SolarWinds Breach Overview December 2020

Attack attributed to Threat Group APT29 (Cozy Bear/Russian SVR). US determined them a State Sponsored Group working with the Russian government.

SolarWinds is a software company primarily dealing with systems management tools. Compromised SolarWinds product was "Orion", a Network Management System (NMS). Backdoor was inserted in the products updates (trojan horse) and downloaded by customers.

NMS prime target for attacks:

- NMS must be able to communicate with all devices being monitored and manged so outbound ACLs ineffective
- NMS can make configuration changes to all devices – so attackers can too
- Attacker can reshape network traffic to enable MITM opportunities and use credentials stolen for lateral movement

Orion NMS contains broad monitoring and management capabilities.

SolarWinds - 300,000 customers include US federal government (DOD), 425 of Fortune 500 companies. Up to 18,000 known to be impacted.

Malware was deployed as part of a legitimate update from SolarWinds servers that was digitally signed with a valid digital certificate bearing SolarWinds name.

SolarWinds response: "...evidence that the vulnerability was inserted within the Orion products and existed in updates released in March and June 2020, as a result of a compromise of the Orion Build System and was not present in the source code repository of the Orion products"

Sophisticated elements of the attack:

- Zero-day exploit
- Specific infrastructure used for each victim (rendering network-based IOCs not useful)
- Tooling used does not share code with other samples (hard to detect signature)
- Uses delayed execution – malware checks file timestamps to ensure deployed for 12-14 days before it beacons (ensuring sandboxes / pre deployment checks don't pick it up)
- Anti-Sandbox behaviour (Malware will not execute if machine not joined to a domain, and will not deploy if domain resolves to a private IP address)