National Cyber Security Centre | NOMINET CYBER

SolarWinds

In 2020 a malicious, unauthorised modification to SolarWinds Orion was identified. It compromised SolarWinds, which is in the supply chain of many other organisations. The impact of the attack was felt globally.

PDNS
Protective DNS

SolarWinds exposed as vulnerable

Vulnerable SolarWinds Orion instances and signs of attacker behaviour fingerprinted

PDNS logs searched for fingerprints

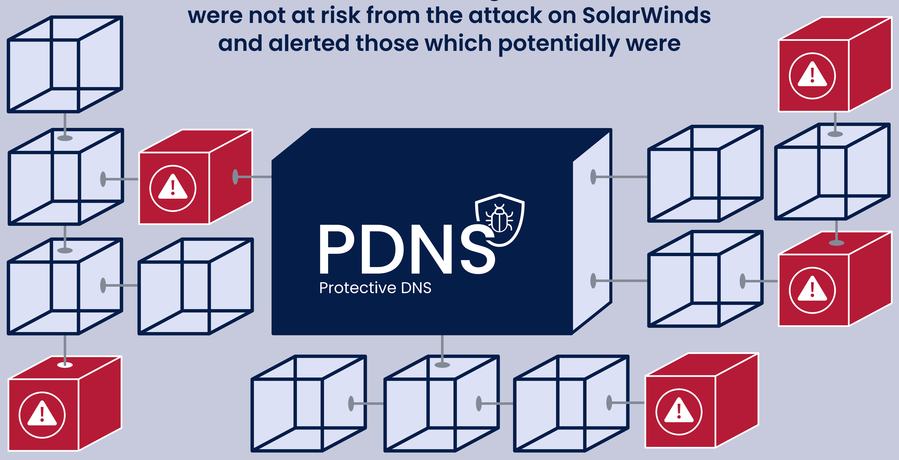
Additional intelligence from PDNS and other ACD services combined to inform remediation

DATA INSIGHTS

It is possible to see which domains were being accessed through PDNS logs. This can reveal the fingerprints of an attack, for example:

1. Access to domains related to the compromised software show where and when technology is likely to be vulnerable.
2. Requests to malicious domains, known to be compromised and can indicate an attack.

PDNS reassured those organisations which were not at risk from the attack on SolarWinds and alerted those which potentially were



Potentially vulnerable organisations identified

Those organisations not at risk reassured

Outcome

ATTACK RESPONSE
Incident management, cyber operations and engagement teams prepared

THREAT INSIGHT
PDNS logs indicate possible exposure of an organisation

RISK ANALYSIS
Insight into the extent of an incident across UK public sector

CYBER INTELLIGENCE
Understanding cyber maturity across UK Government and public services