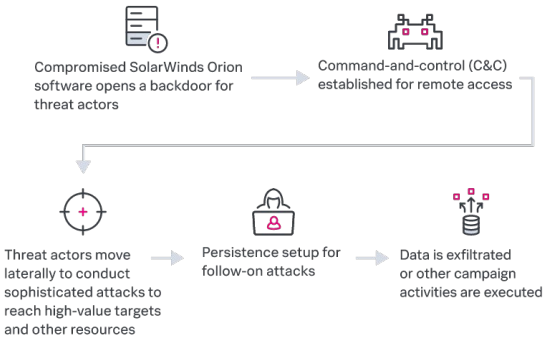
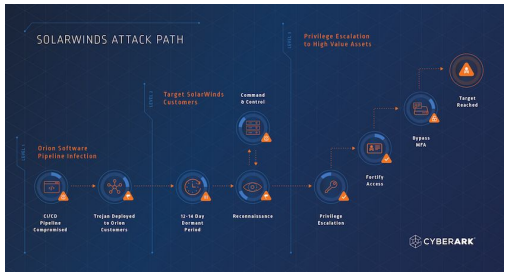
Solarwinds Cyberattack

By: Kilik White



Who and what is Solarwinds?

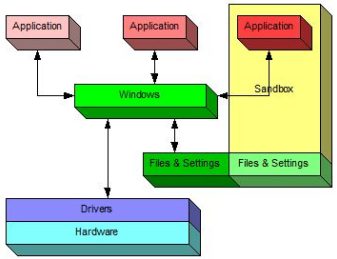
- Solarwinds is a software company that is well known for their System Management tools.
- The most used product there is Orion which is a Network Management System(NMS).
- It is also a widely popular NMS Tool source since over 300,000 customers use software from Solarwinds.
    - A sizeable chunk of them is from the US Federal Government.



How is the Cyberattack tempting

- The NMS needs to communicate to all devices being managed.
- Along with the fact that they monitor and respond to the events to the respective servers and workbenches.
- This means that once the NMS got compromised, all of the data can be stolen.
    - Remember, most of the customers are from the US Federal Government

How did the cyber attack happen?



- The cyberattack is considered a supply chain attack since it directly attacked the NMS software.
- The group APT29 injected malware into the update packages for the NMS software.
- That means that a regular person would think nothing is wrong and it goes unnoticed.
- The malware was smart since it did not infect the computers until 12-14 days after the update.
- And it has anti-sandbox behavior since the malware will not execute unless the machine is joined to the domain.

Aftermath

- This lead to the APT29 group to steal a lot of information from Solarwinds.
- The hack also went undetected for months so it was not in the company's radar until it became an issue.
- They did respond with a published info with stated that, "there is evidence that the vulnerability was inserted within the Orion products between March and June 2020."
- Thankfully it was taken care off so it is now safe to use.

Work Cited

https://www.youtube.com/watch?v=jD02Q3RStaM

https://www.youtube.com/watch?v=XVQvIisuO1o

https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

https://www.sans.org/blog/solarwinds-sans-lightning-summit-recap/