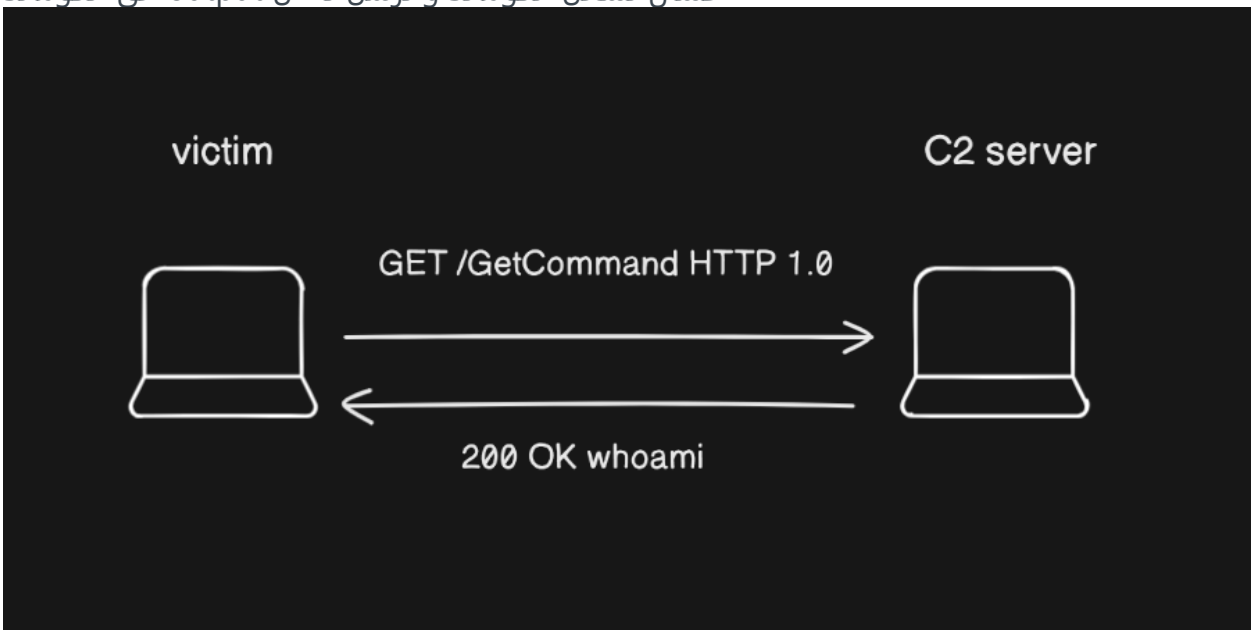
detect beaconing

بسم الله الرحمن الرحيم اليوم الشرح بيكون عن كيف تكشف الbeaconing في الشبكة حقتك

What is beaconing

كثير من الmalware تستخدم بروتوكولات مثل http و https و هذي البروتوكولات تعتبر stateless بمعنى لو تبي تسوي اتصال بين C2 سيرفر و victim راح تحتاج ترسل بين فترة و فترة ريقويست عشان تشغل الكوماند و ترسل له ال output حق الكوماند

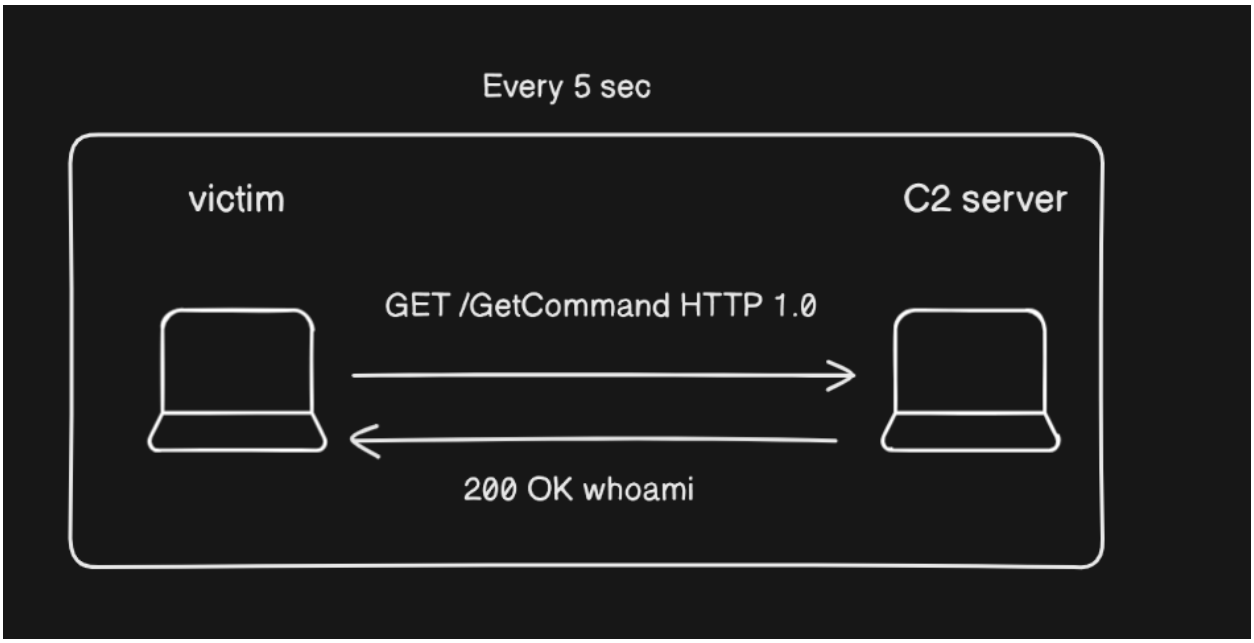


هنا مثال عندي برنامج على جهاز ال victim بيرسل http get عشان ياخذ الكوماند اللي الattacker يبي يشغلة على سبيل المثال whoami و بعدها البرنامج بيشغل whoami و بيرسل ال result على http مرة ثانية ل C2 server

و لكن فيه سلبية ان ال victim ماراح يعرف الكوماند اللي بيتنفذ الين ينرسل ل C2 server ف لازم على سبيل المثال كل 5 ثواني يرسل http ريقويست عشان يشيك هل فيه command راح يتنفذ او لا و المرحلة هذي هي المقصودة باسم beaconing

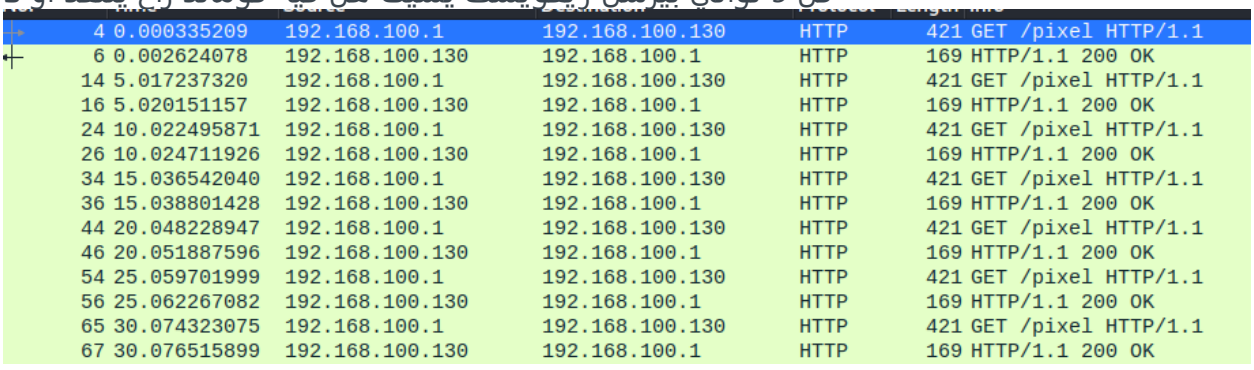
How to detect beaconing

عندنا اكثر من عامل ممكن نستعملة حاليا خلونا نكمل على مثالنا حق ال http



هنا عملية ال beaconing بتكون كل 5 ثواني البرنامج بيشيك السيرفر هل فيه كوماند راح يتنفذ او لا ف ممكن نستغل ال 5 ثواني هذي يعني كل 5 ثواني بيرسل ريقويست ف ممكن نكشفة بالطريقة هذي

هنا بستخدم Cobalt Strike عشان ك C2 server لو نلاحظ في خانه ال sleep خليته 5 ثواني يعني كل 5 ثواني بيرسل ريقويست يشيك هل فيه كوماند راح يتنفذ او لا



4	0.000335209	192.168.100.1	192.168.100.130	HTTP	421	GET /pixel HTTP/1.1
6	0.002624078	192.168.100.130	192.168.100.1	HTTP	169	HTTP/1.1 200 OK
14	5.017237320	192.168.100.1	192.168.100.130	HTTP	421	GET /pixel HTTP/1.1
16	5.020151157	192.168.100.130	192.168.100.1	HTTP	169	HTTP/1.1 200 OK
24	10.022495871	192.168.100.1	192.168.100.130	HTTP	421	GET /pixel HTTP/1.1
26	10.024711926	192.168.100.130	192.168.100.1	HTTP	169	HTTP/1.1 200 OK
34	15.036542040	192.168.100.1	192.168.100.130	HTTP	421	GET /pixel HTTP/1.1
36	15.038801428	192.168.100.130	192.168.100.1	HTTP	169	HTTP/1.1 200 OK
44	20.048228947	192.168.100.1	192.168.100.130	HTTP	421	GET /pixel HTTP/1.1
46	20.051887596	192.168.100.130	192.168.100.1	HTTP	169	HTTP/1.1 200 OK
54	25.059701999	192.168.100.1	192.168.100.130	HTTP	421	GET /pixel HTTP/1.1
56	25.062267082	192.168.100.130	192.168.100.1	HTTP	169	HTTP/1.1 200 OK
65	30.074323075	192.168.100.1	192.168.100.130	HTTP	421	GET /pixel HTTP/1.1
67	30.076515899	192.168.100.130	192.168.100.1	HTTP	169	HTTP/1.1 200 OK

باستخدام wireshark راح يبين معنا ال كل 5 ثواني ينرسل ريقويست و عشان اتأكد زيادة بستخدم procmon

Time of Day	Process Name	PID	Operation	Path
10:19:18.9676254 PM	powershell.exe	22644	TCP Connect	LAPTOP-5UORD6KL:54580 -> 192.168.100.130:http
10:19:18.9680286 PM	powershell.exe	22644	TCP Send	LAPTOP-5UORD6KL:54580 -> 192.168.100.130:http
10:19:18.9705506 PM	powershell.exe	22644	TCP Receive	LAPTOP-5UORD6KL:54580 -> 192.168.100.130:http
10:19:18.9707058 PM	powershell.exe	22644	TCP Disconnect	LAPTOP-5UORD6KL:54580 -> 192.168.100.130:http
10:19:23.9852058 PM	powershell.exe	22644	TCP Connect	LAPTOP-5UORD6KL:54583 -> 192.168.100.130:http
10:19:23.9855287 PM	powershell.exe	22644	TCP Send	LAPTOP-5UORD6KL:54583 -> 192.168.100.130:http
10:19:23.9883965 PM	powershell.exe	22644	TCP Receive	LAPTOP-5UORD6KL:54583 -> 192.168.100.130:http
10:19:23.9885425 PM	powershell.exe	22644	TCP Disconnect	LAPTOP-5UORD6KL:54583 -> 192.168.100.130:http
10:19:29.0013157 PM	powershell.exe	22644	TCP Connect	LAPTOP-5UORD6KL:54595 -> 192.168.100.130:http
10:19:29.0016141 PM	powershell.exe	22644	TCP Send	LAPTOP-5UORD6KL:54595 -> 192.168.100.130:http
10:19:29.0043172 PM	powershell.exe	22644	TCP Receive	LAPTOP-5UORD6KL:54595 -> 192.168.100.130:http
10:19:29.0045325 PM	powershell.exe	22644	TCP Disconnect	LAPTOP-5UORD6KL:54595 -> 192.168.100.130:http
10:19:34.0134327 PM	powershell.exe	22644	TCP Connect	LAPTOP-5UORD6KL:54609 -> 192.168.100.130:http
10:19:34.0137356 PM	powershell.exe	22644	TCP Send	LAPTOP-5UORD6KL:54609 -> 192.168.100.130:http
10:19:34.0160064 PM	powershell.exe	22644	TCP Receive	LAPTOP-5UORD6KL:54609 -> 192.168.100.130:http
10:19:34.0163031 PM	powershell.exe	22644	TCP Disconnect	LAPTOP-5UORD6KL:54609 -> 192.168.100.130:http

طبعا في Sharingan Endpoint بتلاقون انه قفط الاتصال

title	process	remoteip	actions	time	pid	id
beaconing behavior	powershell	192.168.100.130	delete	2023-10-29 22:50:40	22644	1

لأنه يسوي خوارزمية يراقب فيها ال traffic و منها يحدد هل هي beaconing او لا

فيه اداة ممكن تعطيها اي pcap file و راح تحلله لك

RITA

```
This package records the following:
- Each source IP address and destination SNI that communicated
- Summary statistics of the connections between the pair
- Timestamp beaconing statistics
- Data size beaconing statistics
- Beacon scoring results
```

الاداة شغالة بنفس الفكرة بس تاخذ ال Data size كعامل اضافي

Red teamer side?

اتوقع ان الموضوع سهل ما يحتاج اشرح كيف ممكن تسوي bypass لهذا النوع من ال Defense بس كل اللي عليك تسويه تعدل على المالوير حقك و تخليه يرسل بشكل عشوائي على سبيل المثال مرة بعد 3 ثواني مره بعد 9 ثواني و كل ما كان الرقم بالدقايق مثلا تخليه كل يرسل ريقويست كل 3 الى 10 دقايق بيكون اصعب على الاداة انها تكشف ال Beacon حقك لأنها بالغالب تعتمد على ال interval يكون فرق بسيط جدا و يكون بالثواني بس كل مازاد الرقم و الفرق بين الارقام كان اصعب و بنفس الوقت ال Data size لازم نخليه متغير و كأنه اتصال طبيعي كل ما خليت الاتصال كأنه طبيعي اكثر كان افضل

و ممكن ايضا انك تستعمل اكثر من ايبي بحيث كل ايبي ينرسل له كل 3 الى 10 دقايق بحيث يقل الScore
و بحكم ان الادوات بشكل عام عبارة عن Score ف كل ماكان ال Score حقك اقل كان افضل و لازم تجرب انك تشغل المالوير حقك في اي جهاز و تسحب ال pcap و تحلل ب RITA عشان تعرف نسبة ال beaconing عندك و وقتها بتعرف كيف وضع المالوير حقك يحتاج شغل اكثر او لا