كيفية حماية شبكتك من فيروس NIMDA

المحتويات

المقدمة

يوضح هذا المستند طرق تقليل تأثير دودة NIMDA على شبكتك إلى الحد الأدنى. يتناول هذا المستند موضوعين:

- الشبكة مصابة، ما الذي يمكن فعله؟ كيف يمكن تقليل الضرر والسقوط؟
- لم تصب الشبكة بعد بالعدوى، أو أنها مصابة جزئيا فقط. فماذا يمكن فعله لتقليص انتشار هذه الدودة؟

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

معلومات أساسية

للحصول على معلومات أساسية حول دودة NIMDA، يرجى الرجوع إلى الروابط التالية:

- http://www.cert.org/body/advisories/CA200126_FA200126.html
- http://vil.nai.com/vil/content/v_99209.htm
- http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html

الأنظمة الأساسية المدعومة

يتطلب حل التعرف على التطبيق المستند إلى الشبكة (NBAR) الموضح في هذا المستند ميزة التميز المستندة إلى الفئة داخل برنامج Cisco IOS®. وعلى وجه الخصوص، تستخدم القدرة على المطابقة على أي جزء من عنوان URL HTTP ميزة تصنيف المنفذ الفرعي HTTP داخل NBAR. يتم أدناه تلخيص الأنظمة الأساسية المدعومة والحد الأدنى من متطلبات برنامج Cisco IOS:

النظام الأساسي	الحد الأدنى لإصدار برنامج Cisco IOS Software
7200	T(5)12,1
7100	T(5)12,1
3660	T(5)12,1
3640	T(5)12,1
3620	T(5)12,1
2600	T(5)12,1
1700	T(5)12,2

ملاحظة: يلزمك تمكين إعادة التوجيه السريع من Cisco (CEF) لاستخدام التعرف على التطبيق المستند إلى الشبكة (NBAR).

يتم دعم NBAR أيضا على بعض الأنظمة الأساسية لبرنامج Cisco IOS التي تبدأ بالإصدار 12.1E. يمكنك الاطلاع على "البروتوكولات المدعومة" في وثائق التعرف على التطبيق المستندة إلى الشبكة.

تتوفر أيضا العلامات المستندة إلى الفئة وشريط الشبكة الموزع (NBAR) على الأنظمة الأساسية التالية:

النظام الأساسي	الحد الأدنى لإصدار برنامج Cisco IOS Software
7500	E(6)12,1
FlexWAN	E(6)12,1

إن ينشر أنت NBAR، كنت على علم من cisco بق CSCdv06207 id (يسجل زبون فقط). قد يكون الحل البديل الموصوف في CSCdv06207 ضروريا إذا واجهت هذا العيب.

يتم دعم حل قائمة التحكم في الوصول (ACL) في جميع الإصدارات الحالية من برنامج Cisco IOS.

بالنسبة للحلول التي تحتاج فيها إلى إستخدام واجهة سطر أوامر جودة الخدمة (QoS) القابلة لإضافة وحدات أخرى (مثل حركة مرور ARP التي تحد من المعدل أو تنفيذ تحديد المعدل باستخدام واضع السياسات بدلا من CAR)، فأنت بحاجة إلى واجهة سطر أوامر جودة الخدمة القابلة لإضافة وحدات أخرى والتي تتوفر في إصدارات برنامج Cisco IOS 12.0XE و 12.1E و 12.1T وجميع الإصدارات من 12.2.

لاستخدام معدل الوصول الملتزم به (CAR)، يلزمك برنامج Cisco IOS الإصدار 11.1CC وجميع الإصدارات من 12.0

والبرامج الأحدث.

كيفية التقليل من الضرر والحد من التداعيات

يوضح هذا القسم موجهات العدوى التي يمكن أن تنشر فيروس نيمدا، ويقدم نصائح للحد من انتشار الفيروس:

- يمكن أن تنتشر الدودة عبر مرفقات البريد الإلكتروني لنوع صوت MIME/x-wav.**نصائح:**قم بإضافة قواعد على خادم بروتوكول نقل البريد البسيط (SMTP) لحظر أي بريد إلكتروني يحتوي على هذه المرفقات:readme.exeAdmin.dll
- يمكن أن تنتشر الدودة عند إستعراض خادم ويب مصاب مع تمكين تنفيذ JavaScript واستخدام إصدار من Internet Explorer (IE) معرض للمستكشفات التي تمت مناقشتها في MS01-020 (على سبيل المثال، IE 5.0 أو IE 5.01 بدون SP2).**نصائح:**أستخدم Netscape كمتصفح لك، أو قم بتعطيل JavaScript على IE، أو احصل على IE مرقع إلى SP II.أستخدم التعرف على التطبيق المستند إلى شبكة (NBAR) من Cisco لتصفية ملفات readme.eml من أن يتم تنزيلها. هنا مثال أن يشكل NBAR:

```
Router(config)#class-map match-any http-hacks
"*Router(config-cmap)#match protocol http url "*readme.eml
```

بمجرد مطابقة حركة المرور، يمكنك إختيار تجاهل حركة مرور البيانات أو توجيهها المستند إلى السياسة لمراقبة الأجهزة المضيفة المصابة. وتوجد أمثلة على التنفيذ الكامل في إستخدام قوائم التحكم في الوصول والتعرف على التطبيقات المستندة إلى الشبكة لحظر دودة "الرمز الأحمر".

- يمكن أن تنتشر الدودة من آلة إلى أخرى في شكل هجمات ال IIS (فهي تحاول في المقام الأول إستغلال نقاط الضعف الناجمة عن تأثيرات الشفرة الحمراء II، لكنها أيضا نقاط الضعف التي طورتها سابقا MS00-078).**نصائح:**أستخدم مخططات الشفرة الحمراء الموصوفة في:التعامل مع مشكلة عدم انتظام الخادم وارتفاع إستخدام وحدة المعالجة المركزية (CPU) الناتج عن الدودة "الحمراء المشفرة"إستخدام قوائم التحكم في الوصول والتطبيق المستندة إلى الشبكة لحظر الدودة "Code Red"

```
Router(config)#class-map match-any http-hacks
"*Router(config-cmap)#match protocol http url "*.ida
"*Router(config-cmap)#match protocol http url "*cmd.exe
"*Router(config-cmap)#match protocol http url "*root.exe
"*Router(config-cmap)#match protocol http url "*readme.eml
```

بمجرد مطابقة حركة المرور، يمكنك إختيار تجاهل حركة مرور البيانات أو توجيهها المستند إلى السياسة لمراقبة الأجهزة المضيفة المصابة. وتوجد أمثلة على التنفيذ الكامل في إستخدام قوائم التحكم في الوصول والتعرف على التطبيقات المستندة إلى الشبكة لحظر دودة "الرمز الأحمر".حزم مزامنة/بدء بروتوكول (SYN TCP) حسب المعدل. وهذا لا يحمي المضيف، ولكنه يسمح بتشغيل شبكتك بطريقة مخفضة مع الحفاظ على إستمرار العمل. من خلال syn المقيدة للمعدل، تقوم بالتخلص من الحزم التي تتجاوز معدل معين، وبالتالي ستتحقق بعض إتصالات TCP، ولكن ليس كلها. للحصول على أمثلة التكوين، ارجع إلى قسم "تحديد المعدل لحزم نظام TCP" في إستخدام السيارة أثناء هجمات رفض الخدمة (DoS).ضع في الاعتبار حركة مرور بروتوكول تحليل العنوان (ARP) المقيدة للمعدل إذا كان مقدار مسوحات ARP يتسبب في حدوث مشاكل في الشبكة. لتحديد معدل حركة مرور ARP، قم بتكوين ما يلي:

```
class-map match-any arp
  match protocol arp
                    !
                    !
policy-map ratelimitarp
                 class arp
police 8000 1500 1500 conform-action transmit exceed-action drop violate-action drop
```

بعد ذلك، يلزم تطبيق هذا النهج على واجهة LAN ذات الصلة كسياسة إخراج. قم بتعديل الأشكال حسب ما يناسب عدد ARPs في الثانية التي تريد السماح بها على الشبكة.

- يمكن أن تنتشر الدودة عن طريق إبراز إما .eml أو .nws في Explorer مع تمكين Active Desktop (W2K/ME/W98 بشكل افتراضي). وهذا يتسبب في قيام THUMBVW.DLL بتنفيذ الملف ومحاولة تنزيل

README.EML المشار إليه فيه (وفقا لإصدار IE وإعدادات المنطقة الخاصة بك).**تلميح:** كما هو موصى به أعلاه، أستخدم NBAR لتصفية README.eml من التنزيل.

- يمكن أن تنتشر الدودة عبر محركات الأقراص المعينة. من المحتمل أن يقوم أي جهاز مصاب بتخطيط محركات أقراص الشبكة بتعريض كافة الملفات الموجودة على محرك الأقراص المخطط والدلائل الفرعية الخاصة به للعدو**نصائح:**قم بحظر بروتوكول نقل الملفات المبسط (TFTP) (المنفذ 69) حتى لا تتمكن الأجهزة المصابة من إستخدام بروتوكول TFTP لنقل الملفات إلى الأجهزة المضيفة غير المصابة. تأكد من أن وصول TFTP للموجهات ما يزال متوفرا (حيث قد تحتاج إلى المسار لترقية الرمز). إذا كان الموجه يشغل برنامج Cisco IOS الإصدار 12.0 أو إصدار أحدث، فسيكون لديك دائما خيار إستخدام بروتوكول نقل الملفات (FTP) لنقل الصور إلى الموجهات التي تشغل برنامج Cisco IOS Software.حظر NetBIOS. يجب ألا يترك NetBIOS شبكة محلية (LAN). يجب على موفري الخدمة تصفية NetBIOS عن طريق حظر المنافذ 137 و 138 و 139 و 445.
- وتستخدم الدودة محرك SMTP الخاص بها لإرسال رسائل البريد الإلكتروني لإصابة أنظمة أخرى بالعدوى.**تلميح:** حظر المنفذ 25 (SMTP) على الأجزاء الداخلية من شبكتك. لا يحتاج المستخدمون الذين يستردون بريدهم الإلكتروني باستخدام بروتوكول مكتب البريد 3 (POP) (المنفذ 110) أو بروتوكول الوصول إلى بريد الإنترنت (IMAP) (المنفذ 143) إلى الوصول إلى المنفذ 25. السماح فقط للمنفذ 25 بأن يكون مفتوحا ليواجه خادم SMTP للشبكة. قد لا يكون هذا ملائما للمستخدمين الذين يستخدمون Eudora و Netscape و Outlook Express من بين آخرين، حيث إن لديهم محرك SMTP خاص بهم وسيقومون بإنشاء إتصالات خارجية باستخدام المنفذ 25. وقد يلزم تطبيق بعض التحقيقات على الاستخدامات المحتملة للخوادم الوكيلة أو آلية أخرى.
- تنظيف خوادم التطبيقات/CallManager من Cisco**تلميح:** يتعين على المستخدمين الذين لديهم خوادم تطبيق "إدارة المكالمات" و"إدارة المكالمات" في شبكاتهم القيام بما يلي لإيقاف انتشار الفيروس. يجب عدم الاستعراض للوصول إلى الجهاز المصاب من "إدارة الاتصالات" ويجب أيضا عدم مشاركة أي محركات أقراص على خادم "إدارة الاتصالات". اتبع التعليمات الواردة في تنظيف فيروس NIMDA من خوادم تطبيقات Cisco CallManager 3.x و CallManager لتنظيف فيروس NIMDA.
- قم بتصفية فيروس نيمدا على ال CSS 11000**تلميح:** يجب على المستخدمين الذين لديهم CSS 11000 اتباع التعليمات الواردة في تصفية فيروس NIMDA على CSS 11000 لتنظيف فيروس NIMDA.
- إستجابة نظام اكتشاف الاقتحام الآمن (CS IDS) من Cisco لفيروس NIMDA**تلميح:** تحتوي معرفات CS على مكونين مختلفين متاحين. الأولى هي المعرفات المستندة إلى المضيف (HIDS) التي تحتوي على مستشعر المضيف والمعرفات المستندة إلى الشبكة (NDS) التي تحتوي على مستشعر الشبكة، والتي يستجيب كل منها بطريقة مختلفة إلى فيروس NIMDA. للحصول على شرح أكثر تفصيلا ومسلك العمل الموصى به، ارجع إلى كيفية إستجابة معرفات Cisco الآمنة للفيروس NIMDA.

معلومات ذات صلة

- إستخدام قوائم التحكم في الوصول والتطبيق المستندة إلى الشبكة لحظر الدودة "Code Red"
- التعامل مع مشكلة عدم انتظام الخادم وارتفاع إستخدام وحدة المعالجة المركزية (CPU) الناتج عن الدودة "الحمراء المشفرة"
- إستخدام السيارة أثناء هجمات رفض الخدمة
- إشعارات وتوجيهات أمان Cisco
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).