOMBREUX BALAYAGES D'ADRESSES DANS LES JOURNAUX DE MON PARE-FEU. CETTE AUGMENTATION EST-ELLE LIEE AU VER BLASTER ?

Vous avez probablement affaire au ver Nachi. Consultez le document :

http://www.cisco.com/warp/public/707/cisco-sn-20030820-nachi.shtml

63. QUELLE METHODE PRECONISE CISCO POUR IDENTIFIER ET SURVEILLER PASSIVEMENT L'ACTIVITE DE BLASTER AU TRAVERS D'UN ROUTEUR CISCO ?

Consultez l'exemple de Cisco NetFlow dans l'avis de sécurité Cisco concernant le ver Blaster :

http://www.cisco.com/warp/public/707/cisco-sn-20030814-Blaster.shtml

64. A L'AIDE DE L'APPLICATION DE SURVEILLANCE CISCO NETFLOW, J'AI PU IDENTIFIER DES MACHINES INFECTEES AUX NOMBREUX PETITS FLUX DE TRAFIC EMIS PAR LES HOTES INFECTES. CE PROFIL DE TRAFIC EST-IL CARACTERISTIQUE DES VERS ET DES VIRUS ?

Oui. Dans la plupart des cas, Cisco NetFlow signale ce type d'activité. Consultez le document Arbor Networks Peakflow X :

http://www.arbor.net

65. POUVONS-NOUS BLOQUER DES PAQUETS SUR LES PORTS D'ACCES DE NIVEAU 2 DE COMMUTATEURS CISCO CATALYST 4000 ET 5500 EXECUTANT CISCO CATALYST OS ? ILS SONT EQUIPES DU MODULE SUPERVISOR ENGINE 2 MAIS L'ADRESSE IP D'ADMINISTRATION SE TROUVE SUR UN AUTRE VLAN, A L'INSTAR DES CLIENTS.

Il est possible d'appliquer des ACL de VLAN sur les périphériques Cisco Catalyst OS. Pour en savoir plus, visitez le site :

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a008016113d.html

66. UN ENVOI MASSIF DE DONNEES AU ROUTEUR NOUS A CAUSE DES PROBLEMES. MALGRE LA PRESENCE D'ACL, L'UC A ETE SURCHARGEE. COMMENT LIMITER LE TRAFIC QUI TRAVERSE LE ROUTEUR ?

La fonction de limitation de débit et NBAR permettent de filtrer le trafic avant qu'il atteigne les ACL. Pour en savoir plus, visitez :

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801aedd6.shtml

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

67. LA TECHNOLOGIE DE TUNNELING VPN PEUT-ELLE CONTOURNER UN PARE-FEU MATERIEL, PERMETTANT A UN ORDINATEUR PROTEGE CONTRE LES ATTAQUES PROVENANT D'INTERNET D'ETRE INFECTE PAR UNE MACHINE INTERNE AU TRAVERS DU TUNNEL ?

Oui, Cisco Security Agent travaille avec le client Cisco VPN au travers de la fonction AYT (Are You There). Vous pouvez configurer le VPN pour ne pas activer le tunnel si Cisco Security Agent n'est pas installé sur le système distant. Cisco Security Agent protège le système distant.

68. POUVONS-NOUS ELABORER NOS PROPRES SIGNATURES ? COMMENT COMMENCER ?

Vous pouvez créer des signatures personnalisées. Elles peuvent jouer un rôle important dans vos outils de « mitigation » des attaques de ver. Pour en savoir plus sur les signatures personnalisées, consultez le site de Cisco IDS.

69. LE FILTRAGE D'ISMP OU DU PORT 135 A L'AIDE D'UNE LISTE D'ACCES (AUCUNE LISTE D'ACCES N'EST UTILISEE ACTUELLEMENT) SUR LES ROUTEURS PRINCIPAUX RISQUE-T-IL D'ACCROÎTRE SENSIBLEMENT LES TEMPS DE LATENCE ?

Non. Les ACL IP et les ACL étendues offrent une commutation rapide.

70. EN THEORIE, UN ROUTEUR PEUT-IL ANALYSER UN TRAFIC CRYPTE S'IL DISPOSE D'UN EXEMPLAIRE DE LA CLE PRIVEE ?

En théorie, un routeur IPSec (IP Security) pourrait mettre fin à une connexion aux deux extrémités et lancer une attaque de type « man in the middle ». Toutefois ce schéma ne peut pas être mis en pratique pour plusieurs raisons. L'une des recommandations est d'inspecter le trafic après décryptage. Par exemple, pour inspecter le trafic SSL (Secure Sockets Layer), vous pouvez l'arrêter au niveau d'un module SSL sur une plate-forme Cisco Catalyst 6500, puis utiliser le module IDSM-2 (IDS Services Module) pour inspecter le trafic décrypté avant de le transmettre au serveur Web.

71. LE BLOCAGE DES PORTS 133, 135, ETC. A-T-IL UN IMPACT SUR WINDOWS ACTIVE DIRECTORY ?

Oui. Il est essentiel de filtrer ces ports uniquement lorsque l'activité normale ne prévoit pas de les utiliser. Pour limiter la propagation de ces vers alors que ces ports sont nécessairement ouverts, d'autres technologies, par exemple des dispositifs antivirus et HIPS doivent être mises en œuvre.

72. EST-IL POSSIBLE DE LIMITER L'ACTION DE CISCO SECURITY AGENT A L'ATTRIBUTION, VIA DHCP, D'ADRESSES IP A DES POSTES DE TRAVAIL EXECUTANT CSA ?

Cisco Security Agent fonctionne parfaitement dans un environnement DHCP. Toutefois, les serveurs DHCP ne bénéficient pas actuellement d'une fonction AYT, contrairement au client Cisco VPN.

73. POUVEZ-VOUS ETRE INFECTE PAR LES SERVICES GNUTELLA ? COMMENT BLOQUER CES APPLICATIONS CLIENT ?

Cisco IDS peut prendre des mesures pour arrêter ces types de trafic. Pour cela, vous devez disposer de Cisco IDS 4.1 et de la mise à jour Signature Update 49.

74. QU'EST-CE QUI DISTINGUE LA FONCTION CISCO NETFLOW SUR LA CARTE MSFC (MULTILAYER SWITCH FEATURE CARD) DE CISCO CATALYST 6509 DE CELLE DU MODULE DE SUPERVISION, NOMMEE MLS PLUTOT QUE NETFLOW ? TOUTES DEUX FOURNISSENT LES MEMES INFORMATIONS, MAIS MLS SEMBLE PLUS PERFORMANTE.

La commande « ship cache flow » et/ou l'exportation de données NetFlow à partir de la carte MSFC sur Cisco Catalyst 6500 en mode hybride (il semble que ce soit le mode d'exploitation utilisé dans la question) révèle uniquement les flux commutés par logiciel. La mise en cache MLS équivaut à la fonction de mise en cache NetFlow d'autres plates-formes. Les commandes « sh mls » et/ou l'exportation de données NetFlow à partir de la carte PFC (Policy feature card) montrent tous les flux, y compris les flux matériels.

75. BLASTER PEUT-IL SE TRANSMETTRE PAR UNE CONNEXION DE VPN ?

Oui. Assurez-vous que le point d'extrémité est protégé avant de l'autoriser à utiliser le VPN.

76. QUELLE EST L'EFFICACITE D'UN ROUTAGE IP X.X.X.X NUL AU NIVEAU DU PORT LOCAL POUR ARRETER LES ANALYSES DE PAQUETS SORTANTS ET LES TRANSFERTS UNICAST REVERSE PATH FORWARDING EN VUE D'EMPECHER L'ACCES D'ADRESSES SOURCE IMITEES DEPUIS LE MEME EMPLACEMENT ?

Les techniques de routage nul, URPF (en mode strict ou « loose » et en fonction de la situation), des ACL et des ACL virtuelles bloquent efficacement le trafic indésirable. Comme d'ordinaire, ces techniques et fonctionnalités doivent être adaptées à la situation : contactez le centre d'assistance technique Cisco ou l'équipe chargée de votre compte pour obtenir des conseils spécifiques.

77. QU'EST-CE QUI DIFFERENCIE LE FONCTIONNEMENT D'UN VER DE CELUI D'UN VIRUS ? LEQUEL EST LE PLUS DANGEREUX ?

Un virus est une partie de code rattachée à un document ou un programme, qui s'exécute à l'ouverture du document ou du programme. Un ver est généralement un programme autonome capable d'infecter d'autres systèmes spontanément, puis de se copier pour étendre la contamination. A l'instar de son homologue biologique, le virus nécessite des « vecteurs » pour se transmettre d'un système à l'autre. La gravité des dommages dépend des actions perpétrées. Certains virus sont programmés pour effacer le disque dur une fois activé. En général, les vers n'infligent pas de dégâts trop importants sur les systèmes car ils ont besoin d'une plate-forme pour se propager vers d'autres systèmes. Toutefois, dans le cas de SQL Slammer, le taux d'infection du ver est tellement élevé qu'il provoque une congestion de la liaison.

78. AVEC NBAR, QUEL EST LE POINT DE SURCHARGE DU SYSTEME ?

Tous les paquets traversent l'UC pour être inspectés par NBAR. L'impact sur les performances dépend du nombre de modules PDLM (packet description language module) chargés et du nombre de types de trafic différents examinés.

79. CISCO SECURITY AGENT EST-IL LA SOLUTION HIDS ACHETEE PAR CISCO A OKENA ?

Oui, il comporte quelques améliorations et intégrations de produit.

80. QUELLE EST LA REFERENCE PRODUIT/MODULE DU MODULE IDS DE LA GAMME CISCO CATALYST 6500 ?

La référence du module IDS de Cisco Catalyst 6500 est : WS-SVC-IDS2-BUN-K9.

81. ENVISAGEZ-VOUS DE PRENDRE EN CHARGE LES PROGLEMES DE SECURITE DES DISPOSITIFS CISCO (CISCO CALL MANAGER, ACCESS CONTROL SERVER, CWLSE) PAR UNE « METHODE CISCO DISTANTE » DE DIAGNOSTIC ET DE RESOLUTION ?

Cisco Security Agent est en cours de validation sur la plupart des dispositifs Cisco tels que Cisco Call Manager ou Cisco Unity™.

82. COMMENT CONFIGURER CISCO IDS SUR UN PARE-FEU CISCO PIX ? LE SITE CISCO.COM CONTIENT-IL DES « MEILLEURES PRATIQUES » SUR CE THEME ?

Visitez le site :

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/63syslog/index.htm

83. CISCO IDS PEUT-IL CONFIGURER AUTOMATIQUEMENT LE PARE-FEU CISCO PIX 515 POUR BLOQUER ET DESACTIVER UNE CONNEXION SUSPECTE ?

Oui. La sonde de Cisco IDS peut être configuré (à partir de signatures) pour ordonner au pare-feu Cisco PIX 515 de bloquer et de désactiver des connexions suspectes.

84. CERTAINS VERS PEUVENT-ILS OBLIGER VOTRE ORDINATEUR A SE CONNECTER SPONTANEMENT ET VOUS EMPECHER DE TELECHARGER DES MISES A JOUR D'ANTIVIRUS ?

Ils peuvent tout à fait obliger l'ordinateur à se connecter spontanément au réseau pour infecter d'autres machines. Jusqu'à présent, cela n'a jamais empêché le téléchargement de signatures de virus, mais une variante pourrait avoir cet effet. Si vous pensez être victime de ce problème, supprimez le fichier nsblast.exe ainsi que toute référence à msblast dans votre registre.

85. CISCO ENVISAGE-T-IL D'ETENDRE NBAR A D'AUTRES PLATES-FORMES QUE CELLES DE LA GAMME CISCO 7200 ?

NBAR est disponible sur plusieurs plates-formes Cisco et notamment avec les gammes 3600, 3700, 7200 et 7500.

86. NOUS UTILISONS DES LISTES D'ACCES POUR AUTORISER ET REFUSER L'ACCES A INTERNET PAR ADRESSES IP EXPLICITES. EST-CE LA MEILLEURE METHODE DE PROTECTION ? NOUS UTILISONS UN PARE-FEU CISCO 505E.

Pas exactement. Blaster utilise des adresses imitées, aussi vérifiez que vous filtrez toutes les adresses sortantes qui ne font pas partie de votre sous-réseau. De plus, empêchez le trafic des ports 135, 4444 et UDP 69 de traverser votre pare-feu. Pour en savoir plus, visitez les sites :

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801aedd6.shtml

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml

87. COMMENT DIFFERENCIER LES PAQUETS SYN D'UNE ATTAQUE DOS DISTRIBUEE DES PAQUETS SYN VALIDES EMIS PAR DES NAVIGATEURS ET D'AUTRES APPLICATIONS TCP ?

L'association de Cisco IDS et de Cisco NetFlow avec un système de détection des anomalies tel que les produits Peakflow d'Arbor Networks permet de détecter de nombreux trafics DOS et notamment les flux SYN.

http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html

http://www.cisco.com/en/US/tech/tk648/tk362/tk812/tech_protocol_home.html

http://www.arbornetworks.com

88. CISCO PRECONISE-T-IL DE PLACER DES ACL COMMUNES SUR TOUS LES ROUTEURS PAR MESURE PREVENTIVE POUR LES OPERATIONS QUOTIDIENNES ?

http://www.oreilly.com/catalog/hardcisco/index.html

89. OÙ SE RENSEIGNER POUR SAVOIR QUELS SERVICES DE POSTE DE TRAVAIL, OU DE SERVEUR RISQUENT D'ETRE PERTURBES PAR LE FILTRAGE DE PORTS TCP ET UDP SPECIFIQUES PAR LISTE D'ACCES ?

http://www.iana.org/assignments/port-numbers

90. AVEC UN PARE-FEU CISCO PIX 525, EST-IL NECESSAIRE DE BLOQUER LE PROTOCOLE ICMP SUR LES INTERFACES INTERNE ET EXTERNE ?

Vous devez filtrer tous les protocoles non indispensables aux applications de l'entreprise.

91. COMMENT CONTROLER LE TRAFIC QUI PENETRE SUR UN SEGMENT DE LAN (FILTRAGE), Y COMPRIS LE TRAFIC UDP, TOUT EN ASSURANT LA REDONDANCE DE CE SEGMENT ?

Vous devez installer un routeur entre les VLAN. Appliquez ensuite des filtres de port sur ce routeur.

92. EXISTE-T-IL UNE MISE A JOUR DE SECURITE OU UN SYSTEME D'ACTUALISATION DES CORRECTIFS AUQUEL JE PUISSE M'ABONNER POUR ETRE INFORME DES MENACES CONCERNANT LES ROUTEURS ET LES COMMUTATEURS CISCO ?

http://www.cisco.com/go/psirt

93. EST-IL POSSIBLE D'APPLIQUER DES LISTES D'ACCES SUR PLUS DE 300 ROUTEURS SANS VISITER CHACUN INDIVIDUELLEMENT ?

Oui. Vous pouvez utiliser Cisco ACL Manager ou Cisco VMS.

94. POUR LES FOURNISSEURS D'ACCES, LE BLOCAGE DE PORTS EST DIFFICILE. COMMENT GERENT-ILS CE TYPE D'ATTAQUE ?

Les techniques de « blackholing » ou de routage nul, y compris le « blackholing » uRPF déclenché par BGP (Border Gateway Protocol) (qui s'appuie sur une adresse source) peuvent être adaptées aux vastes réseaux des ISP. L'ouvrage « Cisco ISP Essentials » de Barry Greene et Philip Smith constitue une ressource de choix sur le sujet. Pour en savoir plus, visitez le site :

http://www.ispbook.com

95. EST-IL POSSIBLE D'IDENTIFIER DES VERS A PARTIR DE LEUR CONFIGURATION BINAIRE ?

Oui. Chaque ver exploite une vulnérabilité spécifique d'un système. Si vous recherchez les configurations binaires de cette attaque dans vos signatures IDS, vous pourrez identifier le ver et générer une alarme sur votre console de surveillance.

96. SI VOUS AJOUTEZ UN VLAN A VOTRE RESEAU, LE VER NE RISQUE-T-IL PAS DE SE REPANDRE SUR L'ENSEMBLE DU RESEAU APRES AVOIR ATTEINT LE ROUTEUR ?

Non. Le ver passera d'un VLAN à l'autre, considérant chacun comme un réseau distinct (comme prévu). La fonction de génération d'adresses IP du ver tente de générer des adresses IP aléatoires en vue de maximiser le taux d'infection. Toutefois, dans le cas de Blaster, la génération de nombres aléatoires n'est pas optimale et crée une adresse entièrement aléatoire dans 60 % des cas seulement. Le reste du temps (40 % des cas), Blaster génère une adresse IP de type A.B.C.0, où A et B correspondent aux deux premiers octets de l'adresse IP du système infecté. C est tiré du troisième octet dans 60 % des cas seulement. Le reste du temps, le ver vérifie si C est supérieur à 20 et, le cas échéant, soustrait à C une valeur aléatoire inférieure à 20. Une fois les trois premiers octets de l'adresse IP sélectionnés, le ver génère le dernier octet séquentiellement par incréments de 1, jusqu'à 254.

97. MON PARE-FEU, CONFIGURE PAR DEFAUT POUR REFUSER LES CONNEXIONS ENTRANTES AU NIVEAU DES PORTS 135 ET 139, A BLOQUE LE VER BLASTER. DES ACL ETENDUES SUR NOTRE ROUTEUR, A LA SORTIE DU PARE-FEU CISCO PIX, DECHARGERAIENT-ELLES EFFICACEMENT LE PARE-FEU ?

Oui.

98. SELON LE CENTRE D'ASSISTANCE TECHNIQUE (TAC) CISCO, QUEL EST LE POIDS DE L'AJOUT D'ACL AUX PORTS D'UN ROUTEUR SUR LES PERFORMANCES DE L'UC ?

Les listes d'accès et les listes d'accès étendues offrent une commutation rapide, notamment dans le cas du logiciel Cisco IOS 11.2. L'augmentation de l'utilisation de l'UC est donc inférieure à 5 %.

99. J'AI RELEVE DES ANALYSES DU PORT 4444 DANS LES TRACES DE RENIFLAGE. PRES DE LA MOITIE DES ADRESSES SOURCE N'ETAIENT PAS VALIDES. CE VER IMITE-T-IL L'ADRESSE DE LA SOURCE ? CELA INDIQUE-T-IL QUE LES SOURCES ANALYSEES ETAIENT INFECTEES ?

Le ver choisit une adresse entièrement aléatoire dans 40 % des cas. Le reste du temps (60 % des cas), Blaster génère une adresse IP présente dans le bloc réseau du système qu'il infecte. Les analyses du port 4444/TCP peuvent révéler que le ver recherche un autre hôte à infecter (Blaster recherche un système cible mais vérifie auparavant si le système choisi a déjà été infecté). Ces analyses peuvent être le fait d'une variante de Blaster recherchant des hôtes infectés ou de tiers qui recherchent les hôtes contaminés par Blaster puisque ce ver laisse ouvert le port 4444/TCP. Ces analyses peuvent révéler des recherches d'hôtes infectés et des tentatives d'accéder à ces hôtes à partir de ce port.

100. NOTRE RESEAU EST ENVAHI DE PAQUETS ICMP. NOUS AVONS REFUSE L'ACCES DE CES PAQUETS. EN RECHERCHANT LEUR PROVENANCE, NOUS AVONS DECOUVERT QUE L'ADRESSE SOURCE DE CES PAQUETS ETAIT IMITEE. QUE DEVONS-NOUS FAIRE ?

En général, il n'y a pas grand-chose à faire avec les paquets imités. Tout d'abord, assurez-vous que vous avez placé les ACL « anti-spoofing » appropriées ou l'outil de vérification de chemin inverse à l'extérieur de vos routeurs et pare-feu. Ensuite, nous conseillons de limiter le débit des messages ICMP sur les routeurs et d'inciter votre fournisseur d'accès à en faire autant afin d'éviter que le trafic ICMP n'engorge vos liaisons extérieures.

POUR NOUS FAIRE PART DE VOS QUESTIONS, SUGGESTIONS ET AUTRES INFORMATIONS RELATIVES AUX SOLUTIONS, PRODUITS ET TECHNOLOGIES DE RESEAU, VISITEZ LE FORUM CISCO POUR PROFESSIONNELS DES RESEAUX A L'ADRESSE : WWW.CISCO.COM/GO/NETPRO.