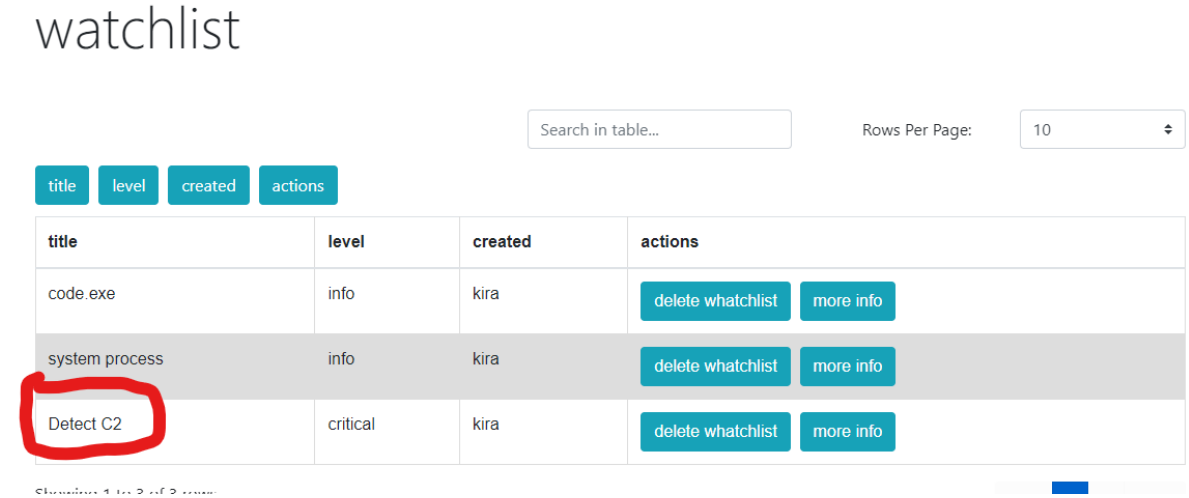
Detect C2 binary

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

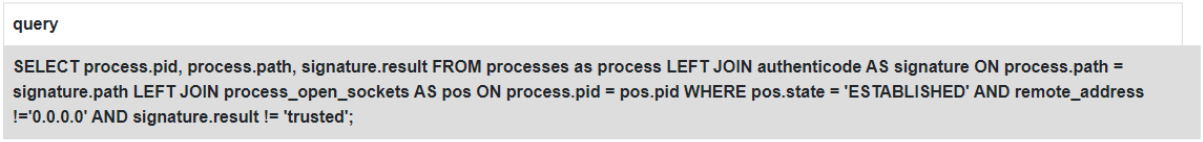
Sharingan_Endpoint

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



طبعا هنا عندي watchlist و فكرتها انها مثل ال watchlist على كاربون بلاك

طبعا الrules تقدر تكتبها ب SQL و راح تتعامل معها مثل ما تتعامل مع osquery



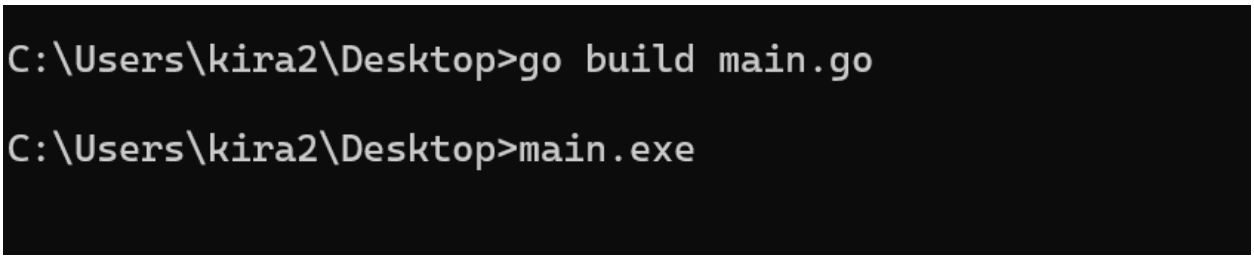

```
SELECT process.pid, process.path, signature.result FROM processes as process LEFT JOIN authenticode AS signature ON process.path = signature.path LEFT JOIN process_open_sockets AS pos ON process.pid = pos.pid WHERE pos.state = 'ESTABLISHED' AND remote_address !='0.0.0.0' AND signature.result != 'trusted';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

طبعا هذا query ال SQL حقنا اللي بنستخدمه و طريقة عمله كالتالي: -بيشيك على كل البروسيسز الشغاله -بيشيك على كل اتصالات الشبكه 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 البايزري نفسها ماتكون موثوقة او بعباره اخرى

```
windows signed executable
```

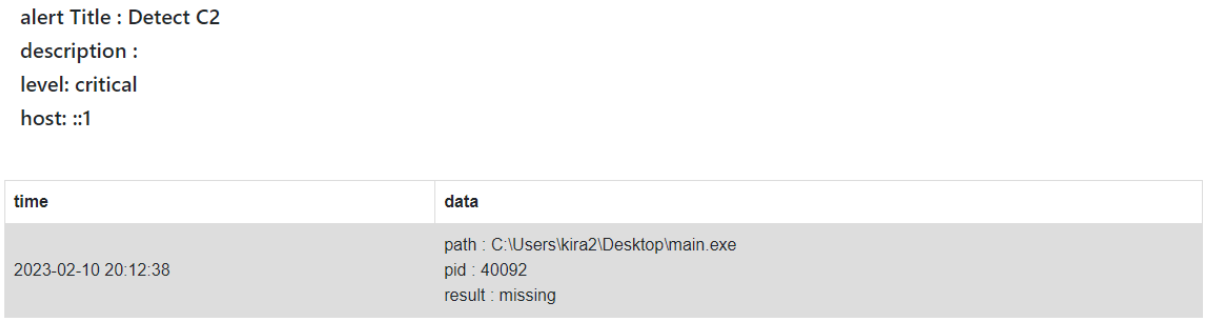
بعد ما يتأكد من كل هذي الشروط بيرجع لك اذا هل فيه باينري متصله على ايبي خارجي و الباينري نفسها ماهي signed و الاتصال اكتمل
طبعا بعد ما اضفت ال watchlist هذي راح اشغل باينري بسيطه على جهازي

Demo



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

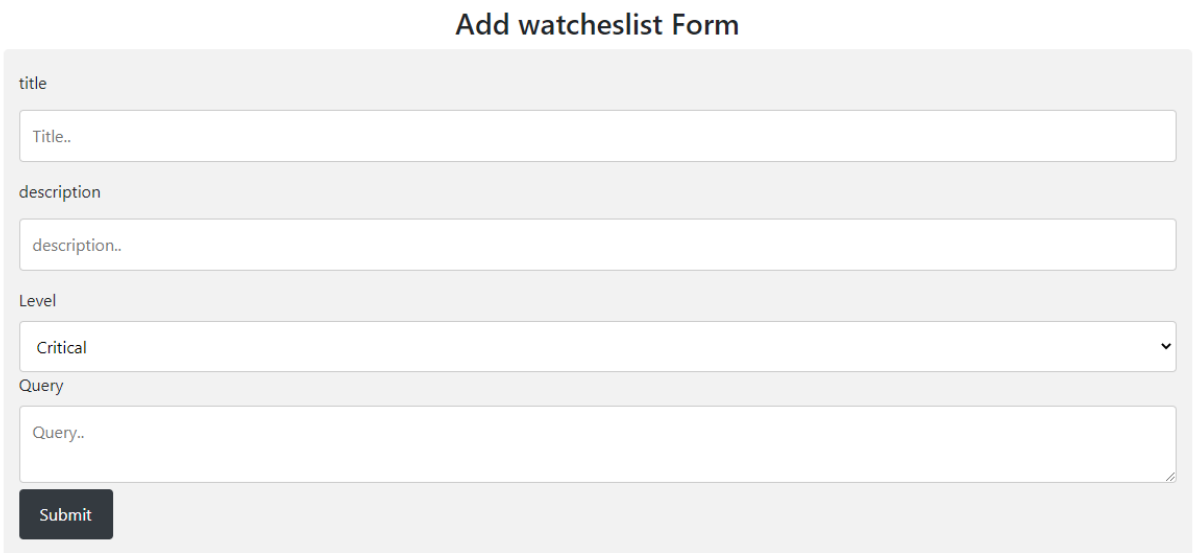
بعد ما شغلت ال main.exe جاني علطول alert ان فيه باينري مطابقة لنفس ال watchlist اللي كتبناها
و لو ضغطت على ال more info



بيعطيني معلومات اكثر طبعا الUI للحين مو مضبوط بس لازم تركزون على شي مهم شوي في الSQL فوق

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

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



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