ElastAlert: Suspicious Network Connection

1 message

<rangammabokka46@gmail.com> Sat, May 24, 2025 at 1:46 PM
Reply-to: rangammabokka46@gmail.com
To: rangammabokka46@gmail.com

Suspicious Network Connection

At least 1 events occurred between 2025-05-24 13:28 India Standard Time and 2025-05-24 13:38 India Standard Time

@timestamp: 2025-05-24T08:08:36.415Z
_id: iQVcAZcBkOXE-VJ34IKd
_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"
}
destination: {
"domain": "172-104-149-86.ip.linodeusercontent.com",
"ip": "172.104.149.86",
"port": 80
}
ecs: {
"version": "1.12.0"
}
event: {
"action": "Network connection detected (rule: NetworkConnect)",
"category": [
"network"
],
"code": "3",
"created": "2025-05-24T08:15:53.688Z",
"ingested": "2025-05-24T08:15:53.484878500Z",
"kind": "event",
"module": "sysmon",
"provider": "Microsoft-Windows-Sysmon",
"type": [
"start",
"connection",
"protocol"
]
}
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: Network connection detected:
RuleName: -
UtcTime: 2025-05-24 08:08:36.415
ProcessGuid: {7e25c1a1-4eb9-6831-a200-000000002600}
ProcessId: 6704
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User: VITICM-SOC\ranga
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.52.131
SourceHostname: Viticm-SOC.localdomain
SourcePort: 50400
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 172.104.149.86
DestinationHostname: 172-104-149-86.ip.linodeusercontent.com
DestinationPort: 80
DestinationPortName: http
network: {
  "community_id": "1:IpFTDCq/g/fvsNvaFft0JfDHwy0=",
  "direction": "egress",
  "protocol": "http",
  "transport": "tcp",
  "type": "ipv4"
}
num_hits: 2
num_matches: 2
process: {
  "entity_id": "{7e25c1a1-4eb9-6831-a200-000000002600}",
  "executable": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
  "name": "powershell.exe",
  "pid": 6704
}
related: {
  "ip": [
    "192.168.52.131",
    "172.104.149.86"
  ],
  "user": [
    "ranga"
  ]
}
source: {
  "domain": "Viticm-SOC.localdomain",
  "ip": "192.168.52.131",
  "port": 50400
}
user: {
  "domain": "VITICM-SOC",
  "id": "S-1-5-18",
  "name": "ranga"
}
winlog: {
  "api": "wineventlog",
  "channel": "Microsoft-Windows-Sysmon/Operational",
  "computer_name": "Viticm-SOC",
  "event_id": "3",
  "opcode": "Info",
  "process": {
    "pid": 2460,
    "thread": {
      "id": 3152
    }
  },
  "provider_guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
  "provider_name": "Microsoft-Windows-Sysmon",
  "record_id": "27094",
  "task": "Network connection detected (rule: NetworkConnect)",
  "user": {
    "domain": "NT AUTHORITY",

```
        "identifier": "S-1-5-18",
        "name": "SYSTEM",
        "type": "User"
    },
    "version": 5
}
```