Sunburst Case Study

Solar Winds

Malware
(supply chain attack)

Description:

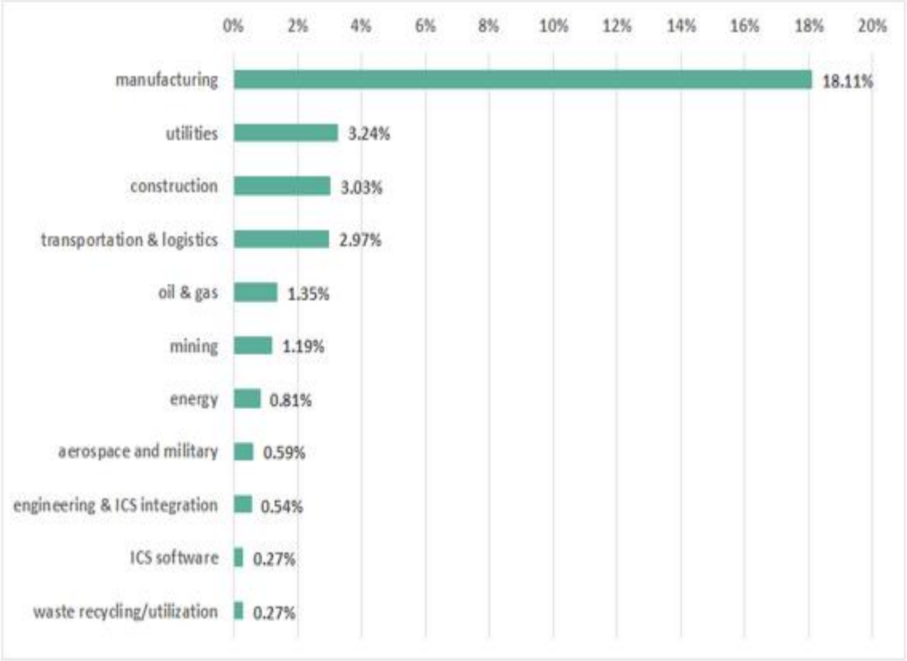
Hundreds of industrial organizations have apparently received a piece of malware named “SUNBURST” as part of a supply chain attack.

Research:

- Solar Winds' analysis of the attack revealed that up to 18,000 of its customers may have received trojanized update for its ORION monitoring product.
- Nearly 2000 domains were impacted, and 30% of them were associated with industrial organizations.
- 200 of its customers received the malicious Solar Winds update

Statistics:

Affected countries



Company description:

SolarWinds Inc. is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure. It is headquartered in Austin, Texas, with sales and product development offices in a number of locations in the United States and several other countries.

Summary of the security incident and data breach:

An analysis of command and control (C&C) mechanisms used by the Sunburst malware, specifically DNS responses, has allowed researchers to determine which organizations may have **received Sunburst** and which might have been breached further by the SolarWinds hackers

Timeline

Solarwinds Attack

1. **Attackers Hostnames Match Victim Environment**
2. IP Addresses located in Victim's Country
3. Temporary File Replacement and Temporary Task Modification
4. Lateral Movement using Different Credentials
5. Teardrop malware used
6. BEACON malware used

Vulnerabilities

Overall Summary

FireEye has uncovered a widespread campaign, that we are tracking as UNC2452. The actors behind this campaign gained access to numerous public and private organizations around the world.

Vulnerability #1

Actor sets the hostnames on their command and control infrastructure to match legitimate hostname which allows to blend in the environment, void suspicion and evade detection.

Vulnerability #2

Leaked configured hostname in RDP SSL certificates.

Vulnerability #3

Geolocating IP addresses used for remote access.

Vulnerability #4

Examine logs for SMB sessions that show access to legitimate directories.

Costs

- 18000 customers affected
- 32% of industrialist damaged
- 2000 domains
- 200 of companies ran into loss
- 20 various sectors like energy, mining damaged
- Manufacturing hit with 18.11% average loss

Prevention

- In-depth malware analysis
- DGA – Domain generation algorithm
- Blocklists
- Network Command and Control (c2)
- Steganography
- MITRE Attack techniques