دليل تخفيف آثار الحجب المنتشر للخدمة DDoS

نطاق الحجب المنتشر للخدمة DDoS: بنية نظام اسم النطاق DNS لنطاق المستوى الأعلى لرمز البلد ccTLD

ورشة عمل عمليات نطاقات المستوى الأعلى TLD-OPS

الإصدار 1.0 – 25 نيسان (أبريل) 2018

نظرة عامة على ورشة العمل

كان الهدف من ورشة العمل هو استكشاف كيفية إمكانية تعاون أعضاء عمليات نطاقات المستوى الأعلى TLD-OPS لوضع دليل تخفيف آثار الحجب المنتشر للخدمة DDoS. وكان التركيز على الحجب المنتشر للخدمة المستهدف في بنية نظام اسم النطاق الرسمي أحادي الاتجاه ومتعدد الاتجاهات، التي يتم تشغيلها من قبل نطاق المستوى الأعلى لرمز البلد ccTLD وشركائهم مزودي نظام اسم النطاق.

التحفيز

جاءت ورشة العمل استجابة لورشة عمل تخفيف آثار الحجب المنتشر للخدمة لعمليات نطاقات المستوى الأعلى التي عقدت في الاجتماع ICANN58 في كوبنهاغن في 12 آذار (مارس) 2017. ونظرا لأن هجمات الحجب المنتشر للخدمة قد يكون لها تأثير شديد على الهدف (والضرر الثانوي المحتمل للآخرين)، فإن اللجنة الدائمة لعمليات نطاقات المستوى الأعلى تعتقد أنه من المهم استنفار التجربة الجماعية لمجتمع عمليات نطاقات المستوى الأعلى لوضع وتوثيق إطار عمل لإعداد أفضل نطاقات مستوى أعلى لرمز البلد استجابة لهجمات الحجب المنتشر للخدمة.

وسهلت ورشة العمل هذا الحوار من خلال تبادل الخبرات والمناقشات وتوليد الأفكار.

ورشة العمل # 2 لتخفيف آثار الحجب المنتشر للخدمة DDoS لعمليات نطاقات المستوى الأعلى – ICANN61 TLD-OPS، 29-10-2017، ملاحظات عامة

عقدت ورشة العمل لمجموعة أصغر مكونة من: 22 شخصا. وقد سمح هذا بحركة نشاط وتعاون جيدين. اجتمعنا أمام مخطط واحد، مررنا على نتائج ورشة العمل السابقة، ووسعنا كل موضوع للتركيز على العناصر التي ستكون جزءا من الدليل، لكل مرحلة من مراحل دورة الحياة. والنتائج المأخوذة في المخططات مفسرة في هذه الوثيقة.

دورات الحياة لتخفيف آثار الحجب المنتشر للخدمة DDoS "الفعال" هي:

- التحديد
- الحماية
- الاكتشاف
- الاستجابة
- التعافي

لا يقتصر نطاق هذه الوثيقة على وضع إطار أمني معقد لتخفيف آثار، بل الهدف هو تسليط الضوء على المكونات المهمة في كل دورة حياة ليكون نطاق المستوى الأعلى لرمز البلد فعالا في تخفيف آثار هجوم الحجب المنتشر للخدمة (إذا نفذت ومتى تم تنفيذها).

وقد ذكر في ورشة العمل أنه من الأفضل دائما تنفيذ أفضل الممارسات مثل عمليات خدمات تقنية المعلومات (مكتبة البنية التحتية للمعلوماتية ITIL) وإدارة أمن المعلومات (الأمن السيبراني).

التحديد:

هدف التحديد هو توثيق وفهم البنية التحتية لنظام اسم النطاق لنطاق المستوى الأعلى لرمز البلد قبل حدوث الهجوم -- لمعرفة من يجب الاتصال به، من يجب الاعتماد عليه، من الذي يجب أن يخطر (ومسار التصعيد لحل المشكلة). وتأكد من وجود علاقة قوية مع مزودي خدمات الإنترنت، البائعين، الحكومة، الصحافة، المشتركين ومستخدمي الإنترنت لنطاق المستوى الأعلى لرمز البلد الخاص بك. وهذا هو العمل الذي يجب القيام به على أساس مستمر قبل وقوع هجوم.

جهات الاتصال	
فريق إدارة نطاق المستوى الأعلى لرمز البلد **ccTLD** الخاص بك	اللقب، الاسم، رقم الهاتف، رقم هاتف المنزل، البريد الإلكتروني المنزلي (رئيس مجلس الإدارة)
رقم طوارئ **IANA**	306-6308 (310) 1+ (يجب تحديثه)
موردون متعددو الاتجاهات	البريد الإلكتروني وأرقام الهواتف للسيطرة النوعية على أداء المنظمة / شبكة المراكز، أرقام الاتصال
منبع مزود خدمة الإنترنت للعبور	البريد الإلكتروني وأرقام الهواتف للسيطرة النوعية على أداء المنظمة / شبكة المراكز، أرقام الاتصال
مزود خدمة الإنترنت داخل الدولة	البريد الإلكتروني وأرقام الهواتف للسيطرة النوعية على أداء المنظمة / شبكة المراكز
فريق الاستجابة لحالات طوارئ الحاسب الآلي **CERT**	البريد الإلكتروني وأرقام الهواتف للسيطرة النوعية على أداء المنظمة / شبكة المراكز اسم جهة الاتصال، رقم الهاتف، البريد الإلكتروني
مشغلو المحللات الرئيسية (المتكرر)	عناوين بروتوكول الإنترنت IP المشغل، البريد الإلكتروني، أرقام الهواتف
قائمة جهات اتصال عمليات نطاقات المستوى الأعلى **TLD-OPS**	الوصول إلى قائمة جهات اتصال TLD-OPS
الصحافة	اسم جهة الاتصال، رقم الهاتف، البريد الإلكتروني
الجهة الرقابية	اسم جهة الاتصال، رقم الهاتف، البريد الإلكتروني
موردو البرمجيات	اسم جهة الاتصال، رقم الهاتف، البريد الإلكتروني
استشاري الطب الشرعي	اسم جهة الاتصال، رقم الهاتف، البريد الإلكتروني
المشتركون	طريقة للوصول إلى المشتركين بفعالية
جهات الاتصال الأخرى ذات الصلة	

التوثيق بوضوح للبنية التحتية لنظام اسم النطاق لنطاق المستوى الأعلى لرمز البلد:

من المهم للغاية التوثيق بوضوح للبنية التحتية لنظام اسم النطاق لنطاق المستوى الأعلى لرمز البلد ccTLD DNS، أي خوادم الأسماء التي لديك قيد العمل، موقعها الفعلي، اتصالات الشبكة، مزودي العبور، اتصالات نقطة تبادل شبكات الإنترنت IXP، مزودين متعددي الاتجاهات، قدرة كل عبور ورابط IXP.

هذا هو الأصل الذي تحتاج إلى حمايته.

خادم أسماء ccTLD، عناوين IPv4 وIPv6.

- Example…
- ;; AUTHORITY SECTION:

- .dk. 172800 IN NS a.nic.dk
- .dk. 172800 IN NS b.nic.dk
- …
- ;; ADDITIONAL SECTION:
- a.nic.dk. 172800 IN A 212.88.78.122
- b.nic.dk. 172800 IN A 193.163.102.222
- b.nic.dk. 172800 IN AAAA 2a01:630:0:80::53
- …

دقة طوبولوجيا نظام اسم النطاق والشبكة والخادم:

توثيق بنية الشبكة والخادم والبرنامج الخاص بالبنية التحتية لنظام اسم النطاق لنطاق المستوى الأعلى لرمز البلد وتحديث هذا على أساس منتظم.

<أدخل مخططات الشبكة هنا>

- تقديم روابط لمخططات الشبكة والطوبولوجيا

عناوين بروتوكول الإنترنت IP الرئيسة المخفية

النسخة الرئيسة المخفية	
عنوان بروتوكول الإنترنت **IP**	تفاصيل قائمة الوصول (في حال كنت بحاجة إلى إضافة مزود جديد)
كيفية الإضافة	خطوات سريعة لإضافة خوادم أسماء جديدة …

البنية التحتية للدخول للامتدادات الأمنية لنظام اسم النطاق DNSSEC

إضافة تفاصيل بنية DNSSEC التحتية وتخزين / حماية مفتاحها هنا.

خوادم أسماء متكررة مهمة باستخدام ccTLD (على سبيل المثال قد يكون خوادم أسماء متكررة لمزود خدمة الإنترنت كبير داخل بلدك لخدمة مجموعة كبيرة من السكان)

المتكرر	
اسم مزود خدمة الإنترنت	عناوين بروتوكول الإنترنت IP
كيفية الإدراج في القائمة البيضاء	خطوات سريعة لإدراج الخوادم المتكررة في القائمة البيضاء؟

الحفاظ على معلوماتك محدثة:

الوصول إلى المعلومات الهامة	
كلمة مرور آمنة	الموقع (لتسجيل الدخول في أجهزة التوجيه والخوادم)
جرد المعدات	الموقع (ما هو عنوان IP، الاسم)
خطة الاتصالات	الموقع (كيف نتصل، نتواصل)
الأدوار والمسئوليات	الموقع (من يفعل ماذا ومتى)
خطط التعافي من الكوارث **DR**، استمرارية الأعمال **BCP**	الموقع

عملية إدارة المخاطر:

تحديد المخاطر والتأثير المرتبط بها واحتمالية حدوثها، ورسم خريطة لهذا على تحليل التأثير على الأعمال لخدمة (خدمات) حل ccTLD. وإنشاء عملية لمراجعة هذه الوثيقة بانتظام وتحديثها.

عملية إدارة التغيير:

من الأهمية بمكان أن تظل هذه المعلومات حديثة؛ يجب تنفيذ عمليات للحفاظ على هذه المعلومات حديثة. وبإنشاء عملية ربع سنوية لمراجعة هذه الوثيقة وتحديثها.

الحماية:

الهدف من الحماية هو وضع وتطبيق الضمانات المناسبة لضمان تسليم خدمات نظام اسم النطاق رسمية لنطاق المستوى الأعلى لرمز البلد، ولتمكين القدرة على احتواء أو الحد من تأثير هجوم الحجب المنتشر للخدمة.

وعلى وجه التحديد ضد هجمات الحجب المنتشر للخدمة، تتمثل نتيجة الحماية في وضع وتنفيذ أفضل الممارسات الأمنية مثل ضوابط الوصول، التقنيات الواقية، التنوع وهندسة نظام اسم النطاق. ويركز هذا القسم على تحديد أفضل الممارسات (العمليات) الأمنية للتقنية، الأشخاص والشركاء.

التقنية:

تنفيذ الضمانات لضمان عمليات آمنة ومستقرة.

قوائم الوصول:

- قائمة ضبط الوصول ACL عند اللزوم، تسمح فقط بحركة المرور إلى المنفذ الوجهة 53 (TCP/UDP)
- قائمة ضبط الوصول ACL لخارج إدارة النطاق

تعدد الاتجاهات:

- تنفيذ طوبولوجيا نظام اسم النطاق متعددة الاتجاهات العالمية لزيادة مرونة التسليم
- نشر عقد محلية متعددة الاتجاهات لزيادة مرونة التسليم (عقد نظام اسم النطاق بدون عبور عالمي)، ويفضل أن يكون من خلال:
  - توسيع نظام اسم النطاق متعدد الاتجاهات عالمي بعقد متعددة الاتجاهات محلية تخدم مجتمع محلل "مهم" محدد (مزود خدمة إنترنت رئيسي في البلد، الحكومة، شبكات إقليمية)
  - إضافة عقد متعددة الاتجاهات محلية في نقاط تبادل شبكات الإنترنت IXP الرئيسية

الضمانات الأخرى:

- تنوع برنامج خادم نظام اسم النطاق (Bind، NSD، Knot، إلخ ...)
- ترشيح الثقب الأسود المنطلق عن بعد (RTBH)
- أجهزة تخفيف آثار الحجب المنتشر للخدمة
- تنفيذ تقييد معدل الاستجابة RRL (ضرورة)
- حماية واجهة الإدارة (منفذ / كبل فعلي منفصل، العبور، نفق VPN، ...)
- موارد نظام كافية (من عرض السعة)
- كفاية اتصال وتنوع الشبكة في اختيار مزود الخدمة (ISP، IXP، إلخ)

الأشخاص / العملية:

تدريب فريق تقنية المعلومات

- تدريبات الوعي الأمني
- التمرين السنوي <- مشاركة نص على عمليات نطاقات المستوى الأعلى ومحاكاة هجوم الحجب المنتشر للخدمة
- تقسية التكوين العام (أفضل الممارسات، ...) واختبار PEN
- كيفية استخدام أدوات مراقبة نظام اسم النطاق الخارجية (مثل DNSMON، DNS-OARC، BGPMon أو ما شابه؟)
- عدم إحداث تغييرات يدوية، استخدام التكوين العام وإدارة عملية التغيير

العمل مع مزودي خدمات الإنترنت (مزودي العبور) مقدما

- اكتشاف كيف يمكنهم المساعدة في تخفيف آثار أحداث الحجب المنتشر للخدمة المستقبلية
- التأكد من فهمهم لأهمية نطاق المستوى الأعلى لرمز البلد ccTLD الخاص بك

الشركاء:

العمل مع الشركاء حيث يمكن أن تكون خدمات تخفيف آثار الحجب المنتشر للخدمة مفيدة:

- إضافة مزودين متعددي الاتجاهات دائمين من الخارج
- تأمين مزودين متعددي الاتجاهات من الخارج للطوارئ
- التحقق من خدمات إجلاء الحجب المنتشر للخدمة

الاكتشاف:

يتمثل الهدف من الاكتشاف في وضع وتنفيذ الأنشطة المناسبة لتحديد -- في الوقت المناسب -- حدوث هجوم الحجب المنتشر للخدمة، وتحديد نطاق واتساع هجمات الحجب المنتشر للخدمة. وكلما كانت آلية الاكتشاف أفضل، كانت أساليب التخفيف أكثر فعالية.

تتمثل نتائج الاكتشاف في عمليات مراقبة واكتشاف نظام اسم النطاق الداخلية والخارجية.

المراقبة:

المراقبة الداخلية

- مراقبة مرور SNMP (الموجه، الخوادم، الروابط)
- مرونة إخطار إنذارات العتبة (الرسائل القصيرة، البريد الإلكتروني)
- فهم العملية العادية لكل عقدة.
- أدوات تحليل نظام اسم النطاق
- التقاط PCAP (يوفر صورة كاملة عند وقوع الحادث، لكن يمكن لحجوم المرور إنشاء حجب خدمة داخلي عند حدوث هجوم الحجب المنتشر للخدمة، راجع الملاحظة الواردة أدناه)

المراقبة الخارجية

- External RIPE Atlas DNSMON (زمن استجابة استعلام نظام اسم النطاق، فقدان الاستعلام والاتجاهات)
- إحصائيات رابط مرور مزود خدمة الإنترنت (الاستخدام الفعلي للمرور الصادرة بالنسبة لعقدة نظام اسم النطاق الخاص بك)
- مراقبة ICANN SLA (واجهة برمجة التطبيقات لنظام مراقبة ICANN (MoSAPI)) (لا تزال في مرحلة التبني المبكر لنطاقات ccTLD)
- Netlabs 360 - https://ddosmon.net/

أدوات قابلة للتطوير (وظيفية في ظل وضع الحجب المنتشر للخدمة)

- PCAP، قد تتعطل بعض الأدوات تحت الحجب المنتشر للخدمة أو تؤثر سلبا على العمليات
  - الإجراء لتعطيل جمع البيانات مؤقتا في الظروف المعاكسة
  - انتقال السجل البعيد في الزمن الحقيقي للتأكد من عدم حدوث فقدان للبيانات

تحديد نوع الهجوم:

فهم الهجوم

- نوع الهجوم
- قائمة الهجمات الكلاسيكية، ملف التعريف، الأدوات وتخفيف آثارها
- المنشأ (من أين يأتي؟)
- العقد (ما المتأثر)
- ما هو التأثير الحقيقي على مستخدمي الإنترنت؟

الاستجابة:

يتمثل الهدف من الاستجابة في وضع وتنفيذ الأنشطة المناسبة لاتخاذ إجراء بشأن هجوم الحجب المنتشر للخدمة المكتشف. وتدعم وظيفة الاستجابة القدرة على تخفيف تأثير حدث الحجب المنتشر للخدمة المحتمل.

تتضمن نتيجة الاستجابة تخطيط الاستجابة، الاتصالات، التحليل والتخفيف.

خطط الاستجابة:

لا تنزعج! من المرجح أن يكتشف المجتمع حدوث الحجب المنتشر للخدمة على نطاق المستوى الأعلى لرمز البلد الخاصة بك في نفس وقت اكتشافك له، وسوف يرغب المجتمع في مساعدتك على تخفيف آثار هذا الهجوم.

- التواصل
- مواصلة التحليل
- حل المشكلة
- التركيز على جوهر المشكلة
- التوثيق {لما قمت بتغييره، والملاحظات}

خطة الاتصالات:

الاتصال هو المفتاح في تخفيف آثار الهجوم.

آليات الاتصال	
فريق الاستجابة لحالات طوارئ الحاسب الآلي **CERT** المحلي	الاتصال بـ CERT المحلي حتى إذا لم يتم تحديد الهجوم بشكل كامل
TLD-OPS	إرسال بريد إلكتروني إلى tld-ops@dns-oarc.net طلب المساعدة في تحديد هوية الهجوم أكثر
جسر التشاور	الطلب من TLD-OPS/ICANN فتح جسر التشاور للتعاون بشأن التخفيف
التوعية	الطلب / الإذن لأعضاء TLD-OPS بالوصول إلى قائمة مراسلات إلكترونية / مجموعات بديلة للمساعدة في تخفيف آثار الهجوم
الأطراف الأخرى	

التعافي:

يتمثل الهدف من التعافي في وضع وتنفيذ الأنشطة المناسبة للحفاظ على خطط المرونة واستعادة أي قدرات أو خدمات تعطلت بسبب هجوم الحجب المنتشر للخدمة. وتدعم وظيفة التعافي، التعافي في الوقت المناسب للعمليات العادية لتقليص التأثير من هجوم الحجب المنتشر للخدمة.

تتضمن نتائج التعافي تخطيط التعافي، التحسينات، الدروس المستفادة والاتصالات.

التعافي:

- الرجوع عن التدابير المؤقتة
- استعادة بنية نظام اسم النطاق التحتية إلى الحالة الأصلية
- توثيق التغييرات الدائمة
- تجميع الملاحظات

الدروس المستفادة:

- عقد اجتماع تحليل العملية بعد الإتمام مع أصحاب المصلحة (الداخليين) ذات الصلة
- الوثيقة:
  - ما الذي نجح
  - ما الذي لم ينجح
  - تحديد التحسينات

التحسينات:

- التحديد
- التقييم
- المشاركة
- تنفيذ التحسينات

الاتصالات:

- التواصل مع الشركاء، العملاء، الموظفين، المشتركين