معلومات لقطة Forensic لنقطة النهاية الآمنة من Cisco

المحتويات

المقدمة

يصف هذا المستند المعلومات ذات الامتيازات التي يمكن أن تجمعها لقطة Forensic من نقاط النهاية.

تمت المساهمة بواسطة بيدرو ميديانا، مهندس برامج Cisco.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدة التحكم Cisco "Secure Endpoint"
- Cisco "Orbital"

المتطلبات

- الوصول إلى "نقطة النهاية الآمنة" مع مستخدم مسؤول أو غير مسؤول
- الوصول إلى Cisco "المداري"

ملاحظة: إذا كان المستخدم الخاص بك غير مسؤول، فيجب عليك طلب تمكين ميزة "لقطات جنائية لغير المسؤولين" من خلال فريق دعم TAC.

معلومات عامة

وبمجرد طلب لقطة للطب الشرعي، سيتم تقديم المعلومات على شكل جدول، استنادا إلى المعلومات المطلوبة، يمكن للمستخدم العثور على أي معلومات مطلوبة استنادا إلى جدول الوصف هذا:

الاسم	ماذا يعني	المخاوف المتعلقة بالخصوصية
عناصر AutoExec	العناصر التي يتم تشغيلها عند بدء تشغيل الجهاز	None
مراقبة تشفير Bitlocker	حالة التشفير لكل محرك أقراص يتم تحميله	بعض الرؤية في إصدارات غير مشفرة الملفات
مراقبة جدول ذاكرة	المهام التي تم البحث عنها مؤخرا	محفوظات المستعرض الأخيرة.

التخزين المؤقت ل DNS		
يستضيف بيانات الملف	العناصر في ملف الأجهزة المضيفة	None
البرامج المثبتة على المضيف	التطبيقات المثبتة	None
منافذ الاستماع	قوائم البرامج التي تحتفت مستمعي الشبكة	None
تجزئات الوحدات النمطية المحملة	تجزئة ميق تشغيل ملفات مكتبة الارتباط الديناميكي (DLL)	None
عمليات الوحدات النمطية المحملة	اسم العمليات الجاري تشغيلهاو راسمو فرعمو العملية الخاص اهب	None
الوحدات النمطية المحملة مقابل العمليات	تعييي فرعم الوحدة النمطية نم الوحدات النمطية المحملة إلى PID نم لودج العمليات	None
جلسات تسجيل الدخول	المستخدمون الذين مت تسجيل دخولهم، امب في كلذ مدختسم النظام	None
محركات أقراص معينة	نقاط التحميل المحلية والبعيدة، عون ماظن الملفات، معلومات قسم التمهيد، معلومات التشفير.	None
إتصاالت الشبكة - العمليات	تخطيط إتصاالت الشبكة الداخلية والصادرة بمعرف شخصي محدد، وعرض رطس رماوأ ءدب التشغيل الذي أدب العملية.	التعرض المحتمل لاتصاالت الشب الخاصة بتطبيقات معينة، والتي ق تكون خاصة.
واجهات الشبكة	قائمة بجميع واجهات الشبكة المادية والافتراضية على الجهاز	None
سجل توصيفات الشبكة	قائمة الشبكات التي ماق الجهاز باالتصال اهب.	التعرض المحتمل لمعرف SSID ل WiF
إصدار ماظن التشغيل	إصدار ماظن التشغيل	None
محفوظات PowerShell	قائمة بكافة أوامر PowerShell التي متي تشغيلها على الجهاز وتخزينها على النظام.	إمكانية كشف كلمات المرور، ومفتا API السرية، والبيانات الحساسة ا التي مت ترميزها إلى جمارب نصية.
دليل الإحضار المسبق	ميزة إدارة الذاكرة - ماظن لواحيس التشغيل التحميل المسبق للجداول التي يتم تحميلها بشكل متكرر لتوفير وقت ءدب التشغيل.	التعرض لعادات المستخدم.
بيانات الملفات الأخيرة	أحدث الملفات التي مت إستخدامها / الوصول إليها	التعرف على عادات المستخدم وأسما الملفات الخاصة.
يتم تشغيل نآلا تجزئة الملف	الاسم، المسار، رطس الأوامر، PID، مالك كافة الملفات التنفيذية ديق التشغيل.	None
مراقبة تشغيل الخدمات	الاسم ونوع الخدمة و PID ونوع ءدب التشغيل لكافة الخدمات ديق التشغيل	None
المهام المجدولة	قائمة بكافة المهام التلقائية التي مت تعيينها لتشغيلها بشكل دوري على النظام	None
الموارد المشتركة	افتح وسراش في النظام	None

عناصر بدء التشغيل	العناصر التي يتم تشغيلها عند بدء تشغيل الجهاز - مختلفة عن AutoEXEC في أن هذه العناصر يتم تخزينها في مفاتيح السجل	None
مراقبة حالة شبكة النظام	إحصائيات الشبكة	None
بيانات ملف الدليل المؤقت	الملفات المؤقتة التي تم إنشاؤها بواسطة العمليات	تعرض محتمل لمحفوظات إستعراض المستخدم.
شهادات الجذر الموثوق فيها	عملية تفريغ بيانات مخزن الشهادات الجذر الموثوق بها	None
مفتاح تسجيل uBSTOR	محفوظات أجهزة USB المتصلة	كشف الأرقام التسلسلية للجهاز.
مجموعات المستخدمين	المجموعات المحلية الموجودة على الجهاز	None
مراقبة المستخدم	عرض الملفات التي تم تنفيذها مؤخرا	التعرض المحتمل للسلوك المخفي تشغيل التشفير أو أدوات المسح.
المستخدمون	المستخدمون المحليون على الجهاز	None
المستخدمون - تم تسجيل الدخول	المستخدمون المحليون الذين تم تسجيل دخولهم إلى الجهاز حاليا	None
مراقبة عوامل تصفية حدث WMI	مراقبة سجل الأحداث لعناصر محددة	None
مراقبة منتجات AV من Windows	الذي تم تثبيت برنامج مكافحة الفيروسات على النظام، إن وجد	None
مراقبة إدخالات BAM ل Windows	يقدم دليل على تنفيذ الملفات	يمكن أن تكشف السلوكيات
متغيرات بيئة Windows	إظهار معلومات المسار ومتغيرات النظام، وما إلى ذلك.	None
إصلاحات Windows السامة	قائمة بكافة برامج التصحيح المثبتة	None
بحث عن مجالات Windows NT	قائمة المجالات التي يمكن للجهاز المصادقة عليها	None
مراقبة Windows ShellBags	يوفر معلومات حول وصول المستخدم إلى المجلدات وتفضيلات عرض ذلك المجلد، إلخ.	التعرض لعادات المستخدم.
مراقبة Windows ShimCache	تعقب التوافق مع الملفات التنفيذية	تعرض سلوكيات المستخدم.
مراقبة امتدادات الكروم	قوائم امتدادات الكروم	تعرض سلوكيات المستخدم.
Windows Office MRU	تسرد أحدث الملفات المستخدمة لكل تطبيق من تطبيقات Office	كشف أسماء الملفات الحساسة، س المستخدم

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).