ElastAlert: Sysmon Network Connection Detection

1 message

<rangammabokka46@gmail.com> Fri, May 23, 2025 at 10:31 PM
Reply-to: rangammabokka46@gmail.com
To: rangammabokka46@gmail.com

Sysmon Network Connection Detection

At least 1 events occurred between 2025-05-23 22:21 India Standard Time and 2025-05-23 22:31 India Standard Time

@timestamp: 2025-05-23T17:01:15.907Z
_id: osYX_pYB7hfSOEXm41Ia
_index: .ds-winlogbeat-8.10.2-2025.05.14-000001
agent: {
"ephemeral_id": "364f04e0-834f-453e-b8c0-e2010ecfedc6",
"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": "2025-05-23T17:01:39.059Z",
"ingested": "2025-05-23T17:01:40.502476500Z",
"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: 2025-05-23 17:01:15.907
ProcessGuid: {7e25c1a1-a9db-6830-2502-000000002400}

ProcessId: 6408
Image: C:\Windows\System32\PING.EXE
FileVersion: 10.0.19041.1 (WinBuild.160101.0800)
Description: TCP/IP Ping Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: ping.exe
CommandLine: ping 8.8.8.8 -n 10
CurrentDirectory: C:\Users\ranga\AppData\Local\Temp\
User: VITICM-SOC\ranga
LogonGuid: {7e25c1a1-9077-6830-36dc-060000000000}
LogonId: 0x6DC36
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=2F46799D79D22AC72C241EC0322B011D,SHA256=7AF50FA112932EA3284F7821B2EEA2B7582F558DBA8972
31BB82182003C29F8B,IMPHASH=8C3BE1286CDAD6AC1136D0BB6C83FF41
ParentProcessGuid: {7e25c1a1-a9d7-6830-2302-000000002400}
ParentProcessId: 6968
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe /c ""C:\Users\ranga\AppData\Local\Temp\simulate_malware.bat" "
ParentUser: VITICM-SOC\ranga
num_hits: 1
num_matches: 1
process: {
  "args": [
    "ping",
    "8.8.8.8",
    "-n",
    "10"
  ],
  "args_count": 4,
  "command_line": "ping 8.8.8.8 -n 10",
  "entity_id": "{7e25c1a1-a9db-6830-2502-000000002400}",
  "executable": "C:\\Windows\\System32\\PING.EXE",
  "hash": {
    "md5": "2f46799d79d22ac72c241ec0322b011d",
    "sha256": "7af50fa112932ea3284f7821b2eea2b7582f558dba897231bb82182003c29f8b"
  },
  "name": "PING.EXE",
  "parent": {
    "args": [
      "C:\\Windows\\system32\\cmd.exe",
      "/c",
      "C:\\Users\\ranga\\AppData\\Local\\Temp\\simulate_malware.bat "
    ],
    "args_count": 3,
    "command_line": "C:\\Windows\\system32\\cmd.exe /c \"\"C:\\Users\\ranga\\AppData\\Local\\Temp\\simulate_malware
.bat\" \"",
    "entity_id": "{7e25c1a1-a9d7-6830-2302-000000002400}",
    "executable": "C:\\Windows\\System32\\cmd.exe",
    "name": "cmd.exe",
    "pid": 6968
  },
  "pe": {
    "company": "Microsoft Corporation",
    "description": "TCP/IP Ping Command",
    "file_version": "10.0.19041.1 (WinBuild.160101.0800)",
    "imphash": "8c3be1286cdad6ac1136d0bb6c83ff41",
    "original_file_name": "ping.exe",
    "product": "Microsoft® Windows® Operating System"
  },
  "pid": 6408,
  "working_directory": "C:\\Users\\ranga\\AppData\\Local\\Temp\\"
}
related: {
  "hash": [
    "7af50fa112932ea3284f7821b2eea2b7582f558dba897231bb82182003c29f8b",
    "2f46799d79d22ac72c241ec0322b011d",
    "8c3be1286cdad6ac1136d0bb6c83ff41"
  ],
  "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": "TCP/IP Ping Command",
        "FileVersion": "10.0.19041.1 (WinBuild.160101.0800)",
        "IntegrityLevel": "Medium",
        "LogonGuid": "{7e25c1a1-9077-6830-36dc-060000000000}",
        "LogonId": "0x6dc36",
        "ParentUser": "VITICM-SOC\\ranga",
        "Product": "Microsoft® Windows® Operating System",
        "TerminalSessionId": "1"
    },
    "event_id": "1",
    "opcode": "Info",
    "process": {
        "pid": 2408,
        "thread": {
            "id": 3124
        }
    },
    "provider_guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
    "provider_name": "Microsoft-Windows-Sysmon",
    "record_id": "25552",
    "task": "Process Create (rule: ProcessCreate)",
    "user": {
        "domain": "NT AUTHORITY",
        "identifier": "S-1-5-18",
        "name": "SYSTEM",
        "type": "User"
    },
    "version": 5
}
```