What is a supply chain?
DACYS - TP7

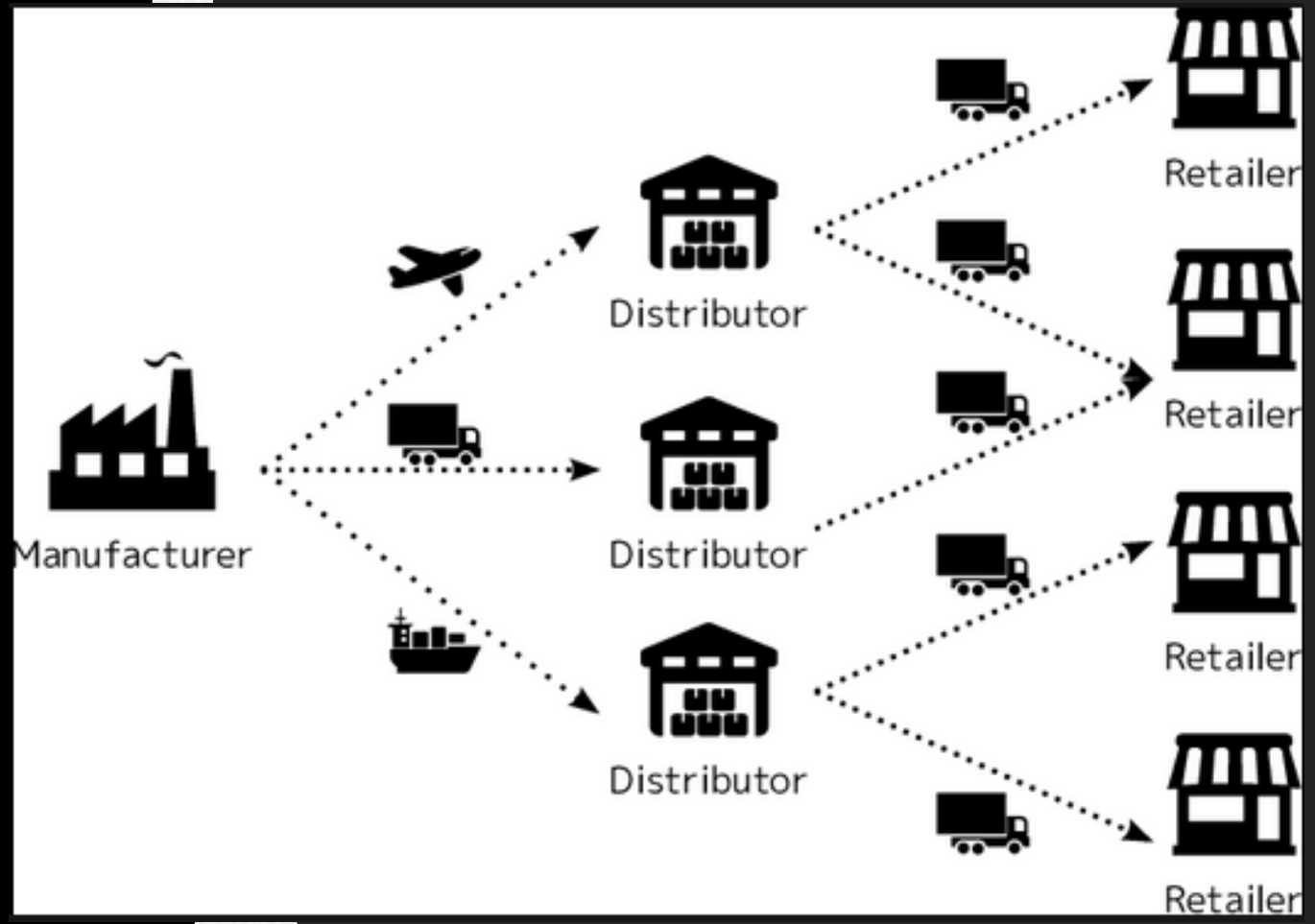
Nuno Peralta

Nsp@isep.ipp.pt

isep Instituto Superior de Engenharia do Porto

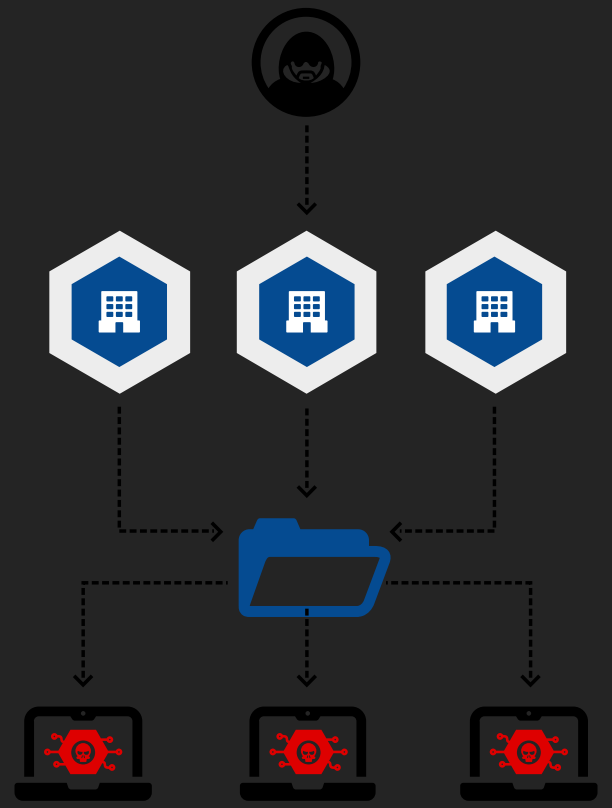
Então... o que é uma supply chain?

Exemplo prático



Mas qual a necessidade?!

Exemplo concreto



O que é a SolarWinds?

https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

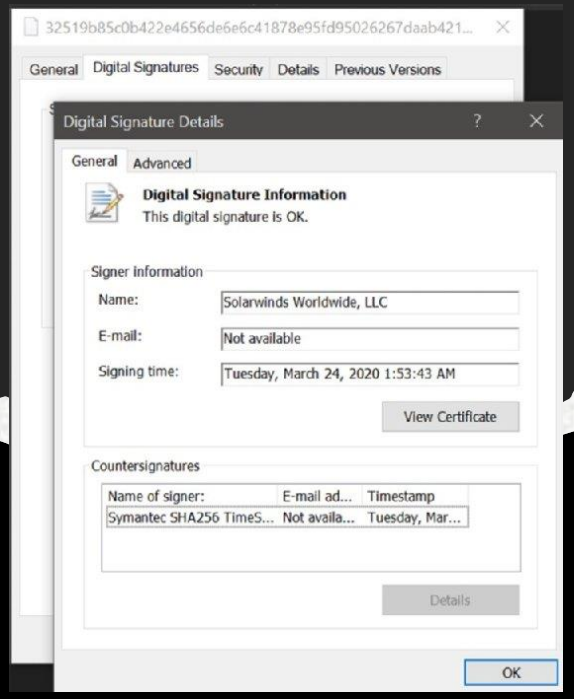
Resumidamente

- SolarWinds is a major software company based in Tulsa, Okla., which provides system management tools for network and infrastructure monitoring, and other technical services to hundreds of thousands of organizations around the world. Among the company's products is an IT performance monitoring system called Orion.

Ainda mais resumido...

The SolarWinds hack was a major event not because a single company was breached, but because it triggered a much larger supply chain incident that affected thousands of organizations, including the U.S. government.

O impacto



In this hack, suspected nation-state hackers that have been identified as a group known as Nobelium by Microsoft -- and often simply referred to as the SolarWinds Hackers by other researchers -- gained access to the networks, systems and data of thousands of SolarWinds customers. The breadth of the hack is unprecedented and one of the largest, if not the largest, of its kind ever recorded.

More than 30,000 public and private organizations -- including local, state and federal agencies -- use the Orion network management system to manage their IT resources. As a result, the hack compromised the data, networks and systems of thousands when SolarWinds inadvertently delivered the backdoor malware as an update to the Orion software.

Mas como aconteceu... Temporalmente

- **September 2019.** Threat actors gain unauthorized access to SolarWinds network
- **October 2019.** Threat actors test initial code injection into Orion
- **Feb. 20, 2020.** Malicious code known as Sunburst injected into Orion
- **March 26, 2020.** SolarWinds unknowingly starts sending out Orion software updates with hacked code

Propagação

More than 18,000 SolarWinds customers installed the malicious updates, with the malware spreading undetected. Through this code, hackers accessed SolarWinds's customer information technology systems, which they could then use to install even more malware to spy on other companies and organizations.T

"Killswitch"

Microsoft also confirmed that it found signs of the malware in its systems, as the breach was affecting its customers as well. Reports indicated Microsoft's own systems were being used to further the hacking attack, but Microsoft denied this claim to news agencies. Later, the company worked with FireEye and GoDaddy to block and isolate versions of Orion known to contain the malware to cut off hackers from customers' systems.

They did so by turning the domain used by the backdoor malware used in Orion as part of the SolarWinds hack into a kill switch. The kill switch here served as a mechanism to prevent Sunburst from operating further.

Takeaways

Everything is a weapon?

Verifications?

-By who?

Prevention?

How can it be defended?