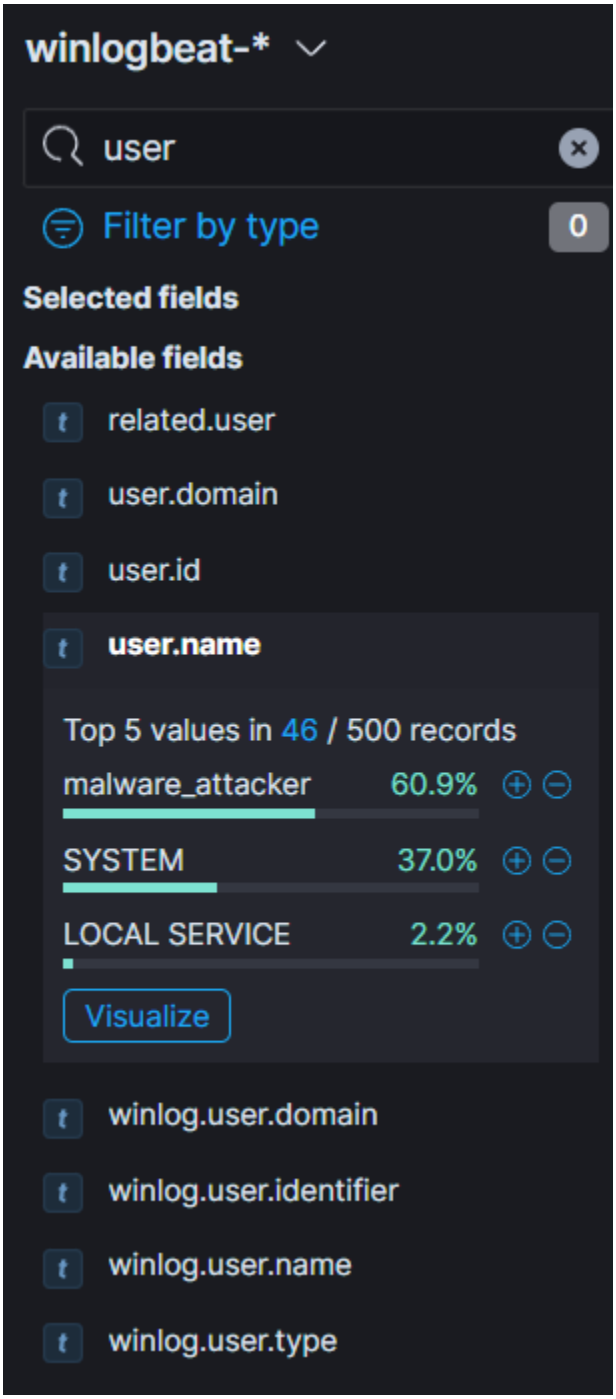
First, once we enter the website we navigate to Kibana -> Discover and filter for the past 15 years (or so, doesn't really matter as long as all 56880 logs are visible)

Q1. Please provide the user account on which malicious actions were executed.



Seen on the left side, we can filter by field names. In the user.name field we find the username the task requires, malware_attacker.

Q2. We need the IP of the compromised machine

First, we filter the logs by **user.name:"malware_attacker"**. This reduces the amount of logs to 5572. Then, we filter the field by “ip” and find the host_ip field contains one ip, the one we need.

Q3. For this one I temporally changed the log filtering to include **and process.name: ("powershell.exe" OR "cmd.exe" OR "java.exe" OR "rip.exe")**. This way, we can look through past commands that were executed. We end up with 419 results. Then, we need to look through the process.comand.line field, and take a look through the commands. I copied them in a text box so I can read them properly. One struck me as odd, **C:\Windows\system32\cmd.exe /c ""C:\Users\plant\OneDrive\Desktop\stuff-i-want\Defeat-Defender.bat””**. It looks like this is a script that was executed to disable Windows Defender, so I tried this and it was correct. It could have been a false positive, but it was suspicious either way.

Q4. For this one I filtered the fields by process.name and the tool is the first result.

Q5. For this one I did a lot of trial and error, but eventually I tried to filter by **process.name : "powershell.exe" and user.name:"malware_attacker"** and Add process.command_line in the selected fields to look only through powershell commands executed by the attacker. One struct me as odd, **powershell -command "start Winupdate.exe"**. After checking with ChatGPT, no such executable actually exists, and after checking it, turns out it was the right answer.

Q6. For this one I removed the filtering of the logs and copied the event.codes and sent them to ChatGPT. After that, one of the possible results is 4672, which is also correct.

Made with love by: AndreiCat