Cyber Kill Chain in Blue Team Perspective

نموذج ا لـCyber Kill chain من منظور الفريق الدفاعي

مقدمة:

النموذج هو مجموعة من الخطوات التي تتصل فيما بينها لتشكل سلسلة من الاحدث التي ينفذها المهاجم لاختراق النظام وكل مرحلة تحتوي على العديد من الأساليب والأدوات التي يمكن استخدامها.

أهمية النموذج:

يمثل هذا النموذج لاي باحث في مجال الامن السيبراني خطوات منظمه لكيفية حدوث الهجمة وبالأخص الفريق الدفاعي، حيث إن الباحث يستطيع من خلاله إعادة تركيب كيفية حدوث الهجمة مما يجعل الاستجابة لها أسرع وذا كفاءة عالية.

خطوات النموذج:

1- الاستطلاع والاستقصاء

في هذه المرحلة يتم جمع معلومات عن الضحية بطريقه مباشره مثل فحص منافذ الشبكة او بطريقه غير مباشره مثل برامج التواصل الاجتماعي او البحث في أي من محركات البحث

2- التسلح

في هذه المرحلة يتم انشاء البرنامج الخبيث اما ان يكون ransomware او virus او worm او أي من أنواع البرامج الخبيثة الذي يستغل ثغره معينه

3- التسليم

في هذه المرحلة يتم توصيل البرنامج الخبيث الى جهاز الضحية وهناك أكثر من طريقه منها ارسال البرنامج عن طريق بريد الكتروني احتيالي او عن طريق رابط وهمي، ويمكن دمج هذه العملية مع الهندسة الاجتماعية لتكون أكثر كفاءه

4- الاستغلال

في هذه المرحلة يتم تشغيل البرنامج الخبيث في جهاز الضحية

5- التثبيت

في هذه المرحلة يتم تثبيت الباب الخلفي وتنزيل برامج تساعد المهاجم على فحص اجهزه الشبكة او غيرها

6- الاوامر والتحكم

في هذه المرحلة يتصل المهاجم بجهاز الضحية وينشئ قناة تواصل مخفية لينفذ أوامر اضافية

7- **الاجراءات على الهدف**

في هذه المرحلة يقوم المهاجم بتنفيذ مبتغاه من عملية الاختراق وتتنوع اهداف المهاجمين بحسب الدافع، تشتمل على تسريب البيانات، تشفير الملفات، وطلب فدية.

مثال عملي:

في هذا المثال المحلل يقوم بالاستجابة الى الحوادث السيبرانية من مركز العمليات السيبرانية

والذي يستخدم برنامج splunk لجمع ومراقبة بيانات المنظمة في نظام مركزي واحد

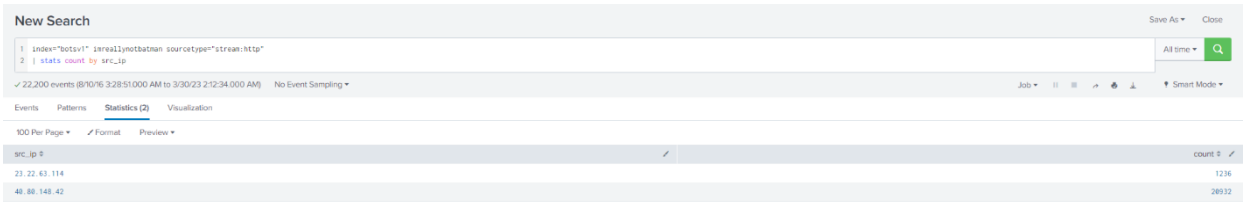
السيناريو:

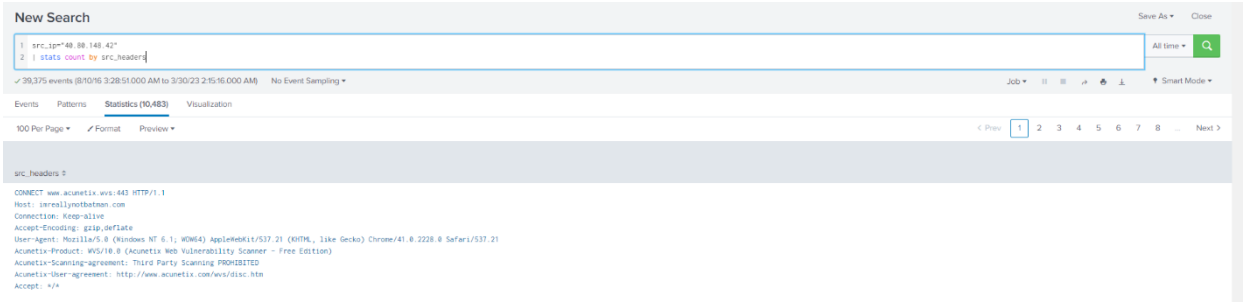
تعرض موقع Wayne Enterprises لهجمة مما تبين لاحقا ان كل من يزور الموقع يرى صفحة الويب التالية:

وهدفنا هو تحليل كيف وقع هذا الهجوم من خلال نموذج:cyber kill chain

الخطوات:

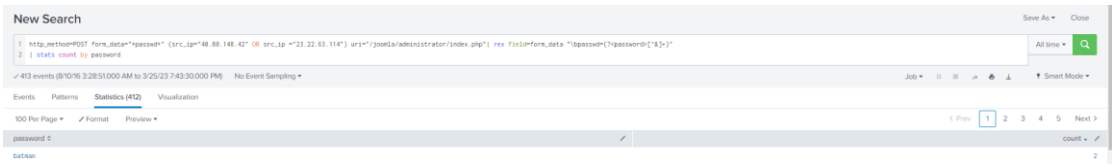
1- الاستطلاع والاستقصاء



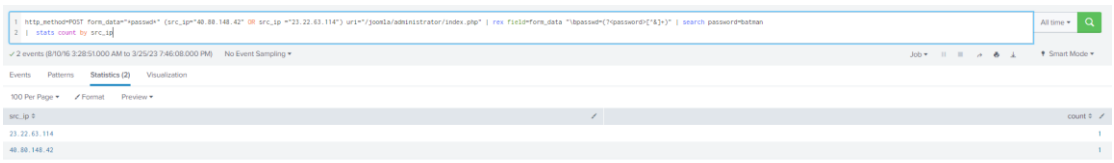


بناء على المعطيات موقع الويب تواصل مع عنوانين IP و عند البحث في العنوان صاحب اعلى عدد من البيانات نجد في متغير src_headers معلومات تشير أن الموقع يتعرض لعملية فحص ثغرات من خلال تطبيق Acunetix

ونجد ان أحد العمليات هي brute force والتي تحاول اختراق حساب مشرف الموقع والذي لديه صلاحيات عالية نجح البرنامج في إيجاد كلمة المرور الصحيحة والتي هي"batman"



والتي استعملها المهاجم فيما بعد لتسجيل الدخول من جهاز اخر

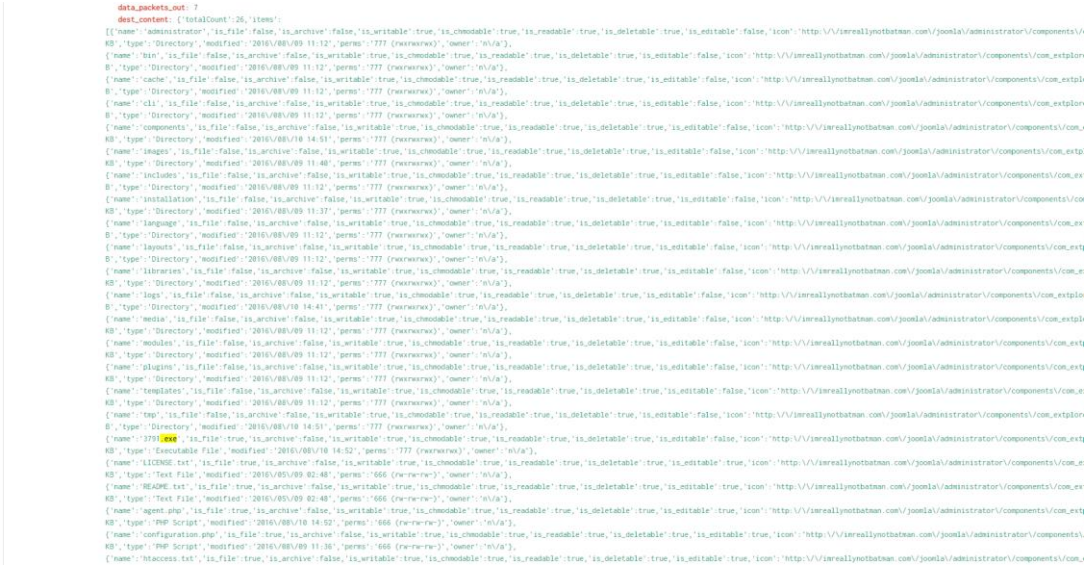


2- <u>التسلح</u>

في هذه الخطوة المهاجم انشئ الملف الخبيث والذي تم رفعه للموقع فيما بعد باسم 3791.exe

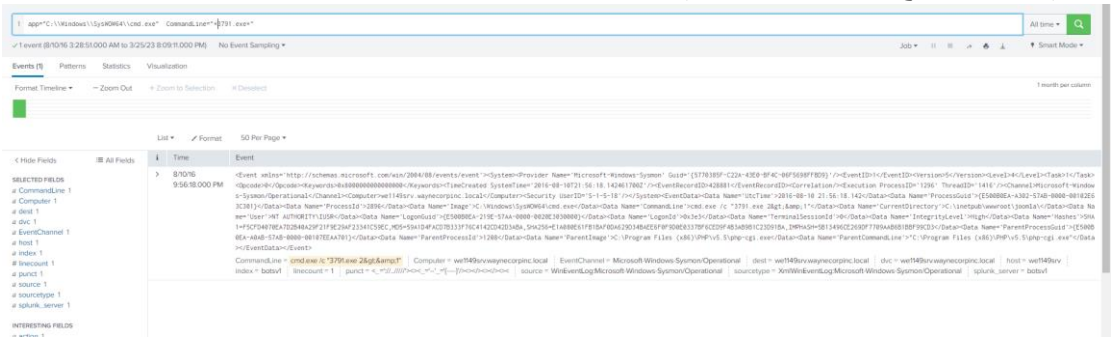
3- <u>التسليم</u>

بعدما حصل المهاجم على كلمة المرور الصحيحة تمكن من رفع الملف المذكور في الخطوة رقم اثنان الى الخادم الذي يعمل عليه الموقع



4- الاستغلال

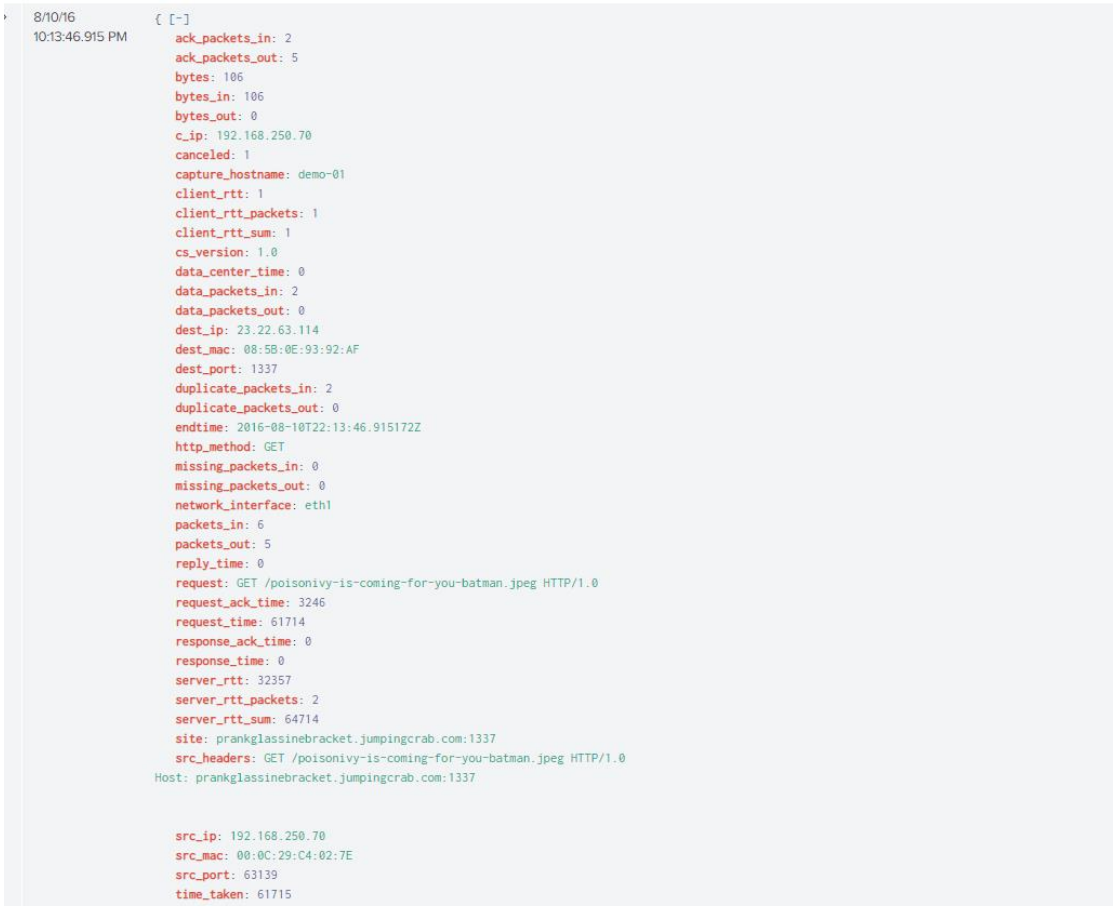
هنا تم تنفيذ البرنامج الخبيث على الخادم



5- التثبيت

في هذه المرحلة تم عمل طلب http من الخادم وهذه إشارة خطيره لان الخادم المفترض ألا ينشئ طلبات وانما يستجيب لها.

نلاحظ هنا انه طلب صوره باسم poisonivy-is-coming-for-you-batman.jpeg



6- الاوامر والتحكم

في هذا المثال لم يقم المهاجم بعمل أي اتصال ب جهاز الضحية

7- الاجراءات على الهدف

في هذه المرحلة نفذ المهاجم مبتغاه من الهجمة وهو تغير محتوى صفحة الويب وأبدلها بالصورة المرفقة في وصف السيناريو

المصادر:

https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/
https://cyberdefenders.org/blueteam-ctf-challenges/15#nav-overview