


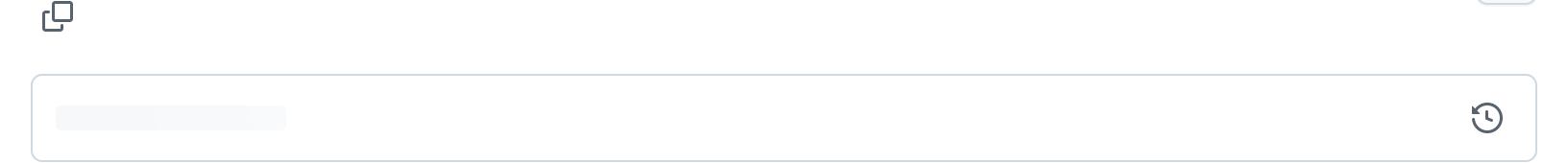
 [elastic](#) / [detection-rules](#) Public

 Notifications  Fork 498  Star 2k

[Code](#) [Issues](#) 145 [Pull requests](#) 22 [Actions](#) [Security](#) [Insights](#)

[detection-rules](#) / [rules](#) / [windows](#) / [defense_evasion_execution_msbuild_started_by_office_app.toml](#) 



Executable File · 73 lines (63 loc) · 2.4 KB

[Code](#) [Blame](#) [Raw](#)   

```
1  [metadata]
2  creation_date = "2020/03/25"
3  maturity = "production"
4  updated_date = "2022/03/31"
5
6  [rule]
7  author = ["Elastic"]
8  description = ""
9  An instance of MSBuild, the Microsoft Build Engine, was started by Excel or Word. This is unusual b
10 Engine and could have been caused by an Excel or Word document executing a malicious script payload
11 ""
12 false_positives = [
13     ""
14     The Build Engine is commonly used by Windows developers but use by non-engineers is unusual. It
15     this program to be started by an Office application like Word or Excel.
16     "",
17 ]
18 from = "now-9m"
19 index = ["winlogbeat-*", "logs-endpoint.events.*", "logs-windows.*"]
20 language = "eql"
21 license = "Elastic License v2"
22 name = "Microsoft Build Engine Started by an Office Application"
23 note = ""## Config
24
25 If enabling an EQL rule on a non-elastic-agent index (such as beats) for versions <8.2, events will
```

```
26     ""
27     references = ["https://blog.talosintelligence.com/2020/02/building-bypass-with-msbuild.html"]
28     risk_score = 73
29     rule_id = "c5dc3223-13a2-44a2-946c-e9dc0aa0449c"
30     severity = "high"
31     tags = ["Elastic", "Host", "Windows", "Threat Detection", "Defense Evasion"]
32     timestamp_override = "event.ingested"
33     type = "eq1"
34
35     query = '''
36     process where event.type in ("start", "process_started") and
37         process.name : "MSBuild.exe" and
38         process.parent.name : ("eqnedt32.exe",
39                                "excel.exe",
40                                "fltldr.exe",
41                                "msaccess.exe",
42                                "mspub.exe",
43                                "outlook.exe",
44                                "powerpnt.exe",
45                                "winword.exe" )
46     '''
47
48
49     [[rule.threat]]
50     framework = "MITRE ATT&CK"
51     [[rule.threat.technique]]
52     id = "T1127"
53     name = "Trusted Developer Utilities Proxy Execution"
54     reference = "https://attack.mitre.org/techniques/T1127/"
55     [[rule.threat.technique.subtechnique]]
56     id = "T1127.001"
57     name = "MSBuild"
58     reference = "https://attack.mitre.org/techniques/T1127/001/"
59
60
61
62     [rule.threat.tactic]
63     id = "TA0005"
64     name = "Defense Evasion"
65     reference = "https://attack.mitre.org/tactics/TA0005/"
66     [[rule.threat]]
67     framework = "MITRE ATT&CK"
68
69     [rule.threat.tactic]
70     id = "TA0002"
71     name = "Execution"
```

```
72     reference = "https://attack.mitre.org/tactics/TA0002/"
```