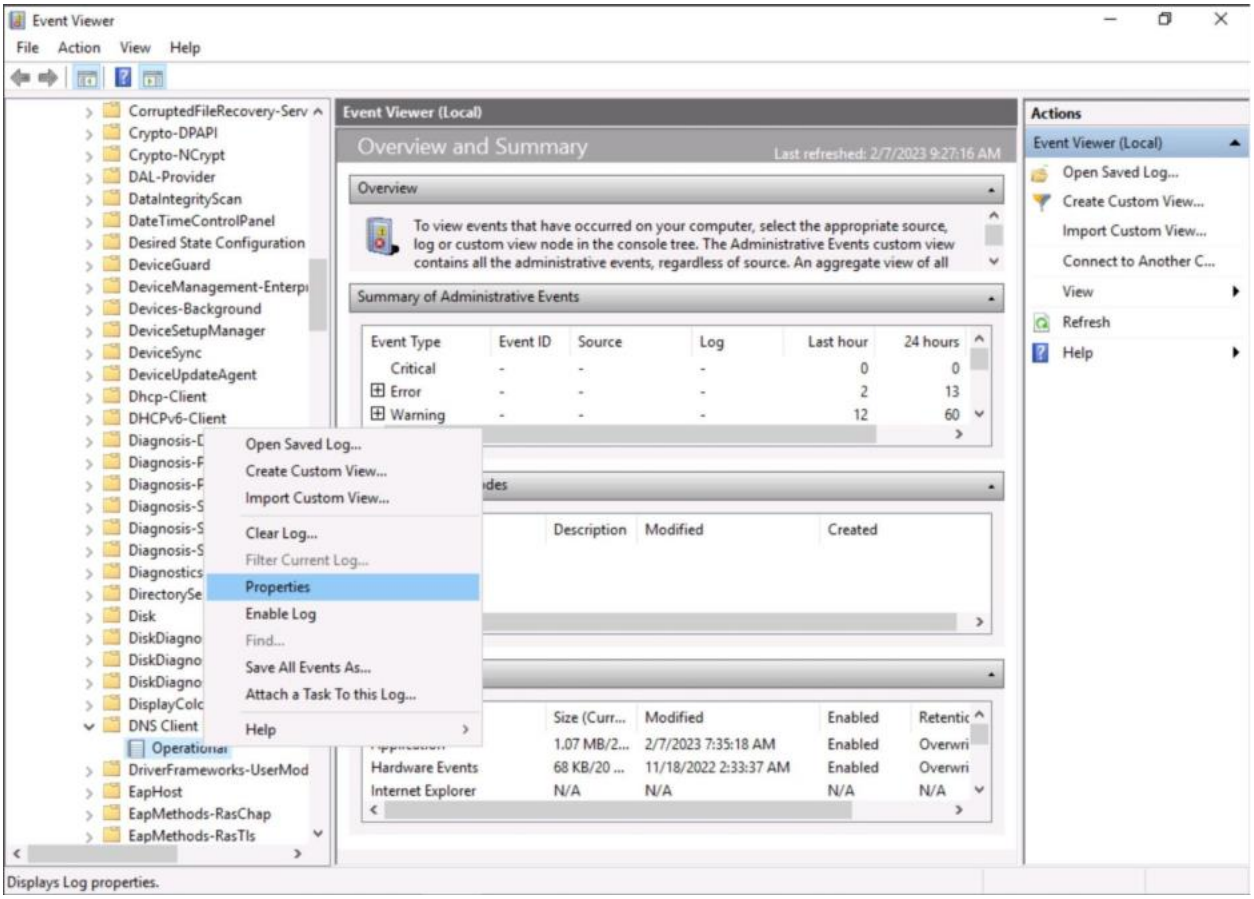
Investigating DNS Activity

Adrian Cortez

In this project, I investigated suspicious network activity originating from the private network, as reported by the ISP security team. I focused the investigation on the PC10 client system, which has a history of security issues due to poor user hygiene. To identify potential Indicators of Compromise (IoCs), I enabled DNS logging and analyzed the data for patterns related to malicious or unauthorized activity, aiming to trace and mitigate threats within the network.

Enter PC10 and open Event Viewer. Navigate to Applications and Service Logs > Microsoft > Windows > DNS Client Events.

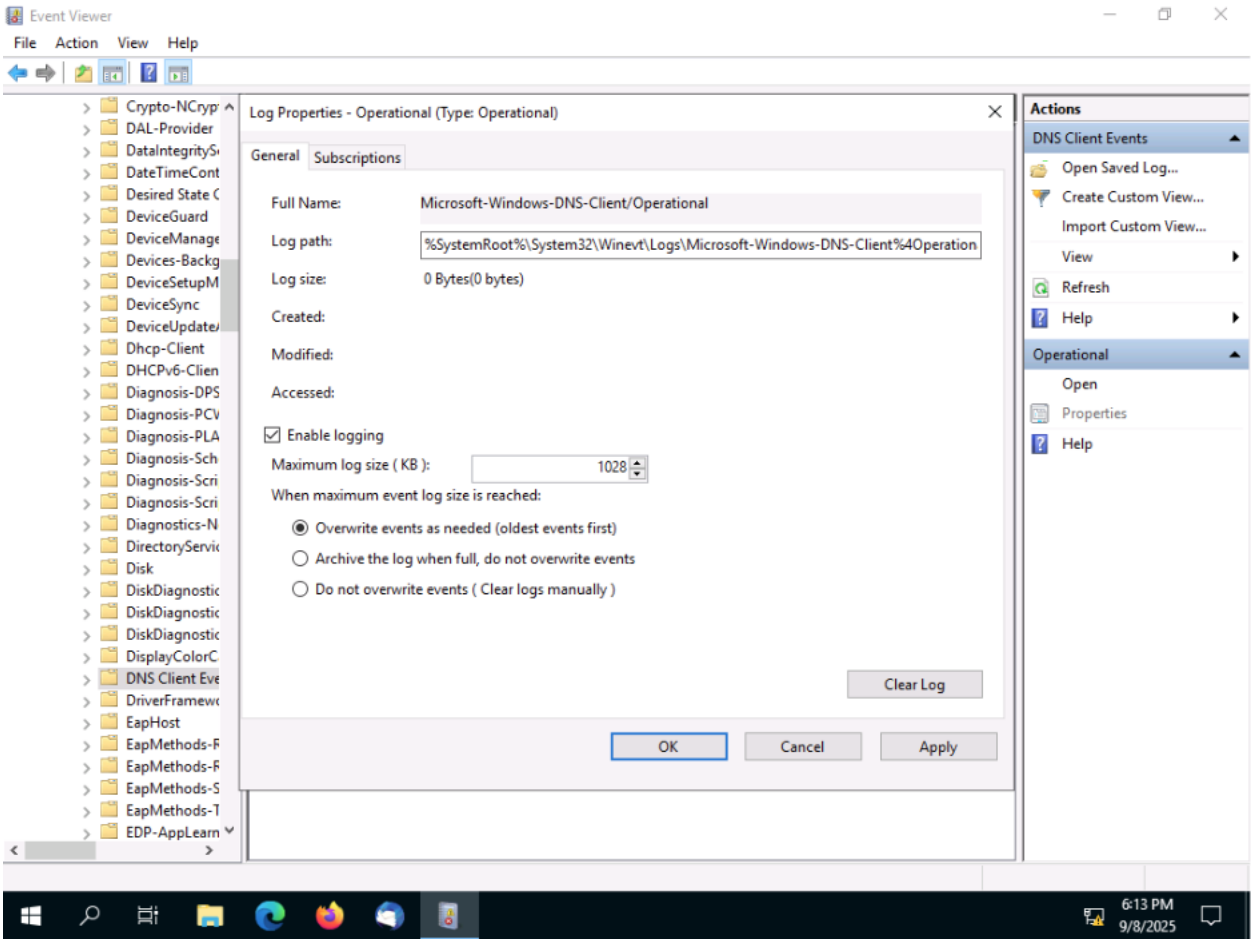
Right click the Operations file and go to properties.



Select to mark the checkbox **Enable logging**, then select **OK**.

In a real-world investigation, you would allow the log to collect entries for a period, then begin reviewing the recorded events to look for suspicious activities. In this exercise, I will

be initiating a script that will perform the activities that will be labeled as "suspicious" as I perform threat hunting.

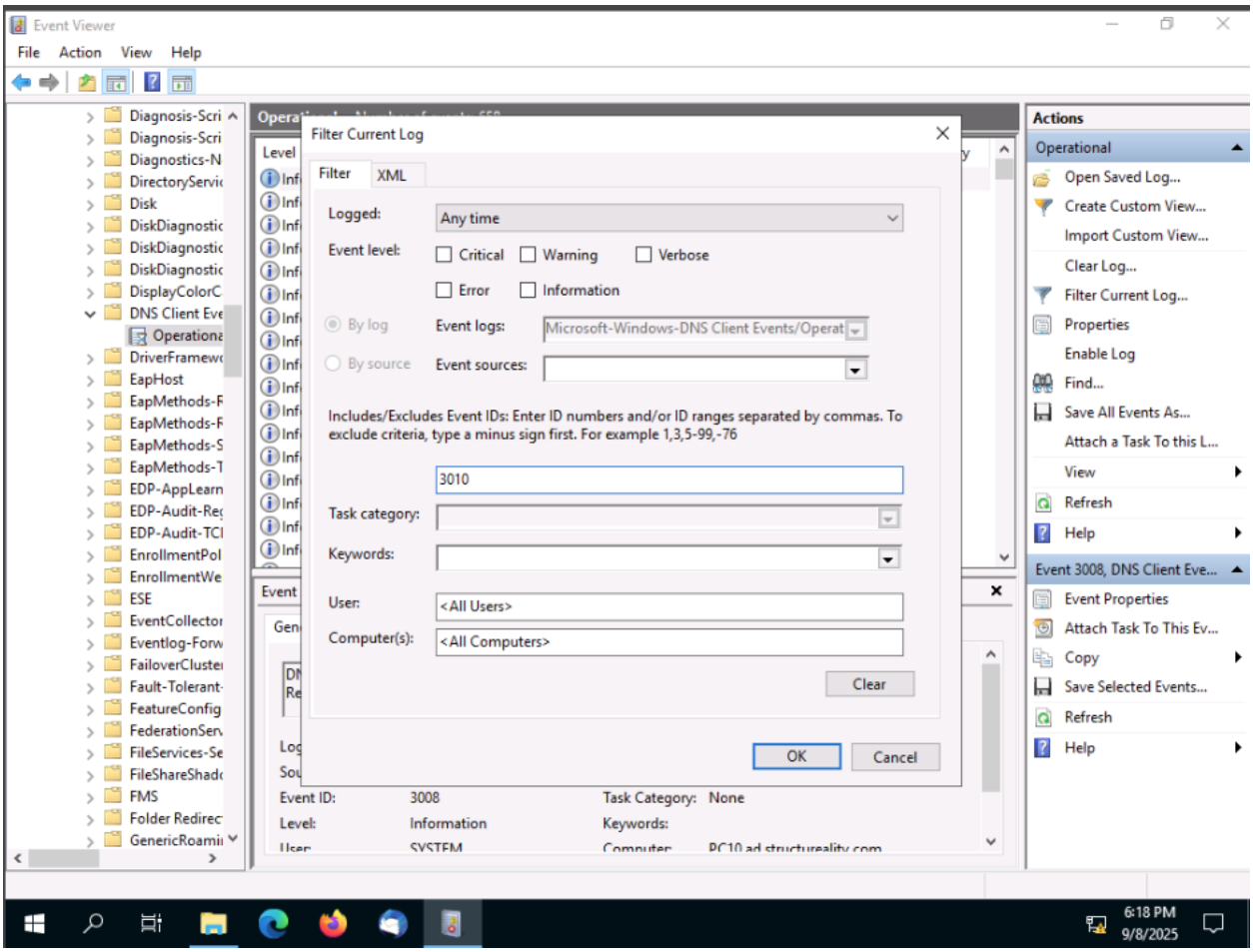


I created a simple script that will run a malicious DNS query for us to track.

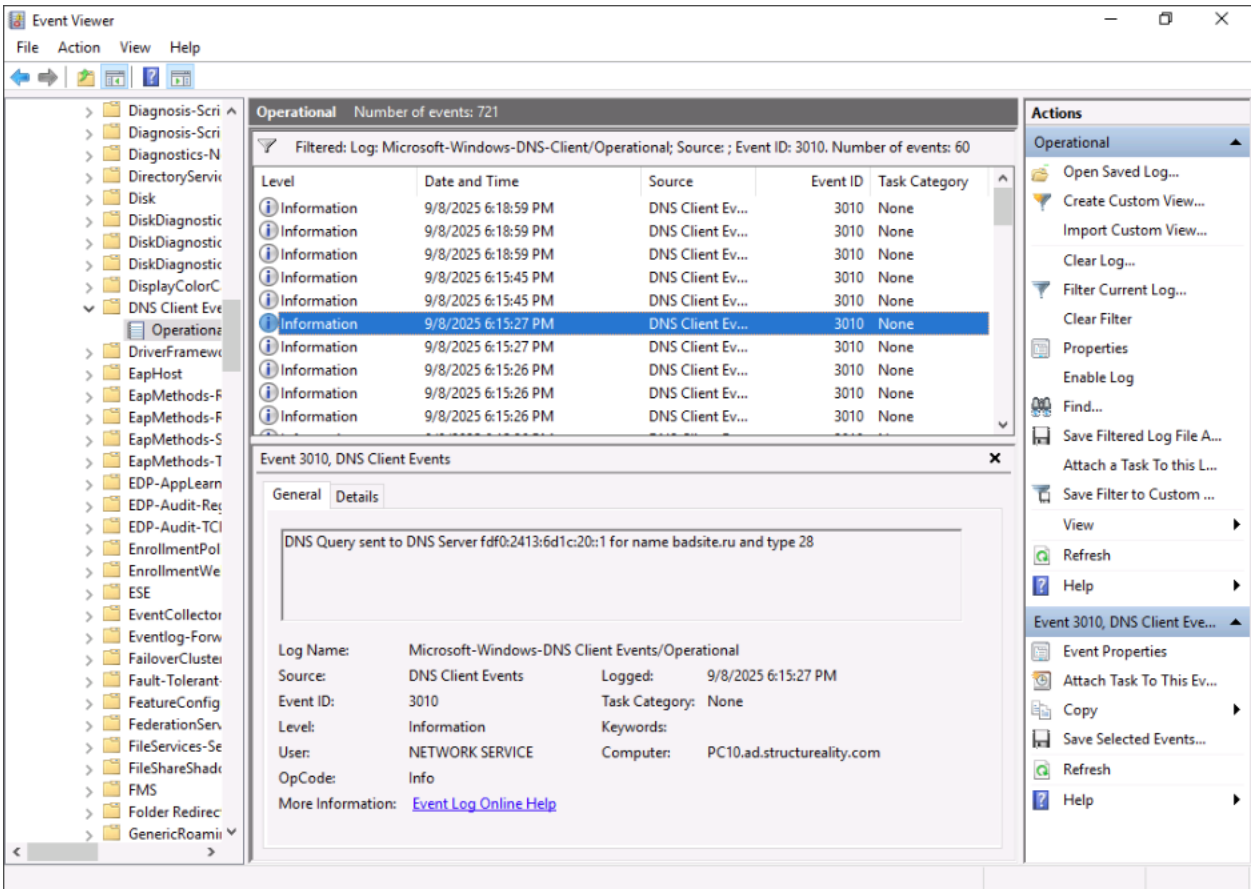
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\jaime> .\lab04demo2.ps1
1
2
3
4
5
Maximum number of attempts reached. Terminating script.
PS C:\Users\jaime> type ./lab04dem2.ps1
```

Go back into Event Viewer and filter the log. In this log, the Microsoft assigned Event ID of 3010 is for the initial DNS query.

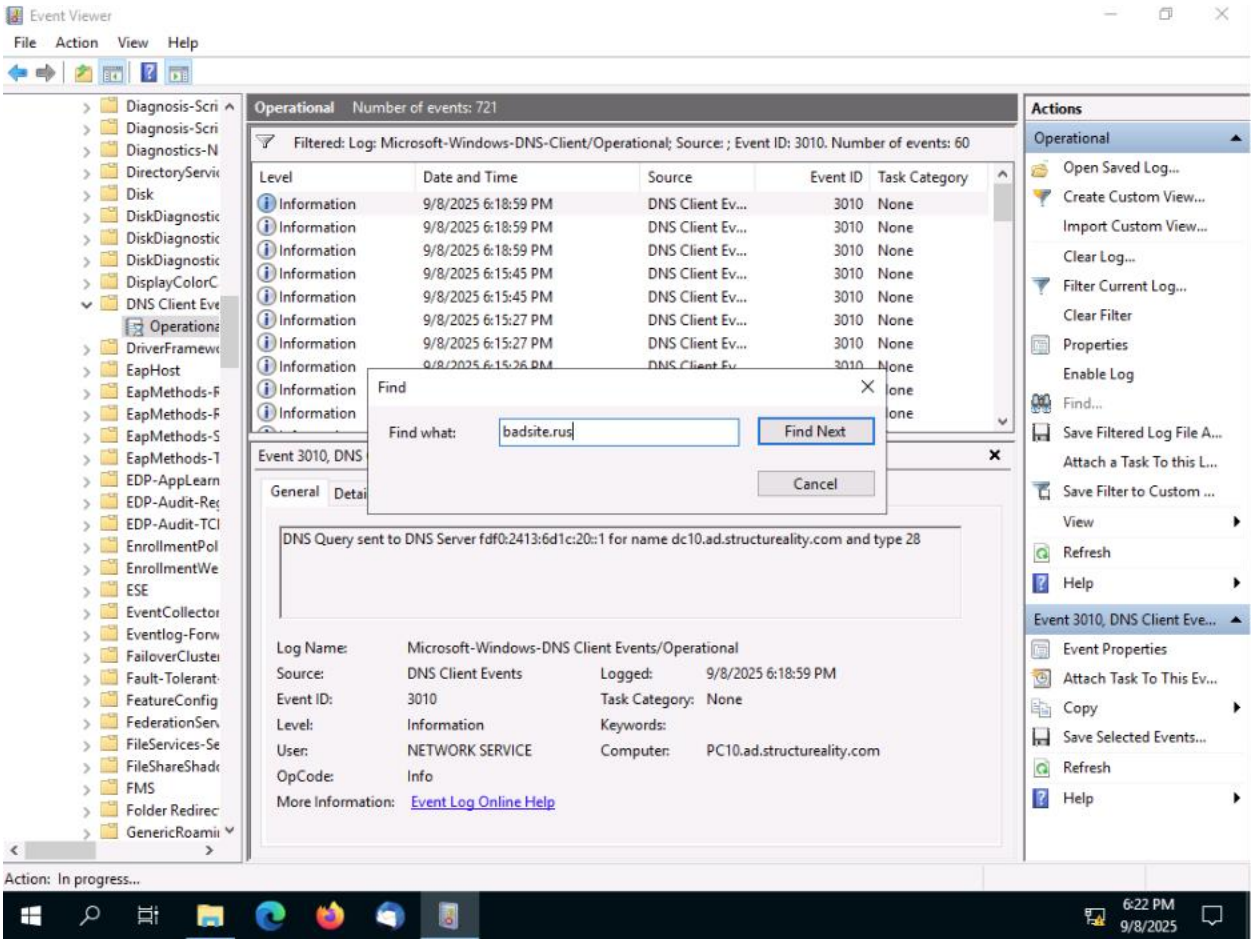


Now, we can find the FQDN of the DNS threat.



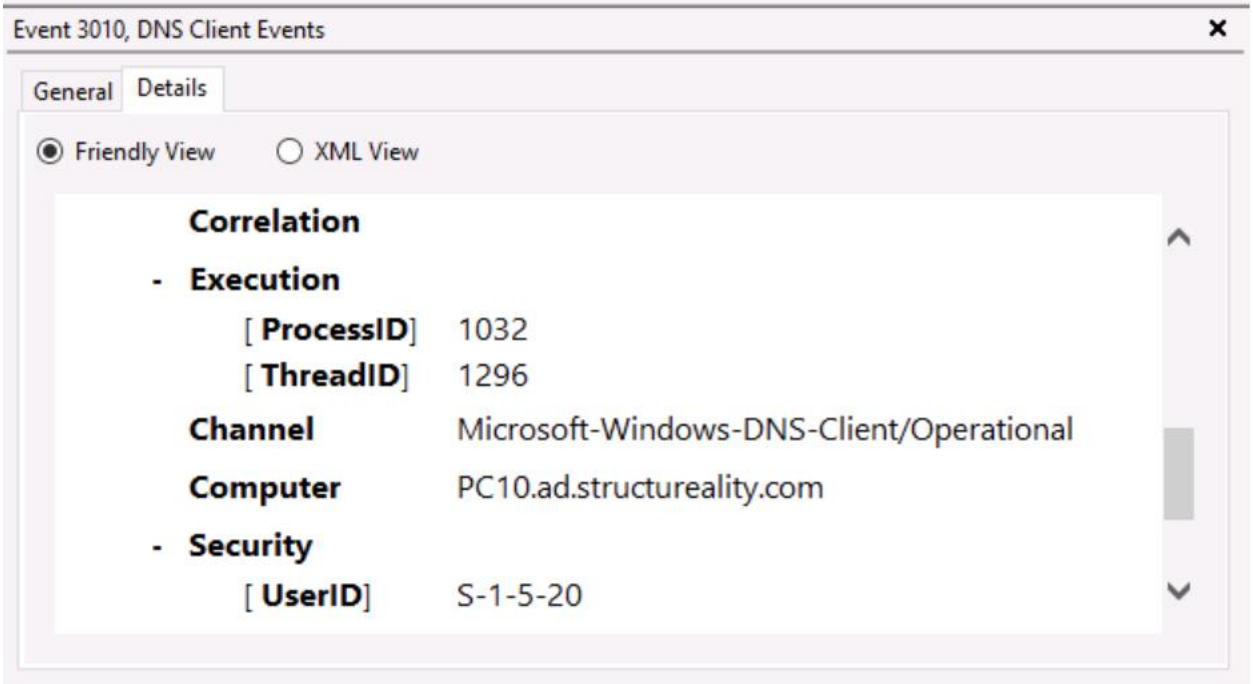
Evidently, the malicious FQDN is badsite.ru.

We can use the Find Next section in the filter to see the time between each malicious DNS entry.



We can use this to find the interval of time between each query to the malicious site. It ends up being 5 seconds between intervals. This repeated attempt to resolve a FQDN on a regular interval by unknown software is known as beaconing.

You can find the PID of the query in the details tab.



This value represents the PID (Process ID) of the program that initiated the query. If the problematic process remained active over time (unlike the lab04demo2.ps1 script, which only runs for around 10 seconds), this PID could be used in a tasklist command to identify the name of the process—similar to what was done in an earlier part of this lab. Once you've determined which process is responsible, you can decide on the appropriate next steps. These may include investigating how the process was introduced to the system and deciding how to address it (such as stopping its execution and removing it from the system entirely).

When analyzing the results of a security tool, vulnerability scanner, or investigation, several key considerations should be kept in mind. First, it's essential to confirm whether identified vulnerabilities are valid before taking any corrective action. Only true positives require resolution—false positives can be disregarded. Second, prioritize the confirmed issues to help the security team address them in an appropriate order based on severity and urgency. Lastly, when possible, provide recommendations for how to respond or remediate the issues. As a cybersecurity analyst, you may already know how to fix certain problems, and sharing this insight with the security team can streamline their response efforts and improve efficiency.