Suricata - Feature #5067

smb/dcerpc: Match dcerpc (over smb) requests before bind_ack

02/10/2022 10:38 AM - Eloy Pérez

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Eloy Pérez</td>
</tr>
<tr>
<td>Category:</td>
<td>TBD</td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td>Rust</td>
</tr>
</tbody>
</table>

Description

Windows computers made a heavy use of the dcerpc protocol. I was working with a Windows Server 2019 and observed that, probably for optimization purposes, using DCERPC over SMB it sends a bind message, and then it submits a request without receiving the bind_ack, which is returned later. This behavior can be appreciated in the following capture:

```
TCP        0x000024d2 -> 0x000048b3 [ACK] SEQ=35504 ACK=73/ WND=2147483647 L0R
SMB2  186 Create Request File: samr
SMB2  219 Create Response File: samr
DCERPC  242 Request: call_id: 3, Fragment: Single, opnum: 7, 0
DCERPC  218 Response: call_id: 3, Fragment: Single, Ctx: 0
DCERPC  222 Request: call_id: 7, Fragment: Single, opnum: 1, 0
DCERPC  218 Response: call_id: 7, Fragment: Single, Ctx: 0
DCERPC  286 Bind: call_id: 2, Fragment: Single, 2 context item
SMB2  130 Write Response

SAMR  218 OpenAlias request
SAMR  222 Close request
SAMR  218 Close response
SMB2  171 Read Request Len:1024 Off:0 File: samr
DCERPC  230 Bind_ack: call_id: 2, Fragment: Single, max_xml=1
DCERPC  222 Request: call_id: 5, Fragment: Single, opnum: 35
DCERPC  282 Response: call_id: 5, Fragment: Single, Ctx: 0
SMB2  146 Close Request File: samr
```

A bind is submitted, then an OpenAlias request, and finally, the client requests for the bind_ack (in SMB the bind_ack needs to be requested by the client).

To match requests in this case, I propose to create a flag for the dcerpc.iface, that allows users to choose if they want to match dcerpc requests (over smb) after the bind is issued and before the bind_ack is received.

I let pcap with SMB traffic that shows this behaviour. In this case the traffic was created by executing the tool Bloodhound over a Windows Server 2019 (joined to a domain). The same tool executed over Windows 10 creates a different traffic where the bind_ack is received always before any dcerpc request.

Files

- bloodhound-smb-w2019.pcapng (73.7 KB, 02/10/2022, Eloy Pérez)
- smb-over-dcerpc.png (52.5 KB, 02/10/2022, Eloy Pérez)

03/16/2022 1/1