إمكانيات اكتشاف برنامج WSA RangeWare والتحقق من تكامل AMP من Cisco

المحتويات

مسألة

وأ عرف إمكانات توقيع Cisco من (WSA) الويب الآمن جهاز كان إذا ما حول استفسار إجراء تم. تضمن هذه الأسئلة الشائعة كيفية التحضير للتحديث الخاص بـ 3X Ransomware اكتشاف. إذا كان الدمج بين الحماية المتقدمة من البرامج الضارة (AMP) وذكاء تهديد Cisco مهم التحقق من أن WSA يعمل بشكل صحيح على منصة Talos.

البيئة

- جهاز الويب الآمن (WSA) من Cisco
- التكامل المتقدم للحماية من البرامج الضارة
- تكامل معلومات تهديد Cisco Talos
- سمعة الويب وتصفية عنوان URL (WBRS)
- محركات المسح الضوئي المضادة للبرامج الضارة (Webroot و McAfee و Sophos)
- إمكانية رؤية التطبيقات والتحكم فيها (AVC)

قرار

يعتمد جهاز الويب الآمن من Cisco على توقيع واحد مخصص تمت تسميته خصيصًا لبرنامج Trix Ransomware. بدلاً من ذلك، تستخدم الحماية العالمية بنية أمان شاملة تتضمن تقنيات اكتشاف مختلفة لتحديد تهديدات البرامج الضارة المتعددة التي تستخدمها برامج Trix Ransomware، بما في ذلك الأنواع الثلاثة X من برامج الفدية.

طرق اكتشاف WSA

تستخدم منصة WSA تقنيات الكشف هذه لحماية البرامج الفدائية:

- خوارزميات مطابقة النماذج
- تحليل إستكشافي
- تقنيات محاكاة
- يتم دمج ميزة الحماية المتقدمة من البرامج الضارة (AMP) مع ميزة التعرف على تهديدات Cisco Talos
- سمعة الويب وتصفية عنوان URL (WBRS)
- محركات مسح متعددة مضادة للبرامج الضارة بما في ذلك McAfee و Webroot و Sophos
- إمكانية رؤية التطبيقات والتحكم فيها (AVC)

يتم تحديث قدرات الكشف هذه بشكل مستمر مع نشر قواعد جديدة كل بضع دقائق لضمان الحماية ضد التهديدات الناشئة.

التحقق من تكامل AMP و Talos

لتأكيد التكامل بين الحماية المتقدمة من البرامج الضارة (AMP) وذكاء تهديد Cisco Telos، يمكن للمسؤولين مراجعة هذه السجلات على WSA للتأكد من أنها تعمل بشكل صحيح:

الخطوة 1: مراجعة سجلات الوصول إلى WSA

فحص سجلات الوصول على جهاز WSA للتحقق من تطبيق أحكام AMP على الملفات التي تم تنزيلها وطلبات الويب.

الخطوة 2: فحص سجلات AMP

راجع سجلات AMP للتأكد من نتائج تحليل البرامج الضارة وبيانات إستخبارات التهديدات التي يتم معالجتها.

الخطوة 3: التحقق من نتائج WBRS

تأكد من تعبئة عالمات سمعة الويب (WBRS) ومن إرتباطها بطلبات ويب في السجالت.

إذا تم نشر أحكام AMP وعالمات WBRS وتطبيقها في السجالت، فإن ذلك يشير إلى أن دمج المعلومات الإستخباراتية AMP و Talos يعمل كما هو متوقع ويوفر قرارات قائمة على القائمة على التهديدات في الوقت الفعلي.

السبب

كان هذا طلبا للمعلومات فيما يتعلق بقدرات اكتشاف WSAs Ransomware بدلا من مشكلة فنية تتطلب أستكشاف الأخطاء وإصلاحها. لقد نشأ الإستفسار عن الحاجة إلى فهم كيفية حماية وكالة الحماية من الفيروسات المتنقلة من أنواع محددة من برامج الحماية من الفيروسات، وللتحقق من أن عمليات دمج معلومات التهديد تعمل بشكل صحيح.

المحتوى ذي الصلة

- [ميزات جهاز الويب الآمن من Cisco وفوائده](#)
- [خدمات تالوس للاستخبارات الخاصة بتهديدات Cisco](#)
- [ورقة بيانات أجهزة الويب الآمنة من Cisco](#)
- [الدعم الفني والتنزيالت من Cisco](#)

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).