SunBurst industrial victims

ics-cert.kaspersky.com/reports/2021/01/26/sunburst-industrial-victims/

January 26, 2021

Kaspersky
ICS CERT

26 January 2021

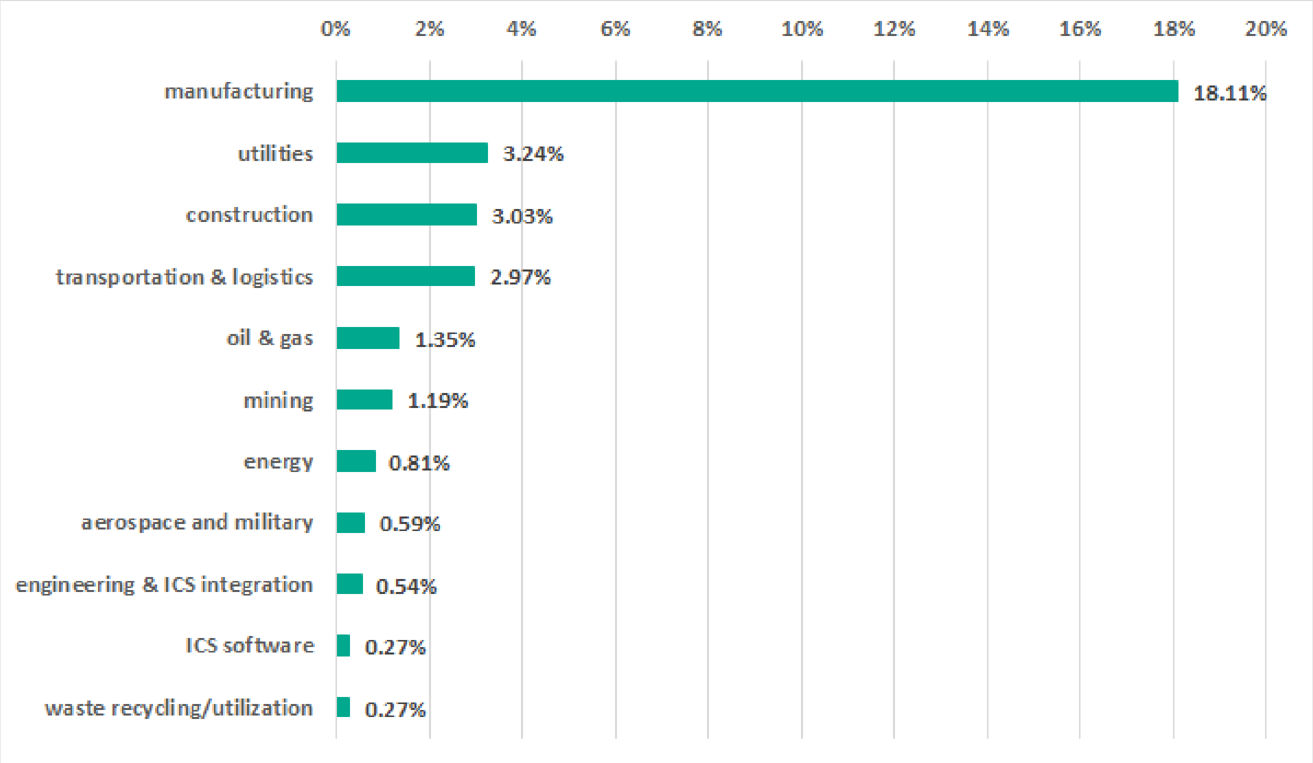
On December 13th, 2020, FireEye, Microsoft, and SolarWinds announced the discovery of a large, sophisticated supply chain attack leveraging Orion IT, an infrastructure monitoring and management platform by SolarWinds.

Many publications have followed up on this major incident and the research is still ongoing. While technical details of the SunBurst backdoor embedded into SolarWinds have already been described and second-stage tools are being discovered, the scale of the attack and the interest of the actor behind the attack are still being investigated. It has been officially confirmed that about 18,000 users may have installed backdoored versions of SolarWinds. Still, there is limited information on the number of organizations where the attack has evolved and second-stage tools may have been deployed, though there are some speculations on the actor's interest based on an analysis of the historical C2 DNS response (see here and here).

We were specifically interested in analyzing how many industrial organizations used backdoored SolarWinds versions and fell victim to the attack. The results of the analysis are below.

First of all, we analyzed all available decoded internal domain names obtained from DNS names generated by the SunBurst DomainName Generation Algorithm using some publicly available lists and third-party lists. The final list of readable and attributable domains consisted of nearly 2000 domain names and information on the industries in which possibly compromised industrial organizations operate is provided below:

The overall percentage of industrial organizations among all organizations on the list is estimated at 32.4%.



We also analysed user information from our telemetry where the backdoored SolarWinds applications were installed and distinguished over 20 organizations in the industrial sector:

manufacturing	8
transportation & logistics	6
utilities	4
construction	4
mining	3
energy	2

The geographical distribution of the industrial organizations is broad and includes the following countries and territories: Benin, Canada, Chile, Djibouti, Indonesia, Iran, Malaysia, Mexico, the Netherlands, the Philippines, Portugal, Russia, Saudi Arabia, Taiwan, Uganda, and the USA. At the same time, the geography of all victims covers almost the entire world, from North America to APAC.

The SolarWinds software is highly integrated into many systems around the globe in different industries. We currently have no evidence that any of the industrial organizations in our telemetry had an escalation from the attackers. Truesec provided a list of possible second-stage victims, which included several industrial organizations headquartered in different countries, based on responses received from a server used by the threat actor. Thus, we shouldn’t rule out the possibility of wider activity in some of the industrial networks if it is in line with the actor’s interests.

Here are our recommendations for possible victims of the SolarWinds compromise:

1. Check whether backdoored SolarWinds versions are installed. Known affected versions include software builds 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF1.
2. Check for known indicators of compromise (IOCs). CISA has published Alert AA20-35A with an extensive list
3. If you have detected a compromised SolarWinds installation or related IOCs, initiate a security incident investigation and launch an incident response procedure, considering all possible attack vectors:
    1. Isolate assets that are known to be compromised, while keeping the system operable
    2. Prevent IOCs that could be useful for the investigation from being deleted
    3. Check all network logs for suspicious network activity
    4. Check system logs and journals for illegitimate user account authentication
    5. Locate suspicious process activity, investigate memory dumps and associated files
    6. Check historical command-line data associated with suspicious activity
4. If you consider yourself a victim of the SolarWinds compromise, you can reach us at ics-cert@kaspersky.com for further assistance or consultancy.

Update 28.01.2021

Netresec has pointed out the fact that the TrueSec list of possible second-stage victims is incorrect due to their methodology and provided its own list based on updated information on the C2 logic of picking 2nd stage victims. The Netresec list also contains several industrial-related victims.

SunBurst

SunBurst