Files

c76a397

Go to file

.github
detection_rules
docs
kibana
kql
rta
rules
_deprecated
apm
cross-platform
integrations
linux
macos
ml
network
promotions
windows
collection_email_powershell_ex...
collection_posh_audio_capture....
collection_posh_keylogger.toml
collection_posh_screen_grabbe...
collection_winrar_encryption.to...
command_and_control_certutil...
command_and_control_comm...
command_and_control_dns_tu...
command_and_control_encryp...
command_and_control_iexplor...
command_and_control_port_fo...
command_and_control_rdp_tu...
command_and_control_remote...
command_and_control_remote...
command_and_control_remote...
command_and_control_remote...
command_and_control_sunbur...
command_and_control_teamvi...
credential_access_cmdline_du...

detection-rules / rules / windows

/ defense_evasion_execution_msbuild_started_by_office_app.toml

brokensound77 Expand timestamp override tests (#1907) 6bdfdda · 2 years ago History

Code Blame Executable File · 73 lines (63 loc) · 2.4 KB Raw

```
[metadata]
creation_date = "2020/03/25"
maturity = "production"
updated_date = "2022/03/31"

[rule]
author = ["Elastic"]
description = """
An instance of MSBuild, the Microsoft Build Engine, was started by Excel or Word. This
Engine and could have been caused by an Excel or Word document executing a malicious sc
"""
false_positives = [
    """
    The Build Engine is commonly used by Windows developers but use by non-engineers is
    this program to be started by an Office application like Word or Excel.
    """,
]
from = "now-9m"
index = ["winlogbeat-*", "logs-endpoint.events.*", "logs-windows.*"]
language = "eql"
license = "Elastic License v2"
name = "Microsoft Build Engine Started by an Office Application"
note = """## Config

If enabling an EQL rule on a non-elastic-agent index (such as beats) for versions <8.2,
"""
references = ["https://blog.talosintelligence.com/2020/02/building-bypass-with-msbuild.
risk_score = 73
rule_id = "c5dc3223-13a2-44a2-946c-e9dc0aa0449c"
severity = "high"
tags = ["Elastic", "Host", "Windows", "Threat Detection", "Defense Evasion"]
timestamp_override = "event.ingested"
type = "eql"

query = '''
process where event.type in ("start", "process_started") and
  process.name : "MSBuild.exe" and
  process.parent.name : ("eqnedt32.exe",
                         "excel.exe",
                         "fltldr.exe",
                         "msaccess.exe",
                         "mspub.exe",
                         "outlook.exe",
                         "powerpnt.exe",
                         "winword.exe" )
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1127"
name = "Trusted Developer Utilities Proxy Execution"
reference = "https://attack.mitre.org/techniques/T1127/"
[[rule.threat.technique.subtechnique]]
id = "T1127.001"
```

credential_access_copy_ntds_s...
credential_access_credential_d...
credential_access_dcsync_replic...
credential_access_disable_kerb...
credential_access_domain_back...
credential_access_dump_regist...

```
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/"
```