الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ توجيهية
للتأمين ضد هجمات حجب الخدمة الموزعة

عـــام

إخلاء المسؤولية / الحقوق القانونية

قامت الوكالة الوطنية للأمن السيبراني (NCSA) بإعداد ووضع هذا المنشور, بعنوان " مبادئ توجيهية للتأمين ضد هجمات حجب الخدمة الموزعة- الإصدار 2.0 - لمساعدة المؤسسات على فهم هجمات حجب الخدمة الموزعة والتخفيف من حدتها.

وتكون الوكالة مسؤولة عن مراجعة هذه الوثيقة والمحافظة عليها.

وعلى الوكالة الإقرار بصفتها مصدر ومالك, بغض النظر عن طريقة نسخ أي نسخة سواء أكانت كلية أو جزئية من هذه الوثيقة؛ بما يخص "مبادئ توجيهية للتأمين ضد هجمات حجب الخدمة الموزعة".

وفي حالة طلب أي نسخ بخصوص هذه الوثيقة بقصد التسويق التجاري, يلزم الحصول على إذن كتابي من الوكالة الوطنية للأمن السيبراني. ولها الأحقية في تقييم مدى فعالية وإمكانية تطبيق جميع النسخ المطورة فيما يخص الأغراض التجارية.

ولا يجوز تفسير الإذن الصادر عن الوكالة الوطنية للأمن السيبراني على أنه تأييد للنسخ المطورة ولا يجوز للمطور بأي حال من الأحوال الإعلان عن ذلك أو إساءة تفسيره بأي شكل من أشكال في وسائل الإعلام أو المناقشات الشخصية / الاجتماعية..

مراقبة الوثائق

تفاصيل الوثيقة	
رقم هوية الوثيقة	IAG-NGE-DDOS
الإصدار	إصدار 2.0
التصنيف والنوع	عام
الخلاصة	تم إعداد هذه الوثيقة كدليل لمساعدة المؤسسات على فهم وتخفيف تهديد هجمات "حجب الخدمة الموزعة."

المراجعة / الموافقة

الاسم	القسم / المهمة	تمت المراجعة / الموافقة	الإصدار	التاريخ
دانة العبد الله	شؤون الحوكمة والضمان السيبرانى الوطني		2.0	

سجل النسخ المنقحة

الإصدار	المؤلف:	وصف المراجعة	التاريخ
1.0	شؤون الحوكمة والضمان السيبرانى الوطني	منشور	مارس 2018
2.0	شؤون الحوكمة والضمان السيبرانى الوطني	منشور	يناير 2023
2.0	شؤون الحوكمة والضمان السيبرانى الوطني	منشور + تعديلات تصحيحية طفيفة	ديسمبر 2023

التفويض القانوني

يحدد القرار الأميري رقم (1) لسنة 2021 فيما يخص إنشاء الوكالة الوطنية للأمن السيبراني، صلاحياتها. وتتمتع الوكالة الوطنية للأمن السيبراني بسلطة الإشراف على أمن البنية التحتية الوطنية الحيوية وتنظيمها وحمايتها من خلال اقتراح وإصدار السياسات والمعايير وضمان الامتثال.

وقد تم إعداد هذه الوثيقة مع الأخذ في الاعتبار بالقوانين المعمول بها في دولة قطر. وفي حالة نشوء تعارض بين هذه الوثيقة (أحكام أو بنود محددة) وقوانين دولة قطر، تسود قوانين دولة قطر. وبذلك، يعتبر أي مصطلح من هذا القبيل (أحكام أو بنود محددة) محذوفًا من هذه الوثيقة، دون المساس بالأحكام المتبقية من هذه الوثيقة. ويلزم في هذه الحالة إجراء تعديلات لضمان الامتثال للقوانين السارية ذات الصلة بدولة قطر.

جدول المحتويات

1 المقدمة

1.1 السياق

تواجه أنظمة المعلومات اليوم مخاطر غير مسبوقة من مجموعة من الجهات الفاعلة في التهديد. وتشمل هذه المخاطر عدم توافر المعلومات. ويتم التعرض لهذا الخطر من خلال عدة هجمات مثل هجمات التهديد المستمر المتقدم التي تمحو أنظمة التخزين، وهجمات حجب الشبكة وحجب الخدمة الموزعة، والهجمات المادية على أنظمة المعلومات ومرافق المعالجة الخاصة بها، وما إلى غير ذلك.

وتعتبر هجمات حجب الخدمة الموزعة (DDoS) واحدة من أكبر المخاوف بالنسبة لشبكات المؤسسات المتاحة في الوقت الحاضر. وفي حين أنه لا يوجد حل وسط لأنظمة المعلومات نفسها، فإن الهجمات تجعل النظام غير قابل للوصول لمستخدميه الشرعيين من خلال هجوم الفيضان الإلكتروني.

وتتزايد هجمات حجب الخدمة الموزعة من حيث الكم والتعقيد والخداع.

2 الغرض والنطاق والاستخدام

2.1 الغرض

تهدف هذه الوثيقة إلى مساعدة المؤسسات في دولة قطر على فهم هجمات حجب الخدمة الموزعة واستراتيجياتها وتقنياتها للتخفيف منها.

2.2 النطاق

جميع مؤسسات البنية التحتية الحرجة بدولة قطر.

2.3 الاستخدام

ستساعد الإرشادات الواردة في هذه الوثيقة المؤسسات على تأمين البنية التحتية العامة ضد هجمات حجب الخدمة الموزعة. وتوفر الوثيقة فهمًا لأنواع مختلفة من هذه الهجمات كما تعرض طرقًا معالجتها.

3 التعريفات الرئيسية

المؤسسات/المؤسسة	مؤسسات البنية التحتية الحرجة بدولة قطر.

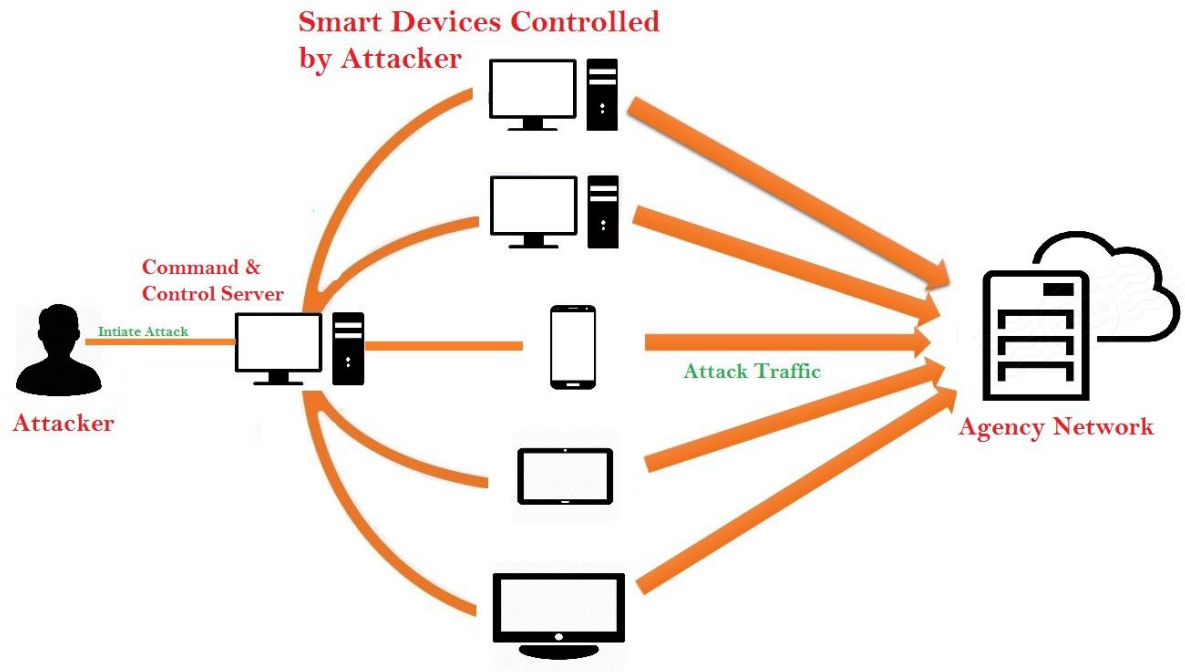
4 الإرشادات

4.1 ما هو هجوم حجب الخدمة الموزعة؟

هجوم حجب الخدمة (DoS) هو أي هجوم يمنع مستخدمًا شرعيًا من الوصول إلى مورد الشبكة. ويستخدم هجوم حجب الخدمة الموزعة موارد الشبكة المتعددة كمصدر لمسار الهجوم المحدد. ويكمن الغرض الأساسي من استخدام الموارد المتعددة في كونه وسيلة لتضخيم وتعزيز قدرات مهاجم واحد، بالإضافة إلى أنه يساعد في إخفاء هوية المهاجم وتعقيد جهود التخفيف.

ويوجد هناك أنواع مختلفة من هجمات حجب الخدمة الموزعة. وتعتبر الهجمات الكمية أكثر أنواع هجمات حجب الخدمة الموزعة شيوعًا. وتستخدم هذه الهجمات أنظمة مصابة متعددة - والتي غالبًا ما تكون جزءًا من شبكة البوت نت- لتعطيل طبقات الشبكة بكمية كبيرة من حركة المرور التي تعيق مرور الحركة المشروعة مما يتسبب في عدم توفر أنظمة فترة الهجوم. وقد توصل الهجوم غير الكمي إلى العديد من التقنيات مثل هجمات البروتوكول وهجمات التطبيقات من خلال جعل الهدف يمكن الوصول إليه من خلال الكشف عن نقاط الضعف في البروتوكولات. حيث تعمل هجمات التطبيقات على معرفة نقاط الضعف وعيوب منطق تسلسل الأعمال. ويعد الهجوم الانعكاسي هجوم مختلط يستخدم فيه المهاجم عناوين IP للمصدر مزورة بالاقتران مع قابلية بروتوكول محددة لتضخيم وتوجيه هجوم حجب الخدمة الموزعة.

وفي معظم الحالات، يستخدم المهاجم موارد الكمبيوتر المخترقة دون علم المالك. وضمن النطاق الأكبر لأمن المعلومات، تندرج هجمات حجب الخدمة الموزعة ضمن عمود "التوافر" في ثالوث أمن المعلومات السرية والسلامة والتوافر.



الشكل أ: رسم توضيحي لحجب الخدمة الموزعة

4.2 أنواع هجمات حجب الخدمة الموزعة

4.2.1 الهجمات الكمية

الهجمات الكمية (النطاق الترددي) هي أكثر هجمات حجب الخدمة الموزعة شيوعًا، ويُقصد بهجوم حجب الخدمة الموزعة الكمي أي هجوم يحاول التغلب على الهدف من خلال تشبع سعة الشبكة المتاحة. وتكون هجمات حجب الخدمة الموزعة الكمية ممكنة بسبب سعة الشبكة الصغيرة نسبيًا للهدف مقارنة بالسعة الإجمالية لجميع الأجهزة المتصلة بالإنترنت. وفي الوقت الحاضر خاصةً مع ظهور إنترنت الأشياء (IoT)، هناك مئات الملايين من الأجهزة التي يمكن للمهاجمين استخدامها لإرسال حركة مرور زائفة إلى الهدف، ومن الأمثلة على ذلك هجوم داين في 21 أكتوبر 2016 حيث استخدم المهاجمون الآلاف من كاميرات المراقبة CCTVs المتصلة بالإنترنت لشن هجوم على شركة داين مما تسبب في تعطيل الخدمات المهمة التي أثرت على الشركات الكبرى مثل آمازون وسبوتيفاي واتش بي أو.

4.2.2 هجمات البروتوكول

هجمات البروتوكول هي مجموعة متنوعة من الهجمات المختلفة التي تهدف إلى إحداث اضطراب في البيئة من خلال استغلال ضعف أو عدم كفاءة معين في البروتوكول. وتستغل العديد من هذه الهجمات نقاط الضعف في بروتوكولات الطبقة الثالثة والرابعة مثل بروتوكول التحكم بالنقل وبروتوكولات الإنترنت وبروتوكول حزم بيانات المستخدم. وتستنفد هجمات البروتوكول كل قدرة المعالجة للهدف المهاجم أو الموارد المهمة الوسيطة مثل جدار الحماية الذي يتسبب في تعطيل الخدمة.

4.2.3 هجمات التطبيقات

تعتبر الهجمات على مستوى التطبيق أو الطبقة 7 في نموذج الربط البيني للأنظمة المفتوحة هي مجموعة متنوعة من الهجمات التي تهدف إلى إحداث اضطراب في بيئة ما من خلال استغلال نقاط ضعف أو عدم كفاءة معينة في أحد التطبيقات. ويعتبر الفارق الرئيسي بين مستوى التطبيق والهجمات الأخرى، أن تكون حركة المرور "في البروتوكول"، مما يعني أن حركة المرور مشروعة من منظور البروتوكول. ومن خلال كونها "في البروتوكول"، غالبًا ما يكون من الصعب تمييز الهجمات عن حركة المرور المشروعة؛ حيث تنشئ هجمات التطبيقات اتصالًا بالهدف ثم تستنفد موارد الخادم من خلال احتكار العمليات والمعاملات.

4.2.4 هجمات حجب الخدمة الموزعة ذو النطاق الترددي المنخفض

هجوم صعب للغاية ويصعب اكتشافه إذ أنه هجوم يرسل فيه المهاجم حركة مرور ضارة بمعدل إرسال أقل لتضليل تقنيات اكتشاف هجمات حجب الخدمة الموزعة التقليدية الخارجة عن المألوف. وغالبًا ما تهدف هذه الهجمات إلى ترك الاتصالات مفتوحة على الهدف من خلال إنشاء عدد منخفض نسبيًا من الاتصالات على مدار فترة وترك هذه الجلسات مفتوحة لأطول فترة ممكنة. وتتضمن الطرق الشائعة إرسال طلبات بروتوكول نقل النص الفائق الآمن (http) الجزئية، مثل برنامج Slowloris و Slowpost (أداة حجب الخدمة الموزعة تكمل عملية تأكيد الاتصال) وإرسال حزم بيانات صغيرة أو البقاء متصلا من أجل منع الجلسة من الانتقال إلى مهلة الخمول. وغالبًا ما تتداخل نواقل الهجوم هذه مع الهجمات الكمية عالية السرعة وتتحرك تحت الرادار مما يجعل من الصعب جدًا منعها بل وأيضًا الكشف عنها.

4.3 فهم المخاطر:

ليست كل الشركات والمؤسسات الحكومية هدفًا مشتركًا وليس لديها ملف خطورة عالية يستدعي تعرضها للهجوم. وتحتاج معظم المؤسسات إلى فهم ملفها التعريفي ضمن سيناريو الهجوم. ويكون المؤسسات المالية والمنظمات المشاركة في الفعاليات الكبيرة (مثل كأس العالم والانتخابات) وقلة أخرى، مخاطر أعلى بكثير من الشركات / المؤسسات الأخرى غير المذكورة أعلاه. وتحتاج المؤسسة إلى تقييم ملفها الشخصي الحالي، والمعلومات المسجلة حول هجمات العامين الماضيين لتحديد مستوى الخطر. وعلاوة على ما سبق، فهناك أيضًا معايير أخرى تحتاج إلى تقييم. وعلى المؤسسة أن تسال نفسها ما هي الأنظمة التي تعتبر مهمة؟ وما هو نظام الذي يمكنه الصمود في وجه هجوم حجب الخدمة الموزعة دون تعطيل أي خدمة مهمة؟ وبناء على هذه الإجابات سوف تساعدها في تحديد مستوى حماية هجوم حجب الخدمة الموزعة (الاستثمار) الذي سيكون ضروريًا للحفاظ على التوافر.

4.3.1 احتمالية التعرض للهجوم:

يعتمد تصنيف المخاطر هذا بشكل أساسي على حجم وصناعة المؤسسة، والمعلومات المسجلة (ما إذا كانت قد تعرضت المؤسسة للهجوم في السنوات القليلة الماضية؟) وكيف يمكن أن ترتبط بدوافع المهاجم؟ وبالنسبة لهذه المهمة، يرجى الاطلاع على إطار عمل إدارة مخاطر أمن المعلومات (ISRMF).

4.3.2 من الذي يمكنه مهاجمة المؤسسة الخاصة بك؟

يمكن أن تكون الجهات الفاعلة في تهديد هجوم حجب الخدمة الموزعة إما داخلية أو خارجية. ويشمل وكلاء التهديد الداخلي موظفًا / موظفين داخليين، ومتعاقدين، وما إلى غير ذلك. ويشمل وكلاء التهديد الخارجي المتسللين، ومجرمي الإنترنت، والجهات الفاعلة التي ترعاها الدولة.

ويساعد تحديد الجهات الفاعلة في التهديد المؤسسات على فهم قدرات المهاجم وتعقيد الهجوم، كما أنه عامل قوي في اتخاذ قرار بشأن استراتيجيات التخفيف الخاصة بالمؤسسة.

4.3.3 دوافع المهاجم:

يمكن أن تختلف دوافع المهاجم فقد يكون هذا الهجوم للحصول على مكاسب مالية، أو ثأر شخصي، أو تقدير الذات، أو الانتماءات السياسية أو الدينية، أو النشاط أو أي سبب آخر مختلف.

4.3.4 تحديد مجالات المخاطر:

لكي تحدد المؤسسة مجالات الخطر، ينبغي عليها:

1. فهم مخاطر الصناعة الشاملة
2. تحديد أنظمة الأعمال المهمة
3. تكلفة وقت التوقف

وعلى الجانب الفني، تحتاج المؤسسات إلى:

1. التحقق من قدرة معدات الشبكة
2. تحديد جميع الخدمات المتاحة للجمهور
3. إنشاء قائمة بمناطق المحتويات الديناميكية

4.3.5 لماذا تعتبر هجمات حجب الخدمة الموزعة فعالة جدًا؟

ساعدت عدة عوامل في استخدام هجمات حجب الخدمة الموزعة على نطاق واسع، وتأتي سهولة استخدامها على رأس القائمة حيث لا يحتاج المهاجم إلى دراسة البنية التحتية المستهدفة أو النظام الأساسي لتنفيذ هجوم حجب الخدمة الموزعة، ومع ذلك يمكن أن تكون هذه الهجمات معقدة في بعض الأحيان، خاصة باستخدام انترنت الأشياء وشبكات توزيع المحتوى.

وهناك عوامل مهمة أخرى تتمثل في صعوبة تشخيص هجمات حجب الخدمة الموزعة، حيث تتطلب الحد الأدنى من موارد المهاجم والمصادر المخادعة حيث يمكن أن يكون عنوان بروتوكول الإنترنت لمصدر الهجوم مزيفًا وعادة ما يكون مزيفًا.

4.3.6 تأثير هجمات حجب الخدمة الموزعة:

بناءً على أنواع هجمات حجب الخدمة الموزعة، يمكن أن يكون التأثير واحدًا أو أكثر مما يلي:

تشبع الرابط: عندما يتم إرسال المزيد من حركة المرور إلى رابط ما أكثر مما يمكن نقله، يتم إسقاط حركة المرور الزائدة بواسطة جهاز الشبكة المصدر. وينتج عن هذا فقدان كبير في الحزمة، مما يتسبب إما في تدهور الأداء أو انقطاع الشبكة بالكامل.

زيادة الحمل على أجهزة الشبكة: يتسبب في استخدام موارد أعلى من المعتاد على أجهزة الشبكة مثل أجهزة التوجيه والمحولات وجدران الحماية. وقد يتم إعادة تشغيل الأجهزة أو تعليقها أو تدهور أدائها.

زيادة استخدام الذاكرة على أجهزة الشبكة: قد تؤدي هجمات حجب الخدمة الموزعة إلى استنفاد الذاكرة على الأجهزة التي تتعقب حالة اتصال الشبكة مثل جدران الحماية أو نظام منع الاختراق/ نظام كشف الاختراق أو موازنات التحميل.

زيادة استخدام الموارد على خوادم التطبيقات: ستؤدي هجمات حجب الخدمة الموزعة الخاصة بالتطبيقات إلى زيادة مفاجئة في استخدام وحدة المعالجة المركزية أو الذاكرة.

زيادة استخدام الموارد في أنظمة قواعد البيانات: يمكن أن تتسبب هجمات حجب الخدمة الموزعة للتطبيقات في زيادة استخدام الموارد على أنظمة دعم التطبيقات مثل خادم قاعدة البيانات.

الوصول إلى الحدود العشوائية: قد يتسبب هجوم حجب الخدمة الموزعة في الوصول إلى الحد الأقصى لمكدس الشبكة "إذا تم تحديده" مما يؤدي إلى رفض الاتصالات المشروعة الأخرى.

زيادة تكاليف الشبكة: يمكن أن يؤدي هجوم حجب الخدمة الموزعة إلى زيادة تكاليف تقنية المعلومات عن طريق زيادة استخدام الرابط بشكل مصطنع.

إخفاء نواقل الهجوم الأخرى: ينتج عن هجوم حجب الخدمة الموزعة الكثير من حركة المرور التي قد تجعل من الصعب اكتشاف المزيد من الهجمات الدقيقة التي قد تحدث في وقت واحد.

وبغض النظر عن التأثير الفني على الجهاز كما هو مذكور أعلاه، فإنه يؤدي دائمًا إلى فقدان الخدمة أو عدم توفرها، مما قد يكون له تأثير مالي أو متعلق بالسمعة أو قانوني.

4.4 كيفية التخفيف من هجمات حجب الخدمة الموزعة

4.4.1 الضوابط العامة - الاستعداد

1. التصميم:
   - حماية الخدمات الهامة مثل خوادم نظام اسم النطاق والخدمات الهامة الأخرى مثل البريد الإلكتروني والويب وما إلى غير ذلك.
   - استخدام نطاقات IP مختلفة لخدمات متنوعة بناءً على الأهمية.
   - اعتبار تقنيات تخفيف هجمات حجب الخدمة الموزعة المناسبة مثل "التنقيح" عند تصميم شبكتك.
   - التأكد من أن لديك تخطيط استمرارية العمل واتخاذ الإجراءات الملائمة لاستعادة القدرة على العمل بعد الكوارث، راجع 4-9 إدارة استمرارية العمل في معيار تأمين المعلومات الوطنية. ويلزم على الوكالات إنشاء دليل للتعامل مع أزمة هجمات حجب الخدمة الموزعة، والذي يتضمن خطة الاتصال، واستراتيجية الاستجابة للحوادث.
2. الوثيقة:
   - توثيق تفاصيل البنية التحتية لتكنولوجيا المعلومات الخاصة بك، ويلزم أن يتضمن ذلك تعيينات عنوان IP، ومخططات هيكل الشبكة، وإعدادات التوجيه، وتكوينات أجهزة الشبكة والأمان، والأجهزة، وتفاصيل البرامج وما إلى غير ذلك. راجع معيار تأمين المعلومات الوطنية، الوثائق 4-12 والقسم 5-2 أمان الشبكة.
   - إنشاء قائمة بيضاء لعناوين IP (الداخلية والخارجية) والبروتوكولات التي يجب السماح بها دائمًا وأولوياتها.
3. الخبرات الفنية:
   - تقوية البنية الأساسية (الشبكة. الأنظمة الأساسية، التطبيقات، البرامج مفتوحة المصدر) التي يمكن أن تتأثر بهجوم حجب الخدمة الموزعة.
   - استخدام الحد من معدل عنوان المصدر.
   - استخدم تحدي HTTP / HTTPS جافا سكريبت للتعرف على العملاء الشرعيين المستندة إلى المتصفح.
   - الالتزام بأفضل الممارسات أثناء تكوين إعدادات مدة بقاء (TTL) نظام اسم النطاق. ويمكن أن تسهل القيم المنخفضة إعادة توجيه قواعد البيانات إذا تم مهاجمة عناوين IP الأصلية. إذ إن قيمة 600 هي قيمة جيدة لمدة البقاء.
4. المراقبة:
   - وضع أساس لأداء البنية التحتية الخاصة بك حتى يمكن التعرف على الحالات غير الطبيعية بسرعة.
   - استخدم عمليات الكشف الخارجة عن المألوف لمراقبة مقاييس الأداء واكتشاف ما إذا كان يوجد هجمات حجب الخدمة الموزعة قيد التقدم.
5. جهة الاتصال في حالات الطوارئ:
   - إنشاء قائمة جهات اتصال للوصول إلى الموظفين (الفرق الداخلية ومُوزّدي الدعم) أثناء وقوع حادث بما في ذلك هجمات حجب الخدمة الموزعة. راجع إلى 4-8 إدارة الحوادث في معيار تأمين المعلومات الوطنية
   - إنشاء اتصال مع الوكالة الوطنية للأمن السيبراني ووكالات تطبيق القانون ومزود خدمة الإنترنت الخاص بك

6. تقييم عروض الجهات الخارجية:
   - الاهتمام بنشر الاستجابة للطوارئ على مدار الساعة طوال أيام الأسبوع باستخدام تقنية خدمة مكافحة هجمات حجب الخدمة الموزعة المتقدمة (على سبيل المثال، المقدمة من بائع خدمة مكافحة هجمات حجب الخدمة الموزعة أو مزود خدمة الإنترنت الخاص بك).
   - استخدام مجموعة من الخدمات / التقنيات (السحابة والمحلية) لسد الثغرات. ومن الأمثلة على ذلك حماية نظام اسم النطاق وجدران حماية تطبيقات الويب ومراكز الفحص والأجهزة المحلية للهجمات غير الكمية وحماية واجهة برمجة التطبيقات.
   - استخدام شبكة توزيع المحتوى (CDN)، وهي شبكة موزعة جغرافيًا من الخوادم الوكيلة ومراكز البيانات الخاصة بها. وتوفر شبكات توزيع المحتوى إمكانات هائلة للتخفيف من هجمات حجب الخدمة الموزعة.

4.4.2 عند بدء الهجوم:

4.4.2.1 تحليل الهجوم

1. تحديد تدفق الهجوم. تأكد مما إذا كنت الهدف أو ضحية جانبية أو جزء من شبكة البوت نت المخترقة.
2. قم بعمل نسخ ضرورية من ملفات السجل للخوادم والشبكات وأجهزة الأمان المتأثرة كدليل جنائي
3. حدد الخدمات المتأثرة ومصدر عناوين IP للهجوم والبروتوكولات والمنافذ المستخدمة في الهجوم.
4. تحقق مما إذا كان هناك أي تحذير أو تهديد محتمل تم إصداره قبل الهجوم.

4.4.2.2 التخفيف من حدة الهجمات

1. بناءً على المعلومات التي تم جمعها، حاول التخفيف من حدة الهجوم من خلال الإجراءات التالية:
   - حظر حركة المرور الضارة على شبكتك إما عن طريق حظر عناوين IP أو البروتوكولات أو المنافذ المحددة على أجهزة التوجيه أو جدران الحماية أو أجهزة البوابة الحدودية إن أمكن.
   - إذا كان ذلك ممكنًا، اطلب من مزود خدمة الإنترنت الخاص بك حظر حركة المرور الضارة من جهته.
   - إيقاف تشغيل أي تطبيق أو ميزة معينة لتطبيق مستهدف، إذا كان ذلك ممكنًا (طالما أنه ليس تطبيقًا تجاريًا أساسيًا).
   - إنهاء الاتصالات أو الخدمات غير المرغوب فيها على الخوادم وأجهزة التوجيه.
   - إذا كان هجوم حجب الخدمة الموزعة قد أضر بثغرة أمنية في الأنظمة (الخوادم والتطبيق والشبكة وأجهزة الأمان)، فاستخدم بدائل مثل جدران حماية التطبيقات ونظام كشف التسلل المرتكز على المضيف (HIDS) والتصحيح الظاهري للتغلب على هذه الثغرة حتى يتم معالجة النظام.
   - إذا كان ذلك ممكنًا وإذا لزم الأمر، يمكنك استدعاء تخطيط استمرارية العمل والحماية من الكوارث لتبديل عمليات تكنولوجيا المعلومات إلى مواقع بديلة
   - قم بالإبلاغ عن الحادث إلى الوكالة الوطنية للأمن السيبراني ووكالات تطبيق القانون وفقًا لما تتطلبه اللوائح والقوانين.
   - ضوابط محددة على أساس نوع الهجوم:

الهجوم الكمي:

1. حظر عناوين IP " حماية خطوط شبكة الإنترنت " من جانب مزود خدمة الإنترنت، يمكن أن يكون هذا النهج فعالاً في التخفيف من الهجمات المبسطة، ولكنه غالبًا لن يكون قادرًا على تخفيف السيناريوهات الأكثر تعقيدًا.
2. ضع في اعتبارك استخدام التوجيه الفارغ مع بروتوكول البوابة الحدودية (BGB) للمساعدة في منع الأجهزة الموجودة على الإنترنت من إرسال حركة المرور إلى عنوان IP الخاص بالوكالة.
3. استخدم حلول التحليل الذكي للمخاطر لتحديد حركة المرور التي يجب تجاهلها أو السماح بها استنادًا إلى تاريخ المصدر الخاص بحركة المرور الضارة أو المشروعة.

هجمات البروتوكول:

1. الحظر باستخدام الأجهزة المحلية. قد يوفر نظام منع الاختراق / نظام كشف الاختراق مساعدة محدودة، وقد توفر جدران حماية التطبيقات (فعلى سبيل المثال، جدران حماية بتطبيق الويب WAF) حماية أفضل ضد هذه الهجمات.
2. غالبًا ما تكون خدمة تخفيف هجمات حجب الخدمة الموزعة المخصصة، مثل تلك التي يوفرها موردو الجهات الخارجية، هي الأكثر فاعلية، مع إمكانات متقدمة خاصة بتحديد ومنع حركة مرور بروتوكول هجمات حجب الخدمة الموزعة.
3. استخدام ملفات تعريف الارتباط SYN لحماية الخادم SYN Queue من الامتلاء في ظل تدفق SYN لدى بروتوكول التحكم بالنقل (هجوم حجب الخدمة يعتمد على إساءة استخدام الطريقة القياسية التي يتم بها إنشاء اتصال الخادم بروتوكول التحكم بالنقل).

هجمات التطبيقات:

1. هي تمامًا مثل هجمات البروتوكول، فقد يكون الحظر باستخدام الأجهزة المحلية مثل نظام منع الاختراق / نظام كشف الاختراق وجدران الحماية ناجحًا نظرًا لطبيعة النطاق الترددي المنخفض لهذه الهجمات. وقد يكون النجاح محدودًا في الهجوم الأكثر تعقيدا.
2. قد توفر الحلول مثل جدران حماية تطبيقات الويب أو حلول برامج مكافحة البرامج الضارة أو حلول مكافحة إفساد نظام اسم النطاق أو الأجهزة المتخصصة حماية أفضل.
3. يمكن أيضًا اعتبار حظر التطبيقات (تعطيل الميزة مؤقتًا) في حالات معينة إذا لم يتم استخدام الخدمة التي يتم مهاجمتها أو لم يكن لها تأثير كبير على الأعمال.

4.4.3 عند توقف الهجوم:

4.4.3.1 الالتعاش من الهجوم

1. تأكد من انتهاء هجمات حجب الخدمة الموزعة وإمكانية الوصول إلى جميع الخدمات مرة أخرى.
2. تأكد من أن أداء نظامك يتماشى مع قاعدة مرجعية الأداء الخاصة بك.
3. تأكد من التراجع عن أي تدابير تخفيفية مثل حظر حركة مرور معينة أو بروتوكول أو منافذ.
4. قم بإعادة الأنظمة من موقع مواجهة الكارثة إلى الموقع الأصلي (في حال استدعاء مواجهة الكارثة/ استمرارية الأعمال).
5. مراجعة الحادث من البداية؛ تحديد الدروس المستفادة بما في ذلك ما في ذلك ما كان يمكن القيام به بشكل أفضل؟
6. ضع خطة لتنفيذ الدروس المستفادة بغية تجنب وقوع تجربة مماثلة في المستقبل.

5 الامتثال والإنفاذ

5.1 الامتثال والإنفاذ

تم نشر هذه المبادئ التوجيهية لمساعدة المؤسسات على فهم تهديد هجمات حجب الخدمة الموزعة بشكل أفضل وكيفية التخفيف منها.

هذه المبادئ التوجيهية تكمل سياسة تصنيف البيانات الوطنية ومعيار تأمين المعلومات الوطنية.

6 المرفقات

6.1 الاختصارات

APT تهديد مستمر متقدم

DDoS هجمات حجب الخدمة الموزعة

ISP مزود خدمة الإنترنت

NCSA الوكالة الوطنية للأمن السيبراني

6.2 المراجع

لا توجد مراجع

6.3 قائمة الأشكال

الشكل أ: رسم توضيحي لحجب الخدمة الموزعة

6.4 الإبلاغ عن الحوادث إلى الوكالة الوطنية للأمن السيبراني

يمكن للمؤسسات التي تواجه هجوم حجب الخدمة الموزعة إبلاغ الوكالة الوطنية للأمن السيبراني عن الحادث بإحدى الطرق التالية:

الاتصال بالخط الساخن الخاص بالوكالة الوطنية للأمن السيبراني على رقم 16555 (خدمة على مدار الساعة طوال أيام الأسبوع)

إرسال بريد الإلكتروني على البريد الالكتروني الخاص بالوكالة الوطنية للأمن السيبراني ncsoc@ncsa.gov.qa

قد تجد المؤسسات أيضًا الإرشادات التالية مفيدة في الاستعداد لمواجهة أي هجوم / حادث.

إرشادات لإدارة الحوادث - الإجراءات المطلوبة مسبقًا