In recent news, the cloud-based IT management service JumpCloud publicly shared details gathered from the investigation of an intrusion into a customer's network. This intrusion, referred to as an "Advanced Persistent Threat (APT)", suggests persistent and advanced malware activity targeted at a specific subset of a network.

The JumpCloud intrusion serves as a clear illustration of North Korean threat actors' inclination towards supply chain targeting. It is evident that North Korean threat actors are continuously adapting and exploring novel methods to penetrate targeted networks. This demonstrates a profound understanding of the infrastructure and attack surfaces.

### Infrastructure Analysis

<table>
<thead>
<tr>
<th>Infrastructure Type</th>
<th>Associated Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related to Infrastructure</td>
<td>fruitful networks. which yields a multitude of potential subsequent intrusions. The DPRK demonstrates a profound understanding of the</td>
</tr>
<tr>
<td>JumpsCloud Intrusion</td>
<td>as a clear illustration of their inclination towards supply chain targeting, It is evident that North Korean threat actors are continuously adapting and exploring novel methods to in intrate targeted</td>
</tr>
<tr>
<td>GitHub Security Alert</td>
<td>Following the profile of the associated infrastructure from both the JumpCloud intrusion and the GitHub security alert,</td>
</tr>
<tr>
<td>Additional Pivots</td>
<td>By mapping out the associated infrastructure, it is possible to show the links between the diverse set of IP addresses and pick up</td>
</tr>
</tbody>
</table>

### Infrastructure Map Noting JumpCloud and GitHub Overlap

The map illustrates the overlap and connection between the two infrastructure sets, highlighting the associated domains and IP addresses.

### Conclusion

Based on the IOCs shared by JumpCloud, we were able to analyze the threat actor's infrastructure. The following list is

- **Infrastructure Analysis**

  - Related to Infrastructure
  - JumpsCloud Intrusion
  - GitHub Security Alert
  - Additional Pivots

  By mapping out the associated infrastructure, it is possible to show the links between the diverse set of IP addresses and pick up additional perspectives. T

- **Infrastructure Map Noting JumpCloud and GitHub Overlap**

  The map illustrates the overlap and connection between the two infrastructure sets, highlighting the associated domains and IP addresses.

- **Conclusion**

  Based on the IOCs shared by JumpCloud, we were able to analyze the threat actor's infrastructure. The following list is