

Detect C2 binary

بسم الله الرحمن الرحيم اليوم ان شاء الله سيكون شرح عن احد طرق كشف اي ريفيرس شيل مالوير على جهازك

Sharingan_Endpoint

قاعد اشتغل حاليا على اداة اسمها Sharingan_Endpoint و هي تعتبر EDR او على الأقل هذا اللي اطمح له الاداة ما نزلتها الى الان ف ما تقدر تحملها و تجربها و لكن بشرح عن كيف تقفط ريفيرس شيل مالوير باستخدامها و نفس التكنيك ممكن تستخدمه في اي EDR ممكن يكون عندك المبدأ واحد

watchlist

Search in table... Rows Per Page: 10

title	level	created	actions
code.exe	info	kira	delete watchlist more info
system process	info	kira	delete watchlist more info
Detect C2	critical	kira	delete watchlist more info

طبعا هنا عندي watchlist و فكرتها انها مثل ال watchlist على [كاربون بلاك](#) طبعا ال rules تقدر تكتبها ب SQL و راح تتعامل معها مثل ما تتعامل مع [osquery](#)

query

```
SELECT process.pid, process.path, signature.result FROM processes as process LEFT JOIN authenticode AS signature ON process.path = signature.path LEFT JOIN process_open_sockets AS pos ON process.pid = pos.pid WHERE pos.state = 'ESTABLISHED' AND remote_address != '0.0.0.0' AND signature.result != 'trusted';
```

```
SELECT process.pid, process.path, signature.result FROM processes as process LEFT JOIN authenticode AS signature ON process.path = signature.path LEFT JOIN process_open_sockets AS pos ON process.pid = pos.pid WHERE pos.state = 'ESTABLISHED' AND remote_address != '0.0.0.0' AND signature.result != 'trusted';
```

طبعا هذا query ال SQL حقنا اللي بنستخدمه و طريقة عمله كالتالي: -بيشيك على كل البروسيسز الشغاله -بيشيك على كل اتصالات الشبكة و بعدين بيسوي فلتره اذا كان الاتصال طبيعي و اذا كان الاتصال مو على ايبي 0.0.0.0 ممكن بعد تحط 127.0.0.1 براحتك و اخر شي و هو الاهم ان الباينري نفسها ماتكون موثوقة او بعباره اخرى

windows signed executable

بعد ما يتأكد من كل هذي الشروط بيرجع لك اذا هل فيه باينري متصله على ايبي خارجي و الباييري نفسها ماهي signed و الاتصال اكتمل طبعاً بعد ما اضيفت ال watchlist هذي راح اشغل باينري بسيطه على جهازك

Demo

```
C:\Users\kira2\Desktop>go build main.go
```

```
C:\Users\kira2\Desktop>main.exe
```

هنا عندي برنامج بالgo وظيفته يسوي reverse shell على ايبي 127.0.0.1 و بورت 443

Detect C2

critical

::1

2023-02-10 20:12:38

[more info](#)

[delete alert](#)

بعد ما شغلت ال main.exe جاني علطول alert ان فيه باينري مطابقة لنفس ال watchlist اللي كتبناها

و لو ضغطت على ال more info

alert Title : Detect C2

description :

level: critical

host: ::1

time	data
2023-02-10 20:12:38	path : C:\Users\kira2\Desktop\main.exe pid : 40092 result : missing

بيعطيني معلومات اكثر طبعاً ال UI للحين مو مضبوط بس لازم تركزون على شي مهم شوي في ال SQL فوق

```
SELECT process.pid, process.path, signature.result
```

رجعت لي ال pid و ال path و ال result و هي نفسها اللي انطبعت في الصفحة ف ممكن انك تختار ال columns اللي تبنيها ترجع لك حسب اللي تبغاه

Add watcheslist Form

title
<input type="text" value="Title.."/>
description
<input type="text" value="description.."/>
Level
<div>Critical</div>
Query
<div><input type="text" value="Query.."/></div>
<div>Submit</div>

طبعا اضافه watchlist بسيطه جدا بس تحط المعلومات هنا و راح يتم تفعيلها على كل ال agents