<Sysmon schemaversion="4.90">

<EventFiltering>

<!-- Log DNS queries for specific domains -->

<DnsQuery onmatch="include">

<QueryName condition="contains">parkerpublic.com</QueryName>

<QueryName condition="contains">altcloudzone.live</QueryName>

<QueryName condition="contains">tumbleproperty.com</QueryName>

<QueryName condition="contains">sombrat.com</QueryName>

<QueryName condition="contains">myappearinc.com</QueryName>

<QueryName condition="contains">ciborkumari.xyz</QueryName>

<QueryName condition="contains">bodis.com</QueryName>

<QueryName condition="contains">pastebin.mozilla.org</QueryName>

<QueryName condition="contains">gororama.com</QueryName>

<QueryName condition="contains">softeruplive.com</QueryName>

</DnsQuery>

<!-- Log process creation to correlate with DNS events -->

<ProcessCreate onmatch="include" />

</EventFiltering>

</Sysmon>

cd C:\BAH

sysmon64.exe -i sysmon-dns.xml -accepteula

**Step-by-Step Solution**

**1. Install and Configure Sysmon for DNS Query Logging**

Sysmon will log DNS queries for the specified domains, including during Windows boot, as it operates as a boot-start driver.

* **Download Sysmon**:
  + Download from the [Sysinternals website](https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon) or via winget install sysmon.
  + Extract to C:\Sysmon.
* **Create a Sysmon Configuration File**:
  + Create sysmon-dns.xml to log DNS queries for the target domains and process creation events. Use a targeted filter to reduce log noise:

xml

Copy

<Sysmon schemaversion="4.90">

<EventFiltering>

*<!-- Log DNS queries for specific domains -->*

<DnsQuery onmatch="include">

<QueryName condition="contains">parkerpublic.com</QueryName>

<QueryName condition="contains">altcloudzone.live</QueryName>

<QueryName condition="contains">tumbleproperty.com</QueryName>

<QueryName condition="contains">sombrat.com</QueryName>

<QueryName condition="contains">myappearinc.com</QueryName>

<QueryName condition="contains">ciborkumari.xyz</QueryName>

<QueryName condition="contains">bodis.com</QueryName>

<QueryName condition="contains">pastebin.mozilla.org</QueryName>

<QueryName condition="contains">gororama.com</QueryName>

<QueryName condition="contains">softeruplive.com</QueryName>

</DnsQuery>

*<!-- Log process creation to correlate with DNS events -->*

<ProcessCreate onmatch="include" />

</EventFiltering>

</Sysmon>

* + Save in C:\Sysmon.
  + The condition="contains" ensures partial matches, capturing subdomains or variations (e.g., sub.parkerpublic.com).
* **Install Sysmon**:
  + Open an elevated Command Prompt or PowerShell.
  + Run:

text

Copy

cd C:\Sysmon

sysmon64.exe -i sysmon-dns.xml -accepteula

* + This starts Sysmon, logging events from boot.
* **Verify Logging**:
  + In Event Viewer (eventvwr.msc), go to Applications and Services Logs > Microsoft > Windows > Sysmon > Operational.
  + Check for Event ID 22 (DNS Query) and Event ID 1 (Process Create).

**2. Enable Process Monitor for Boot-Time Logging**

Process Monitor captures detailed process activity, including stack traces, to identify the component (e.g., DLL) making DNS calls.

* **Download Process Monitor**:
  + Get from the [Sysinternals website](https://learn.microsoft.com/en-us/sysinternals/downloads/procmon).
  + Extract to C:\Procmon.
* **Configure Boot Logging**:
  + Open Process Monitor as Administrator.
  + Go to Options > Enable Boot Logging.
  + Enable Generate thread profiling events and Capture stack traces.
  + Reboot to start logging. Logs save to C:\Windows\Procmon.PML.

**3. Supplement with tshark for Network-Level DNS Capture**

Since you previously used tshark to capture DNS queries, integrate it to capture network-level DNS traffic, especially for non-standard DNS resolution missed by Sysmon. This requires scheduling tshark to run at boot.

* **Install Wireshark/tshark**:
  + Download Wireshark from [wireshark.org](https://www.wireshark.org/) or via winget install wireshark.
  + Ensure tshark is installed (typically in C:\Program Files\Wireshark).
* **Create a tshark Capture Script**:
  + Create a batch file dns\_capture.bat in C:\Scripts:

bat

Copy

@echo off

"C:\Program Files\Wireshark\tshark.exe" -i <interface> -f "udp port 53" -w C:\Logs\dns\_capture.pcap

* + Replace <interface> with your network interface (find it via tshark -D, e.g., Ethernet0).
  + Create C:\Logs if it doesn’t exist.
* **Schedule tshark at Boot**:
  + Open Task Scheduler (taskschd.msc).
  + Create a task:
    - General: Name it “DNS Capture”, run with highest privileges, select “Run whether user is logged on or not”.
    - Trigger: “At system startup”.
    - Action: Start a program, set to C:\Scripts\dns\_capture.bat.
    - Conditions/Settings: Allow task to run on demand, stop after 30 minutes (adjust as needed).
  + Save with admin credentials.
  + Reboot to test. The capture file saves to C:\Logs\dns\_capture.pcap.
* **Filter tshark Capture**:
  + After capturing, analyze the pcap:

text

Copy

tshark -r C:\Logs\dns\_capture.pcap -Y "dns.qry.name contains parkerpublic.com or dns.qry.name contains altcloudzone.live or dns.qry.name contains tumbleproperty.com or dns.qry.name contains sombrat.com or dns.qry.name contains myappearinc.com or dns.qry.name contains ciborkumari.xyz or dns.qry.name contains bodis.com or dns.qry.name contains pastebin.mozilla.org or dns.qry.name contains gororama.com or dns.qry.name contains softeruplive.com"

* + This lists DNS queries matching the domains, including source IP and timestamps.

**4. Analyze Sysmon Logs to Identify the Process**

* **Check Sysmon Logs**:
  + In Event Viewer, filter Microsoft-Windows-Sysmon/Operational for Event ID 22.
  + Look for queries matching the target domains.
  + Note the ProcessID, Image (e.g., C:\Windows\System32\svchost.exe), and QueryName.

**5. Analyze Process Monitor Logs to Pinpoint the Component**

* **Open Boot Log**:
  + In Process Monitor, open C:\Windows\Procmon.PML.
* **Filter for DNS Activity**:
  + Set filters:
    - Operation contains UDP (DNS uses UDP port 53).
    - Path contains parkerpublic.com (or other domains, one at a time).
    - Process Name is <process> (from Sysmon).
* **Check Stack Traces**:
  + For UDP events, right-click and view Stack.
  + Identify modules (e.g., dnsapi.dll, custom DLLs) or functions in the call chain.
  + Example: A trace showing suspicious.dll!ResolveDomain indicates suspicious.dll is responsible.
* **Save Evidence**:
  + Export filtered logs as CSV or PML.
  + Screenshot stack traces.

**6. Analyze tshark Logs for Verification**

* **Review tshark Output**:
  + The tshark -r command above lists DNS queries.
  + Correlate timestamps and source IPs with Sysmon/Procmon logs.
  + If a process bypasses Windows DNS APIs, tshark will still capture the traffic.
* **Identify Process**:
  + Use Resource Monitor (resmon) post-boot to spot processes with UDP port 53 activity.
  + Cross-reference with Sysmon’s process IDs.

**7. Address Potential Malicious Activity**

Some domains (parkerpublic.com, tumbleproperty.com, sombrat.com, softeruplive.com) are linked to Royal/BlackSuit ransomware, as noted in your prior conversation. Others (ciborkumari.xyz, bodis.com, pastebin.mozilla.org) may indicate adware, data exfiltration, or malicious scripts. Take these steps:

* **Isolate the System**:
  + Disconnect from the network if suspicious processes are active.
* **Scan for Malware**:
  + Run Microsoft Defender or a tool like Malwarebytes to scan for ransomware or adware.
  + Check for unrecognized DLLs in stack traces.
* **Mitigate**:
  + Block domains in the hosts file:

text

Copy

127.0.0.1 parkerpublic.com

127.0.0.1 altcloudzone.live

...

* + Use a firewall rule to block outbound traffic to these domains.

**8. Prove the Findings**

* **Document**:
  + Process: svchost.exe (PID 1234) queried sombrat.com.
  + Stack Trace: Shows malicious.dll!DnsResolve from C:\Program Files\Unknown\malicious.dll.
  + tshark: Confirms DNS query at 2025-05-20 14:53:00.
* **Verify**:
  + If svchost.exe, use tasklist /svc to identify the service.
  + Analyze DLLs with Get-Item malicious.dll | Select-Object VersionInfo or a dependency walker.
* **Test**:
  + Block a domain and confirm the process stops querying it.

**Notes**

* **Performance**:
  + Sysmon and Procmon boot logging generate large files. Filter for the 10 domains to reduce size.
  + Limit tshark captures (e.g., stop after 30 minutes) to manage disk space.
* **Custom DNS**:
  + tshark ensures capture of non-standard DNS resolution (e.g., direct UDP packets).
* **Windows 11**:
  + Fully compatible with Sysmon 15.x and Procmon 3.x on Windows 11 24H2.
* **Security**:
  + Run tools as Administrator.
  + Protect sysmon-dns.xml from tampering.
* **Prior Context**:
  + Your use of tshark for parkerpublic.com and softeruplive.com inspired the network capture integration.
  + The ransomware concern for sombrat.com, etc., prompted the mitigation steps.

**Example Output**

* Sysmon: svchost.exe (PID 1234) queried sombrat.com at 2025-05-20 14:53:00.
* Procmon: Stack trace shows malicious.dll!ResolveDomain.
* tshark: UDP packet to DNS server for sombrat.com.
* Conclusion: malicious.dll in svchost.exe is the culprit, likely ransomware-related.