ESET Tech Center

Does ESET provide protection against attacks by the SilverFish group

Anne | ESET Nederland - 2021-04-01 - Reacties (0) - Customer Advisories

Summary

On March 15, 2021, PRODAFT released a report with information about the SilverFish group. In this report, they were able to analyze various servers and samples allowing them to link the SilverFish group with the infamous SolarWinds attacks, which became public around December 2020.

Details

Most notable about the SilverFish techniques is that a lot of “off-the-shelf” tooling is used; e.g. Empire and Cobalt Strike. All ESET products provide detection for these tactics. In less than 10 cases in the Netherlands ESET has detected the “build_eu.ps1” script with the ESET detection name: “Generik.IUCHTKE”. ESET’s DNA detections, also known as heuristic detections, have already learned to recognize and block these techniques. Other detection names for SilverFish are: Generik.BPFKNDO, XML/Agent.AK and Win32/Injector.EOVP. All other known available Indicators of Compromise are also detected and blocked respectively.

If you’re using ESET Enterprise Inspector, the following (generic) rules will detect commands used by SilverFish:

- Permission Groups Discovery [F1102]
- PowerShell executed with long cmdline [D0415]
- PowerShell suspicious activity executed - EncodedCommand [D0414]
- Mshta with inline script executed [F0439]
- Mshta.exe executed process [A0404]
- Mshta.exe executed under a different name [F0440][C]
- Mstha.exe has dropped a suspicious executable [A0312]
- Suspicious script interpreter started – mshta [F0447e]

Note: This is a non-exhaustive list of ESET Enterprise Inspector rules that will be triggered by SilverFish.

We would like to remind you that to prevent these techniques from compromising your systems we always advise you to:

- Make sure correct network segmentation is in place

- Make sure you are up to date with your patching
- Make sure your ESET products are up to date

Feedback & Support

If you have feedback or questions about this issue, please contact us using local ESET Technical Support.