olafhartong/sunburst_countermeasures.md

gist.github.com/olafhartong/71ffdd4cab4b6acd5cbcd1a0691ff82f

FireEye Sunburst KQL Detections

FireEye released a very interesting article regarding a third-party compromise of Solarwinds, the detections that are possible in Defender for Endpoint are listed below

Blog post

All FireEye detections

```
DeviceEvents
| where ActionType contains "ExploitGuardNonMicrosoftSignedBlocked"
| where InitiatingProcessFileName contains "svchost.exe" and FileName
contains "NetSetupSvc.dll"

let
SunburstMD5=dynamic(["b91ce2fa41029f6955bff20079468448","02af7cec58b9a5da

let SupernovaMD5="56ceb6d0011d87b6e4d7023d7ef85676";
DeviceFileEvents
| where MD5 in(SunburstMD5) or MD5 in(SupernovaMD5)
```

```
let
SunburstURL=dynamic(["panhardware.com","databasegalore.com","avsvmcloud.c

DeviceNetworkEvents
| where ActionType == "ConnectionSuccess"
| where RemoteUrl in(SunburstURL)

DeviceProcessEvents
| where InitiatingProcessFileName =~ "solarwinds.businesslayerhost.exe"
| where not(FolderPath endswith
@"\SolarWinds\Orion\APM\APMServiceControl.exe"
                or FolderPath endswith
@"\SolarWinds\Orion\ExportToPDFCmd.Exe"
                or FolderPath endswith
@"\SolarWinds.Credentials\SolarWinds.Credentials.Orion.WebApi.exe"
                or FolderPath endswith
@"\SolarWinds\Orion\Topology\SolarWinds.Orion.Topology.Calculator.exe"
                or FolderPath endswith @"\SolarWinds\Orion\Database-
Maint.exe"
                or FolderPath endswith
@"\SolarWinds.Orion.ApiPoller.Service\SolarWinds.Orion.ApiPoller.Service.

                or FolderPath endswith @"\Windows\SysWOW64\WerFault.exe"
                )

DeviceFileEvents
| where InitiatingProcessFileName =~ "solarwinds.businesslayerhost.exe"
| where FileName endswith "exe" or FileName endswith "dll" or FileName
endswith "ps1" or FileName endswith "jpg" or FileName endswith "png"
```

Copy link

fouapon commented May 26, 2021 • edited

the rule on DeviceProcessEvents table triggered an alert for the FolderPath "C:\Windows\SysWOW64\ARP.EXE"
Could you confirm that this is not a suspicious activity?
Thanks